



Product Guide

McAfee ePolicy Orchestrator 5.3.0 Software

COPYRIGHT

Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

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

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

LICENSE INFORMATION

License Agreement

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

Contents

Preface	11
About this guide	11
Audience	11
Conventions	11
Find product documentation	12

Introducing McAfee ePolicy Orchestrator software

1 Protecting your networks with ePolicy Orchestrator software	15
Benefits of ePolicy Orchestrator software	15
Components and what they do	15
How the software works	16
2 Using the ePolicy Orchestrator interface	19
Log on and log off	19
Navigating the interface	19
Using the ePolicy Orchestrator navigation Menu	19
Customizing the navigation bar	20
Server settings categories	20
Working with lists and tables	22
Filter a list	23
Search for specific list items	23
Select table row checkboxes	23

Setting up ePolicy Orchestrator

3 Planning your ePolicy Orchestrator configuration	27
Considerations for scalability	27
When to use multiple McAfee ePO servers	27
When to use multiple remote Agent Handlers	28
Internet protocols in a managed environment	28
4 Setting up your McAfee ePO server	31
Server configuration overview	31
Use automatic Product Installation Status	32
Essential features for manual or Guided Configuration	34
Configure essential features	34
Use a proxy server	36
Enter your license key	37
Configure Product Improvement Program	37
Uninstall McAfee Product Improvement Program	37
5 User accounts and permission sets	39
User accounts	39

Manage user accounts	39
Supported user name and password formats	40
Create a custom logon message	41
Configuring Active Directory user logon	41
The Audit Log	45
Client certificate authentication	46
When to use client certificate authentication	47
Configure ePolicy Orchestrator client certificate authentication	47
Modify McAfee ePO server certificate-based authentication	48
Disable McAfee ePO server client certificate authentication	48
Configure users for certificate authentication	49
Update CRL file	49
Problems with client certificate authentication	50
SSL certificates	50
Create a self-signed certificate with OpenSSL	53
Other useful OpenSSL commands	55
Convert an existing PVK file to a PEM file	56
Permission sets	56
How users, groups, and permission sets fit together	57
Manage permission sets	58

6 Repositories 61

Repository types and what they do	61
Types of distributed repositories	63
Repository branches and their purposes	64
Repository list files	65
How repositories work together	65
Setting up repositories for the first time	66
Manage source and fallback sites	66
Create source sites	66
Switch source and fallback sites	67
Edit source and fallback sites	67
Delete source sites or disabling fallback sites	68
Verify access to the source site	68
Configure proxy settings	68
Configure proxy settings for the McAfee Agent	69
Configure settings for global updates	70
Configure agent policies to use a distributed repository	70
Use SuperAgents as distributed repositories	71
Create SuperAgent distributed repositories	71
Replicate packages to SuperAgent repositories	72
Delete SuperAgent distributed repositories	72
Create and configure repositories on FTP or HTTP servers and UNC shares	73
Create a folder location	73
Add the distributed repository to ePolicy Orchestrator	73
Avoid replication of selected packages	75
Disable replication of selected packages	76
Enable folder sharing for UNC and HTTP repositories	76
Edit distributed repositories	76
Delete distributed repositories	76
Using UNC shares as distributed repositories	77
Use local distributed repositories that are not managed	78
Work with the repository list files	79
Export the repository list SiteList.xml file	79
Export the repository list for backup or use by other servers	80
Import distributed repositories from the repository list	80

Import source sites from the SiteMgr.xml file	80
Pull tasks	81
Replication tasks	81
Repository selection	82
7 Registered servers	83
Register McAfee ePO servers	83
Register LDAP servers	85
Register SNMP servers	86
Using database servers	87
Register a database server	87
Modify a database registration	88
Remove a registered database	88
Sharing objects between servers	88
Export objects and data from your McAfee ePO server	88
Import items into ePolicy Orchestrator	89
8 Agent Handlers	91
How Agent Handlers work	91
Connect an Agent Handler in the DMZ to a McAfee ePO server in a domain	92
Handler groups and priority	93
Manage Agent Handlers	93
Assign McAfee Agents to Agent Handlers	94
Manage Agent Handler assignments	94
Create Agent Handler groups	95
Manage Agent Handler groups	95
Move agents between handlers	96

Managing your network security

9 The System Tree	101
The System Tree structure	101
The My Organization group	102
The My Group	102
The lost and found group	102
System Tree groups	103
Inheritance	103
Considerations when planning your System Tree	103
Administrator access	104
Environmental borders and their impact on system organization	104
Subnets and IP address ranges	105
Operating systems and software	105
Tags and systems with similar characteristics	105
Active Directory synchronization	106
Types of Active Directory synchronization	106
Systems and structure	107
Systems only	107
NT domain synchronization	107
Criteria-based sorting	107
How settings affect sorting	108
IP address sorting criteria	109
Tag-based sorting criteria	109
Group order and sorting	109
Catch-all groups	109
How a system is added to the System Tree when sorted	109
Create and populate System Tree groups	111

Create groups manually	112
Manually add systems to an existing group	112
Export systems from the System Tree	113
Import systems from a text file	113
Sort systems into criteria-based groups	114
Import Active Directory containers	116
Import NT domains into an existing group	118
Schedule System Tree synchronization	119
Manually update a synchronized group with an NT domain	120
Move systems within the System Tree	121
How Transfer Systems works	121
Transfer systems between McAfee ePO servers	122
Export and import ASSC keys between McAfee ePO servers	123
How the Automatic Responses feature interacts with the System Tree	124
Throttling, aggregation, and grouping	124
Default rules	125
10 Tags	127
Create tags using the New Tag Builder	127
Manage tags	128
Create, delete, and modify tag subgroups	129
Exclude systems from automatic tagging	130
Create a query to list systems based on tags	130
Apply tags to selected systems	131
Clear tags from systems	131
Apply criteria-based tags to all matching systems	132
Apply criteria-based tags on a schedule	132
11 Agent-server communication	135
Working with the agent from the McAfee ePO server	135
How agent-server communication works	135
SuperAgent and how it works	138
McAfee Agent relay capability	142
Peer-to-Peer communication	144
Collect McAfee Agent statistics	146
Change the agent user interface and event log language	146
Configure selected systems for updating	147
Respond to policy events	147
Scheduling client tasks	148
Run client tasks immediately	149
Locate inactive agents	149
Windows system and product properties reported by the agent	150
Queries provided by the McAfee Agent	151
Managing agent-server communication	152
Allow agent deployment credentials to be cached	152
Change agent communication ports	153
12 Security keys	155
Security keys and how they work	155
Master repository key pair	156
Other repository public keys	156
Manage repository keys	156
Use one master repository key pair for all servers	157
Use master repository keys in multi-server environments	157
Agent-server secure communication (ASSC) keys	158
Manage ASSC keys	158

View systems that use an ASSC key pair	160
Use the same ASSC key pair for all servers and agents	160
Use a different ASSC key pair for each McAfee ePO server	161
Backup and restore keys	161
13 Software Manager	163
What's in the Software Manager	163
Check in, update, and remove software using the Software Manager	164
Checking product compatibility	165
Reconfigure Product Compatibility List download	166
14 Product Deployment	169
Choosing a product deployment method	169
Benefits of product deployment projects	170
The Product Deployment page explained	172
Viewing Product Deployment audit logs	173
View Product Deployment	173
Deploy products using a deployment project	174
Monitor and edit deployment projects	175
Deploy new product example	176
Global updating	177
Deploy update packages automatically with global updating	178
15 Manual package and update management	181
Bring products under management	181
Check in packages manually	182
Delete DAT or engine packages from the master repository	182
Manually moving DAT and engine packages between branches	182
Check in Engine, DAT, and ExtraDAT update packages manually	183
16 Policy management	185
Policies and policy enforcement	185
Policy application	187
Create and maintain policies	187
Create a policy from the Policy Catalog page	188
Manage an existing policy on the Policy Catalog page	188
Configuring policies for the first time	189
Manage policies	189
Change the owners of a policy	190
Move policies between McAfee ePO servers	190
Assign a policy to a System Tree group	192
Assign a policy to a managed system	192
Assign a policy to systems in a System Tree group	193
Enforce policies for a product in a System Tree group	193
Enforce policies for a product on a system	193
Copy policy assignments	194
Edit Policy and Task Retention page	195
Policy assignment rules	196
Policy assignment rule priority	196
User-based policy assignments	197
About system-based policy assignments	197
Using tags to assign system-based policies	198
Create policy assignment rules	198
Manage policy assignment rules	198
Create policy management queries	199
Create a query to define compliance	200

Generate compliance events	200
View policy information	201
View groups and systems where a policy is assigned	202
View policy settings	202
View policy ownership	202
View assignments where policy enforcement is disabled	202
View policies assigned to a group	203
View policies assigned to a specific system	203
View policy inheritance for a group	203
View and reset broken inheritance	203
Compare policies	204
Share policies among McAfee ePO servers	204
Distribute your policy to multiple McAfee ePO servers	204
Register servers for policy sharing	205
Designate policies for sharing	205
Schedule server tasks to share policies	205
Policy management questions	206
17 Client tasks	209
How the Client Task Catalog works	209
Deployment tasks	210
Deployment packages for products and updates	210
Product and update deployment	212
Configuring product and update deployments for the first time	212
Deployment tags	212
Use the Product Deployment task to deploy products to managed systems	213
Configure a deployment task for groups of managed systems	213
Configure a deployment task to install products on a managed system	214
Update tasks	215
View Assigned Client Task	216
Update managed systems regularly with a scheduled update task	217
Evaluate new DATs and engines before distribution	218
Manage client tasks	218
Create client tasks	218
Edit client tasks	219
Delete client tasks	219
Compare client tasks	220
18 Server tasks	221
Create a server task	221
Accepted Cron syntax when scheduling a server task	222
The Server Task Log	222
View server task information in the server task log	223
Manage the Server Task Log	223
19 Managing SQL databases	225
Maintaining SQL databases	225
Use a remote command to determine the Microsoft SQL database server and name	225
Configure a snapshot and restore the SQL database	226
Configure Disaster Recovery Server Task	226
Use Microsoft SQL to backup and restore database	227
Use a remote command to determine the Microsoft SQL database server and name	227
Use Microsoft SQL Server Management Studio to find McAfee ePO server information	228
The Threat Event Log	228
View and purge the Threat Event Log	230
Schedule purging the Threat Event Log	230

Monitoring and reporting on your network security status

20	Dashboards and monitors	235
	Using dashboards and monitors	235
	Manage dashboards	236
	Export and import dashboards	237
	Manage dashboard monitors	238
	Move and resize dashboard monitors	239
	Default dashboards and their monitors	240
	Specify first-time dashboards and dashboard refresh intervals	242
21	Queries and reports	243
	Query and report permissions	243
	About queries	244
	Query Builder	245
	Configuring queries and reports for the first time	246
	Work with queries	246
	Manage custom queries	247
	Run a query	248
	Run a query on a schedule	248
	Create a query group	249
	Move a query to a different group	249
	Export and import queries	249
	Export query results to other formats	250
	Multi-server rollup querying	251
	Create a Rollup Data server task	252
	About reports	253
	Structure of a report	253
	Work with reports	254
	Create a report	254
	Edit an existing report	255
	View report output	259
	Group reports together	259
	Run reports	260
	Run a report on a schedule	260
	Export and import reports	261
	Configure the template and location for exported reports	261
	Delete reports	262
22	Events and responses	263
	Using automatic responses	263
	Throttling, aggregation, and grouping	264
	Default rules	264
	Response planning	265
	Configuring responses for the first time	265
	Determine how events are forwarded	266
	Determine which events are forwarded immediately	266
	Determine which events are forwarded	267
	Configure Automatic Responses	267
	Assign permissions to notifications	267
	Assign permissions to Automatic Responses	268
	Manage SNMP servers	268
	Determine which events are forwarded to the server	271
	Choose a notification event interval	271
	Create and edit Automatic Response rules	271
	Describe a rule	272

Set filters for the rule	272
Set thresholds for the rule	272
Configure the action for Automatic Response rules	273
Event and response questions	274
23 Issues	277
Issues and how they work	277
Work with issues	277
Create basic issues manually	277
Configure responses to automatically create issues	278
Manage issues	279
Purge closed issues	280
Purge closed issues manually	280
Purge closed issues on a schedule	280
24 Disaster Recovery	283
What is Disaster Recovery	283
Disaster Recovery components	284
How Disaster Recovery works	286
Disaster Recovery Snapshot and backup overview	286
McAfee ePO server recovery installation overview	288
Create Snapshot	290
Create Snapshot from Dashboard	290
Create Snapshot from Web API	290
Configure Disaster Recovery server settings	292
A Ports overview	295
Change console-to-application server communication port	295
Change agent-server communication port	296
Ports required for communicating through a firewall	299
Traffic quick reference	301
B Opening a remote console connection	303
Index	305

Preface

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

Contents

- ▶ *About this guide*
- ▶ *Find product documentation*

About this guide

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

Audience





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

The information in this guide is intended primarily for:

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

Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

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

Task

- 1 Go to the McAfee ServicePortal at <http://support.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

Introducing McAfee ePolicy Orchestrator software

-
- Chapter 1 *Protecting your networks with ePolicy Orchestrator software*
Chapter 2 *Using the ePolicy Orchestrator interface*

1

Protecting your networks with ePolicy Orchestrator software

ePolicy Orchestrator software is a key component of the McAfee Security Management Platform, which provides unified management of endpoint, network, and data security. Reduce incident response times, strengthen protection, and simplify risk and security management with ePolicy Orchestrator automation features and end-to-end network visibility.

Contents

- ▶ *Benefits of ePolicy Orchestrator software*
- ▶ *Components and what they do*
- ▶ *How the software works*

Benefits of ePolicy Orchestrator software

ePolicy Orchestrator software is an extensible management platform that enables centralized policy management and enforcement of your security policies.

Using ePolicy Orchestrator software, you can perform these network security tasks:

- Manage and enforce network security using policy assignments and client tasks.
- Update the detection definition (DAT) files, anti-virus engines, and other security content required by your security software to ensure that your managed systems are secure.
- Create reports, using the built-in query system wizard, that display informative user-configured charts and tables containing your network security data.

Components and what they do

These components make up ePolicy Orchestrator software.

- **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.
- **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 McAfee ePO 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 McAfee ePO server. The 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 McAfee ePO 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. 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.



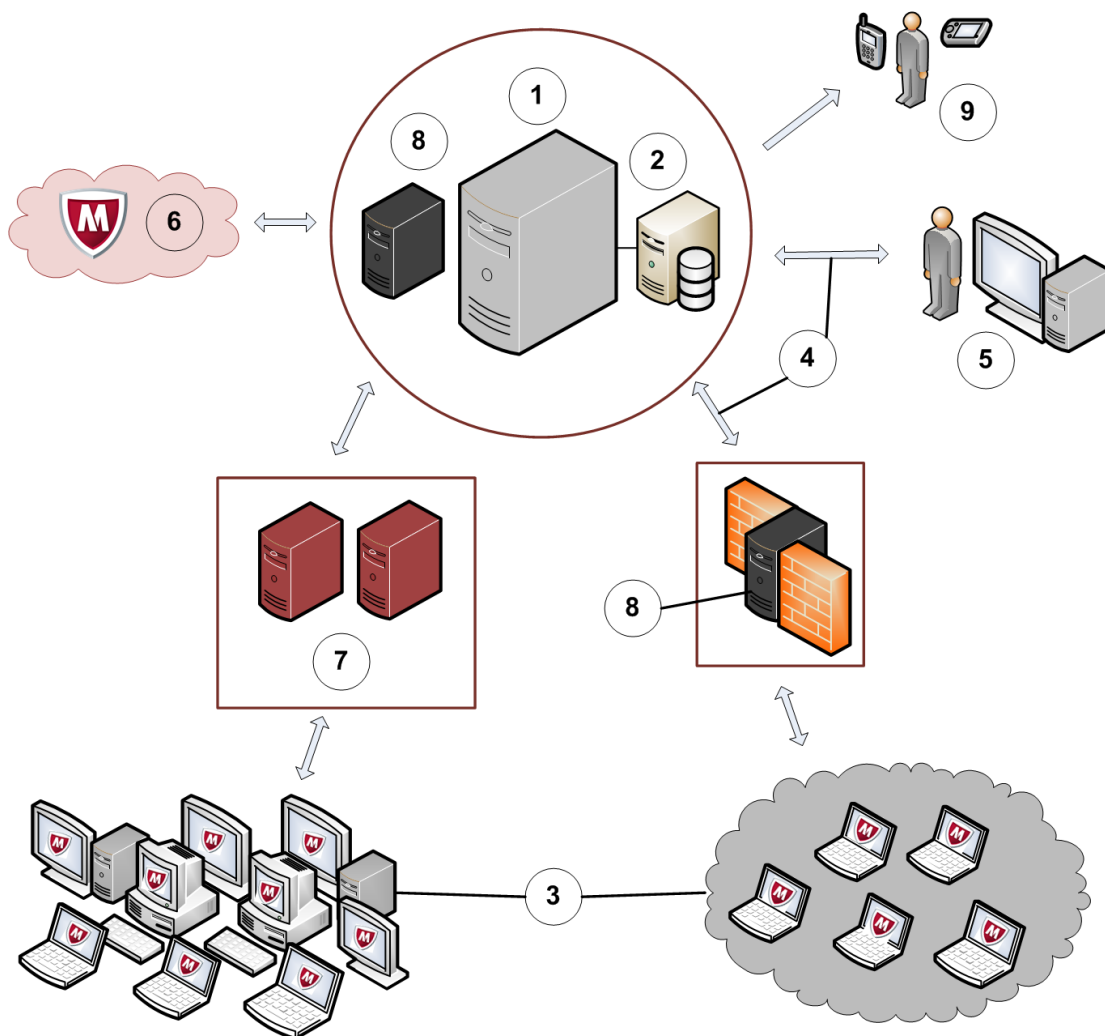
Depending on the needs of your organization and the complexity of your network, you might only use some of these components.

How the software works

ePolicy Orchestrator 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 McAfee

ePO 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 McAfee ePO server and components inter-relate in your secure network environment.



- 1 Your McAfee ePO 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 McAfee ePO server.
- 9 Automatic Response notifications are sent to security administrators to notify them that an event has occurred.

2

Using the ePolicy Orchestrator interface

Log on to the ePolicy Orchestrator interface to configure your McAfee ePO server, and to manage and monitor your network security.

Contents

- ▶ *Log on and log off*
- ▶ *Navigating the interface*
- ▶ *Working with lists and tables*

Log on and log off

To access the ePolicy Orchestrator software, enter your user name and password on the logon screen.

Before you begin

You must have a user name and password assigned before you can log on to ePolicy Orchestrator.

Whether you connect to your McAfee ePO server from a remote connection or from the McAfee ePO server icon, the first screen you see is the ePolicy Orchestrator logon screen.

Task

- 1 Type your user name, password, and click **Log On**.

Your ePolicy Orchestrator software displays the default dashboard.

- 2 To end your ePolicy Orchestrator session, click **Log Off**.

Once you log off, your session is closed and can't be opened by other users.

Navigating the interface

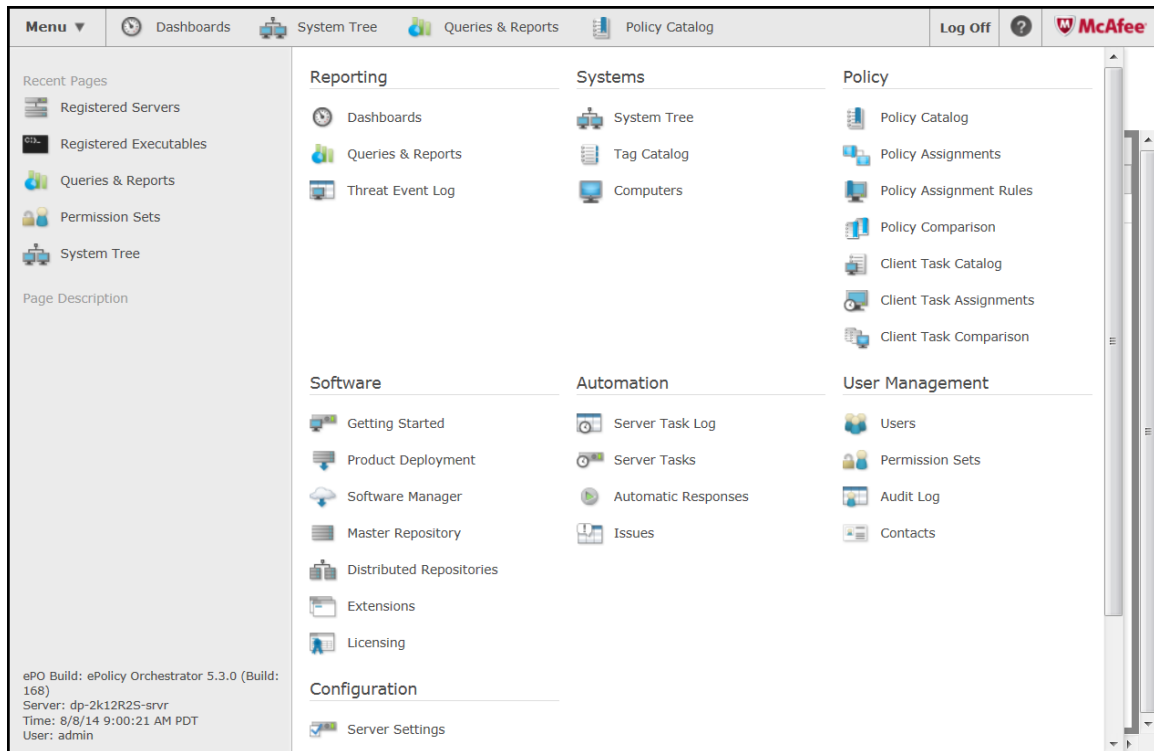
The McAfee ePO interface uses menu-based navigation with a Favorites bar you can customize to get where you want to go quickly.

Menu sections represent top-level features. As you add managed products to McAfee ePO, the Menu options increase.

Using the ePolicy Orchestrator navigation Menu

Open the ePolicy Orchestrator Menu to navigate the ePolicy Orchestrator interface.

The Menu uses categories that include various features and functionality of McAfee ePO. 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.



Customizing the navigation bar

Customize the navigation bar for 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 place more icons on the navigation bar than can be viewed, an overflow menu is created on the right side of the bar. Click the down-arrow 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.

Server settings categories

These default server settings categories are available in your McAfee ePO software.

When you add software to your McAfee ePO server, product-specific server settings are added to the server settings category list. You can modify server settings by navigating to the Server Settings page in the Configuration section of the McAfee ePO interface.



For information on product-specific server settings, see the associated product documentation.

Table 2-1 Default server settings categories and their descriptions

Server settings category	Description
Active Directory Groups	Specifies the LDAP server to use for each domain.
Active Directory User Login	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 is fully configured.

Table 2-1 Default server settings categories and their descriptions (continued)

Server settings category	Description
Agent Contact Method	Specifies the priority of methods that McAfee ePO uses when it attempts to contact a McAfee Agent. To change the priority, select Agent Contact Method under Setting Categories , click Edit , then select the priority. Each contact method must have a different priority level. The methods to contact a McAfee Agent are: <ul style="list-style-type: none"> • Fully Qualified Domain Name • NetBIOS name • IP Address
Agent Deployment Credentials	Specifies whether users are allowed to cache agent deployment credentials.
Certificate Based Authentication	Specifies whether Certificate Based Authentication is enabled, and the settings and configurations required for the Certificate Authority (CA) certificate being used.
Dashboards	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.
Disaster Recovery	Enables and sets the keystore encryption passphrase for Disaster Recovery.
Email Server	Specifies the email server that McAfee ePO uses to send email messages.
Event Filtering	Specifies which events the agent forwards.
Event Notifications	Specifies how often McAfee ePO checks your notifications to see if any trigger Automatic Responses.
Global Updating	Specifies whether and how global updating is enabled.
License Key	Specifies the license key used to register this McAfee ePO software.
Login Message	Specifies whether a custom message is displayed when users log on to the McAfee ePO console, and the message content.
Policy and Task Retention	Specifies whether the policies and client task data is removed when you delete the product extension.
Policy Maintenance	Specifies whether policies for unsupported products are visible or hidden. Required only after McAfee ePO is upgraded from a previous version.
Ports	Specifies the ports used by the server when it communicates with agents and the database.
Printing and Exporting	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.
Product Compatibility List	Specifies whether the Product Compatibility List is automatically downloaded and whether it displays any incompatible product extensions.
Product Improvement Program	Specifies whether McAfee ePO can collect data proactively and periodically from the managed client systems.
Proxy Settings	Specifies the type of proxy settings configured for your McAfee ePO server.
Server Information	Specifies Java, OpenSSL, and Apache server information, such as name, IP address, and version information.
Security Keys	Specifies and manages the agent-server secure communication keys and repository keys.
Server Certificate	Specifies the server certificate that your McAfee ePO server uses for HTTPS communication with browsers.

Table 2-1 Default server settings categories and their descriptions *(continued)*

Server settings category	Description
Software Evaluation	Specifies the information required to enable check-in and deployment of evaluation software from the Software Manager.
Source Sites	Specifies which source sites your server connects to for updates, as well as which sites are be used as fallback sites.
System Details Settings	Specifies which queries and systems properties are displayed in the System Details page for your managed systems.
System Tree Sorting	Specifies whether and how System Tree sorting is enabled in your environment.
User Session	Specifies the amount of time a user can be inactive before the system logs them out.

Working with lists and tables

Use ePolicy Orchestrator search and filter functions to sort lists of data.

Lists of data in ePolicy Orchestrator could have hundreds or thousands of entries. Manually searching for specific entries in these ePolicy Orchestrator lists could be difficult without the Quick Find search filter.

The number in this figure shows the Quick Find search filtering for queries that include `malware`.

The screenshot displays the McAfee ePolicy Orchestrator interface. At the top, there is a navigation bar with 'Menu', 'Dashboards', 'Getting Started', 'Computers', and 'Queries & Reports'. The 'Queries & Reports' section is active, showing a 'Reporting' header and a 'Queries & Reports' sub-header. On the left, there is a 'Groups' sidebar with a list of categories: All, Agent Management, Detections, Endpoint Security, Policy Assignment, Product Deployment, System Management, Threat Events, and User Auditing. The main content area is divided into 'Queries' and 'Reports' tabs. A search bar labeled 'Quick find: malware' is highlighted with a red circle and the number '1'. Below the search bar, there are two query cards: 'All Threat Events by System Tree Group' and 'Malware Detection History', each with a 'Run' button. The interface also shows a bottom bar with 'Actions' and '2 items'.

Filter a list

You can use preset or your own custom filters to select specific rows in the lists of data in the ePolicy Orchestrator interface.

Task

For option definitions, click ? in the interface.

- 1 From the bar at the top of a list, select the preset or custom filter that you want to use to filter the list.

Only items that meet the filter criteria are displayed.

- 2 Select the checkboxes next to the list items that you want to focus on, then select **Show selected rows**.

Only the selected rows are displayed.

Search for specific list items

Use the Quick Find filter to find items in a large list.

For option definitions, click ? in the interface.

Task

- 1 Enter your search terms in the **Quick Find** field.

- 2 Click **Apply**.

Only items that contain the terms you entered in the **Quick Find** field are displayed.



Click **Clear** to remove the filter and display all list items.

Example: Find detection queries

Here is an example of a valid search for a specific list of queries.

- 1 Click **Menu | Queries & Reports**. Click **Query**.

All queries that are available in McAfee ePO appear in the list.

- 2 Limit the list to specific queries, for example, "detection." In the **Quick Find** field, type `detection`, then click **Apply**.

These queries appear in the list:

- **Malware Detection History**
- **Today's Detections per Product**




Some lists contain items translated for your location. When communicating with users in other locales, remember that query names could differ.

Select table row checkboxes

The ePolicy Orchestrator user interface has special table row selection actions and shortcuts that allow you to select table row checkboxes using **click** or **Shift** and **click**.

Some output pages in the ePolicy Orchestrator user interface display a checkbox next to each list item in the table. These checkboxes allow you to select rows individually, as groups, or all the rows in the table.

This table lists the actions used to select table row checkboxes.

To Select	Action	Response
Individual rows	Click checkbox for individual rows	Selects each individual row independently
Group of rows	Click one checkbox, hold Shift , and click last checkbox in group	<p>Selected first and last row to create a group of selected rows.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Using Shift + Click to select more than 1,500 rows in a table simultaneously might cause a spike in CPU utilization and trigger an error message describing a script error. </div>
All rows	Click the top checkbox in table headings	Selects every row in the table

Setting up ePolicy Orchestrator

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

-
- Chapter 3 *Planning your ePolicy Orchestrator configuration*
 - Chapter 4 *Setting up your McAfee ePO server*
 - Chapter 5 *User accounts and permission sets*
 - Chapter 6 *Repositories*
 - Chapter 7 *Registered servers*
 - Chapter 8 *Agent Handlers*

3

Planning your ePolicy Orchestrator configuration

To use your McAfee ePO server effectively, you must create a comprehensive plan specific to your environment.

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

- ▶ *Considerations for scalability*
- ▶ *Internet protocols in a managed environment*

Considerations for scalability

How you manage your scalability depends on whether you use multiple McAfee ePO servers, multiple remote Agent Handlers, or both.

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

- **Vertical scalability** — Adding and upgrading to bigger, faster hardware to manage larger and larger deployments. Scaling your McAfee ePO server infrastructure vertically is accomplished by upgrading your server hardware, and using multiple McAfee ePO servers throughout your network, each with its own database.
- **Horizontal scalability** — Accomplished by increasing the deployment size that a single McAfee ePO 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 McAfee ePO servers

Depending on the size and make-up of your organization, using multiple McAfee ePO 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 McAfee ePO server and database.

When to use multiple remote Agent Handlers

Multiple remote Agent Handlers help you manage large deployments without adding additional McAfee ePO 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 McAfee ePO 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 McAfee ePO 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 to 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.

Internet protocols in a managed environment

ePolicy Orchestrator software is compatible with both Internet Protocol versions: IPv4 and IPv6.

McAfee ePO 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 McAfee ePO 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 McAfee ePO 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 on IPv6, address-related properties such as IP address, subnet address, and subnet mask are reported in IPv6 format. When transmitted between client and McAfee ePO 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:0000:0000:0000:00A9:1234].

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.

4

Setting up your McAfee ePO server

Get up-and-running quickly by configuring the essential features of your McAfee ePO server.

Contents

- ▶ *Server configuration overview*
- ▶ *Use automatic Product Installation Status*
- ▶ *Essential features for manual or Guided Configuration*
- ▶ *Configure essential features*
- ▶ *Use a proxy server*
- ▶ *Enter your license key*
- ▶ *Configure Product Improvement Program*
- ▶ *Uninstall McAfee Product Improvement Program*

Server configuration overview

Set up your McAfee ePO server to meet the unique needs of your environment using multiple methods.

The essential features of your McAfee ePO server that you must configure are:

- **Product Installation Status** — Automatically starts installing and configuring the licensed security software to your McAfee ePO server. You can:
 - Allow the default security software to install on your McAfee ePO server.
 - Click **Stop** and use **Software Manager** to manually check in new and updated security software to your McAfee ePO server and **Master Repository** from within the console.




The Product Installation Status page only starts if you have selected **Enable Automatic Product Installation** option during McAfee ePO installation.

- **System Tree** — Contains all systems managed by your McAfee ePO server and allows you to perform actions on those systems.
- **Policy Catalog** — Where you configure the policies that control the security software deployed to your managed systems.
- **Client Task Catalog** — Where you create, assign, and schedule client tasks to run automatically on your managed systems.

This table lists the configuration steps to install your licensed product software automatically or manually.

Table 4-1 Overview of different configuration methods

Automatic product software download	Manual product software download
<p>1 ePolicy Orchestrator installation completes and you start the software.</p> <p>2 From the logon screen, log on to the ePolicy Orchestrator user interface. The Product Installation Status page appears and starts installing the latest revisions of your licensed security software on your McAfee ePO server. The page displays the Products and their Status.</p> <p>3 If all Product Status are Complete, continue with step 5. If any Product Status appears as Failed, click the checkbox next to the product name and Retry.</p> <p>4 If the failed product installation continues to fail:</p> <ul style="list-style-type: none"> • Try using the Manual product software download to install the failed product with Software Manager. • Call McAfee Technical Support. • Continue with the McAfee ePO configuration and try to install the product software later. <p>5 Complete these steps as needed for your environment:</p> <ul style="list-style-type: none"> • Add systems to your System Tree. • Configure general server settings. • Create user accounts. • Configure permission sets. • Configure policies. • Configure advanced server settings and features. • Set up additional components. 	<p>1 ePolicy Orchestrator installation completes and you start the software.</p> <p>2 From the logon screen, log on to the ePolicy Orchestrator user interface.</p> <p>3 Run ePolicy Orchestrator Guided Configuration to perform these processes:</p> <ul style="list-style-type: none"> • Add McAfee security software to your Master Repository. • Add systems to the System Tree. • Create and assign at least one security policy to your managed systems. • Schedule a client update task. • Deploy your security products to your managed systems. <div data-bbox="954 842 1523 940" style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  Using the Guided Configuration is not required. You can perform each of these steps manually. </div> <p>4 Complete these steps as needed for your environment:</p> <ul style="list-style-type: none"> • Configure general server settings. • Create user accounts. • Configure permission sets. • Configure policies. • Configure advanced server settings and features. • Set up additional components.

Use automatic Product Installation Status

The Product Installation Status page appears automatically after you initially log on to McAfee ePO. It automatically installs your security software to the McAfee ePO server or you can **Stop** it and manually check in the security software.

Before you begin

The Product Installation Status page only starts if you have selected **Enable Automatic Product Installation** option during McAfee ePO installation.

The Product Installation Status page is only available for the first 24 hours after you initially log on to McAfee ePO. After all subsequent user logins, the default dashboard page appears. After 24 hours, Product Installation Status disappears from the **Menu | Automation** list.

Task

For option definitions, click ? in the interface.

- 1 Click the **Launch ePolicy Orchestrator** icon on your ePolicy Orchestrator server desktop, to see the Log On screen.
- 2 Type your credentials and pick a language in the **Log On** dialog box.

The Product Installation Status page appears and automatically starts downloading and installing the licensed software available to your organization. You can monitor the automatic software installation process in the page using:

- **Products** — Displays all licensed software and its latest available version.
- **Status** — Displays one of these values:
 - **Updating** — While the software is downloading and installing.
 - **Completed** — When the software is successfully installed.
 - **Failed** — If an error occurs during the download or install process.
 - **Stopped** — If you clicked **Stop** at the top of the page.

You can click **Menu | Software | Software Manager** at any time to see details of the software installation process.



You can also use the McAfee ePO user interface to configure other elements while the automatic software installation process is running.

- 3 You can complete the software installation process using either method shown in this table.

Automatic installation	Manual installation
<p>In the Product Installation Status page, wait for the Status listed for each product to change to Complete.</p> <div data-bbox="347 1339 391 1388" data-label="Image"> </div> <p>If any product installation fails, select the checkbox next to the product name to retry the installation. If the installation continues to fail, try using Software Manager to complete the installation.</p>	<p>In the Product Installation Status page, click Stop and click OK in the dialog box that tells you must complete the software installation process using Software Manager.</p> <p>The product status values change to Stopped.</p> <p>To complete the software installation process, click Menu Software Software Manager.</p> <p>See <i>Software Manager</i> for detailed instructions to complete the software installation process manually.</p>

- 4 Complete your ePolicy Orchestrator configuration by performing these tasks, as needed:
 - **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.
 - **Create user accounts and configure permission sets** — User accounts provide a way for users to access the server and permission sets grant rights and access to ePolicy Orchestrator features.

- **Configure advanced server settings and features** — Your McAfee ePO server provides advanced features and functionality to help you automate the management of your network security.
- **Set up 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.

Your McAfee ePO server is now protecting your managed systems.

Essential features for manual or Guided Configuration

Several McAfee ePO server features are essential for its use, and must be set up during manual or Guided Configuration. These features are required before you can deploy and manage security software on the systems in your network.

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

- 1 Get McAfee security software checked in to your Master Repository, so it can be deployed to systems in your network. Use the Product Installation Status page or the Software Manager to install your product software.
- 2 Add your systems to the McAfee ePO 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 current.
- 5 Deploy your security software to your managed systems.

The Guided Configuration is not required. If you perform these steps manually, we recommend that you use a similar workflow during your configuration process. Regardless of the method you choose to configure these features, you can modify your McAfee ePO configuration using the Guided Configuration tool, or by navigating directly to each page from the Menu.

Configure essential features

Use the Guided Configuration tool to configure essential features. Or you can use these tasks to guide you when manually configuring your McAfee ePO server.

For option definitions, click ? in the interface.

Task

- 1 Click the **Launch ePolicy Orchestrator** icon on your McAfee ePO server desktop, to see the Log On screen.
- 2 Type your user name, password, and select a language, if needed, and click **Log On**. ePolicy Orchestrator starts and displays the Dashboard dialog box.
- 3 Use either automatic Product Installation Status or Software Manager to install your product software. See *Use automatic Product Installation Status* or *Software Manager* for details.
- 4 Click **Menu | Reporting | Dashboards**, select **Guided Configuration** from the **Dashboard** drop-down, then click **Start**.
- 5 Review the **Guided Configuration** overview and instructions, then click **Start**.


- 6 On the **Software Selection** page:
- Under the **Software Not Checked In** product category, click **Licensed** or **Evaluation** to display available products.
 - In the **Software** table, select the product you want to check in. The product description and all available components are displayed in the following table.
 - Click **Check In All** to check in product extensions to your McAfee ePO server, and product packages into your Master Repository.
 - Click **Next** at the top of the screen when you're finished checking in software and ready to move on to the next step.
- 7 On the **System Selection** page:
- 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 dialog box opens.
 - Select which method you want to use to add your systems to the **System Tree**.

Add systems using...	To...	Then...
AD Sync	Synchronize your McAfee ePO 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 .	<ol style="list-style-type: none"> In the AD Sync dialog box, select the synchronization type you want to use and specify the appropriate settings. 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.	<ol style="list-style-type: none"> 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. Click Add Systems to move on to the next step.

- 8 On the **Policy Configuration** page:

Select...	To...	Then...
Accept Defaults	Use the My Default policy setting for the software you deploy and continue your configuration.	This step is complete.
Configure Policy	Specify custom policy settings now for each software product you checked in.	<ol style="list-style-type: none"> In the Policy Configuration dialog box, click OK. Select a product from the Product list and click My Default to edit the default policy settings. Click Next to move on to the next step.

- 9 On the **Software Updating** page:

Select...	To...	Then...
Create Defaults	Automatically create a default product update client task that runs daily at 12:00 P.M.	This step is complete.
Set Task Schedule	Manually configure the schedule for your product update client task.	<ol style="list-style-type: none"> Using the Client Task Assignment Builder, specify a Product and Task Name for your product update task. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 5px 0;">  Do not change the Task Type selection. Task Type must be set to Product Update. </div> <ol style="list-style-type: none"> Configure the Lock task inheritance and Tags options, then click Next. Specify the schedule for the update task, then click Next. Review the summary and click Save.

10 On the **Software Deployment** page:

- In the **System Tree**, select the location that contains the systems where you want to deploy your software, then click **Next**. Click **OK** to continue.
- 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 before you can deploy your other security software.

- Select the software packages you want to deploy to your managed systems, then click **Deploy**.

11 On the **Configuration Summary** page, click **Finish** to close the **Guided Configuration**.

12 Complete your ePolicy Orchestrator configuration by performing these tasks, as needed:

- Configure general server settings** — Server settings in this group affect functionality that you do not need to modify for your server to operate correctly. If you want, you can customize some aspects of how your server works.
- Create user accounts and configure permission sets** — User accounts provide a means for users to access the server, and permission sets grant rights and access to ePolicy Orchestrator features.
- Configure advanced server settings and features** — Your McAfee ePO server provides advanced features and functionality to help you automate the management of your network security.
- 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.

Your McAfee ePO server is now protecting your managed systems.

Use a proxy server

If you use a proxy server in your network environment, you need to specify the proxy settings on the **Server Settings** page.

For option definitions, click ? in the interface.

Task

- 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**.

Enter your license key

Your license key entitles you to a full installation of the software, and populates the ePolicy Orchestrator Software Manager with the licensed McAfee software your company owns.

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 or after 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**.

Configure Product Improvement Program

The McAfee Product Improvement Program helps improve McAfee products. It collects data proactively and periodically from the client systems managed by the McAfee ePO server.

McAfee Product Improvement Program collects the following types of data:

- System environment (software and hardware details)
- Effectiveness of installed McAfee product features
- McAfee product errors and related Windows events

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Configuration | Server Setting**, select **Product Improvement Program** from the **Setting Categories**, then click **Edit**.
- 2 Select **Yes** to allow McAfee to collect anonymous diagnostic and usage data, then click **Save**.



[Click here to learn more about the McAfee Product Improvement Program.](#)

Uninstall McAfee Product Improvement Program

The McAfee Product Improvement Program can be uninstalled at any time.

Task

For option definitions, click ? in the interface.

- 1 Log on to the McAfee ePO server as an administrator.
- 2 Click **Menu | Policy | Client Task Catalog**, select **McAfee Agent | Product Deployment** as **Client Task Types**, then click **Actions | New Task**.
- 3 Create a new task to uninstall the McAfee Product Improvement Program from the required client systems.
- 4 Assign the task to the client systems and send an agent wake-up call.
- 5 Click **Menu | Software | Master Repository**, click **Delete** next to the **McAfee Product Improvement Program** package, then click **OK**.
- 6 Click **Menu | Software | Extensions**, then select **McAfee Product Improvement Program**.
- 7 Click **Remove**, then click **OK**.

5

User accounts and permission sets

Each user account is associated with one or more permission sets, which define what the user is allowed to do with the software.

Contents

- ▶ *User accounts*
- ▶ *Client certificate authentication*
- ▶ *Permission sets*

User accounts

User accounts allow you to control how users access and use the software. Even the smallest network installations needs to specify and control the access users have to different parts of the system.

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 McAfee ePO 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.

While user accounts and permission sets are closely related, they are created and configured using separate steps.

Contents

- ▶ *Manage user accounts*
- ▶ *Supported user name and password formats*
- ▶ *Create a custom logon message*
- ▶ *Configuring Active Directory user logon*
- ▶ *The Audit Log*

Manage user accounts

You can create, edit, and delete user accounts manually with the User Management page.



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

For option definitions, click ? in the interface.

Task

- 1 Open the **User Management** page: click **Menu** | **User Management** | **Users**.
- 2 Select one of these actions.

Action	Steps
Create a user	<ol style="list-style-type: none"> 1 Click New User. 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 an administrator, or select the appropriate permission sets for the user. 7 Click Save to return to the Users tab. <p>The new user appears in the Users list of the User Management page.</p>
Edit a user	<ol style="list-style-type: none"> 1 From the Users list, select the user you want to edit, then click Action Edit. 2 Edit the account as needed. 3 Click Save. <p>The user changes appear in the Users list of the User Management page.</p>
Delete a user	<ol style="list-style-type: none"> 1 From the Users list, select the user you want to delete, then click Action Delete. 2 When prompted, click OK. <p>The user disappears from the Users list of the User Management page.</p>

See also

[Supported user name and password formats on page 40](#)

Supported user name and password formats

Review these supported formats when creating SQL database user names and passwords.

All printable characters in the ISO8859-1 characters set are supported, with these exceptions.

Platform	Unsupported password and user name characters
McAfee ePO	<ul style="list-style-type: none"> • Leading spaces, trailing spaces, or passwords that contain only spaces • Double quotes (") • Leading backslashes (\) • Colons in user names (:) • Semicolons in user names (;)

See also

[Manage user accounts on page 39](#)

Create a custom logon message

Create and display a custom logon 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**.

Configuring Active Directory user logon

You can reduce the overhead of managing user accounts and access by configuring Active Directory user logon.

Contents

- ▶ *Managing ePolicy Orchestrator users with Active Directory*
- ▶ *Windows authentication and authorization strategies*
- ▶ *Enable Windows authentication in the McAfee ePO server*
- ▶ *Configure Windows authentication*
- ▶ *Configure Windows authorization*

Managing ePolicy Orchestrator users with Active Directory

You can use pre-existing Windows authenticated user credentials to automatically create ePolicy Orchestrator users and assign permissions to them.

This process is accomplished by mapping ePolicy Orchestrator permission sets to Active Directory groups in your environment. This feature can reduce the management overhead when you have a large number of ePolicy Orchestrator users in your organization. To complete the configuration, you must work through the following process:

- Configure user authentication.
- Register LDAP servers.
- Assign permission sets to the Active Directory group.

User authentication

ePolicy Orchestrator users can be authenticated with ePolicy Orchestrator 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 autcreation server setting. User autcreation 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 ePolicy Orchestrator permission set.

Windows authentication and authorization strategies

You can take many approaches 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 problems with user authentication.

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 a McAfee ePO 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 McAfee ePO 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.

Enable Windows authentication in the McAfee 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.

Configure Windows authentication

There are many ways to use existing Windows account credentials within ePolicy Orchestrator.

Before you begin

You must have first prepared your server for Windows authentication.

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, configure Windows authentication.

Task

For option definitions, click ? in the interface.

- 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. (for example, `internaldomain.com`) Domain controllers and WINS servers must have fully-qualified domain names. (for example, `dc.internaldomain.com`)



You can specify multiple domains or domain controllers, but only one WINS server. Click + to add more 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 attempts 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.

Configure Windows authorization

Users attempting to log on to a McAfee ePO server with Windows authentication need a permission set assigned to one of their Active Directory groups.

For option definitions, click ? in the interface.

Task

- 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 **New Permission Set**.
- 3 Select any individual users the permission set applies 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 applies.

Selecting an item in the **Browse** pane displays 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 can be added. To add more, repeat steps 4 and 5 until you are finished.

- 6 Click **Save**.

The permission set is applied to all users from the groups you specified by logging on to the server using Windows authentication.

The Audit Log

Use the Audit Log to maintain and access a record of all ePolicy Orchestrator 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 these columns:

- **Action** — The name of the action the ePolicy Orchestrator 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.
- **User Name** — User name of the logged-on user account that was used to take the action.



Audit Log information appears in the language of the Enterprise Administrator locale.

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.

See also

[View and purge the Audit Log on page 45](#)

[Schedule purging the Audit Log on page 46](#)

View and purge the Audit Log

You can view and purge a history of user actions.

When viewing the Audit Log, the available data depends on how often and by what age the Audit Log is purged.



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** and the Audit Log is displayed.
- 2 Select one of these actions.

Action	Steps
View the Audit Log	<ol style="list-style-type: none"> 1 Click any of the column titles to sort the table by that column (alphabetically). 2 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. 3 Click any entry to view its details.
Purge the Audit Log	<ol style="list-style-type: none"> 1 Click Actions Purge. 2 In the Purge dialog box, next to Purge records older than, type a number and select a time unit 3 Click OK. <p>All the Audit Log records are permanently deleted.</p>

See also

[The Audit Log on page 45](#)

Schedule purging the Audit Log

You can automatically purge the Audit Log with a scheduled server task.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **New Task**.
- 2 Name and describe the task. Next to **Schedule Status**, select **Enabled**, then click **Next**.
- 3 Select **Purge Audit Log** from the drop-down list.
- 4 After **Purge records older than**, define the length of time (amount and unit) before purging the Audit Log entries.
- 5 Click **Next**.
- 6 Schedule the task as needed, then click **Next**.
- 7 Review the task's details, then click **Save**.

See also

[The Audit Log on page 45](#)

Client certificate authentication

Clients can use a digital certificate as authentication credentials when they log on to a McAfee ePO server.

Contents

- ▶ [When to use client certificate authentication](#)
- ▶ [Configure ePolicy Orchestrator client certificate authentication](#)
- ▶ [Modify McAfee ePO server certificate-based authentication](#)

- ▶ [Disable McAfee ePO server client certificate authentication](#)
- ▶ [Configure users for certificate authentication](#)
- ▶ [Update CRL file](#)
- ▶ [Problems with client certificate authentication](#)
- ▶ [SSL certificates](#)
- ▶ [Create a self-signed certificate with OpenSSL](#)
- ▶ [Other useful OpenSSL commands](#)
- ▶ [Convert an existing PVK file to a PEM file](#)

When to use client certificate authentication

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

Client 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.
- Requires additional work to maintain certificates compared to password-based authentication.

Configure ePolicy Orchestrator client 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 Select **Enable Certificate Based Authentication**.
- 4 Click **Browse** next to **CA certificate for client certificate (P7B, PEM)**.

- 5 Navigate to and select the certificate file, then click **OK**.
- 6 If you have a **Certificate Revoked List (CRL)** file, click **Browse** next to this edit box, navigate to the CRL file, and click **OK**.
- 7 Click **Save** to save all changes.
- 8 Restart ePolicy Orchestrator to activate certificate authentication.

Modify McAfee ePO server certificate-based authentication

Servers require certificates for SSL connections provide higher 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.

For option definitions, click ? in the interface.

Task

- 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**. Navigate to and select the certificate file and click **OK**.



Once a file has been applied the prompt changes to **Replace current CA certificate**.

- 5 If you have provided a PKCS12 certificate file, enter a password.
- 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 Select any advanced settings, if needed.
- 8 Click **Save** to save all changes.
- 9 Restart the server to enable the certificate based authentication settings changes.

Disable McAfee ePO server client certificate authentication

Server certificates can and should be disabled if they are no longer used.

Before you begin

The server must already be configured for client certificate authentication before you can disable server certificates.

Once a server certificate is uploaded it can only be disabled, 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.

Configure 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 the certificate file that was signed using the CA certificate uploaded in the section *Configure ePolicy Orchestrator certificate authentication*. 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 logon form is grayed out and the user is immediately authenticated.

Update CRL file

You can update the Certificate Revoked List (CRL) file installed on your McAfee ePO server to stop access to ePolicy Orchestrator by specific users.

Before you begin

You must already have a CRL file in ZIP or PEM format.

The CRL file is a list of revoked ePolicy Orchestrator users and their digital certificate status. The list includes the revoked certificates, reason(s) for revocation, dates of certificate issue, and the issuing entity. When a user tries to access the McAfee ePO server, the CRL file is checked and it allows or denies access for that user.

Task

- 1 Click **Menu** | **Configuration** | **Server Settings**.
- 2 Select **Certificate Based Authentication** and click **Edit**.
- 3 To update the **Certificate Revoked List** file, click **Browse** next to this edit box, navigate to the CRL file, and click **OK**.
- 4 Click **Save** to save all changes.
- 5 Restart ePolicy Orchestrator to activate certificate authentication.

You can also use the cURL command line to update the CRL file. For example, at the cURL command line type:



To run cURL commands from the command-line, you must have cURL installed and remote access to the McAfee ePO server. See *ePolicy Orchestrator 5.0.0 Scripting Guide* for cURL download details and other examples.

```
curl -k --cert <admin_cert>.pem --key <admin_key>.pem https://<localhost>:<port>/remote/console.cert.updatecrl.do -F crlFile=@<crls>.zip
```

In this command:

- <admin_cert> — Administrator client certificate .PEM file name
- <admin_key> — Administrator client private key .PEM file name
- <localhost>:<port> — McAfee ePO server name and communication port number
- <crls> — CRL .PEM or .zip file name

Now the new CRL file is checked every time a user accesses the McAfee ePO server to confirm the certificate authentication has not been revoked.

Problems with client certificate authentication

Most authentication issues 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.

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.

Replace the server certificate

You can specify the server certificate and private key used by ePolicy Orchestrator from Server Settings.

Task

For option definitions, click ? in the interface.

- 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.

Install the security certificate when using Internet Explorer

Prevent the certificate prompt from appearing every time you log on by installing the security certificate.

Task

- 1 From your browser, start ePolicy Orchestrator. The Certificate Error: Navigation Blocked page appears.
- 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 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 McAfee ePO server instead of "localhost."
- 13 Restart ePolicy Orchestrator.

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

Install the security certificate when using Firefox 3.5 or higher

You can 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 box 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.

Create a self-signed certificate with OpenSSL

There are times when you might not be able to, or want to, wait for a certificate to be authenticated by a certification authority. During initial testing or for systems used on internal networks a self-signed certificate can provide the basic security and functionality needed.

Before you begin

To create a self-signed certificate, you need to install the OpenSSL for Windows software. OpenSSL is available from:

<http://www.slproweb.com/products/Win32OpenSSL.html>

To create and self-sign a certificate to use with your McAfee ePO server use OpenSSL for Windows software.



There are many tools you can use to create a self-sign a certificate. This task describes the process using OpenSSL.

The file structure used in the following task is:



OpenSSL does not create these folders by default. They are used in these examples and can be created to help you find your output files.

- **C:\ssl** — Installation folder for OpenSSL
- **C:\ssl\certs** — Used to store the certificates created
- **C:\ssl\keys** — Used to store the keys created
- **C:\ssl\requests** — Used to store the certification requests created.

Task

- 1 To generate the initial certificate key, type the following command at the command line:

```
C:\ssl\bin>openssl genrsa -des3 -out C:/ssl/keys/ca.key 1024
```

The following screen appears.

```
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.+++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for keys/ca.key:
Verifying - Enter pass phrase for keys/ca.key:

C:\ssl\bin>
```

- 2 Enter a pass phrase at the initial command prompt and verify the pass phrase at the second command prompt.



Make a note of the pass phrase you enter. You need it later in the process.

The file names ca.key is generated and stored in the path C:\ssl\keys\.

The key looks similar to the following example.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE327E8D510D1882

4Evg9bqeteKbo60Wy0cFh6o8gUhc0TDn/odppSeykvQBAasEhFfcF+nHLort8KkS
bS9WDAqczf6SdKMxoGbi9m57X/PZ+7dcTH7YyKNKskfoqED7/VZXktAEhA1Vw+wj
.
.
.
im2DEkLWQ3kI+6HdaQH0OfE99ReHZJzvAU6F6LbUNULLpDe3wvnGwMI681fAF9C3
4+KDI1RhFK3piLpCOM+8L1DpdOg5FC723Z1Drr0uwghKdyD1GRKLw==
-----END RSA PRIVATE KEY-----
```

- 3 To self-sign the certificate key you created, type the following command at the command line:

```
openssl req -new -x509 -days 365 -key C:/ssl/keys/ca.key -out C:/ssl/certs/ca.cer
```

The following screen appears.

```
Enter pass phrase for ca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Oregon
Locality Name (eg, city) []:Beaverton
Organization Name (eg, company) [Internet Widgits Pty Ltd]:McAfee
Organizational Unit Name (eg, section) []:Enterprise
Common Name (eg, YOUR name) []:ePO_Server
Email Address []:tester@mcafee.com

C:\ssl\bin>
```

Type the information needed after the following command prompts:

- Country Name (2 letter code) [AU]:
- State or Province Name (full name) [Some-State]:
- Locality Name (eg, city) []:
- Organization Name (eg, company) [Internet Widgits Pty Ltd]:
- Organizational Unit Name (eg, section) []:

- Common Name (eg, YOUR name) []:



At this command prompt, type the name of your server, for example your McAfee ePO server name.

- Email Address []:

The file named ca.cer is generated and stored in the path C:\ssl\certs\.

The self-signed certificate looks similar to the following example.

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIJAJe1id+Ih0GDMA0GCSqGSIb3DQEBBQUAMIGEMQswCQYD
VQQGEwJVUzEPMAOGA1UECBMGT1JFR090MRIwEAYDVQQHEw1CRUFWRVJUT04xDzAN
.
.
.
NF/Om6VMhuUy4Cyc5CIyTmGzVPDEo8dK20kdLR+tQhDsdqM5qpfd6w52ew2ORKo/
dLGiMtraicXeR2GyWrKJjywow3xBtkvyQQj2xmMWUmDwYjCOYH01KjVOX+fGwcdX
jWTfB10HV8507ASUOqteOwe/BSTMuZWgMA==
-----END CERTIFICATE-----
```



To have a third party, for example VeriSign or Microsoft Windows Enterprise Certificate Authority, create a signed certificate for ePolicy Orchestrator, see KnowledgeBase article [KB72477](#).

- 4 Upload and manage the certificate on the McAfee ePO server.

Other useful OpenSSL commands

You can use other OpenSSL commands to extract and combine the keys in generated PKCS12 certificates and to convert a password protected private key PEM file to a non-password protected file.


Commands to use with PKCS12 certificates

Use the following commands to create a PKCS12 certificate with both the certificate and key in one file.

Description	OpenSSL command format
Create a certificate and key in one file	<code>openssl req -x509 -nodes -days 365 -newkey rsa:1024 -config path \openssl.cnf -keyout path \pkcs12Example.pem -out path \pkcs12Example.pem</code>
Export the PKCS12 version of the certificate	<code>openssl pkcs12 -export -out path \pkcs12Example.pfx -in path \pkcs12Example.pem -name "user_name_string"</code>

Use the following commands to separate the certificate and key from a PKCS12 certificate with them combined.

Description	OpenSSL command format
Extracts the .pem key out of .pfx	<code>openssl pkcs12 -in pkcs12ExampleKey.pfx -out pkcs12ExampleKey.pem</code>
Removes password on key	<code>openssl rsa -in pkcs12ExampleKey.pem -out pkcs12ExampleKeyNoPW.pem</code>

 The ePolicy Orchestrator server can then use the pkcs12ExampleCert.pem as the certificate and the pkcs12ExampleKey.pem as the key (or the key without a password pkcs12ExampleKeyNoPW.pem).

Command to convert a password protected private key PEM file

To convert a password protected private key PEM file to a non-password protected file, type:

```
openssl rsa -in C:\ssl\keys\key.pem -out C:\ssl\keys\keyNoPassword.pem
```



In the previous example, "C:\ssl\keys" is the input and output paths for the file names "key.pem" and "keyNoPassword.pem".

Convert an existing PVK file to a PEM file

The ePolicy Orchestrator browser supports PEM-encoded private keys. This includes both password protected and non-password protected private keys. Using OpenSSL you can convert a PVK-formatted key to a PEM format.

Before you begin

To convert the PVK formatted file, install the OpenSSL for Windows software. This is available from:

<http://www.slproweb.com/products/Win32OpenSSL.html>

Using the OpenSSL for Windows software, convert your PVK format certificate to PEM format.

Task

- 1 To convert a previously created PVK file to a PEM file, type the following at the command line:

```
openssl rsa -inform PVK -outform PEM -in C:\ssl\keys\myPrivateKey.pvk -out C:\ssl\keys\myPrivateKey.pem -passin pass:p@$$w0rd -passout pass:p@$$w0rd
```



In the previous example, "-passin" and "-passout" arguments are optional.

- 2 If prompted, type the password used when you originally created the PVK file.
If the "-passout" argument is not used in the previous example, the newly created PEM-formatted key is not password protected.

Permission sets

Permission sets control the level of access users have to the 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*

- [Manage 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.

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 McAfee ePO 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 *Manage permission sets*.

Administrators

Administrators have read and write permissions and rights to all operations. When you install the server, an 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 administrator accounts for people who require administrator rights.

Permissions exclusive to 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.

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.

Manage permission sets

Control user access, create, modify, export, and import permission sets from the Permission Sets page.





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

Task

For option definitions, click ? in the interface.

- 1 Open the **Permission Sets** page: select **Menu | User Management | Permission Sets**.
- 2 Select one of these actions.

Action	Steps
Add a permission set	<ol style="list-style-type: none"> 1 Click New Permission Set. 2 Type a name for the new permission set. The software does not allow you to use an existing name. Each permission set name must be unique. 3 If you want to immediately assign specific users to this permission set, select their user names in the Users section. 4 If you want to map any Active Directory groups to this permission set, select the server from the Server Name list, then click Add. 5 If you added any Active Directory servers that you want to remove, select them in the Active Directory list box, then click Remove. 6 Click Save to create the permission set. <p>You have created the permission set but you have not yet assigned permissions to it.</p>
Edit a permission set	<ol style="list-style-type: none"> 1 Select a permission set to modify. Its details appear to the right. If you created a permission set, it is already selected for you. 2 Select a category of permissions to modify by clicking Edit in that category row. 3 Change the permissions, then click Save to commit the permission set changes to the database. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  You don't have to click Save when you complete modifying the permission set. The changes are saved for you when you modify each category. The changes you make are immediately reflected in the system, and are propagated to the remainder of your network according to your policy configuration. </div>
Copy a permission set	<ol style="list-style-type: none"> 1 Select a permission set to duplicate from the Permission Sets list, then click Actions Duplicate. 2 Type a new name for the duplicate permission set. By default, the software appends (copy) to the existing name. The software does not allow you to use an existing name. Each permission set name must be unique. 3 Click OK. <p>The permission set is duplicated, but the original is still selected in the Permission Sets list.</p>

Action	Steps
Delete a permission set	<ol style="list-style-type: none"> <li data-bbox="513 237 1523 310">1 Select the permission set that you want to delete from the Permission Sets list. Its details appear to the right. <li data-bbox="513 321 1523 352">2 Click Actions Delete, then click OK. <p data-bbox="513 363 1523 411">The permission set no longer appears in the Permission Sets list.</p>
Export permission sets	<p data-bbox="513 422 1523 453">Click Export All.</p> <p data-bbox="513 457 1523 510">The McAfee ePO server sends an XML file to your browser. What happens next depends on your browser settings. Most browsers ask you to save the file.</p> <div data-bbox="594 531 1523 636" style="background-color: #f0f0f0; padding: 5px;"> <p data-bbox="532 552 578 604"> The XML file only contains roles that have a level of permission defined. If, for example, a particular Permission Set has no permissions for queries and reports, no entry appears in the file.</p> </div>
Import permission sets	<ol style="list-style-type: none"> <li data-bbox="513 657 1523 688">1 Click Import. <li data-bbox="513 699 1523 772">2 Click Browse to navigate to and select the XML file containing the permission sets that you want to import. <li data-bbox="513 783 1523 919">3 Choose whether to keep permission sets with the same name as an imported permission set by selecting the appropriate option. Click OK. If McAfee ePO cannot locate a valid permission set within the indicated file, an error message is displayed and the import process is stopped. <p data-bbox="513 930 1523 991">The permission sets are added to the server and displayed in the Permission Sets list.</p>

6

Repositories

Repositories house your security software packages and their 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.

Contents

- ▶ *Repository types and what they do*
- ▶ *How repositories work together*
- ▶ *Setting up repositories for the first time*
- ▶ *Manage source and fallback sites*
- ▶ *Verify access to the source site*
- ▶ *Configure settings for global updates*
- ▶ *Configure agent policies to use a distributed repository*
- ▶ *Use SuperAgents as distributed repositories*
- ▶ *Create and configure repositories on FTP or HTTP servers and UNC shares*
- ▶ *Using UNC shares as distributed repositories*
- ▶ *Use local distributed repositories that are not managed*
- ▶ *Work with the repository list files*
- ▶ *Pull tasks*
- ▶ *Replication tasks*
- ▶ *Repository selection*

Repository types and what they do

To deliver products and updates throughout your network, McAfee ePO software offers several types of repositories that create a robust infrastructure for updating.

These repositories give you the flexibility to develop an updating strategy so that your systems are always current.

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, McAfee ePO uses Microsoft Internet Explorer proxy settings.

Distributed repositories

Distributed repositories host copies of your Master Repository. Consider using distributed repositories and placing them throughout your network. This configuration ensures that managed systems are updated while network traffic is minimized, especially across slow connections.

As you update your Master Repository, McAfee ePO 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.



Do not configure distributed repositories to reference the same directory as your Master Repository. Doing so locks the files on the Master Repository. This can cause failure for pulls and package check-ins, and can leave the Master Repository in an unusable state.

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 many 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, if you want automatic updating, create SuperAgents in your environment. 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*.

Source site

The source site provides all updates for your Master Repository. The default source site is the McAfee `http` update site, but you can change the source site or create multiple source sites.

We recommend using the McAfee `http` or McAfee `ftp` 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. Manually check in all other packages and updates, including service packs and patches, to the Master Repository.

Fallback site

The fallback site is a source site enabled as the backup site. 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. Managed systems can remain up-to-date using a fallback site. The default fallback site is the McAfee `http` update site. You can enable only one fallback site.

If managed systems use a proxy server to access the Internet, configure agent policy settings to use proxy servers when accessing the 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.
- 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 have access to 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.



The correct permissions must be set to access the folder.

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 by ePolicy Orchestrator, a local administrator must keep the distributed files 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.



See *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 recommendation, and using global updating or scheduling replication tasks frequently, ensures your managed environment is up-to-date. Use unmanaged distributed repositories only if your network or organization's policy doesn't allow managed distributed repositories.

Repository branches and their purposes

You can use the three ePolicy Orchestrator repository branches to maintain up to three versions of the 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 files

The repository list files (`SiteList.xml` and `SiteMgr.xml`) contain the names of all repositories you are managing.

The repository lists include the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository lists to the McAfee Agent during agent-server communication.

If needed, you can export the repository list to external files (`SiteList.xml` or `SiteMgr.xml`). The two files have different uses:

`SiteList.xml` file

- Import to a McAfee Agent during installation.

`SiteMgr.xml` file

- Back up and restore your distributed repositories and source sites if you have to reinstall the server.
- Import the distributed repositories and source sites from a previous installation of the McAfee ePO 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 geographic distribution of your network, you might need distributed repositories.

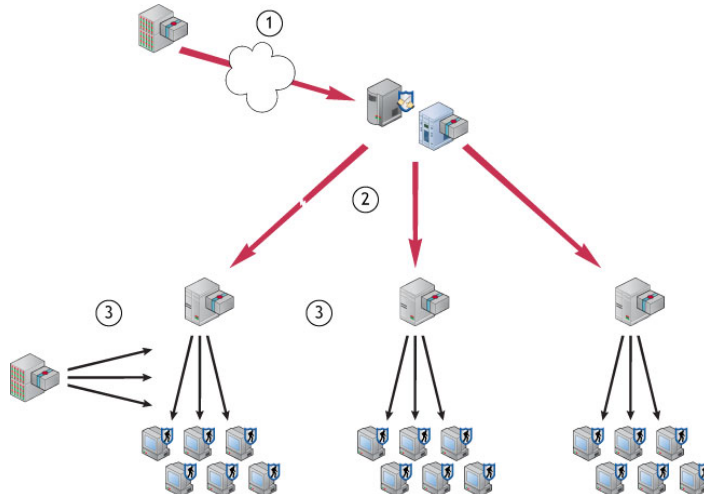


Figure 6-1 Sites and repositories delivering packages to systems

- 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.

Setting up repositories for the first time

Follow these high-level steps when creating repositories for the first time.

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

Manage source and fallback sites

You can change the default source and fallback sites from the Server Settings. For example, you can edit settings, delete existing source and fallback sites, or switch between them.



You must be an administrator or have appropriate permissions to define, change, or delete source or fallback sites.

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

Tasks

- [Create source sites on page 66](#)
Create a new source site from Server Settings.
- [Switch source and fallback sites on page 67](#)
Use Server Settings to change source and fallback sites.
- [Edit source and fallback sites on page 67](#)
Use Server Settings to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.
- [Delete source sites or disabling fallback sites on page 68](#)
If a source or fallback site is no longer in use, delete or disable the site.

Create source sites

Create a new source site from Server Settings.

Task

For option definitions, click ? in the interface.

- 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.

Option	Definition
DNS Name	Specifies the DNS name of the server.
IPv4	Specifies the IPv4 address of the server.
IPv6	Specifies the IPv6 address of the server.

- 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.

Switch source and fallback sites

Use Server Settings to change source and fallback sites.

Depending on your network configuration, you might want to switch the source and fallback sites if you find that HTTP or FTP updating works better.

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**.

Edit source and fallback sites

Use Server Settings 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 the name of the site.
The Source Site Builder wizard opens.
- 4 Edit the settings on the wizard pages as needed, then click **Save**.

Delete source sites or disabling fallback sites

If a source or fallback site is no longer in use, delete or disable the site.

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.

Verify access to the source site

You must make sure that the ePolicy Orchestrator master repository and managed systems can access the Internet when using the McAfeeHttp and McAfeeFtp sites as source and fallback sites.

This section describes the tasks for configuring the connection the ePolicy Orchestrator master repository and the McAfee Agent use to connect to the download site directly or via a proxy. The default selection is **Do not use proxy**.

Tasks

- [Configure proxy settings on page 68](#)
To update your repositories, configure proxy settings to pull DATs.
- [Configure proxy settings for the McAfee Agent on page 69](#)
Configure the proxy settings the McAfee Agent uses to connect to the download site.

Configure proxy settings

To update your repositories, configure proxy settings to pull DATs.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**.
- 2 From the list of setting categories, select **Proxy Settings**, then click **Edit**.
- 3 Select **Configure the proxy settings manually**.
 - a 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. 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, configure both HTTP and FTP proxy authentication information here.

- b Next to Proxy authentication, configure the settings according to whether you pull updates from HTTP repositories, FTP repositories, or both.
 - c Next to Exclusions, select **Bypass Local Addresses**, then specify distributed repositories that the server can connect to directly by typing the IP addresses or the fully-qualified domain name of those systems, separated by semicolons.
 - d Next to Exclusions, select **Bypass Local Addresses**, then specify distributed repositories that the server can connect to directly by typing the IP addresses or the fully-qualified domain name of those systems, separated by semicolons.
- 4 Click **Save**.

Configure proxy settings for the McAfee Agent

Configure the proxy settings the McAfee Agent uses to connect to the download site.

Task

For option definitions, click ? in the interface.

- 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 or FTP source where the agent pulls updates. Select **Use these settings for all proxy types** to make these settings the default settings for all 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** or **Use FTP proxy authentication**, then provide a user name and credentials.
- 9 Click **Save**.

Configure settings for global updates

Global updates automate repository replication in your network. You can use the Global Updating server setting to configure the content that is distributed to repositories during a global update.

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*.

Configure agent policies to use a distributed repository

Customize how agents select distributed repositories to minimize bandwidth use.

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 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.

Use SuperAgents as distributed repositories

Create and configure distributed repositories on systems that host SuperAgents. SuperAgents can minimize network traffic.



In order to convert an agent to a SuperAgent, the agent must be part of a Windows domain.

Tasks

- [Create SuperAgent distributed repositories on page 71](#)
To create a SuperAgent repository, the SuperAgent system must have a McAfee Agent installed and running. We recommend using SuperAgent repositories with global updating.
- [Replicate packages to SuperAgent repositories on page 72](#)
Select which repository-specific packages are replicated to distributed repositories.
- [Delete SuperAgent distributed repositories on page 72](#)
Remove SuperAgent distributed repositories from the host system and the repository list (SiteList.xml). New configurations take effect during the next agent-server communication.

Create SuperAgent distributed repositories

To create a SuperAgent repository, the SuperAgent system must have a McAfee Agent installed and running. We recommend using SuperAgent repositories with global updating.

This task assumes that you know where the SuperAgent systems are located in the System Tree. We recommend creating a SuperAgent tag so that you can easily locate the SuperAgent systems with the Tag Catalog page, or by running a query.

For option definitions, click ? in the interface.

Task

- 1 From the ePolicy Orchestrator console, click **Menu | Policy | Policy Catalog**, then from the **Product** list click **McAfee Agent**, and from the Category list, select **General**.
A list of available general category policies available for use on your McAfee ePO server appears.
- 2 Create a new policy, duplicate an existing one, or open one that's already applied to systems that hosts 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 a standard Windows path, such as `C:\SuperAgent\Repo`.



All requested files from the agent system are served from this location using the agent's built-in HTTP webservice.

- 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 policy is retrieved. If you do not want to wait for the next agent-server communication interval, you can send an agent wake-up call to the systems. When the distributed repository is created, the folder you specified is created on the system if it did not already exist.

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

Replicate packages to SuperAgent repositories

Select which repository-specific packages are replicated to distributed repositories.

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 the 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**.

Delete SuperAgent distributed repositories

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

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu | Policy | Policy Catalog**, then click the name of the SuperAgent policy you want to modify.
- 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. Agents that have not received a new site list after the policy change continue to update from the SuperAgent that was removed.

Create and configure repositories on FTP or HTTP servers and UNC shares

You can host distributed repositories on existing FTP, HTTP servers or UNC shares. Although a dedicated server is not required, the system should be robust enough to handle the load when your managed systems connect for updates.

Tasks

- [Create a folder location on page 73](#)
Create the folder that hosts repository contents on the distributed repository system. Different processes are used for UNC share repositories and FTP or HTTP repositories.
- [Add the distributed repository to ePolicy Orchestrator on page 73](#)
Add an entry to the repository list and specify the folder the new distributed repository uses.
- [Avoid replication of selected packages on page 75](#)
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.
- [Disable replication of selected packages on page 76](#)
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.
- [Enable folder sharing for UNC and HTTP repositories on page 76](#)
On an HTTP or UNC distributed repository, you must enable the folder for sharing across the network, so that your McAfee ePO server can copy files to the repository.
- [Edit distributed repositories on page 76](#)
Edit a distributed repository configuration, authentication, and package selection options as needed.
- [Delete distributed repositories on page 76](#)
Delete HTTP, FTP, or UNC distributed repositories. Doing so also deletes the contents of the distributed repositories.

Create a folder location

Create the folder that hosts repository contents on the distributed repository system. Different processes are used for UNC share repositories and FTP or HTTP repositories.

- 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.

Add the distributed repository to ePolicy Orchestrator

Add an entry to the repository list and specify the folder the new distributed repository uses.



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, configure one of the following server types.

HTTP server type

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

Option	Definition
DNS Name	Specifies the DNS name of the server.
IPv4	Specifies the IPv4 address of the server.
IPv6	Specifies the IPv6 address of the server.

- Enter the port number of the server: 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>.

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.

Option	Definition
DNS Name	Specifies the DNS name of the server.
IPv4	Specifies the IPv4 address of the server.
IPv6	Specifies the IPv6 address of the server.

- Enter the port number of the server: FTP default is 21

- 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
- 6 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
- 7 Click **Next**. The Package Types page appears.
- 8 Select whether to replicate all packages or selected packages to this distributed repository, then click **Next**.
 - If you choose the **Selected packages** option, manually select the **Signatures and engines** and **Products, patches, service packs, etc.** you want to replicate.
 - Optionally select to **Replicate legacy DATs**.



Ensure all packages required by managed systems using this repository are not deselected. Managed systems go to one repository for all packages — if a needed package type is not present in the repository, the task fails. This feature ensures packages that only a few systems use are not replicated throughout your entire environment.

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

Avoid 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.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Software | Distributed Repositories**, then click a 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**.

Disable 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.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Automation | Server Tasks**, then select **Edit** next to a replication server task.
The Server Task Builder wizard opens.
- 2 On the Description page, select the **Schedule status** as **Disabled**, then click **Save**.

Enable folder sharing for UNC and HTTP repositories

On an HTTP or UNC distributed repository, you must enable the folder for sharing across the network, so that your McAfee ePO server can copy files to the repository.

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 McAfee ePO server service, require write access. See your Microsoft Windows documentation to configure appropriate security settings for shared folders.
- 5 Click **OK**.

Edit distributed repositories

Edit a distributed repository configuration, authentication, and package selection options as needed. For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Software | Distributed Repositories**, then click a 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**.

Delete distributed repositories

Delete HTTP, FTP, or UNC distributed repositories. Doing so also deletes the contents of the distributed repositories.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu** | **Software** | **Distributed Repositories**, then click **Delete** next to a repository.
- 2 On the Delete Repository dialog box, click **OK**.



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

Deleted repositories are removed from the repository list.

Using UNC shares as distributed repositories

Follow these guidelines when using UNC shares as distributed repositories.

UNC shares use the Microsoft Server Message Block (SMB) protocol to create a shared drive. Create a user name and password for access to this share.

Correctly configure the share

Make sure that the UNC share is correctly configured.

- **Use an alternate method to write to your repository** — Log on to the server using other methods (another share, RDP, locally) to write to your repository. Do not mix the repository you read from with the repository you write to. Read credentials are shared with endpoints, and write credentials are used exclusively by the McAfee ePO server to update your distributed repository content.
- **Do not use a share on your Domain Controller** — Create a share off your domain controller. A local user on a domain controller is a domain user.

Secure the account you use to read from the UNC share

Follow these guidelines to make sure the account used to access the UNC share is secure.

- **Grant your UNC share account read-only rights for everyone except the McAfee ePO server master repository** — When you set up your share, make sure that the account you created has read-only rights to the directory and to the share permissions. Do not grant remote writing to the share (even for administrators or other accounts). The only account allowed access is the account you recently created.



The McAfee ePO server master repository must be able to write files to the UNC share account.

- **Create the account locally** — Create the account on the file share, not on the domain. Accounts created locally do not grant rights to systems in the domain.
- **Use a specific account** — Create an account specifically for sharing repository data. Do not share this account with multiple functions.
- **Make the account low privilege** — Do not add this account to any groups it does not need, which includes "Administrators" and "Users" groups.
- **Disable extraneous privileges** — This account does not need to log on to a server. It is a placeholder to get to the files. Examine this account's privileges and disable any unnecessary privileges.
- **Use a strong password** — Use a password with 8–12 characters, using multiple character attributes (lowercase and uppercase letters, symbols, and numbers). We recommend using a random password generator so that your password is complex.

Protect and maintain your UNC share

- **Firewall your share** — Always block unrequired traffic. We recommend blocking outgoing and incoming traffic. You can use a software firewall on the server or a hardware firewall on the network.
- **Enable File Auditing** — Always enable security audit logs to track access to your network shares. These logs display who accesses the share, and when and what they did.
- **Change your passwords** — Change your password often. Make sure that the new password is strong, and remember to update your McAfee ePO configuration with the new password.
- **Disable the account and share if it's no longer used** — If you switch to a different repository type other than UNC, remember to disable or delete the account, and close and remove the share.

Use local distributed repositories that are not managed

Copy contents from the Master Repository into an unmanaged distributed repository.

Once an unmanaged repository is 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.
For example, using a Windows 2008 R2 Server, this is the default path on your server: `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\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**.
 - b Click an existing agent policy or create a new agent policy.



Policy inheritance cannot be broken at the level of option tabs that constitute a policy. Therefore, when you apply this policy to systems, ensure that only the correct systems receive and inherit the policy to use the unmanaged distributed repository.

- c On the **Repositories** tab, click **Add**.
- 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.

Work with the repository list files

You can export the repository list files.

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

Tasks

- [Export the repository list `SiteList.xml` file on page 79](#)
Export the repository list (`SiteList.xml`) file for manual delivery to systems, or for import during the installation of supported products.
- [Export the repository list for backup or use by other servers on page 80](#)
Use the exported `SiteMgr.xml` file to restore 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.
- [Import distributed repositories from the repository list on page 80](#)
Import distributed repositories from the `SiteMgr.xml` file after reinstalling a server, or when you want one server to use the same distributed repositories as another server.
- [Import source sites from the `SiteMgr.xml` file on page 80](#)
After re-installing a server, and when you want two servers to use the same distributed repositories, import source sites from a repository list file.

Export the repository list `SiteList.xml` file

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.

Export the repository list for backup or use by other servers

Use the exported `SiteMgr.xml` file to restore 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**.

Import distributed repositories from the repository list

Import distributed repositories from the `SiteMgr.xml` file after reinstalling a server, or when 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.

Import source sites from the SiteMgr.xml file

After re-installing a server, and when you want two servers to use the same distributed repositories, import source sites from a repository list file.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Configuration | Server Settings**, then from the **Setting Categories** list select **Source Sites** and click **Edit**.

- 2 Click **Import**.

- 3 Browse to and select the exported `SiteMgr.xml` file, then click **OK**.

- 4 Select the source sites to import into this server, then click **OK**.

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

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.

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 in to 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.

7

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 ePO can communicate with:

- Other McAfee ePO servers
- Additional, remote, database servers
- LDAP servers
- Syslog servers



McAfee Endpoint Security and the Syslog Management extension must be installed in your McAfee ePO environment before you can configure this registered server.

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

Contents

- ▶ [Register McAfee ePO servers](#)
- ▶ [Register LDAP servers](#)
- ▶ [Register SNMP servers](#)
- ▶ [Using database servers](#)
- ▶ [Sharing objects between servers](#)

Register McAfee ePO servers

You can register additional McAfee ePO servers for use with your main McAfee ePO server to collect or aggregate data, or to allow you to transfer managed systems between the registered servers.

Before you begin

To register one McAfee ePO server with another, you need to know detailed information about the McAfee ePO server SQL database of the server you are registering. You can use the following remote command to determine the Microsoft SQL database server name, database name, and more:

```
https://<server_name>:<port>/core/config
```



These are the variables in the remote command:

- <server_name> — The DNS server name or IP address of the remote McAfee ePO server
- <port> — The assigned McAfee ePO server port number, usually "8443", unless your server is configured to use a different port number

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:

Option	Definition
Authentication type	Specifies the type of authentication to use for this database, including: <ul style="list-style-type: none"> • Windows authentication • SQL authentication
Client task sharing	Specifies whether to enable or disable client task for this server.
Database name	Specifies the name for this database.
Database port	Specifies the port for this database.
Database server	Specifies the name of the database for this server. You can specify a database using DNS Name or IP address (IPv4 or IPv6).
ePO Version	Specifies the version of the McAfee ePO server being registered.
Password	Specifies the password for this server.
Policy sharing	Specifies whether to enable or disable policy sharing for this server.
SQL Server instance	<p>Allows you to specify whether this is the default server or a specific instance, by providing the Instance name.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> 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.</p> <p>Select the Default SQL server instance and type the port number to connect to the SQL server instance.</p> </div>
SSL communication with database server	Specifies whether ePolicy Orchestrator uses SSL (Secure Socket Layer) communication with this database server including: <ul style="list-style-type: none"> • Try to use SSL • Always use SSL • Never use SSL
Test connection	<p>Verifies the connection for the detailed server.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> If you register a server with a different McAfee ePO version, this information-only warning appears: Warning Version mismatch!</p> </div>

Option	Definition
Transfer systems	<p>Specifies whether to enable or disable the ability to transfer systems for this server. When enabled, select Automatic sitelist import or Manual sitelist import.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>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</p> <ul style="list-style-type: none"> • Transferring systems from this McAfee ePO server to the registered McAfee ePO server • and an Agent Handler name appears alpha-numerically earlier than the McAfee ePO server name in the supplied sitelist • and the older Agents use that Agent Handler </div>
Use NTLMv2	Optionally choose to use NT LAN Manager authentication protocol. Select this option when the server you are registering uses this protocol.
User name	Specifies the user name for this server.

4 Click **Save**.

Register 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.

Register 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:
 - **DNS Name** — Specifies the DNS name of the registered server.
 - **IPv4** — Specifies the IPv4 address of the registered server.
 - **IPv6** — Specifies the DNS name of the registered server which has an IPv6 address.
- 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 Servers page.

Using database servers

ePolicy Orchestrator can retrieve data from not only its own databases, but from 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, McAfee ePO 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

A *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.

Register 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**.

Modify 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, then 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.

Remove 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.

Sharing objects between servers

Frequently, the easiest and fastest way to replicate behavior from one McAfee ePO server to another is to export the item describing the behavior and import it onto the other server.

Export objects and data from your McAfee ePO server

Exported objects and data can be used for backing up important data, and to restore or configure the McAfee ePO 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. To view data, export the tables as HTML or PDF files. To use the data in other applications, export the tables or to CSV or XML files.

Task

- 1 From the page displaying the objects or data, click **Actions** and select an option. For example, when exporting a table, select **Export Table**, then click **Next**.
- 2 When exporting content that can be downloaded in multiple formats, such as Query data, an **Export** page with configuration options appears. Specify your preferences, then click **Export**.

- 3 When exporting objects or definitions, such as client task objects or definitions, one of the following occurs:
 - A browser window opens where you can choose **Open** or **Save**.
 - An **Export** page containing a link to the file opens. Left-click the link to view the file in your browser, or right-click the link to save the file.

Import items into ePolicy Orchestrator

Items exported from a McAfee ePO 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.

8

Agent Handlers

Agent Handlers route communication between agents and your McAfee ePO server.

Each McAfee ePO server contains a master Agent Handler. Additional Agent Handlers can be installed on systems throughout your network.

Setting up more Agent Handlers provides the following benefits.

- Helps manage an increased number of products and systems managed by a single, logical McAfee ePO server in situations where the CPU on the database server is not overloaded.
- Provides fault tolerant and load-balanced communication with many agents, including geographically distributed agents.

Contents

- ▶ [How Agent Handlers work](#)
- ▶ [Connect an Agent Handler in the DMZ to a McAfee ePO server in a domain](#)
- ▶ [Handler groups and priority](#)
- ▶ [Manage Agent Handlers](#)

How Agent Handlers work

Agent Handlers distribute network traffic generated by agent-server communication by directing managed systems or groups of systems to report to a specific Agent Handler. Once assigned, a managed system communicates with the assigned Agent Handler instead of with 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.



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

The Agent Handler must be able to authenticate domain credentials. If this is not possible, the account the Agent Handler uses to authenticate to the database must use SQL authentication. For more information about Windows and SQL authentication, see the Microsoft SQL Server documentation.

For more information about changing authentication modes, see the Microsoft SQL Server documentation. If you do, you must also update the SQL Server connection information.

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 particular agents. Click the list to view the agents that cannot communicate with the handler.

Multiple Agent Handlers

You can have more than one Agent Handler in your network. You might have many 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.

Connect an Agent Handler in the DMZ to a McAfee ePO server in a domain

When your McAfee ePO server is in a domain, an Agent Handler installed in the DMZ cannot connect to the McAfee ePO SQL database because the Agent Handler cannot use domain credentials.

To bypass this limitation, configure the Agent Handler to use the SQL database system administrator (sa) account credentials.

Task

For option definitions, click ? in the interface.

- 1 Enable the system administrator account.
 - a Open **SQL Management Studio**, expand **Security | Logins**, and double-click the sa account.
 - b In the **General** tab, type and confirm your password.
 - c On the **Status** tab, set **Login** to **Enabled**, then click **OK**.
 - d Right-click the database instance name and click **Properties**.

The system administrator account is enabled.

- 2 Change the system administrator account to connect to the McAfee ePO database.

- a Open a web browser and go to <https://localhost:8443/core/config-auth>



8443 is the console communication port. If you use a different port to access the McAfee ePO console, include that port number in the address instead.

- b Log on with your McAfee ePO credentials.
- c Delete the entry in the **User Domain** field, then type **sa**.
- d Provide a password for the system administrator account, then click **Test Connection**.
- e If the test is successful, click **Apply**.



If the test is unsuccessful, re-enter your password, then click **Test Connection** again

The Agent Handler uses the system administrator credentials to communicate with the McAfee ePO database.

Handler groups and priority

When using multiple Agent Handlers in your network, group and prioritize them to help ensure network connectivity.

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 communication 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.

Manage Agent Handlers

Set up Agent Handlers in your network and assign McAfee Agents to them.

Tasks

- [Assign McAfee Agents to Agent Handlers on page 94](#)
Assign agents to specific handlers. You can assign systems individually, by group, and by subnet.
- [Manage Agent Handler assignments on page 94](#)
Complete common management tasks for Agent Handler assignments.
- [Create Agent Handler groups on page 95](#)
Handler groups make it easier to manage multiple handlers throughout your network, and can play a role in your fallback strategy.
- [Manage Agent Handler groups on page 95](#)
Complete common management tasks for Agent Handler groups.
- [Move agents between handlers on page 96](#)
Assign agents to specific handlers. You can assign systems using Agent Handler assignment rules, Agent Handler assignment priority, or individually using the System Tree.

Assign McAfee Agents to Agent Handlers

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 or remove more Agent Handlers (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.

Manage Agent Handler assignments

Complete common management tasks for Agent Handler assignments.

To perform these actions, click **Menu** | **Configuration** | **Agent Handlers**, then in Handler Assignment Rules, click **Actions**.

To do this...	Do this...
Delete a handler assignment	Click Delete in the selected assignment row.
Edit a handler assignment	<p>Click Edit for the selected assignment. The Agent Handler Assignment page opens, where you can specify:</p> <ul style="list-style-type: none"> • Assignment name — The unique name that identifies this handler assignment. • Agent criteria — 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. • Handler priority — Choose whether to use all Agent Handlers or a custom handler list. Agents randomly select which handler to communicate with when Use all Agent Handlers is selected. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;">  Use the drag-and-drop handle to quickly change the priority of handlers in your custom handler list. </div>
Export handler assignments	Click Export . The Download Agent Handler Assignments page opens, where you can view or download the AgentHandlerAssignments.xml file.
Import handler assignments	Click Import . The Import Agent Handler Assignments dialog box opens, where you can browse to a previously downloaded AgentHandlerAssignments.xml file.
Edit the priority of handler assignments	Click Edit Priority . The Agent Handler Assignment Edit Priority page opens, where you change the priority of handler assignments using the drag-and-drop handle.
View the summary of a handler assignments details	Click > in the selected assignment row.

Create Agent Handler groups

Handler groups 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**.

Manage Agent Handler groups

Complete common management tasks for Agent Handler groups.

To perform these actions, click **Menu | Configuration | Agent Handlers**, then click the **Handler Groups** monitor.

For option definitions, click ? in the interface.

Action	Steps
Delete a handler group	Click Delete in the selected group row.
Edit a handler group	<p>Click the handler group. The Agent Handler Group Settings page opens, where you can specify:</p> <ul style="list-style-type: none"> • Virtual DNS Name — The unique name that identifies this handler group. • Virtual IP address — The IP address associated with this group. • Included handlers — Choose whether to use a third-party load balancer or a custom handler list. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Use a custom handler list to specify which handlers, and in what order, agents assigned to this group communicate with. </div>
Enable or disable a handler group	Click Enable or Disable in the selected group row.

Move agents between handlers

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

- [Group agents using Agent Handler assignments on page 96](#)
Create Agent Handler assignments to group McAfee Agents together.
- [Group agents by assignment priority on page 97](#)
Group agents together and assign them to an Agent Handler that is using assignment priority.
- [Group agents using the System Tree on page 98](#)
Group agents together and assign them to an Agent Handler using the System Tree.

Group agents using Agent Handler assignments

Create Agent Handler assignments to group McAfee Agents together.

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 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.

- 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**.



Group agents by assignment priority

Group agents together and assign 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**.

Group 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**.

Managing your network security

An essential part of protecting your organization from threats is keeping your McAfee products updated with the latest security content. McAfee ePO helps you do this for all the systems in your network.

Chapter 9	<i>The System Tree</i>
Chapter 10	<i>Tags</i>
Chapter 11	<i>Agent-server communication</i>
Chapter 12	<i>Security keys</i>
Chapter 13	<i>Software Manager</i>
Chapter 14	<i>Product Deployment</i>
Chapter 15	<i>Manual package and update management</i>
Chapter 16	<i>Policy management</i>
Chapter 17	<i>Client tasks</i>
Chapter 18	<i>Server tasks</i>
Chapter 19	<i>Managing SQL databases</i>

9

The System Tree

The System Tree is a graphical representation of how your managed network is organized.

Use ePolicy Orchestrator software to automate and customize your 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 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 the console (drag-and-drop).

Contents

- ▶ *The System Tree structure*
- ▶ *Considerations when planning your System Tree*
- ▶ *Active Directory synchronization*
- ▶ *Types of Active Directory synchronization*
- ▶ *NT domain synchronization*
- ▶ *Criteria-based sorting*
- ▶ *Create and populate System Tree groups*
- ▶ *Move systems within the System Tree*
- ▶ *How Transfer Systems works*
- ▶ *How the Automatic Responses feature interacts with the System Tree*

The System Tree structure

The System Tree is a hierarchical structure that organizes the systems in your network into groups and subgroups.

The default System Tree structure includes these *groups*:

- **My Organization** — The root of your System Tree.
- **My Group** — The default group added from the Getting Started initial software installation.



This group name could have been changed from the default during the initial software installation.

- **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 by default to My Group.



The My Group name could have been changed from the default during the initial software installation.

The My Organization group has these characteristics:

- It can't be deleted.
- It can't be renamed.

The My Group

My Group is a subgroup of the My Organization group and is added by default during the Getting Started initial software installation.



The My Group name could have been changed from the default during the initial software installation.

When the installation URL is run on your network computers they are grouped by default in My Group of the System Tree.

Click **System Tree** | **Actions** to delete or rename My Group in the System Tree.



If you delete systems from the System Tree, be sure that you select the option to remove their agents. If the McAfee Agent is not removed, deleted systems reappear in the Lost&Found group because the McAfee Agent continues to communicate to McAfee ePO Cloud.

The lost and found group

The Lost&Found group is a subgroup of the My Organization group.

Depending on the methods you specify when 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 System Tree list and is not alphabetized among its peers.
- Users must be granted permissions to the Lost&Found group to see its contents.
- 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 that you select the option to remove their agents. If the McAfee Agent is not removed, deleted systems reappear in the Lost&Found group because the McAfee Agent continues to communicate to the server.

System Tree groups

System Tree groups represent a collection of systems and deciding which systems to group together depends on the unique needs of your network and business.

You can group systems based on machine-type (for example, laptops, servers, or desktops), geography (for example, North America or Europe), political boundaries (for example, Finance or Development), or any other criteria that supports your needs.

Groups can include both systems and other groups (*subgroups*).

Groups have these characteristics:

- They are created by administrators or users with the appropriate permissions.
- They can include both systems and other groups (*subgroups*).
- They are administered by an 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 before 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, inheritance can be broken by applying a new policy at any location of the System Tree. 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 adding the systems.

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 users who must manage the systems.

For example, you might have decentralized network administration in your organization, where different administrators have responsibilities over different parts of the network. For security reasons, you might not have an 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 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.

We recommend evaluating these borders in your network and organization, and whether they must be considered when defining the organization of your System Tree.

Topological borders

NT domains or Active Directory containers define your network. 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 use slower WAN or VPN connections, instead of faster LAN connections. You might want to configure updating and agent-server communication policies differently for remote sites to minimize network traffic over slower connections.

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 might need to organize segments of the System Tree by functionality if different groups require different policies.

A business group might run specific software that requires special security policies. For example, arranging your email Exchange Servers into a group and setting specific exclusions for 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.

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 systems with similar characteristics

You can use tags and tag groups to automate 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, use tag-based sorting criteria to automatically populate groups with the appropriate systems. Plus, to help sort your systems, you can create tag groups nested up to four levels deep, with up to 1,000 tag subgroups in each level. For example, if your systems are organized by geographic location, chassis type (server, workstation, or laptop), system function (web server, SQL, or application server), and user, you might have these tag groups:

Location	Chassis type	Platform	Users	
Los Angeles	Desktop	Windows	General	
	Laptop	Macintosh	Sales	
				Training
		Windows	Accounting	
			Management	
	Servers	Linux	Corporate	
		Windows	Corporate	
SQL		Corporate		
San Francisco	Desktop	Windows	General	
	Laptop	Macintosh	Sales	
				Training
		Windows	Accounting	
			Management	
	Servers	Linux	Corporate	
		Windows	Corporate	
SQL		Corporate		

Active Directory synchronization

If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain parts of the System Tree.

Once defined, the System Tree is updated with any new systems (and subcontainers) in your Active Directory.

Leverage Active Directory integration to perform these system management tasks:

- 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.

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, 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 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

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 to organize your systems, select this setting to prevent other ePolicy Orchestrator 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

For additional flexibility with System Tree management, you can configure the order of a group's subgroups, and 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 McAfee 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 McAfee Agent GUID (only systems whose agents have already called into the server for the first time have a McAfee Agent GUID in the database). If a matching system is found, it is left in its 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 a McAfee Agent GUID (the McAfee 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.



Systems that are added by Active Directory or NT Domain synchronization have System Tree sorting disabled by default, so they are not sorted on the first agent-server communication

- 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.



Subgroups of groups with criteria that doesn't match are not considered. A group must have matching criteria or have no criteria in order for its subgroups to be considered for a system.

- 9 This process continues down through the System Tree until a system is sorted into a group.



If the server setting for System Tree sorting is configured to sort only on the first agent-server communication, a flag is set on the system. The flag means that the system can never be sorted again at agent-server communication unless the server setting is changed to enable sorting on every agent-server communication.

- 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.

Create and populate System Tree groups

Create System Tree groups and populate the groups with systems.



You can also populate groups by dragging selected systems to 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

- [Create groups manually on page 112](#)
Create **System Tree** subgroups. .
- [Manually add systems to an existing group on page 112](#)
Add specific systems to a selected group.
- [Export systems from the System Tree on page 113](#)
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.
- [Import systems from a text file on page 113](#)
Create a text file of systems and groups to import into the System Tree.
- [Sort systems into criteria-based groups on page 114](#)
Configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled, and sorting criteria and the sorting order of groups must be configured.
- [Import Active Directory containers on page 116](#)
Import systems from Active Directory containers directly into your **System Tree** by mapping Active Directory source containers to **System Tree** groups.
- [Import NT domains into an existing group on page 118](#)
Import systems from an NT domain into a group you created manually.
- [Schedule System Tree synchronization on page 119](#)
Schedule a server task that updates the System Tree with changes in the mapped domain or Active Directory container.
- [Manually update a synchronized group with an NT domain on page 120](#)
Update a synchronized group with changes to the associated NT domain.

Create groups manually

Create **System Tree** subgroups. .

For option definitions, click ? in the interface.

Task

- 1 Open the New Subgroups dialog box.
 - a Select **Menu | Systems | System Tree**.
 - b Select a group.
 - c Click **New Subgroups**.



Create more than one subgroup at a time.

- 2 Type a name then click **OK**.

The new group appears in the **System Tree**.

- 3 Repeat as necessary until you are ready to populate the groups with systems. Use one of these processes to add systems to your **System Tree** groups:
 - 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.

Manually add systems to an existing group

Add specific systems to a selected group.

For option definitions, click ? in the interface.

Task

- 1 Open the New Systems page.
 - a Select **Menu | Systems | System Tree**.
 - b Click **New Systems**.
- 2 Select whether to deploy the McAfee 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.
- 4 Specify additional options as needed.

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.
- 5 Click **OK**.

Export systems from the System Tree

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.

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.

Import systems from a text file

Create a text file of systems and groups to import into the System Tree.

Tasks

- [Create a text file of groups and systems on page 113](#)
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.
- [Import systems and groups from a text file on page 114](#)
Import systems or groups of systems into the **System Tree** from a text file you have created and saved.

Create a text file of groups and systems

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.

Define the groups and their systems by typing the group and system names in a text file. Then import that information into ePolicy Orchestrator. For large networks, use network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate 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.

Import systems and groups from a text file

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 Open the New Systems page.
 - a Select **Menu | Systems | System Tree**.
 - b Click **New Systems**.
- 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.

Sort systems into criteria-based groups

Configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled, and sorting criteria and the sorting order of groups must be configured.

Tasks

- [Add sorting criteria to groups on page 115](#)
Sorting criteria for System Tree groups can be based on IP address information or tags.
- [Enable System Tree sorting on the server on page 115](#)
For systems to be sorted, System Tree sorting must be enabled on both the server and the systems.
- [Enable or disable System Tree sorting on systems on page 116](#)
The sorting status of a system determines whether it can be sorted into a criteria-based group.
- [Sort systems manually on page 116](#)
Sort selected systems into groups with criteria-based sorting enabled.

Add sorting criteria to groups

Sorting criteria for System Tree groups 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**.

Enable System Tree sorting on the server

For systems to be sorted, System Tree sorting must be enabled on both the server and the systems.

In the following task, if you 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 sort on each agent-server communication, all enabled systems are sorted at each agent-server communication as long as this option is selected.

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.

Enable or disable 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 systems you want.
- 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 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.

Sort systems manually

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**, then select the group that contains the 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.

Import Active Directory containers

Import systems from Active Directory containers directly into your **System Tree** by mapping Active Directory source containers to **System Tree** groups.

Mapping Active Directory containers to groups allows you to:

- 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.
- Delete systems from the **System Tree** when they are deleted from Active Directory.
- Prevent duplicate entries of systems in the **System Tree** when they exist in other groups.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Group Details**, then select a group in the **System Tree** you want to map an Active Directory container to.



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 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 to create a duplicate entry for systems that exist in another group of the **System Tree**.



If you are using Active Directory synchronization as a starting point for security management, and plan to use **System Tree** management functionality after mapping your systems, do not select this option.

- 6 In the **Active Directory domain** section, 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 the McAfee Agent automatically to new systems. If you do, configure the deployment settings.



McAfee recommends that you do not deploy the McAfee Agent during the initial import if the container is large. Deploying the 3.62-MB McAfee Agent package to many systems at once can cause network traffic issues. Instead, import the container, then deploy the McAfee Agent to groups of systems at a time, rather than all at once. Consider revisiting this page and selecting this option after the initial McAfee Agent deployment, so that the McAfee 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 that is 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.



You can schedule an NT Domain/Active Directory synchronization server task for the first synchronization. This server task is useful if you are deploying agents to new systems on the first synchronization, when bandwidth is a larger concern.

12 When the synchronization is complete, view the results with the **System Tree**.

When the systems are imported, distribute agents to them if you did not select to do so automatically.



Consider setting up a recurring NT Domain/Active Directory synchronization server task to keep your **System Tree** current with any changes to your Active Directory containers.

Import NT domains into an existing group

Import systems from an NT domain into a group you created manually.

You can populate groups automatically by synchronizing entire NT domains with specified groups. This approach is an easy way to add all systems in your network to the System Tree at once as a flat list with no system description.

If the domain is large, you can create subgroups to assist with policy management or 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. The subgroups will inherit the policies set for the top-level group.

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 exist in another group of the **System Tree**.



We don't 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.

- 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 the McAfee Agent automatically to new systems. If you do so, configure the deployment settings.



We recommend that you do not deploy the McAfee Agent during the initial import if the domain is large. Deploying the 3.62-MB McAfee Agent package to many systems at once can 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. Once you have finished deploying the McAfee Agent, consider revisiting this page and selecting this option after the initial agent deployment. That way, the McAfee 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 is complete, 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**.



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.



Consider setting up a recurring NT Domain/Active Directory synchronization server task to keep this group current with new systems in the NT domain.

Schedule System Tree synchronization

Schedule a server task that updates the System Tree with changes in the mapped domain or Active Directory container.

Depending on group synchronization settings, this task automates these actions:

- 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 site or group policies and tasks to new systems.
- Prevents or allows duplicate entries of systems that still exist in the System Tree after you moved them to other locations.



The McAfee Agent can't be deployed to all operating systems in this manner. You might need to distribute the McAfee Agent manually to some systems.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **New Task**.
- 2 On the Description page, name the task and choose whether it is enabled once it is created, then click **Next**.
- 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 groups, click **Select Synchronized Groups** and select specific ones.
- 5 Click **Next** to open the Schedule page.
- 6 Schedule the task, then click **Next**.
- 7 Review the task details, then click **Save**.



In addition to running the task at the scheduled time, you can run this task immediately: on the Server Tasks page next to the task, click **Run**.

Manually update a synchronized group with an NT domain

Update a synchronized group with changes to the associated NT domain.

The update includes the following changes:

- Adds systems currently in the domain.
- Removes systems from your System Tree that are no longer in the domain.
- Removes 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.

Move systems within the System Tree

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.
- 2 Click **Actions | Directory Management | Move Systems**. The Select New Group page appears.
- 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**.

How Transfer Systems works

You can use the Transfer Systems command to move managed systems between registered McAfee ePO servers.

You might need to transfer these managed systems when you are upgrading the server hardware and operating system or if you are upgrading the server hardware and the McAfee ePO software version.

This graphic shows the major processes needed to transfer systems from one McAfee ePO server to another.

To transfer managed systems from one McAfee ePO server to another takes these six processes, shown in the previous figure.

- 1 **Export the agent-server secure communication (ASSC) keys** — From the old McAfee ePO server, use **Menu | Server Settings | Security Keys**.
- 2 **Import the ASSC keys** — From the new McAfee ePO server, use **Menu | Server Settings | Security Keys**.
- 3 **Register the secondary McAfee ePO server** — From the old McAfee ePO server, use **Menu | Configuration | Registered Servers**.
- 4 **Move systems to the secondary McAfee ePO server** — From the old McAfee ePO server, use **Menu | System Tree | Systems tab and Actions | Agent | Transfer Systems**.

- 5 **Confirm the systems arrived** — From the new McAfee ePO server, use **Menu | System Tree | Systems** tab.
- 6 **Confirm the systems moved** — From the old McAfee ePO server, use **Menu | System Tree | Systems** tab.

See also

[Export and import ASSC keys between McAfee ePO servers on page 123](#)

[Register McAfee ePO servers on page 83](#)

[Transfer systems between McAfee ePO servers on page 122](#)

Transfer systems between McAfee ePO servers

You can use Transfer Systems to move managed systems between registered McAfee ePO servers.

Before you begin

Before you can move managed systems between two McAfee ePO servers, for example between an old McAfee ePO server and a new one, these changes are required to both McAfee ePO configurations:



These steps accommodate a two-way transfer. If you prefer to enable only a one-way transfer, you do not need to import the agent-server communication (ASSC) keys from the new McAfee ePO server into the old McAfee ePO server.

- Link the agent-server secure communication keys between the two McAfee ePO servers.
 - 1 Export the ASSC keys from both the servers.
 - 2 Import the ASSC keys from the old server to the new server.
 - 3 Import the ASSC keys from the new server to the old server.
- Register the old and new McAfee ePO servers so that you can transfer the systems back and forth.



Be sure that you enable Transfer Systems and select Automatic sitelist import on the Details page of the Registered Server Builder page.

The steps in this task describe transferring systems from an old McAfee ePO server to a new server.

For option definitions, click ? in the interface.

Task

- 1 On the old McAfee ePO server, click **Menu | Systems | System Tree**, then select the systems you want to transfer.
- 2 Click **Actions | Agent | Transfer Systems**.
- 3 From the Transfer Systems dialog box, select the new McAfee ePO server from the drop-down menu and click **OK**.



Once a managed system has been marked for transfer, two agent-server communication intervals 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 communication intervals depends on your configuration. The default agent-server communication interval is one hour.

See also

[How Transfer Systems works on page 121](#)

[Export and import ASSC keys between McAfee ePO servers on page 123](#)

[Register McAfee ePO servers on page 83](#)

Export and import ASSC keys between McAfee ePO servers

Before you can transfer systems between McAfee ePO servers you must export and import the agent-server secure communication (ASSC) keys between the McAfee ePO servers.

Agent-server secure communication keys are used by the agents to communicate securely with the McAfee ePO server. If you transfer a managed system with an encrypted McAfee Agent to a different McAfee ePO server without importing the associated client keys, the transferred system can't connect to the new McAfee ePO server.



To transfer managed systems in both directions, you must register both servers with each other and export and import both sets of ASSC keys.

If you try to register a McAfee ePO server and you enable the **Transfer Systems** option with Automatic sitelist import, before you export and import the ASSC keys between the McAfee ePO servers, this error message appears:

ERROR: Master agent-server key(s) must be imported into the remote server prior to importing the sitelist. Go to Server Settings to export security keys from this server. Note that visiting this link now will cause you to lose any unsaved changes to this registered server.



You must import both the 1024-bit and 2048-bit ASSC keys from the McAfee ePO server to successfully register and import the Automatic Sitelist.

Use these steps to export and import the ASSC keys from one McAfee ePO server to another.



These steps describe exporting the ASSC keys from an *old* McAfee ePO server to a *new* McAfee ePO server.

Task

For option definitions, click ? in the interface.

- 1 From the old McAfee ePO server, click **Menu | Configuration | Server Settings**, click **Security Keys** from the **Setting Categories** column, then click **Edit**.

To export the two ASSC keys, use these steps:

- a To export the 2,048-bit ASSC key, on the Edit Security Keys page in the Agent-server secure communication keys list, select the 2,048-bit key, click **Export**, then in the Export Agent-Server Secure Communication Key dialog box, click **OK**.
- b Save the .ZIP file to a temporary folder on your local machine.
The default name of the 2,048-bit ASSC key file is sr2048<server-name>.zip, where <server-name> is your McAfee ePO server name. For example, in filename sr2048ePO50_server.zip, "ePO50_server" is the server name.
- c To export the 1,024-bit ASSC key, on the Edit Security Keys page in the Agent-server secure communication keys list, select the 1,024-bit key, click **Export**, in the Export Agent-Server Secure Communication Key dialog box, click **OK**, then save the .ZIP file to the same temporary folder on your local machine.

- 2 From the new McAfee ePO server, click **Menu | Configuration | Server Settings**, click **Security Keys** from the **Setting Categories** column, then click **Edit**.

To import the two ASSC keys, use these steps:

- a In the Edit Security Keys page, next to Import and back up keys group, click **Import**.
- b From the Import Keys page, browse to the location where you saved the 2,048- and 1,024-bit ASSC key .ZIP files exported in step 1.

- c From the **Choose File to Upload** dialog box, select the 2,048-bit ASSC key .ZIP file, you are returned to the Import Keys page, and click **Next**.
 - d Confirm you have selected the correct key, in the Summary page, and click **Save**.
 - e To import the 1,024-bit ASSC key, use steps a through d again.
- 3 From the new McAfee ePO server, confirm both the 1024-bit and 2048-bit ASSC keys appear in the Agent-server secure communication keys list, then click **Save**.

Now both ASSC keys are saved in your new McAfee ePO server, you can successfully register the new McAfee ePO server with your old server, then use Transfer Systems to move your managed systems.

How the Automatic Responses feature interacts with the System Tree

Before you plan the implementation Automatic Responses, understand how this feature works with 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 an 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, an 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

Enable the default ePolicy Orchestrator rules 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.

Table 9-1 Default notification rules

Rule name	Associated events	Configurations
Distributed repository update or replication failed	Distributed repository update or replication failed	Sends a notification message when any update or replication fails.
Malware detected	Any events from any unknown products	Sends a notification message: <ul style="list-style-type: none"> • When the number of events is at least 1,000 within an hour. • At most, once every two hours. • With the source system IP address, actual threat names, and actual product information, if available, and many other parameters. • When the number of selected distinct value is 500.
Master repository update or replication failed	Master repository update or replication failed	Sends a notification message when any update or replication fails.
Non-compliant computer detected	Non-Compliant Computer Detected events	Sends a notification message when any events are received from the Generate Compliance Event server task.

The System Tree

How the Automatic Responses feature interacts with the System Tree

10 Tags

Use tags to identify and sort systems. Tags and tag groups allow you to select groups of systems and simplify the creation of tasks and queries.

Contents

- ▶ *Create tags using the New Tag Builder*
- ▶ *Manage tags*
- ▶ *Create, delete, and modify tag subgroups*
- ▶ *Exclude systems from automatic tagging*
- ▶ *Create a query to list systems based on tags*
- ▶ *Apply tags to selected systems*
- ▶ *Clear tags from systems*
- ▶ *Apply criteria-based tags to all matching systems*
- ▶ *Apply criteria-based tags on a schedule*

Create tags using the New Tag Builder

Use the New Tag Builder to create tags quickly.

Tags can use criteria that is 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.

For option definitions, click ? in the interface.

Task

- 1 Open the **New Tag Builder**: click **Menu** | **Systems** | **Tag Catalog** | **New Tag**.
- 2 On the **Description** page, type a name and meaningful description, then click **Next**. The **Criteria** page appears.
- 3 Select and configure the 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 under the selected tag group in the **Tag Tree** on the **Tag Catalog** page.

Manage tags


Once tags are created using the New Tag Builder, use the Actions list to edit, delete, and move the tags.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Tag Catalog**.
- 2 From the **Tags** list, select a tag or multiple tags, click **Actions** and one of these actions from the list.

Action	Steps
Edit a tag The number of affected systems is listed at the top of the page.	From the Edit Tag Builder : <ol style="list-style-type: none"> 1 On the Description page, type a name and meaningful description, then click Next. The Criteria page appears. 2 Select and configure the criteria, then click Next. The Evaluation page appears. To apply the tag automatically, you must configure criteria for the tag. 3 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 are not excluded from the tag. 4 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 updated on the Tag Catalog page under the selected tag group in the Tag Tree .
Delete a tag	Click Delete . The confirmation dialog box appears. Click OK to delete the tag.

Action	Steps
Export a tag	Click Export Table . The Export Data page appears.
Move tags	<p>From the Move Tags dialog box:</p> <ol style="list-style-type: none"> 1 Select the tag group where you want the tags to appear. 2 Click OK to complete the move. <p> You can also drag and drop the tags into the tag groups in the Tag Tree.</p>

Create, delete, and modify tag subgroups


Tag subgroups allow you to nest tag groups up to four levels deep, with up to 1,000 tag subgroups under a single parent group. These tag groups allow you to use criteria-based sorting to automatically add systems to the correct groups.

Use these steps to create, delete, or modify a tag subgroup.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | Tag Catalog**.
- 2 From the **Tag Catalog** page, select one of these actions.

Action	Steps
Create a tag subgroup	<ol style="list-style-type: none"> 1 In the hierarchical Tag Tree list, select the tag group (or parent tag group) where you want to create the new tag subgroup. <p> My Tags is the default top level tag group added during ePolicy Orchestrator installation.</p> <ol style="list-style-type: none"> 2 Click New Subgroup to see the New Subgroup dialog box. 3 In the Name field, type a descriptive name for the new tag subgroup. 4 When finished, click OK to create the new tag subgroup.
Rename a tag subgroup	<ol style="list-style-type: none"> 1 In the hierarchical Tag Tree list, select the tag subgroup you want to rename. 2 Click Tag Tree Actions Rename Group to see the Rename Subgroup dialog box. 3 In the Name field, type the new name for the tag subgroup. 4 When finished, click OK and the tag subgroup is renamed.
Delete a tag subgroup	<ol style="list-style-type: none"> 1 In the hierarchical Tag Tree list, select the tag subgroup you want to delete. 2 Click Actions Delete and an Action: Delete confirmation dialog box appears. 3 If you are sure you want to delete the tag subgroup, click OK and the tag subgroup is removed.

Exclude systems from automatic tagging

Prevent systems from having specific tags applied.



Alternatively, you can use a query to collect systems, then exclude the tags from those systems from the query results.

For option definitions, click ? in the interface.

Task

- 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 tag group, select the tag to exclude, then click **OK**.



To limit the list to specific tags, type the tag name in the text box under **Tags**.

- 4 Verify the systems have been excluded from the tag:
 - a Open the **Tag Details** page: click **Menu | Systems | Tag Catalog**, then select the tag or tag group in the list of tags.
 - b Next to **Systems with tag**, click the link for the number of systems excluded from the criteria-based tag application. The **Systems Excluded from the Tag** page appears.
 - c Verify the systems are in the list.

Create a query to list systems based on tags

Schedule a query to create a list that displays, applies, or removes tags on systems, based on selected tags.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **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, select one of these queries from the **McAfee Groups** tab, then click **OK**.
 - **Inactive Agents**
 - **Duplicate Systems Names**
 - **Systems with High Sequence Errors**
 - **Systems with no Recent Sequence Errors**
 - **Unmanaged Systems**
- 5 Select the language for displaying the results.

- 6 From the **Sub-Actions** list, select one of these subactions to take based on the results.
 - **Apply Tag** — Applies a selected tag to the systems returned by the query.
 - **Clear Tag** — Removes a selected tag on the systems returned by the query. Select **Clear All** to remove all tags from the systems in the query results.
 - **Exclude Tag** — Excludes systems from the query results if they have the selected tag applied to them.
- 7 From the **Select Tag** window, select a tag group from the **Tag Group Tree** and optionally filter the list of tags using the **Tags** text box.



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 that you want them to be taken on the query results. For example, you can apply the Server tag, then remove the Workstation tag. You can also add other subactions, such as assigning a policy to the systems.

- 8 Click **Next**.
- 9 Schedule the task, then click **Next**.
- 10 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.

Apply tags to selected systems

Apply a tag manually to selected systems in the System Tree.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select the group that contains the systems you want.
- 2 Select the systems, then click **Actions | Tag | Apply Tag**.
- 3 In the **Apply Tag** dialog box, select the tag group, select the tag to apply, then click **OK**.



To limit the list to specific tags, type the tag name in the text box under **Tags**.

- 4 Verify that the tags have been applied:
 - a Click **Menu | Systems | Tag Catalog** select, then select a tag or tag group 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 that the systems are in the list.

Clear tags from systems

Remove tags from selected systems.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the group that contains the systems you want.
- 2 Select the systems, then click **Actions | Tag | Clear Tag**.
- 3 In the **Clear Tag** dialog box, perform one of these steps, then click **OK**.
 - Remove a specific tag — Select the tag group, then select the tag.



To limit the list to specific tags, type the tag name in the text box under **Tags**.

- Remove all tags — Select **Clear All**.
- 4 Verify that the tags have been applied:
 - a Click **Menu | Systems | Tag Catalog** select, then select a tag or tag group 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 that the systems are in the list.

Apply criteria-based tags to all matching systems

Apply a criteria-based tag to all non-excluded systems that match the specified criteria.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | Tag Catalog**, then select a tag or tag group from the **Tags** list.
- 2 Click **Actions | Run Tag Criteria**.
- 3 On the **Action** pane, select whether to reset manually tagged and excluded systems.



Resetting manually tagged and excluded systems 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 that the systems have the tag applied:
 - a Click **Menu | Systems | Tag Catalog**, then select a tag or tag group 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 that the systems are in the list.

The tag is applied to all systems that match its criteria.

Apply criteria-based tags on a schedule

Schedule a regular task that applies a tag to all systems that match the tag criteria.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **New Task**.
- 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 a tag from the **Tag** drop-down list.
- 4 Select whether to reset manually tagged and excluded systems.

Resetting manually tagged and excluded systems does two things:

 - Removes the tag on systems that don't match the criteria
 - Applies the tag to systems that match the criteria but were excluded from receiving the tag
- 5 Click **Next** to open the Schedule page.
- 6 Schedule the task for the times you want, then click **Next**.
- 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.

11

Agent-server communication

Client systems use the McAfee Agent to communicate with your McAfee ePO server. Monitor and manage agents from the ePolicy Orchestrator console.

For version-specific information about your agents, see the *McAfee Agent Product Guide*.

Contents

- ▶ *Working with the agent from the McAfee ePO server*
- ▶ *Managing agent-server communication*

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 system properties, agent properties, and other McAfee product information can be viewed.

Contents

- ▶ *How agent-server communication works*
- ▶ *SuperAgent and how it works*
- ▶ *McAfee Agent relay capability*
- ▶ *Peer-to-Peer communication*
- ▶ *Collect McAfee Agent statistics*
- ▶ *Change the agent user interface and event log language*
- ▶ *Configure selected systems for updating*
- ▶ *Respond to policy events*
- ▶ *Scheduling client tasks*
- ▶ *Run client tasks immediately*
- ▶ *Locate inactive agents*
- ▶ *Windows system and product properties reported by the agent*
- ▶ *Queries provided by the McAfee Agent*

How agent-server communication works

McAfee Agent communicates with the McAfee ePO server periodically to send events and, ensure all settings are up-to-date.

These communications are referred to as *agent-server communication*. During each agent-server communication, McAfee 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 McAfee Agent, and the repository list if it has changed since the last agent-server communication. McAfee Agent enforces the new policies locally on the managed system and applies any task or repository changes.

The McAfee ePO server uses an industry-standard Transport Layer Security (TLS) network protocol for secure network transmissions.

When the McAfee Agent is first installed, it calls in to the server within few seconds. Thereafter, the McAfee Agent calls in whenever one of the following occurs:

- The agent-server communication interval (ASCI) elapses.
- McAfee Agent wake-up calls are sent from the McAfee ePO server or Agent Handlers.
- A scheduled wake-up task runs on the client systems.
- Communication is initiated manually from the managed system (using Agent Status monitor or command line).
- McAfee Agent wake-up calls sent from the McAfee ePO server.

Agent-to-Server Communication Interval

The Agent-to-Server Communication Interval (ASCI) determines how often the McAfee Agent calls into the McAfee ePO server.

The Agent-to-Server Communication Interval is set on the **General** tab of the McAfee Agent policy page. The default setting of 60 minutes means that McAfee Agent contacts the McAfee ePO server once every hour. When deciding whether to modify the interval, consider that McAfee Agent performs each of the following actions at each ASCI:

- Collects and sends its properties.
- Sends non-priority events that have occurred since the last agent-server communication.
- Receives new policies and tasks. This action might trigger other resource-consuming action based on tasks, and or schedules received.
- Enforces policies.

Although these activities do not burden any one computer, a number of factors can cause the cumulative demand on the network or McAfee ePO servers, or on Agent Handlers to be significant, including:

- How many systems are managed by the McAfee ePO server
- If your organization has stringent threat response requirements.
- If the network or physical location of clients in relation to servers or Agent Handlers is highly distributed
- If there is inadequate available bandwidth

In general, if your environment includes these variables, you want to perform agent-server communications less often. For individual clients with critical functions, you might want to set a more frequent interval.

Agent-server communication interruption handling

Interruption handling resolves issues that prevent a system from connecting with a McAfee ePO server.

Communication interruptions can happen for many of reasons, and the Agent-Server connection algorithm is designed to reattempt communication if its first attempt fails.

McAfee Agent tries to establish connection using one of these methods. If all these methods fail, McAfee Agent tries to connect again during the next ASC.

- IP address
- Fully qualified domain name
- NetBIOS name

Wake-up calls and tasks

A McAfee Agent wake-up call triggers an immediate agent-server Communication rather than waiting for the current Agent-Server Communication Interval (ASCI) to elapse.



Use **System Tree** actions to wake-up McAfee Agent on non-Windows operating system.

There are two ways to issue a wake-up call:

- **Manually from the server** — This is the most common approach and requires McAfee Agent wake-up communication port be open.
- **On a schedule set by the administrator** — This approach is useful when manual agent-server communication is disabled by policy. The administrator can create and deploy a wake-up *task*, which wakes up McAfee Agent and initiates agent-server Communication.

Some reasons for issuing a wake-up call are:

- You make a policy change that you want to enforce immediately, without waiting for the scheduled ASCI to expire.
- You created a new task that you want to run immediately. The **Run Task Now** option creates a task, then assigns it to specified client systems and sends wake-up calls.
- 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 have converted a particular McAfee Agent to a **SuperAgent**, it can issue wake-up calls to designated network broadcast segments. **SuperAgent** distributes the bandwidth impact of the wake-up call.

Send manual wake-up calls to individual 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 to send or receive updated information before the next agent to 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 Systems** section.
- 4 Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call** as appropriate.
- 5 Accept the default **Randomization** (0 minutes) or type a different value (0 - 60 minutes). Consider the number of systems that are receiving the wake-up call when it is sent immediately, and how much bandwidth is available. If you type 0, agents respond immediately.
- 6 To send incremental 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 Select whether to wake-up agent using **All Agent Handlers** or **Last Connected Agent Handlers**.
- 10 Click **OK** to send the agent or SuperAgent wake-up call.

Send 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 to send or receive the updated information before the next agent to 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 minutes), or type a different value (0 - 60 minutes). If you type 0, agents awaken immediately.
- 8 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.
- 9 To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.
- 10 Click **OK** to send the agent or SuperAgent wake-up call.

SuperAgent and how it works

A SuperAgent is a distributed repository whose content replication is managed by the McAfee ePO server.

The SuperAgent caches information received from an McAfee ePO server, the Master Repository, a HTTP, or a FTP repository, and distributes it to the agents in its broadcast domain. It is recommended to configure a **SuperAgent** in every broadcast domain when managing agents in larger networks.

The Lazy Caching feature allows SuperAgent to retrieve data from the McAfee ePO servers only when requested by a local agent node. Creating a hierarchy of SuperAgent along with lazy caching further saves bandwidth and minimizes the load on the McAfee ePO server. To activate this, turn on **LazyCaching** in the **McAfee Agent | SuperAgent** policy options page, which you access from **Menu | Policy | Policy Catalog**.

A SuperAgent also broadcasts wake-up calls to other agents located on the same network subnet. The SuperAgent receives a wake-up call from the McAfee ePO server, then wakes up the agents in its subnet.



This is an alternative to sending ordinary agent wake-up calls to each agent in the network or sending agent wake-up task to each computer.

SuperAgent and broadcast wake-up calls

Use wake-up calls to initiate agent-server communication, consider converting McAfee Agent on each broadcast domain into a **SuperAgent**.

SuperAgent distributes the bandwidth load of concurrent wake-up calls. Instead of sending wake-up calls from the server to every McAfee 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 McAfee Agent in the same broadcast domain.
- 3 All notified McAfee Agent (McAfee Agent notified by a **SuperAgent** and all **SuperAgents**) exchange data with the McAfee ePO server or Agent Handler.

When you send a **SuperAgent** wake-up call, McAfee Agent without an operating **SuperAgent** on their broadcast domain are not prompted to communicate with the server.

SuperAgent deployment tips

To deploy enough **SuperAgents** to the appropriate locations, first determine the broadcast domains in your environment and select a system (preferably a server) in each domain to host a **SuperAgent**. If you use **SuperAgents**, make sure every McAfee Agent is assigned a **SuperAgent**.

McAfee 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:

- McAfee Agent wake-up communication port (8081 by default).
- McAfee Agent broadcast communication port (8082 by default).


Convert McAfee Agent to SuperAgent

During the global updating process, when the **SuperAgent** receives an update from the McAfee ePO server, it sends wake-up calls to all McAfee Agent in its network. Configure **SuperAgent** policy settings to convert McAfee Agent to **SuperAgent**.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group under System Tree. All the systems within this group appear in the details pane.
- 2 Select a system, then click **Actions | Agent | Modify Policies on a Single System**. The Policy Assignment page for that system appears.
- 3 From the product drop-down list, select **McAfee Agent**. The policy categories under **McAfee Agent** are listed with the system's assigned policy.
- 4 If the policy is inherited, select **Break inheritance and assign the policy and settings below**.
- 5 From the **Assigned policy** drop-down list, select a **General** policy.



From this location, you can edit the selected policy, or create a policy.
- 6 Select whether to lock policy inheritance to prevent any systems that inherit this policy from having another one assigned in its place.
- 7 On the **SuperAgent** tab, select **Convert agents to SuperAgents** to enable broadcast of wake-up calls.

- 8 Click **Save**.
- 9 Send an agent wake-up call.

SuperAgent caching and communication interruptions

The SuperAgent caches the contents of its repository in a specific manner designed to minimize the load on the McAfee ePO server.

If an agent has been converted to a SuperAgent, it can cache content from the McAfee ePO server, the distributed repository, or other SuperAgent to distribute locally to other agents, reducing load on the McAfee ePO server.



- SuperAgent caching in conjunction with repository replication is not recommended.
- The SuperAgent cannot cache content from McAfee HTTP or FTP repositories.

How the cache works

When a client system first requests content, the SuperAgent assigned to that system downloads the requested content from its configured repositories and caches that content. The cache is updated whenever a newer version of the requested package is available in the Master Repository. When a hierarchical structure of SuperAgent is created, the child SuperAgent receives the requested the content update from its parent's cache.

The SuperAgent is guaranteed only to store content required by the agents assigned to it because it does not pull any content from the repositories until requested from a client. This minimizes traffic between the SuperAgent and the repositories. While the SuperAgent is retrieving content from the repository, client system requests for that content are paused.



The SuperAgent must have access to the repository. Without this access, agents receiving updates from the SuperAgent never receive new content. Make sure that your SuperAgent policy includes access to the repository.

Agents configured to use the SuperAgent as their repository receive the content cached in the SuperAgent 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 lazy cache content is purged

You can configure the SuperAgent to purge cache content that are not in use. The cache content is downloaded when a client system requests for an update. The previous content update files may still be available in the local disk but may not be listed in the `Replica.log` file. If a file is not listed in `Replica.log` it is purged because it will not be requested by any client system.



The `Replica.log` file contains information about files and folder in its respective directory. Every directory in the repository contains a `Replica.log` file.

By default the cache content is purged every day. You can configure the purging interval using the SuperAgent policy.

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 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.



- Do not use SuperAgent caching with global updating. Both of these features serve the same function in your managed environment; keeping your distributed repositories up-to-date. However, they are not complementary features. Use SuperAgent caching when limiting bandwidth usage is your primary consideration. Use Global Updating when quick enterprise updating is your primary consideration. See ePO product documentation for more details on Global Updating.
- SuperAgent caching in conjunction with repository replication is not recommended.

SuperAgent hierarchy

A hierarchy of SuperAgents can serve agents in the same network with minimum network traffic utilization.

A SuperAgent caches the content updates from the McAfee ePO server or distributed repository and distributes it to the agents in the network reducing the load on the McAfee ePO server. It is always ideal to have more than one SuperAgent to balance the network load.



Ensure that you enable **Lazy caching** before you set the SuperAgent hierarchy.

Creating a hierarchy of SuperAgents

Use the Repository policy to create the hierarchy. McAfee recommends that you create a three level hierarchy of SuperAgents in your network.

Creating a hierarchy of SuperAgents avoids repetitive download of the content update from the McAfee ePO server or distributed repository. For example, in a client network with multiple SuperAgents (SuperAgent 1, SuperAgent 2, SuperAgent 3, and SuperAgent 4) and a distributed repository, configure the hierarchy in such a way that the client systems receives the content updates from their respective SuperAgents (SuperAgent 2, SuperAgent 3, or SuperAgent 4). The SuperAgent 2, 3, and 4 receive and cache updates from SuperAgent 1, and the SuperAgent 1 receives and caches updates from the distributed repository.



- In the above example, SuperAgent 2, SuperAgent 3, and SuperAgent 4 are configured as SuperAgents for the client systems in their respective broadcast domain.
- The SuperAgents cannot cache content from McAfee HTTP or FTP repositories.

When creating a hierarchy, ensure that the hierarchy doesn't form a cycle of SuperAgent; for example SuperAgent 1 is configured to pull updates from SuperAgent 2, SuperAgent 2 is configured to pull updates from SuperAgent 3, and SuperAgent 3 in turn is configured to pull updates from SuperAgent 1.

To ensure that the parent SuperAgent is up-to-date with the latest content update, SuperAgent wake-up calls broadcast must be enabled.



If the SuperAgents don't serve agents with latest content update, agent falls back to the next repository configured in the policy.

Arrange SuperAgents in a hierarchy

General and Repository policies can be modified to enable and set SuperAgent hierarchy. For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Policy Catalog**, then from the **Product** drop-down menu, select **McAfee Agent**, and from the **Category** drop-down menu, select **General**.
- 2 Click the **My Default** policy to start editing the policy. To create a policy, click **Actions | New Policy**.
The **McAfee Default** policy cannot be modified.
- 3 On the **SuperAgent** tab, select **Convert agents to SuperAgents** to convert the agent to a **SuperAgent** and update its repository with latest content.
- 4 Select **Use systems running SuperAgents as distributed repository** to use the systems that host SuperAgents as update repositories for the systems in its broadcast segment then provide the **Repository Path**.
- 5 Select **Enable Lazy caching** to allow SuperAgents to cache content when it is received from the McAfee ePO server.
- 6 Click **Save**.
The **Policy Catalog** page lists the **General** policies.
- 7 Change the **Category** to **Repository**, then click the **My Default** policy to start editing the policy. If you want to create policy, click **Actions | New Policy**.
- 8 On the **Repositories** tab, select **Use order in repository list**.
- 9 Click **Automatically allow clients to access newly-added repositories** to add new SuperAgent repositories to the list, then click **Move to Top** to arrange the SuperAgents in a hierarchy.



Arrange the hierarchy of the repositories in such a way that the parent SuperAgent is always at the top of the repository list.

- 10 Click **Save**.
After setting the SuperAgent hierarchy you can create and run the McAfee Agent Statistics task to collect a report of network bandwidth saving.

McAfee Agent relay capability

If your network configuration blocks communication between the McAfee Agent and the McAfee ePO server, McAfee Agent can't receive content updates, policies, or send events.

Relay capability can be enabled on McAfee Agent that have direct connectivity to the McAfee ePO server or Agent Handler to bridge communication between the client systems and the McAfee ePO server. You can configure more than one McAfee Agent as a RelayServer to maintain network load balance.

Communicating through a RelayServer

Enabling relay capability in your network converts a McAfee Agent to a RelayServer. A McAfee Agent with relay capability can access the McAfee ePO server or **RelayServer** listed in `SiteList.xml`.

When a McAfee Agent fails to connect to the McAfee ePO server, it broadcasts a message to discover any McAfee Agent with relay capability in its network. Each RelayServer responds to the message and the McAfee Agent establishes a connection with the first RelayServer to respond.

Later, if a McAfee Agent fails to connect to the McAfee ePO server, it tries to connect to the RelayServer that first responded to the discovery message. McAfee Agent discovers each RelayServer in the network at every agent-server communication, and caches the details of the first five unique servers that responded to the discovery message. If the current RelayServer fails to connect with the McAfee ePO server or doesn't have the required content update, McAfee Agent connects to the next RelayServer available in its cache. Enable the policy option **Enable Relay Communication** to allow the client system to discover the relay servers.

When McAfee Agent uses relay to communicate with the McAfee ePO server, the connections are established on two parts; first between McAfee Agent and the RelayServer and, second between RelayServer and the McAfee ePO server. These connections are maintained till the duration of the communication.

Enable relay capability

Configure and assign policies to enable the relay capability on an agent.



If enabling a non-Windows system as a RelayServer, ensure that you manually add an exception for the `macmnsvc` process and the service manager port to the `iptables` and `ip6tables`.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group under System Tree. All the systems within this group appear in the details pane.
- 2 Select a system, then click **Actions | Agent | Modify Policies on a Single System**. The Policy Assignment page for that system appears.
- 3 From the product drop-down list, select **McAfee Agent**. The policy categories under McAfee Agent are listed with the system's assigned policy.
- 4 If the policy is inherited, select **Break inheritance and assign the policy and settings below**.
- 5 From the **Assigned policy** drop-down list, select a **General** policy.



From this location, you can edit the selected policy, or create a policy.

- 6 Select whether to lock policy inheritance to prevent any systems that inherit this policy from having another one assigned in its place.
- 7 On the SuperAgent tab, select these options as appropriate
 - Select **Enable Relay Communication** to allow agents to discover relay servers in the network.
 - Select **Enable RelayServer** to enable relay capability on an agent.



- Ensure that you configure the **Service Manager port to 8082**.
- McAfee recommends that you enable relay capability within the organization's network.
- A RelayServer cannot connect to the McAfee ePO servers using proxy settings.

- 8 Click **Save**.

9 Send a McAfee Agent wake-up call.



- After the first ASCII the status of the RelayServer is updated in the McAfee Agent Properties page or the McTray UI on the client system.
- The log file `Macmnsvc_<hostname>.log` is saved in these locations.
 - On a Windows client system — `<ProgramData>\McAfee\Agent\Logs`
 - On a non-Windows client system — `/var/McAfee/agent/logs`

Disable relay capability

You can use the **General** policy to disable the relay capability on the McAfee Agent.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group under the **System Tree**. All the systems within this group appear in the details pane.
- 2 Select the system on which the relay capability was enabled, then click **Actions | Agent | Modify Policies on a Single System**. The **Policy Assignment** page for that system appears.
- 3 From the product drop-down list, select **McAfee Agent**. The policy categories under **McAfee Agent** are listed with the system's assigned policy.
- 4 From the **Assigned policy** drop-down list, select the **General** policy enforced on the client system and disable the policy.
- 5 On the **SuperAgent** tab, deselect these options as appropriate
 - Deselect **Enable Relay Communication** to stop agents from discovering the **RelayServers** in the network.
 - Deselect **Enable RelayServer** to disable the relay capability on McAfee Agent.
- 6 Click **Save**.
- 7 Send a McAfee Agent wake-up call.

Peer-to-Peer communication

To retrieve updates and install products the McAfee Agent must communicate with the McAfee ePO server. These updates might be available with the agents in the same broadcast domain. Downloading these updates from the peer agents in the same broadcast domain reduces load on McAfee ePO.

Downloading content update from peer agents

You can enable the peer-to-peer communication on a McAfee Agent using the General policy.

A McAfee Agent can be configured as peer-to-peer server and/or client as required using the policy. Configuring a McAfee Agent as a peer-to-peer server enables it to provide updates to others in the broadcast domain when requested. A peer-to-peer server has local disk space allocated to cache updates. The default disk space is 512 MB, but this can be configured using policy. The peer-to-peer server by default caches updates in `<agent data folder>\data\mcafeeP2P`, but this can be customized using policy. You can also configure the policy to purge the updates cached in the local disk.

When an agent requires a content update, it tries to discover peer-to-peer servers with the content update in its broadcast domain. On receiving the request, the agents configured as peer-to-peer servers check if they have the requested content and respond back to the agent. The agent requesting the content, downloads it from the peer-to-peer server that responded first.



Enable the policy option **Enable Peer-to-Peer Communication** to allow the client system to discover the peer-to-peer servers in the broadcast domain.

The peer-to-peer server uses HTTP to serve content to clients.

If a McAfee Agent can't find the content update among its peers in the broadcast domain, it falls back to the repository, as configured in the policy.

The peer-to-peer communication uses port 8082 to discover peer servers and port 8081 to serve peer agents with updates.

Best practices for using Peer-to-Peer communication

Consider these recommendations when enabling peer-to-peer communication in your network.

- We recommend that you enable peer-to-peer servers on PCs or virtual systems. Enabling peer-to-peer server on laptops or other mobile devices is not recommended.
- We recommend that you disable peer-to-peer servers on the systems that have poor network connectivity or are connected using VPN.
- When deploying McAfee Agent or managed products, or updating the products on large number of systems, we recommend that you enable peer-to-peer server on all systems. This limits the network traffic within the local subnet during the deployment or update.
- Peer-to-Peer communication is enabled by default. If your organization restricts peer-to-peer communication, disable the Peer-to-Peer policy.
- We recommend that you configure the **Max disk quota** always greater than the size of sum of commonly used application and updates (For example, if the DAT file size is 150MB and the average product update size is 100MB, the peer-to-peer disk quota should be more than 250MB).

Enable Peer-to-Peer service

Enable peer to peer service in your broadcast domain to reduce load on the McAfee ePO server.



Peer to peer service is enabled by default.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group under System Tree. All the systems within this group appear in the details pane.
- 2 Select a system, then click **Actions | Agent | Modify Policies on a Single System**. The Policy Assignment page for that system appears.
- 3 From the product drop-down list, select **McAfee Agent**. The policy categories under McAfee Agent are listed with the system's assigned policy.
- 4 If the policy is inherited, select **Break inheritance and assign the policy and settings below**.
- 5 From the **Assigned policy** drop-down list, select a **General** policy.



From this location, you can edit the selected policy, or create a policy.

- 6 Select whether to lock policy inheritance to prevent any systems that inherit this policy from having another one assigned in its place.
- 7 On the **Peer-to-Peer** tab, select these options as appropriate
 - Select **Enable Peer-to-Peer Communication** to allow McAfee Agent to discover and use Peer-to-Peer servers in the network.
 - Select **Enable Peer-to-Peer Serving** to enable McAfee Agent to serve content to peer agents.
- 8 Click **Save**.
- 9 Send a McAfee Agent wake-up call.

Collect McAfee Agent statistics

Run the McAfee Agent Statistics client task on the managed nodes to collect **RelayServer** statistics and network bandwidth saved by **Peer-to-Peer** communication and **SuperAgent** hierarchy. For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group under the **System Tree**. All systems within this group appear in the details pane.
- 2 Select a system, then click **Actions | Agent | Modify Tasks on a Single System**. The client tasks assigned for that system appear.
- 3 Click **Actions | New Client Task Assignment**.
- 4 From the product list, select **McAfee Agent**, then select **McAfee Agent Statistics** as the **Task Type**.
- 5 Click **Create New task**. The new client task page appears.
- 6 Select the required option, then click **Save**.



Once the task is deployed on the client system and the status is reported to ePolicy Orchestrator, the statistics are reset to 0.

To see the statistics collected by McAfee Agent, create and run a new **Agent Statistics Information** query.

Change the agent user interface and event log language

When managed systems run in a different language than your administration staff can read, it can be difficult to troubleshoot issues on those systems.

You can change the agent user interface and logging language on a managed system through an ePolicy Orchestrator policy. This setting forces the agent on the target system to run and publish log entries in the selected language.



Some text is controlled by individual McAfee security software products (for example, VirusScan) and will follow the regional/locale settings.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Policy Catalog**.
- 2 Select **McAfee Agent** from the **Product** drop-down list, and **Troubleshooting** in the **Category** drop-down list.
- 3 Click the name of a policy to modify, or duplicate an existing policy.
The **McAfee Default** policy can't be modified.

- 4 Select **Select language used by agent** and select a language from the drop-down list.
- 5 Click **Save**.

When you assign this policy to a system, the agent on that system runs and publishes log messages in the selected language. If this language does not match the current Windows system locale, the log messages appearing in the **Agent Monitor** user interface might not be legible.



Regardless of language selection, some log messages are always published in English to aid McAfee in troubleshooting customer issues.

Configure selected systems for updating

You can choose a set of packages that are updated immediately when **Update Now** is selected on one or more systems from ePolicy Orchestrator server.

Typical reasons for using this functionality include:

- Updating selected systems when troubleshooting
- Distributing new DATs or signatures to a large number of systems, or all systems, immediately
- Updating selected products, patches, or service packs that have been deployed previously

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then select the systems to be updated.
- 2 Click **Actions | Agent | Update Now**.
 - Select **All packages** to deploy all update packages in the repository.
 - Select **Selected packages** to specify which update packages to deploy. Deselect the packages that you do not want to deploy.



The ability to deploy patches and service packs from the Evaluation or Previous repositories is designed to allow update testing on a limited subset of systems before doing a broader deployment. McAfee recommends moving approved patches and service packs to the Current repository when they are ready for general deployment.

- 3 Click **OK**.

Respond to policy events

Set up an automatic response in McAfee ePO that is filtered to see only policy events.



See ePO product documentation for more details on **Automatic Responses**.

For option definitions, click ? in the interface.

Task

- 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**, **Threat**, or **Server** for the **Event type**.
- 5 Click **Enabled** to enable the response and then click **Next**.
- 6 From **Available Properties**, select **Event Description**.

- 7 Click ... in the **Event Description** row and choose one of the following options:
 - **Agent failed to collect properties for any point products** — This event is generated and forwarded when a property collection failure first occurs. A subsequent success event is not generated. Each failing managed product generates a separate event.
 - **Agent failed to enforce policy for any point products** — This event is generated and forwarded when a policy enforcement failure first occurs. A subsequent success event is not generated. Each failing managed product generates a separate event.
- 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 a behavior depending on the action type, then click **Next**.
- 11 Review the summarized response behavior. If correct, click **Save**.

The automatic response performs the described action when a policy event occurs.

Scheduling client tasks

When assigning a client task to a system or group of systems in the System Tree, you can schedule to run them based on various parameters.

On the Schedule tab in the Client Task Assignment Builder, you can configure whether the task should run according to its schedule. If scheduling is disabled, the task can only be run from the **System Tree | Systems** page by clicking **Actions | Agent | Agent | Run Client Task Now** or as a Server Task action.

Client tasks can be scheduled to run at these time intervals:

- **Daily** — Specifies that the task runs every day, at a specific time, on a recurring basis between two times of the day, or a combination of both.
- **Weekly** — Specifies that the task runs on a weekly basis. Such a task can be scheduled to run on a specific weekday, all weekdays, weekends, or a combination of them. You can schedule such a task to run at a specific time of the selected days, or on a recurring basis between two times of the selected days.
- **Monthly** — Specifies that the task runs on a monthly basis. Such a task can be scheduled to run on one or more specific days of each month at a specific time.
- **Once** — Starts the task on the time and date you specify.
- **At System Startup** — Starts the task the next time you start the server.
- **At logon** — Starts the task the next time you log on to the server.
- **Run immediately** — Starts the task immediately.



After the task is run the first time, it is not run again.

Additionally you can:

- Configure the start and end date on which the client task is available or unavailable to run at the scheduled intervals.
- Specify the time at which the task should begin.
- Specify whether to run the task only once at the Start time, or to continue running until a later time. You can also specify the interval at which the task runs during this interval.

- Specify whether the task should run at the local time on the managed system or Coordinated Universal Time (UTC).
- Configure how the task should behave and the action that should be taken if the task runs too long, or whether the task should run if it was missed.

See ePolicy Orchestrator product documentation for details on assigning and scheduling a client task.

Run client tasks immediately

When the McAfee ePO server communicates with the McAfee Agent, you can run client tasks immediately using the **Run Client Task Now** action.

McAfee Agent 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 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 from the client after it finishes.

For option definitions, click ? in the interface.

Task

- 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** as **McAfee Agent** 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 because 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 Task Log**.

Locate inactive agents

An inactive McAfee 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 McAfee 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 **Agent Management** 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 30 days. You can duplicate this default query and modify it to 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 take various actions on the systems identified, including ping, delete, wake up, and redeploy McAfee Agent.

Windows system and product properties reported by the agent

The McAfee Agent reports system properties 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 GUID	Is 64 Bit OS	Server Key
CPU Serial Number	Is Laptop	Sequence Errors
CPU Speed (MHz)	Last Sequence Error	Subnet Address
CPU Type	Last Communication	Subnet Mask
Custom Props 1-4	LDAP Location	System Description
Communication Type	MAC Address	System Location
Default Language	Managed State	System Name
Description	Management Type	System Tree Sorting
DNS Name	Number Of CPUs	Tags
Domain Name	Operating System	Time Zone
Excluded Tags	OS Build Number	To Be Transferred
Free Disk Space	OS OEM Identifier	Total Disk Space
Free Memory	OS Platform	Total Physical Memory
Free System Drive Space	OS Service Pack Version	Used Disk Space
Installed Products	OS Type	User Name
IP Address	OS Version	Vdi
IPX Address		

Agent 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 GUID	Installed Path
Agent-Server Secure Communication Key Hash	IsLazyCachingEnabled
Agent-to-Server Communication Interval	Language
Agent Wake-Up Call	Last Policy Enforcement Status
Agent Wake-Up Communication Port	Last Property Collection Status
Cluster Node	License Status
Cluster Service State	Peer-to-Peer
Cluster Name	Peer-to-Peer Repository Directory
Cluster Host	Prompt User When a Reboot is Required
Cluster Member Nodes	Policy Enforcement Interval
Cluster Quorum Resource Path	Product Version
Cluster IP Address	Plugin Version
DAT Version	Run Now Supported
Engine Version	Service Pack
Force Automatic Reboot After	Show McAfee Tray Icon
Hotfix/Patch Version	RelayServer
	SuperAgent Functionality
	SuperAgent Repository
	SuperAgent Lazychache
	SuperAgent Repository Directory
	SuperAgent Wake-Up Communication Port

View McAfee Agent and product properties

A common troubleshooting task is to verify that the policy changes you made match the properties retrieved from a system.

For option definitions, click ? in the interface.

Task

- 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 appears. The top of the System Information page contains Summary, Properties, and Threat Events windows. It also displays System Properties, Products, Threat Events, and McAfee Agent tabs.

Queries provided by the McAfee Agent

The McAfee ePO server provides a number of standard queries related to the McAfee Agent. The following queries are installed into the Agent Management shared group.

Table 11-1 Queries provided by McAfee Agent

Query	Description
Agent Communication Summary	A pie chart of managed systems indicating whether each McAfee Agent has communicated with the McAfee ePO server within the past day.
Agent Handler Status	A pie chart displaying Agent Handler communication status within the last hour.
Agent Statistics information	A bar chart displaying these McAfee Agent statistics: <ul style="list-style-type: none"> • Number of failed connections to the RelayServers • Number of attempts made to connect to the RelayServer after the maximum allowed connections • Network bandwidth saved by use of SuperAgent hierarchy
Agent Versions Summary	A pie chart of installed agents by version number on managed systems.
Inactive Agents	A table listing all managed systems whose agents have not communicated within the last month.
Repositories and Percentage Utilization	A pie chart displaying individual repository utilization as a percentage of all repositories.
Repository Usage Based on DAT and Engine Pulling	A stacked bar chart displaying DAT and Engine pulling per repository.
Systems per Agent Handler	A pie chart displaying the number of managed systems per Agent Handler.

Managing agent-server communication

Modify ePolicy Orchestrator settings to adapt agent-server communication to the needs of your environment.

Allow agent deployment credentials to be cached

Administrators must provide credentials to successfully deploy agents from your McAfee ePO 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.

For option definitions, click ? in the interface.

Task

- 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.

Change agent communication ports

You can change some of the ports used for agent communication on your McAfee ePO 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

For option definitions, click ? in the interface.

Task

- 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-server communications, type the ports to be used for agent wake-up calls and agent broadcasts, then click **Save**.

12 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*
- ▶ *Other repository public keys*
- ▶ *Manage repository keys*
- ▶ *Agent-server secure communication (ASSC) keys*
- ▶ *Backup and restore keys*

Security keys and how they work

The McAfee ePO 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 server'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.
- When you upgrade, existing keys are migrated to your McAfee ePO 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 repository package contents.
- 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 McAfee 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. Doing so ensures 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.

Manage repository keys

You can manage repository keys using these tasks.

Tasks

- [Use one master repository key pair for all servers on page 157](#)
You can ensure that all McAfee ePO servers and agents use the same master repository key pair in a multi-server environment using **Server Settings**.
- [Use master repository keys in multi-server environments on page 157](#)
Make sure that agents can use content originating from any McAfee ePO server in your environment using **Server Settings**.

Use one master repository key pair for all servers

You can ensure that all McAfee ePO servers and agents use the same master repository key pair in a multi-server environment using **Server Settings**.

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**.
- 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**.
- 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.

Use master repository keys in multi-server environments

Make sure that agents can use content originating from any McAfee ePO server in your environment using **Server Settings**.

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 make sure that agents recognize the content as valid.

You can do this in two ways:

- Use the same master repository key pair for all servers and agents.
- Make sure agents are configured to recognize any repository public key that is used in your environment.

This task 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**.
- 2 Next to **Local master repository key pair**, click **Export Key Pair**, then click **OK**.
- 3 In the **File Download** dialog box, click **Save**.
- 4 Browse to a location on the target McAfee ePO server to save the zip file. Change the name of the file if needed, then click **Save**.
- 5 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**.
- 6 On the **Edit Security Keys** page:
 - a Next to **Import and back up keys**, click **Import**.
 - b Next to **Select file**, browse to and select the master key pair file you saved, then click **Next**.
 - c If the summary information appears correct, click **Save**. The new master key pair appears in the list next to **Agent-server secure communication keys**.
- 7 From the list, select the file you imported in the previous steps, then click **Make Master**. This changes the existing master key pair to the new key pair you just imported.
- 8 Click **Save** to complete the process.

Agent-server secure communication (ASSC) keys

Agents use ASSC keys 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.



Make sure to wait until all agents have updated to the new master before deleting older keys.



Windows agents older than version 4.0 are not supported.

Manage ASSC keys



Generate, export, import, or delete agent-server secure communication (ASSC) keys from the Server Settings page.



Task

For option definitions, click ? in the interface.

- 1 Open the Edit Security Keys page.
 - a Click **Menu | Configuration | Server Settings**.
 - b From the **Setting Categories** list, select **Security Keys**.

2 Select one of these actions.

Action	Steps
Generate and use new ASSC key pairs	<p>1 Next to the Agent-server secure communication keys list, click New Key. In the dialog box, type the name of the security key.</p> <p>2 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 McAfee Agent update task is complete.</p> <p>Make sure that there is an Agent Key Updater package for each version of the McAfee Agent managed by McAfee ePO.</p> <div data-bbox="553 548 1523 653" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  In large installations, only generate and use new master key pairs when you have specific reason to do so. We recommend performing this procedure in phases so that you can more closely monitor progress. </div> <p>3 After all agents have stopped using the old key, delete it.</p> <p>In the list of keys, the number of agents currently using that key is displayed to the right of every key.</p> <p>4 Back up all keys.</p>
Export ASSC keys	<p>Export ASSC keys from one McAfee ePO server to a different McAfee ePO server, to allow agents to access the new McAfee ePO server.</p> <p>1 In the Agent-server secure communication keys list, select a key, then click Export.</p> <p>2 Click OK.</p> <p>Your browser prompts you to download the <code>sr<ServerName>.zip</code> file to the specified location.</p> <div data-bbox="553 1062 1523 1140" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  If you specified a default location for all browser downloads, this file might be automatically saved to that location. </div>
Import ASSC keys	<p>Import ASSC keys that were exported from a different McAfee ePO server, allowing agents from that server to access this McAfee ePO server.</p> <p>1 Click Import.</p> <p>2 Browse to and select the key from the location where you saved it (by default, on the desktop), then click Open.</p> <p>3 Click Next and review the information on the Import Keys page.</p> <p>4 Click Save.</p>

Action	Steps
Designate an ASSC key pair as the master	<p>Change which key pair is specified as the master. Specify a master key pair after importing or generating a new key pair.</p> <ol style="list-style-type: none"> 1 From the Agent-server secure communication keys list, select a key, then click Make Master. 2 Create an update task for the agents to run immediately, so that agents update after the next agent-server communication. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Make sure that the Agent Key Updater package is checked in to the ePolicy Orchestrator Master Repository. Agents begin using the new key pair after the next update task for the McAfee Agent is complete. At any time, you can see which agents are using any of the ASSC key pairs in the list. </div> <ol style="list-style-type: none"> 3 Back up all keys.
Delete ASSC keys	<div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Do not delete any keys that are being used by any agents. If you do, those agents cannot communicate with the McAfee ePO server. </div> <ol style="list-style-type: none"> 1 From the Agent-server secure communication keys list, select the key that you want to remove, then click Delete. 2 Click OK to delete the key pair from this server.

View systems that use an ASSC key pair

You can view the systems whose agents use a specific agent-server secure communication key pair 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**.
- 2 In the **Agent-server secure communication keys** list, select a key, then click **View Agents**.

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

Use the same ASSC key pair for all servers and agents

Verify that all McAfee ePO servers and agents use the same agent-server secure communication (ASSC) key pair.



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.

Task

- 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.

Use a different ASSC key pair for each McAfee ePO server

You can use a different ASSC key pair for each McAfee ePO server to ensure that all agents can communicate with the required McAfee ePO servers in an environment where each 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.

Backup and restore keys

Periodically back up all security keys, and always create a backup before changing 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.

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 Select one of these actions.

Action	Steps
Back up all security keys.	<ol style="list-style-type: none"> 1 Click Back Up All near the bottom of the page. The Backup Keystore dialog box appears. 2 You can optionally enter a password to encrypt the Keystore .zip file or click OK to save the files as unencrypted text. 3 From the File Download dialog box, click Save to create a .zip file of all security keys. The Save As dialog box appears. 4 Browse to a secure network location to store the .zip file, then click Save.
Restore security keys.	<ol style="list-style-type: none"> 1 Click Restore All near the bottom of the page. The Restore Security Keys page appears. 2 Browse to the .zip file containing the security keys, select it, and click Next. The Restore Security Keys wizard opens to the Summary page. 3 Browse to the keys you want to replace your existing key with, then click Next. 4 Click Restore. The Edit Security Keys page reappears. 5 Browse to a secure network location to store the .zip file, then click Save.
Restore security keys from a backup file.	<ol style="list-style-type: none"> 1 Click Restore All near the bottom of the page. The Restore Security Keys page appears. 2 Browse to the .zip file containing the security keys, select it, and click Next. The Restore Security Keys wizard opens to the Summary page. 3 Browse to and select the backup .zip file, then click Next. 4 Click Restore All at the bottom of the page. The Restore Security Keys wizard opens. 5 Browse to and select the backup .zip file, then click Next. 6 Verify that the keys in this file are the ones you want to overwrite your existing keys, then click Restore All.

13 Software Manager

Use the Software Manager to review and acquire McAfee software and software components.

Contents

- ▶ *What's in the Software Manager*
- ▶ *Check in, update, and remove software using the Software Manager*
- ▶ *Checking product compatibility*

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 from 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.

Check in, update, and remove software using the Software Manager

From the Software Manager, you can check in, update, and remove 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.

For option definitions, click ? in the interface.

Task

- 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 the McAfee ePO server.
 - **Checked in Software** — Displays all software (both **Licensed** and **Evaluation**) installed or checked into this server.

If you recently added the license for a product and it appears as **Evaluation**, click **Refresh** to update the Licensed count and display the product as **Licensed** under **Checked In Software**.
 - **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.

Checking product compatibility

You can configure a Product Compatibility Check to automatically download a Product Compatibility List from McAfee.

This list identifies products that are no longer compatible in your McAfee ePO environment.

McAfee ePO performs this check any time the installation and startup of an extension might leave your server in an undesirable state. The check occurs in these situations:

- During an upgrade from a previous version of McAfee ePO.
- When an extension is installed from the **Extensions** menu.
- Before a new extension is retrieved from the **Software Manager**.
- When a new compatibility list is received from McAfee.
- When the Data Migration Tool runs.

See the *McAfee ePolicy Orchestrator Software Installation Guide* for details.

Product Compatibility Check

The Product Compatibility Check uses an XML file, Product Compatibility List, to determine which product extensions are known to be *not compatible* with a version of McAfee ePO.

An initial list is included in the McAfee ePO software package downloaded from the McAfee website. When you run Setup during an installation or upgrade, McAfee ePO automatically retrieves the most current list of compatible extensions from a trusted McAfee source. If the Internet source is unavailable or if the list cannot be verified, McAfee ePO uses the latest version it has available.



The McAfee ePO server updates the Product Compatibility List, in the background once per day.

Remediation

When you view the list of incompatible extensions through the installer or the Upgrade Compatibility Utility, you are notified if a known replacement extension is available.

In some cases during an upgrade:

- An extension blocks the upgrade and must be removed or replaced before the upgrade can continue.
- An extension is disabled, but you must update the extension after the McAfee ePO upgrade completes.

See *Blocked or disabled extensions* for more details.

Disabling automatic updates

You might want to disable the automatic updates of the Product Compatibility List to prevent a new list from being downloaded.

The download occurs as part of a background task, or when the Software Manager content is refreshed. This setting is helpful when your McAfee ePO server does not have inbound Internet access. See *Change Product Compatibility List download* for details.



Re-enabling the Product Compatibility List download setting also re-enables Software Manager automatic updates of the Product Compatibility List.

Using a manually downloaded Product Compatibility List

If your McAfee ePO server does not have Internet access, you might want to use a manually downloaded Product Compatibility List.

You can manually download the list:

- When you install McAfee ePO. See *Blocked or disabled extensions* for details.
- When using **Server Settings | Product Compatibility List** to manually upload a Product Compatibility List. This list takes effect immediately after upload.



Disable automatic updating of the list to prevent overwriting the manually downloaded Product Compatibility List. See *Change Product Compatibility List download* for details.

Click [ProductCompatibilityList.xml](#) to manually download the list.

Blocked or disabled extensions

If an extension is blocked in the Product Compatibility List it prevents the McAfee ePO software upgrade. If an extension is disabled it doesn't block the upgrade, but the extension isn't initialized after the upgrade until a known replacement extension is installed.

Command-line options for installing the Product Compatibility List

You can use these command-line options with the `setup.exe` command to configure Product Compatibility List downloads.

Command	Description
<code>setup.exe DISABLEPRODCOMPATUPDATE=1</code>	Disables automatic downloading of the Product Compatibility List from the McAfee website.
<code>setup.exe PRODCOMPATXML=<full_filename_including_path></code>	Specifies an alternate Product Compatibility List file.



Both command-line options can be used together in a command string.

Reconfigure Product Compatibility List download

You can download the Product Compatibility List from the Internet, or use a manually downloaded list to identifying products that are no longer compatible in your ePolicy Orchestrator environment.

Before you begin

Any manually downloaded Product Compatibility List, must be a valid XML file provided by McAfee.



If you make any changes to the Product Compatibility List XML file, the file is invalidated.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, select **Product Compatibility List** from the **Setting Categories**, then click **Edit**.

A list of disabled incompatible extensions appears in a table on the opening page.

- 2 Click **Disabled** to stop automatic and regular downloads of the Product Compatibility List from McAfee.
- 3 Click **Browse** and navigate to the **Upload Product Compatibility List**, then click **Save**.

Now you have disabled automatic downloading of the Product Compatibility List, your McAfee ePO server uses the same list until you upload a new list, or connect your server to the Internet and enable automatic downloading.

14 Product Deployment

ePolicy Orchestrator simplifies the process of deploying security products to the managed systems in your network by providing a user interface to configure and schedule deployments.

There are two processes you can follow to deploy products using ePolicy Orchestrator:

- Product Deployment projects, which streamline the deployment process and provide more functionality.
- Individually created and managed client task objects and tasks.

Contents

- ▶ *Choosing a product deployment method*
- ▶ *Benefits of product deployment projects*
- ▶ *The Product Deployment page explained*
- ▶ *Viewing Product Deployment audit logs*
- ▶ *View Product Deployment*
- ▶ *Deploy products using a deployment project*
- ▶ *Monitor and edit deployment projects*
- ▶ *Deploy new product example*
- ▶ *Global updating*
- ▶ *Deploy update packages automatically with global updating*

Choosing a product deployment method

Deciding which product deployment method to use depends on what you have already configured.

Product Deployment projects offer a simplified workflow and increased functionality for deploying products to your ePolicy Orchestrator managed systems. However, you can't use a **Product Deployment** project to act on or manage client task objects and tasks created in a version of the software before 5.0.

If you want to maintain, and continue to use client tasks and objects created outside of a **Product Deployment** project, use the client task object library and assignment interfaces. You can maintain these existing tasks and object while using the **Product Deployment** project interface to create new deployments.

Benefits of product deployment projects

Product deployment projects simplify the process of deploying security products to your managed system by reducing the time and overhead needed to schedule and maintain deployments throughout your network.

Product deployment projects streamline the deployment process by consolidating many of the steps needed to create and manage product deployment tasks individually. They also add the ability to:

- **Run a deployment continuously** — This allows you to configure your deployment project so that when new systems matching your criteria are added, products are deployed automatically
- **Stop a running deployment** — If, for some reason, you need to stop a deployment once it's started, you can. Then you can resume that deployment when you're ready.
- **Uninstall a previously deployed product** — If a deployment project has been completed, and you want to uninstall the associated product from the systems assigned to your project, select **Uninstall** from the Action list.

The following table compares the two process for deploying products — individual client task objects and product deployment projects.

Table 14-1 Product deployment methods compared


Client task objects	Function comparison	Product deployment project
Name and description	Same	Name and description
Collection of product software to deploy	Same	Collection of product software to deploy
Use tags to select target systems	Enhanced in Product Deployment project	Select when the deployment occurs: <ul style="list-style-type: none"> • Continuous — Continuous deployments use System Tree groups or tags which allow you to move systems to those groups or assign systems tags and cause the deployment to apply to those systems. • Fixed — Fixed deployments use a fixed, or defined, set of systems. System selection is done using your System Tree or Managed Systems Query output tables.
Deployment schedule	Similar	Simplified deployment schedule allows you to either run the deployment immediately or run it once at a scheduled time.
Not available	New in Product Deployment project	Monitor the current deployment status, for example deployments scheduled but not started, in progress, stopped, paused, or completed.
Not available	New in Product Deployment project	View a historical snapshot of data about the number of systems receiving the deployment.
		 For fixed deployments only.

Table 14-1 Product deployment methods compared *(continued)*

Client task objects	Function comparison	Product deployment project
Not available	New in Product Deployment project	View the status of individual system deployments, for example systems installed, pending, and failed.
Not available	New in Product Deployment project	Modify an existing deployment assignment using: <ul style="list-style-type: none"> <li data-bbox="824 415 1105 506">• Create New for modifying an existing deployment <li data-bbox="824 520 894 548">• Edit <li data-bbox="824 596 959 623">• Duplicate <li data-bbox="824 638 922 665">• Delete <li data-bbox="1170 415 1382 478">• Stop and Pause Deployment <li data-bbox="1170 520 1463 583">• Continue and Resume Deployment <li data-bbox="1170 596 1300 623">• Uninstall

The Product Deployment page explained

The Product Deployment page is a single location where you can create, monitor, and manage your product deployment projects.

The page is separated into two main areas (areas 1 and 2 in this image), with the second area further separated into five smaller areas.

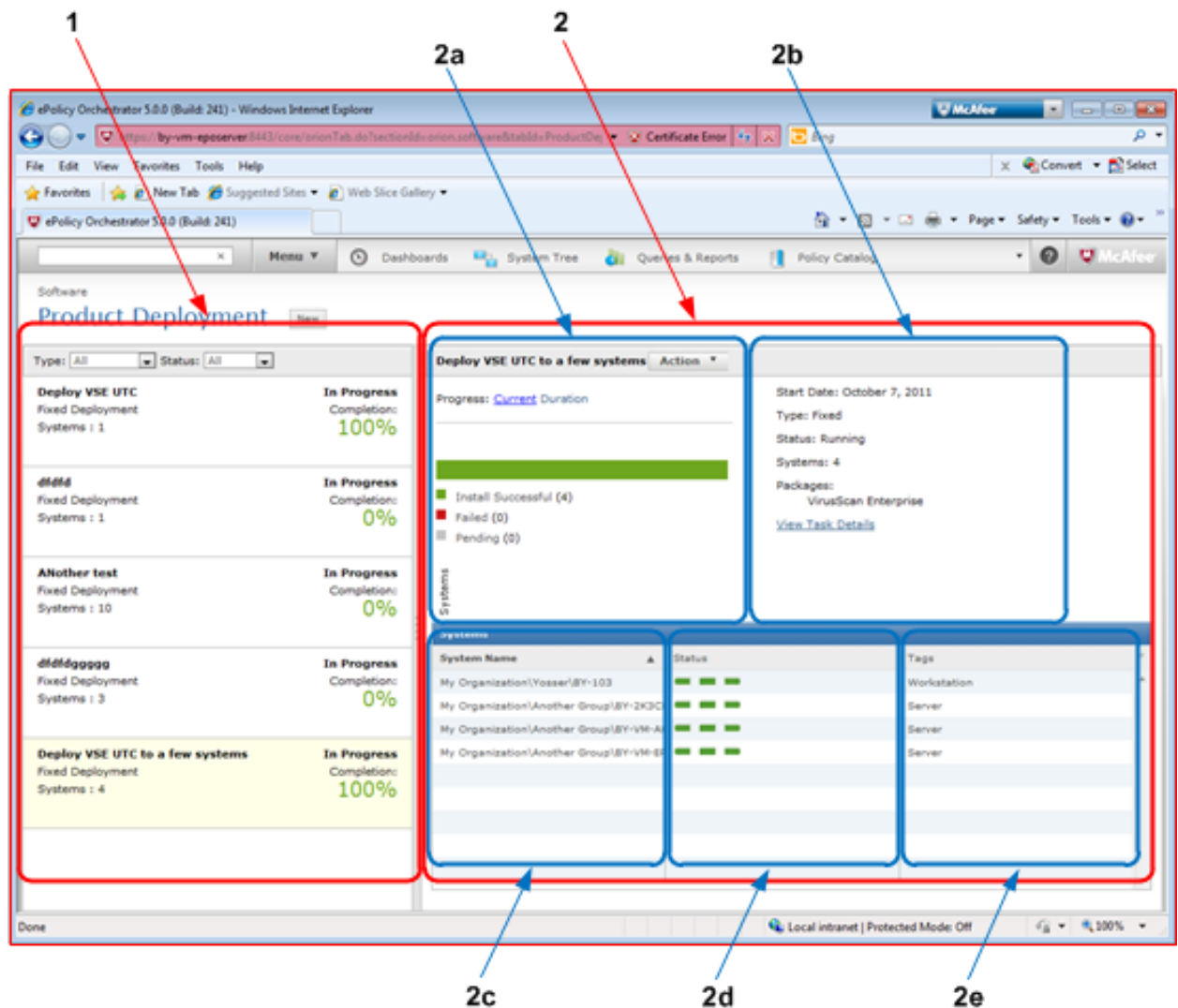


Figure 14-1 Product Deployment page

These main areas are:

- 1 *Deployment summary* — Lists the product deployments and allows you to filter them by type and status and quickly view their progress. If you click a deployment, details for the deployment are displayed in the deployment details area.



An exclamation point icon indicates either an uninstall of the deployment is in progress or the package the deployment uses has been moved or deleted.

- 2 *Deployment details* — Lists the details of the selected deployment and includes the following areas:

- 2a *Status monitor* — The progress and status display varies depending on the type of deployment and its status:
- Continuous deployments display a calendar if the deployment is pending, or a bar chart during the deployment.
 - Fixed deployments display a calendar if the deployment is pending, or either a bar chart if **Current** is selected, or a histogram if **Duration** is selected.



You can use Action to modify a deployment.

- 2b *Details* — The details display allows you to view deployment configuration details, status, and if needed, click **View Task Details** to open the Edit Deployment page.
- 2c **System name** — Displays a filterable list of target systems receiving the deployment. The systems are displayed according to the deployment type and whether the systems were selected individually, as tags, as System Tree groups, or query output tables.



Clicking **System Actions** displays the filtered list of systems in a dialog box with more detail and allows you to perform actions on the systems, such as update and wake-up.

- 2d **Status** — Displays a three-section bar indicating the progress of the deployment and its status.
- 2e **Tags** — Displays tags associated with the row of systems.

Viewing Product Deployment audit logs

Audit logs from your deployment projects contain records of all product deployments made from the console using the Product Deployment feature.

These audit log entries are displayed in a sortable table within the Deployment details area of the Product Deployment page, as well as on the Audit Log page, which contains log entries from all auditable user actions. You can use these logs to track, create, edit, duplicate, delete, and uninstall product deployments. Click a log entry to display entry details.

View Product Deployment

During the Initial Product Deployment process, ePolicy Orchestrator automatically creates a product deployment. You can use this product deployment as a base to create other product deployments.

Before you begin

There are no default product deployments. You must run the Getting Started to create a product deployment.

For detailed information about product deployment, see *Product Deployment*.

Task

For option definitions, click ? in the interface.

- 1 Find the initially created product deployment: select **Menu** | **Product Deployment**.

The initially created product deployment uses the name of the **System Tree** group you configured in the Getting Started and is in the **Deployment summary** list as Initial Deployment My Group. For example, "Initial Deployment My Group."

- To view the product deployment details, select the name of the product deployment assigned to the initial product deployment URL you created. The page changes to display details of the product deployment configuration.



Don't change this default product deployment. This deployment is running daily to update your managed systems if any of the products, or the McAfee Agent, are updated.

Now you know the location and configuration of the initially created product deployment. You can duplicate this product deployment to, for example deploy the **McAfee Agent** to platforms using different operating systems.

You can also modify the initially created client task named, for example Initial Deployment My Group. To find the client task click **Menu | Client Task Catalog** and it is listed in the Client task Types under Product Deployment.

Deploy products using a deployment project

Deploying your security products to managed systems using a deployment project allows you to easily select products to deploy, the target systems, and schedule the deployment.

For option definitions, click ? in the interface.

Task

- Click **Menu | Software | Product Deployment**.
- Click **New Deployment** to open the **New Deployment** page and to start a new project.
- Type a name and description for this deployment. This name appears on the **Product Deployment** page after the deployment is saved.
- Choose the type of deployment:
 - Continuous** — Uses your System Tree groups or tags to configure the systems receiving the deployment. This allows these systems to change over time as they are added or removed from the groups or tags.
 - Fixed** — Uses a fixed, or defined, set of systems to receive the deployment. System selection is done using your System Tree or **Managed Systems Queries** table output.

If you want to automatically update your security products, select **Auto Update**. This will also deploy the hotfixes and patches for your product automatically.



You cannot uninstall a product if you have selected **Auto Update**.

- To specify which software to deploy, select a product from the **Package** list. Click + or - to add or remove packages.



Your software must be checked into the Master Repository before it can be deployed. The **Language** and **Branch** fields are populated automatically, as determined by the location and language specified in the Master Repository.

- In the **Command line** text field, specify any command-line installation options. See the product documentation for software you're deploying for information on command-line options.
- In the **Select the systems** section, click **Select Systems** to open the **System Selection** dialog box. The **System Selection** dialog box is a filter that allows you to select groups in your System Tree, Tags, or a subset of grouped or tagged systems. The selections you make in each tab within this dialog box are concatenated to filter the complete set of target systems for your deployment.

For example, if your System Tree contains "Group A," which includes both Servers and Workstations, you can target the entire group, just the Servers or Workstations (if they are tagged accordingly), or a subset of either system type in group A.



Fixed deployments have a limit of 500 systems to receive the deployment.

If needed, configure the following:

- **Run at every policy enforcement (Windows only)**
- **Allow end users to postpone this deployment (Windows only)**
- **Maximum number of postponements allowed**
- **Option to postpone expires after**
- **Display this text**

8 Pick a start time or schedule for your deployment:

- **Run Immediately** — Starts the deployment task during the next ASCII.
- **Once** — Opens the scheduler so you can configure the start date, time, and randomization.

9 When you're finished, click **Save** at the top of the page. The **Product Deployment** page opens with your new project added to the list of deployments.

After you create a deployment project, a client task is automatically created with the deployment settings.

Monitor and edit deployment projects

Use the Product Deployment page to create, track, and change deployment projects.

In the task below, the first few steps describe using the interface to select and monitor an existing deployment project, while the last steps describe selecting Actions to modify that deployment project.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Product Deployment**. The Product Deployment page appears.
- 2 Filter the list of deployment projects using either, or both, of the following:
 - **Type** — Filters the deployments that appear by All, Continuous, or Fixed.
 - **Status** — Filters the deployments that appear by All, Finished, In Progress, Pending, Running, or Stopped.
- 3 Click a deployment in the list on the left side of the page to display its details on the right side of the page.
- 4 Use the progress section of the details display to view a:
 - Calendar displaying the start date for pending continuous and fixed deployments.
 - Histogram displaying systems and the time to completion for fixed deployments.
 - Status bar displaying system deployment and uninstallation progress.

5 Click **Action** and one of the following to modify a deployment:

- **Edit**
- **Delete**
- **Duplicate**
- **Mark Finished**
- **Resume**
- **Stop**
- **Uninstall**

6 In the details section, click **View Task Details** to open the Edit Deployment page, where you can view and modify the settings for the deployment.

7 In the Systems table, click one of the following in the **Filter** list to change which systems appear:



The options in the list vary depend on the current status of the deployment.

- For the Uninstall action, the filters include — **All, Packages Removed, Pending, and Failed**
- For all other actions, the filters include — **All, Install Successful, Pending, and Failed**

8 In the **Systems** table, you can:

- Check the status of each row of target systems in the Status column. A three-section status bar indicates the progress of the deployment.
- Check the tags associated with the target systems in the Tags column.
- Click **System Actions** to display the list of systems in a new page where you can perform system-specific actions on the systems you select.

Deploy new product example

After your McAfee ePO installation and initial product deployment, any additional product deployments must be created using a Product Deployment project or manually using a Client Task object.

This example walks you through creating a Product Deployment project for McAfee VirusScan Enterprise.

Task



- 1 Select **Menu | Software | Product Deployment**, then click **New Deployment**.
- 2 On the New Deployment page, configure these settings.

Option	Description
Name and Description	Type a name and description for this deployment. This name appears on the Deployment page after the deployment is saved.
Type	From the list, select Continuous . This type uses your System Tree groups or tags to configure the systems receiving the deployment. Selecting this type allows these systems to change over time as they are added to or removed from the groups or tags. To automatically update your security products, select Auto Update , which also deploys the hotfixes and patches for your product automatically. You cannot uninstall a product if you selected Auto Update .
Package	From the list, select VirusScan Enterprise .

Option	Description
Language and Branch	If not using the defaults, select the language and branch.
Command line	In the text field, specify any command-line installation options. See the <i>McAfee VirusScan Enterprise Installation Guide</i> for details.
Select the systems	<p>Click Select Systems to open the System Selection dialog box.</p> <p>The System Selection dialog box is a filter that allows you to select groups in your System Tree, tags, or a subset of grouped or tagged systems. The selections you make in each tab within this dialog box are concatenated to filter the complete set of target systems for your deployment.</p> <p>If needed, configure the following:</p> <ul style="list-style-type: none"> • Run at every policy enforcement (Windows only) • Allow end users to postpone this deployment (Windows only) • Maximum number of postponements allowed • Option to postpone expires after • Display this text
Select a start time	<p>Pick a start time or schedule for your deployment:</p> <ul style="list-style-type: none"> • Run Immediately — Starts the deployment task after the next ASCII. • Once — Opens the scheduler so that you can configure the start date, time, and randomization.
Save	When finished, click Save at the top of the page. The Product Deployment page opens with your new project added to the list of deployments.

After you create a deployment project, a client task is automatically created with the deployment settings.

- 3 On the Product Deployment page, confirm that the product deployment project is correctly working by checking this information.

Option	Description
Deployment summary	<p>Click the product deployment project that you created in the previous step. The details appear on the right side of the page.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;">  The infinity symbol  appears under In Progress because this is a continuous deployment. </div>
Deployment details	<p>Allows you to:</p> <ul style="list-style-type: none"> • Click Actions to modify the selected deployment. • View Progress, Status, and Details of the selected deployment. • View the Systems, System Actions, Status, and Tags associated with the selected deployment.

Global updating

Global updating automates replication to your distributed repositories and keeps your managed systems current.

Replication and update tasks are not required. Checking contents into your Master Repository initiates a global update. The entire process finishes within an hour in most environments.

You can also specify which packages and updates initiate a global update. However, when you only specify that certain content initiates a global update, make sure 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

- 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 SuperAgent 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, such as when the client computer is turned off or there are no SuperAgents, the minimum catalog version is supplied at the next agent-server communication, 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 agent-server communication, it is not supplied with the list of packages to update, and 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 access the repository where its updates come from. 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.

Deploy update packages automatically with global updating

You can enable global updating on the server to automatically deploy 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.

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.

Product Deployment

Deploy update packages automatically with global updating

15 Manual package and update management

When you need to roll out new products outside of your normally scheduled tasks, you can check them in manually.

Contents

- ▶ *Bring products under management*
- ▶ *Check in packages manually*
- ▶ *Delete DAT or engine packages from the master repository*
- ▶ *Manually moving DAT and engine packages between branches*
- ▶ *Check in Engine, DAT, and ExtraDAT update packages manually*

Bring products under management

A product's extension must be installed before ePolicy Orchestrator can manage the product.

Before you begin

Make sure that the extension file is in an accessible location on the network.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu | Software | Extensions | Install Extension**.



You can only have one task updating the Master Repository at once. If you try to install an extension at the same time as a Master Repository update is running, the following error appears:

Unable to install extension com.mcafee.core.cdm.CommandException: Cannot check in the selected package while a pull task is running.

Wait until the Master Repository update is done and try to install your extension again.

- 2 Browse to and select the extension file, then click **OK**.
- 3 Verify that the product name appears in the **Extensions** list.

Check in packages 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 interface.

Task

- 1 Open the Check In Package wizard.
 - a Select **Menu | Software | Master Repository**.
 - b Click **Check In Package**.
- 2 Select the package type, then browse to and select the package file.
- 3 Click **Next**.
- 4 Confirm or configure the following:
 - **Package info** — Confirm this is the correct package.
 - **Branch** — Select the 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 a McAfee or a 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.

Delete DAT or engine packages from the master repository

Delete DAT or engine 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.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Master Repository**.
- 2 In the row of the package, click **Delete**.
- 3 Click **OK**.

Manually moving DAT and engine packages between branches

Move packages manually between the Evaluation, Current, and Previous branches after they are checked in to the Master Repository.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Software | Master Repository**.
- 2 In the row of the package, click **Change Branch**.
- 3 Select whether to move or copy the package to another branch.
- 4 Select which branch receives the package.



If you have McAfee® NetShield® for NetWare in your network, select **Support NetShield for NetWare**.

- 5 Click **OK**.

Check in Engine, DAT, and ExtraDAT update packages manually

Check in 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 Open the Check In Package wizard.
 - a Select **Menu | Software | Master Repository**.
 - b Click **Check In Package**.
- 2 Select the package type, browse to and select a package file, then click **Next**.
- 3 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.
- 4 Next to **Options**, select **Move the existing package to the Previous branch** to move the existing package (of the same type that you are checking in) to the **Previous** branch.
 - 5 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.

Manual package and update management

Check in Engine, DAT, and ExtraDAT update packages manually

16 Policy management

Policies make sure 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. This is accomplished through application and enforcement of product policies. Policies ensure a product's features are configured correctly. Client tasks are the scheduled actions that run on the managed systems hosting any client-side software.

Contents

- ▶ *Policies and policy enforcement*
- ▶ *Policy application*
- ▶ *Create and maintain policies*
- ▶ *Configuring policies for the first time*
- ▶ *Manage policies*
- ▶ *Edit Policy and Task Retention page*
- ▶ *Policy assignment rules*
- ▶ *Create policy management queries*
- ▶ *Create a query to define compliance*
- ▶ *Generate compliance events*
- ▶ *View policy information*
- ▶ *Share policies among McAfee ePO servers*
- ▶ *Distribute your policy to multiple McAfee ePO servers*
- ▶ *Policy management questions*
- ▶ *Assign Policy page*

Policies and policy enforcement

A *policy* is a collection of settings that you create and configure, then enforce. Policies make sure that the managed security software products are configured and perform correctly.

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. The Policy Catalog page displays policies by product and category. When you open an existing policy or create a policy, the policy settings are organized across tabs.

Where policies are displayed

To see all policies 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 where they have permissions.

To see which policies, per product, are applied to a specific group of the System Tree, click **Menu | Systems Section | System Tree | Assigned Policies**, 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 duplicate 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.

On 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 site lists 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 will not receive the new site list with this information, so they report to a different Agent Handler listed in an expired site list.

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-server communication interval (ASCI) settings on the General tab of the McAfee Agent policy pages, or the McAfee Agent Wake-up 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 change.

Exporting and importing policies

If you have multiple servers, you can export and import policies between them using XML files. In such an environment, you only 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 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 more servers, all through the McAfee ePO console.

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. 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. 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 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. Any user can assign any policy in the Policy Catalog page, but only the creator 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, we recommend that you first duplicate the policy, then assign the duplicate to a location. This provides you ownership of the assigned policy.



You can specify multiple users as owners of a single policy.

Create and maintain policies

Create and maintain policies from the Policy Catalog page.

Tasks

- [Create a policy from the Policy Catalog page on page 188](#)
Custom policies created using the Policy Catalog are not assigned to any groups or systems. You can create policies before or after a product is deployed.
- [Manage an existing policy on the Policy Catalog page on page 188](#)
Edit, duplicate, rename, or delete a policy.

Create a policy from the Policy Catalog page

Custom policies created using the Policy Catalog are not assigned to any groups or systems. You can create policies before or after a product is deployed.

For option definitions, click ? in the interface.

Task

- 1 Open the **New Policy** dialog box.
 - a Click **Menu | Policy | Policy Catalog**.
 - b Select the product and category from the drop-down lists.
All created policies for the selected category appear in the **Details** pane.
 - c Click **New Policy**.
- 2 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
- 3 Type a name for the new policy and click **OK**.
The policy appears in the Policy Catalog.
- 4 Click the name of the new policy.
The Policy Settings wizard opens.
- 5 Edit the policy settings as needed.
- 6 Click **Save**.


Manage an existing policy on the Policy Catalog page

Edit, duplicate, rename, or delete a policy.

Task

For option definitions, click ? in the interface.

- 1 To select an existing policy, 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 Select one of these actions.

Action	Steps
<p>Edit policy settings</p> <p> The number of affected systems is listed at the top of the page.</p>	<ol style="list-style-type: none"> 1 Locate the policy, then click the policy name. 2 Edit the settings as needed, then click Save.
<p>Duplicate a policy</p>	<ol style="list-style-type: none"> 1 Locate the policy, then click Duplicate in that policy's row. The Duplicate Existing Policy dialog box appears. 2 Type the name of the new policy in the field, then click OK. The new policy appears on the Policy Catalog page. 3 Click the new policy in the list. 4 Edit the settings as needed, then click Save. The new policy appears in the details pane.
<p>Rename a policy</p>	<ol style="list-style-type: none"> 1 Locate the policy, then click Rename in a policy row. The Rename Policy dialog box appears. 2 Type a new name for the existing policy, then click OK. The renamed policy appears in the details pane.
<p>Delete a policy</p>	<ol style="list-style-type: none"> 1 Locate the policy, then click Delete in the policy row. 2 Click OK when prompted. The deleted policy is removed from the details pane.


Configuring policies for the first time

Follow these high-level steps the first time you configure your policies.

- 1 Plan product policies for the segments of your System Tree.
- 2 Create and assign policies to groups and systems.

Manage policies

Assign and maintain the policies in your environment.

 The number of affected systems is listed at the top of the page.

Tasks

- [Change the owners of a policy on page 190](#)
By default, ownership is assigned to the user who creates the policy. If you have the required permissions, you can change the ownership of a policy.
- [Move policies between McAfee ePO servers on page 190](#)
In order to move policies between McAfee ePO, 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.
- [Assign a policy to a System Tree group on page 192](#)
Assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.
- [Assign a policy to a managed system on page 192](#)
Assign a policy to a specific managed system. You can assign policies before or after a product is deployed.
- [Assign a policy to systems in a System Tree group on page 193](#)
Assign a policy to multiple managed systems within a group. You can assign policies before or after a product is deployed.
- [Enforce policies for a product in a System Tree group on page 193](#)
Enable or disable policy enforcement for a product in a group. Policy enforcement is enabled by default, and is inherited in the System Tree.
- [Enforce policies for a product on a system on page 193](#)
Enable or disable policy enforcement for a product on a managed system. Policy enforcement is enabled by default, and is inherited in the System Tree.
- [Copy policy assignments on page 194](#)
Copy 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.

Change the owners of a policy

By default, ownership is assigned to the user who creates the policy. If you have the required permissions, you can change the ownership of a policy.
For option definitions, click ? in the interface.

Task

- 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 policy you want, then click the owner of the policy.
The **Policy Ownership** page appears.
- 3 Select the owners of the policy from the list, then click **OK**.

Move policies between McAfee ePO servers

In order to move policies between McAfee ePO, 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

- [Export a single policy on page 191](#)
Export a single policy to an XML file, then use this file to import the policy to another McAfee ePO server, or to keep as a backup of the policy.
- [Export all policies of a product on page 191](#)
- [Import policies on page 191](#)
You can import a policy XML file. Regardless of whether you exported a single policy or all named policies, the import procedure is the same.

Export a single policy

Export a single policy to an XML file, then use this file to import the policy to another McAfee ePO server, or to keep as a backup of the policy.

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, 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 McAfee ePO server.

Export all policies of a product

For option definitions, click ? in the interface.

Task

- 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 McAfee ePO server.

Import policies

You can import a policy XML file. Regardless of whether you exported a single policy or all named policies, the import procedure is the same.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Policy Catalog**, then click **Import** next to **Product policies**.
- 2 Browse to and select the 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.

Assign a policy to a System Tree group

Assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select a product.
Each assigned policy per category appears in the details pane.
- 2 Locate the policy category you want, then click **Edit Assignment**.
- 3 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from**.
- 4 Select the policy from the **Assigned policy** drop-down list.



From this location, you can also edit the selected policy's settings, or create a 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**.

Assign a policy to a managed system

Assign a policy to a specific managed system. You can assign policies before or after a product is deployed.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group under System Tree.
All systems within this group (but not its subgroups) appear in the details pane.
- 2 Select a system, then click **Actions | Agent | Modify Policies on a Single System**.
The **Policy Assignment** page for that system appears.
- 3 Select a product.
The categories of selected product are listed with the system's assigned policy.
- 4 Locate the policy category you want, 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 policy from the **Assigned policy** drop-down list.



From this location, you can also edit settings of the selected policy, or create a 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**.

Assign a policy to systems in a System Tree group

Assign a policy to multiple managed systems within a group. You can assign policies before or after a product is deployed.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu** | **Systems** | **System Tree** | **Systems**, then select a group in the System Tree.
All systems in this group (but not its subgroups) appear in the details pane.
- 2 Select the systems you want, 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**.

Enforce policies for a product in a System Tree group

Enable or disable policy enforcement for a product in a group. Policy enforcement is enabled by default, and is inherited in the System Tree.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu** | **Systems** | **System Tree** | **Assigned Policies**, then select a group in the **System Tree**.
- 2 Select the product you want, then click the link next to **Enforcement Status**.
The **Enforcement** page appears.
- 3 To change the enforcement status, 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**.

Enforce policies for a product on a system

Enable or disable policy enforcement for a product on a managed system. Policy enforcement is enabled by default, and is inherited in the System Tree.

For option definitions, click ? in the interface.

Task

- 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 a system, then click **Actions | Modify Policies on a Single System**.
The **Policy Assignment** page appears.
- 3 Select a **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**.
- 5 Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.
- 6 Click **Save**.

Copy policy assignments

Copy 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

- *Copy policy assignments from a group on page 194*
You can copy policy assignments from one group in the System Tree to another.
- *Copy policy assignments from a system on page 194*
Copy policy assignments from a specific system.
- *Paste policy assignments to a group on page 195*
You can paste policy assignments to a group after you copy them from a group or system.
- *Paste policy assignments to a specific system on page 195*
Paste policy assignments to a specific system after copy the policy assignments from a group or system.

Copy policy assignments from a group

You can copy policy assignments from one group in the System Tree to another.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select a 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**.

Copy policy assignments from a system

Copy policy assignments from a specific system.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group in the System Tree.
The systems belonging to the selected group appear in the details pane.
- 2 Select a system, then click **Actions | Agent | Modify Policies on a Single System**.
- 3 Click **Actions | Copy Assignments**, select the products or features for which you want to copy policy assignments, then click **OK**.

Paste policy assignments to a group

You can paste policy assignments to a group after you copy them from a group or system.
For option definitions, click ? in the interface.

Task

- 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, the **Enforce Policies and Tasks** policy appears in the list. 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**.

Paste policy assignments to a specific system

Paste policy assignments to a specific system after copy the policy assignments from a group or system.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a group in the **System Tree**.
All 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, the **Enforce Policies and Tasks** policy appears in the list. This policy controls the enforcement status of other policies.

- 4 Confirm the replacement of assignments.

Edit Policy and Task Retention page

Use this page to specify whether policy and client task data is removed when you delete a product management extension.

Table 16-1 Option definitions

Option	Definition
Policy and Task Retention	Specifies whether policy and client task data is removed when you delete a product management extension. Options include: <ul style="list-style-type: none"> • Keep policy and client task data • Remove policy and client task data — The default removes the policy and client task data.

Policy assignment rules

Policy assignment 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 assignments 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 system that is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included systems unrestricted access to Internet content. Rule B has priority level 2, and heavily restricts the same system's access to Internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the system 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. 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.

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."

Policy type	Assignment type	Policy name	Policy settings
Generic policy	Policy assigned in the System Tree	A	Prevents Internet access from all systems to which the policy is assigned.
System-based	Policy assignment rule	B	Allows Internet access from systems with the tag "IsLaptop."
System-based	Policy assignment rule	C	Allows unrestricted Internet access to all users in the Admin user group from all systems.
User-based	Policy assignment rule	C	Allows unrestricted Internet access to all users in the Admin user group from all systems.

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.

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.



When a user logs on to a managed system for the first time, there can be a slight delay while the McAfee 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.

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 McAfee ePO server applies the policies that you assigned to each user.



To use user-based policy assignments, register and configure a registered LDAP server for use with your McAfee ePO server.

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** — Assign policies to systems 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

Leverage tags to simplify automating policy assignment.

System-based policies 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.


Create policy assignment rules

Creating policy assignment rules allow you to enforce policies for users or systems based on configured rule criteria.

For option definitions, click ? in the interface.

Task

- 1 Open the **Policy Assignment Builder**.
 - a Click **Menu | Policy | Policy Assignment Rules**.
 - b Click **New Assignment Rule**.
- 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 on the **Selection Criteria** page.



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**.
- 4 Click **Add Policy** to select the policies that you want to be enforced by this policy assignment rule.
- 5 Click **Next**.
- 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**.

Manage policy assignment rules

Perform common management tasks when working with policy assignment rules.

Task

- 1 Click **Menu | Policy | Policy Assignment Rules**.
- 2 Select one of these actions:

Action	Steps
Delete a policy assignment rule	Click Delete in the selected assignment row.
Edit a policy assignment rule	Click the selected assignment. The Policy Assignment Builder wizard opens. Work through each page of this wizard to modify this policy assignment rule.
Export policy assignment rules	Select Actions Export . The Download Policy Assignment Rules page opens, where you can view or download the PolicyAssignmentRules.xml file.
Import policy assignment rules	Select Actions 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.
Edit the priority of a policy assignment rule	Click Actions Edit Priority . The Edit Priority page opens, where you change the priority of policy assignment rules using the drag-and-drop handle.
View the summary of a policy assignment rule	Click > in the selected assignment row.

Create policy management queries

Retrieve the policies assigned to a managed system, or policies broken in the system hierarchy. You can create either of the following Policy Management queries:

- **Applied Policies** — Retrieves policies assigned to a specified managed system.
- **Broken Inheritance** — Retrieves information on policies that are broken in the system hierarchy.

Task

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

- 1 Select **Menu | Reporting | Queries & Reports**, then click **New Query**.
The Query Builder opens.
- 2 On the Result Type page, select **Policy Management** from the **Feature Group** list.
- 3 Select a Result Type, 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 that 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.



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 action on items in any table or drill-down table.
 - 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**.
 - To use 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**.

Create 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 Select **Menu | Reporting | Queries & Reports**, then click **New Query**.
- 2 On the **Result Type** page, select **System Management** for Feature Group, and select **Managed Systems** for 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**.



These properties define compliance for systems managed by this McAfee ePO server.

- 5 Select the columns to be included in the query, then click **Next**.
- 6 Select the filters to be applied to the query, click **Run**, then click **Save**.

Generate 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 McAfee 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**.

View policy information

View detailed information about your policies, including policy owners, assignments, and inheritance.

Tasks

- [View groups and systems where a policy is assigned on page 202](#)
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.
- [View policy settings on page 202](#)
View details for a policy assigned to a product category or system.
- [View policy ownership on page 202](#)
View the owners of a policy.
- [View assignments where policy enforcement is disabled on page 202](#)
View assignments where policy enforcement, per policy category, is disabled.
- [View policies assigned to a group on page 203](#)
View the policies assigned to a System Tree group, sorted by product.
- [View policies assigned to a specific system on page 203](#)
View the product policies assigned to a system in the System Tree.
- [View policy inheritance for a group on page 203](#)
View the policy inheritance of a specific group.
- [View and reset broken inheritance on page 203](#)
Identify the groups and systems where policy inheritance is broken.
- [Compare policies on page 204](#)
Compare like policies using Policy Comparison. This allows you to determine which settings are different and which are the same.

View groups and systems where a policy is assigned

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.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Policy Catalog**, then select a product and category.
All created policies for the selected category appear in the details pane.
- 2 Under **Assignments** on the row of the 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.

View policy settings

View details for a policy assigned to a product category or system.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Policy Catalog**, then select a product and category.
All created policies for the selected category appear in the details pane.
- 2 Click next to a 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.

View policy ownership

View the owners of a policy.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Policy Catalog**, then select a 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**.

View assignments where policy enforcement is disabled

View assignments where policy enforcement, per policy category, is disabled.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Policy Catalog**, then select a 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.

View policies assigned to a group

View the policies assigned to a System Tree group, sorted by product.

For option definitions, click ? in the interface.

Task

- 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.

View policies assigned to a specific system

View the product policies assigned to a system in the System Tree.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Systems | System Tree | Systems**, then select a 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.

View policy inheritance for a group

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 policy row, under **Inherit from**, displays the name of the group from which the policy is inherited.

View and reset broken inheritance

Identify the groups and systems where policy inheritance is broken.

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. The 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**.

Compare policies

Compare like policies using Policy Comparison. This allows you to determine which settings are different and which are the same.

Many of the values and variables included on the Policy Comparison page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the policy you want to compare.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy Comparison**, then select a product, category, and **Show** settings from the lists. These settings populate the policies to compare in the **Policy 1** and **Policy 2** lists.
- 2 Select the policies to compare in the **Compare policies** row from the **Policy 1** and the **Policy 2** column lists. The top two-rows of the table display the number of settings that are different and identical. You can also change the **Show** setting, to reduce the data being displayed, from **All Policy Settings** to, **Policy Differences** and **Policy Matches**.
- 3 Click **Print**, to open a printer friendly view of this comparison.

Share policies among McAfee ePO servers

Administrators use policy sharing to designate policies that are developed on one server to be transmitted to other servers for implementation.

Administrators only need to perform three steps to share policies between servers.

- 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.

Distribute your policy to multiple McAfee ePO servers

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

- [Register servers for policy sharing on page 205](#)
Register servers to share a policy.
- [Designate policies for sharing on page 205](#)
You can designate a policy for sharing among multiple McAfee ePO servers.
- [Schedule server tasks to share policies on page 205](#)
You can schedule a server task so that policies are shared among multiple McAfee ePO servers.

Register servers for policy sharing

Register servers to 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**.

Designate policies for sharing

You can designate a policy for sharing among multiple McAfee ePO servers.

For option definitions, click ? in the interface.

Task

- 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**.

Shared policies are automatically pushed to McAfee ePO servers with policy sharing enabled. When you click **Share** in step 2, the policy is immediately pushed to all registered McAfee ePO servers that have policy sharing enabled. Changes to shared policies are similarly pushed.

Schedule server tasks to share policies

You can schedule a server task so that policies are shared among multiple McAfee ePO servers.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **New Task**.
- 2 On the **Description** page, specify the name of the task and any notes, then click **Next**.



New server tasks are enabled by default. If you do not want this task to be enabled, in the **Schedule** status field, select **Disabled**.

- 3 From the **Actions** drop-down menu, select **Share Policies**, then click **Next**.

- 4 Specify the schedule for this task, then click **Next**.
- 5 Review the summary details, then click **Save**.

Policy management 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.

Assign Policy page

Use this page to assign a McAfee ePO configuration policy to a group or system in the System Tree.

Table 16-2 Option definitions

Option	Definition
Policy	Specifies the policy that is assigned to the selected group or systems for the given product and category. Three list boxes choose the policy: <ul style="list-style-type: none">• Product — Specifies the product that has manageable policies.• Category — Specifies the category from which you want to select a configuration policy. The available categories depend on which product or component is selected.• Policy — The specific policy you want to assign.
Inheritance	Determines whether the 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.

See also

Policies and policy enforcement on page 185

Policy application on page 187

Create and maintain policies on page 187

Configuring policies for the first time on page 189

Assign a policy to a System Tree group on page 192

Assign a policy to a managed system on page 192

Assign a policy to systems in a System Tree group on page 193

17 Client tasks

Create and schedule client tasks to automate how you manage systems in your network. Client tasks are commonly used for the following activities.

- Product deployment
- Product functionality
- Upgrades and updates

For information about which client tasks are available and what they can help you do, see the product documentation for your managed products.

Contents

- *How the Client Task Catalog works*
- *Deployment tasks*
- *Use the Product Deployment task to deploy products to managed systems*
- *Update tasks*
- *Manage client tasks*

How the Client Task Catalog works

Use the Client Task Catalog to create client task objects you can reuse to help manage systems in your network.

The 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 McAfee ePO 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.



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

Deployment tasks are client tasks that are used to deploy managed security products to your managed systems from the Master Repository.

You can create and manage individual deployment task objects using the client task catalog, then assign them to run on groups or individual system. Alternatively, you can create Product Deployment projects to deploy products to your systems. Product Deployment projects automate the process of creating and scheduling client task objects individually. They also provide additional automated management functionality.

Important considerations

When deciding how to stage your Product Deployment, consider:

- Package size and available bandwidth between the Master Repository and 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.
- 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.

Deploying products on selected 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.

Deployment packages for products and updates

The McAfee ePO software deployment infrastructure supports deploying products and components, as well as updating both.

Each product that McAfee ePO can deploy provides a product deployment package zip file. The zip file contains product installation files, which are compressed in a secure format. McAfee ePO can deploy these packages to any of your managed systems.

These zip files are used for both detection definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. We recommend 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

Package type	Description	Origination
SuperDAT (SDAT.exe) files File type: SDAT.exe	The SuperDAT files contain both DAT and engine files in one update package. If bandwidth is a concern, we recommend updating DAT and engine files separately.	McAfee website. Download and check SuperDAT files in to the master repository manually.
Supplemental detection definition (ExtraDAT) files File type: ExtraDAT	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 McAfee ePO. Pull tasks do not retrieve ExtraDAT files.	McAfee website. Download and check supplemental DAT files in to the master repository manually.
Product deployment and update packages File type: zip	A product deployment package contains installation software.	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.
McAfee Agent language packages File type: zip	A McAfee Agent language package contains files necessary to display McAfee Agent information in a local language.	Master Repository — Checked in at installation. For future versions of the McAfee Agent, you must check McAfee Agent language packages into the Master Repository manually.

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 McAfee ePO when they are checked in.

The McAfee Agent only trusts package files signed by McAfee ePO 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 repository is used, there are differences.

Product deployment vs. update packages

Product deployment packages	Update packages
Must be manually checked in to the master repository.	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.
Can be replicated to the master repository and installed automatically on managed systems using a deployment task.	Can be replicated to the master repository and installed automatically on managed systems with global updating.
If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.	If not implementing global updating for product updating, an update client task must be configured and scheduled for managed systems to retrieve the package.

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:
 - If you are using global updating, create and schedule an update task for laptop systems that leave the network.
 - If you are not using global updating, perform the following tasks.
 - 1 Use a replication task to copy the contents of the master repository.
 - 2 Create and schedule an update task for agents to retrieve and install the update on managed systems.

Configuring product and update deployments for the first time

Follow this process to ensure that 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.
- 3 Configure product deployment and update client tasks.

Deployment tags

When a deployment task is created, a tag with the task name is automatically created and applied to the systems on which the task is enforced.

These tags are added to the **Deployment Tags** group on the **Tag Catalog** page every time a deployment task is created and enforced to systems. This group is a read-only group, and tags in this group can't be manually applied, modified, deleted, or used in a criteria configuration to filter systems.

Use the Product Deployment task to deploy products to managed systems

Deploy products to managed systems with the Product Deployment client task. You can create this task for a single system, or for groups of the System Tree.

Tasks

- [Configure a deployment task for groups of managed systems on page 213](#)
Configure a product deployment task to deploy products to groups of managed systems in the System Tree.
- [Configure a deployment task to install products on a managed system on page 214](#)
Deploy products to a single system using a product deployment task.


Configure a deployment task for groups of managed systems


Configure a product deployment task to deploy products to groups of managed systems in the System Tree.

For option definitions, click ? in the interface.

Task

- 1 Open the New Task dialog box.
 - a Select **Menu | Policy | Client Task Catalog**.
 - b Under Client Task Types, select a product.
 - c Click **New Task**.
- 2 Select **Product Deployment**, then click **OK**.
- 3 Type a name for the task you are creating and add any notes.
- 4 Next to Target platforms, select the types of platform to use the deployment.
- 5 Next to Products and components, set the following:
 - Select a product from the first drop-down list. The products listed are products that you have checked in to the Master Repository. If you do not see the product you want to deploy listed here, check in the product package.
 - Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
 - To specify command-line installation options, type the 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 If you want to automatically update your security products, select **Auto Update**.
This will also deploy the hotfixes and patches for your product automatically.

 If you set your security product to update automatically, you cannot set the **Action** to **Remove**.
- 7 (Windows only) Next to Options, select whether you want to run this task for every policy process, then click **Save**.
- 8 Click **Menu | Systems Section | System Tree | Assigned Client Tasks**, then select the required group in the System Tree.

Client tasks

Use the Product Deployment task to deploy products to managed systems

- 9 Select the **Preset** filter as **Product Deployment (McAfee Agent)**.

Each assigned client task per selected category appears in the details pane.

- 10 Click **Actions | New Client Task Assignment**.

- 11 On the Select Task page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select the task you created to deploy your product.

- 12 Next to **Tags**, select the platforms you are deploying the packages to, then click **Next**:

- **Send this task to all computers**
- **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.



To limit the list to specific tags, type the tag name in the text box under **Tags**.

- 13 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click **Next**.

- 14 Review the summary, then click **Save**.

At every scheduled run, the deployment task installs the latest sensor package to systems that meet the specified criteria.

Configure a deployment task to install products on a managed system

Deploy products to a single system using a 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 Open the New Task dialog box.
 - a Select **Menu | Policy | Client Task Catalog**.
 - b Under Client Task Types, select a product.
 - c Click **New Task**.
- 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 types of platform to use the deployment.

- 5 Next to **Products and components** set the following:
 - Select a product from the first drop-down list. The products listed are those products 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, 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 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 If you want to automatically update security products that are already deployed, select **Auto Update**. This will also deploy the hotfixes and patches for your products automatically.

 If you set your security product to update automatically, you cannot set the **Action** to **Remove**.
- 7 Next to **Options**, select if you want to run this task for every policy enforcement process (Windows only), then click **Save**.
- 8 Click **Menu | Systems | System Tree | Systems**, then select the system on which you want to deploy a product, then click **Actions | Agent | Modify Tasks on a single system**.
- 9 Click **Actions | New Client Task Assignment**.
- 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 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** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.

 To limit the list to specific tags, type the tag name in the text box under **Tags**.
- 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**.

Update tasks

If you do not use global updating, determine when agents on managed systems go for updates.

You can create and configure update Client Tasks to control when and how managed systems receive update packages.

If you use 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 at the highest level of the System Tree, so that all systems inherit the task. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact. For networks with offices in different time zones, balance network load by running the task at the local system time of the managed system, rather than at the same time for all systems.
- If you are using scheduled replication tasks, schedule the task at least an hour after the scheduled replication task.
- 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 that 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 more tasks to update products that do not use the McAfee Agent for Windows.
- Create a task to update your main workstation applications, to ensure that they all receive the update files. Schedule it to run daily or several times a day.

View Assigned Client Task

During the Initial Product Deployment process, ePolicy Orchestrator automatically creates a product deployment client task. You can use this assigned client task as a basis for creating other product deployment client tasks.

Before you begin

There are no default product deployment client tasks. You must run the Initial Product Deployment to create the initial product deployment client task.

Task

For option definitions, click ? in the interface.

- 1 To see the initial product deployment client task, click **Menu | Client Task Catalog**.
- 2 Find the initial product deployment client task: from the **Client Task Types** list, select **McAfee Agent | Product Deployment**.

The initially created product deployment client task uses the name of the **System Tree** group you configured in the **Agent Deployment URL** as `InitialDeployment_<groupName>`. For example, "InitialDeployment_AllWindowsSystems." This task appears in the **Name** column of the **McAfee Agent | Product Deployment** table.

- 3 To open the client task, click the name of the task configured in the **Agent Deployment URL** to display the client task details.
- 4 To close the page, click **Cancel**.

Now you know the location and configuration of the default product deployment client task. You can duplicate this client task to, for example, deploy the McAfee Agent to platforms using different operating systems.

Update managed systems regularly with a scheduled update task

Create and configure update tasks. If you use global updating, we recommend using a daily update client task to ensure systems are current with the latest DAT and engine files.

For option definitions, click ? in the interface.

Task

- 1 Open the New Task dialog box.
 - a Select **Menu** | **Policy** | **Client Task Catalog**.
 - b Under Client Task Types, select a product.
 - c Click **New Task**.
- 2 Verify 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 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 Select a package type, then click **Save**.



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.

- 6 Click **Menu** | **Systems** | **System Tree** | **Systems**, then select the system on which you want to deploy the product update, then click **Actions** | **Agent** | **Modify Tasks on a single system**.
- 7 Click **Actions** | **New Client Task Assignment**.
- 8 On the Select Task page, make the following selections:
 - **Product** — Select **McAfee Agent**.
 - **Task Type** — Select **Product Update**.

Then select the task you created for deploying the product update.

- 9 Next to Tags, select the platforms you are deploying the packages to, then click **Next**:
 - **Send this task to all computers**
 - **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.



To limit the list to specific tags, type the tag name in the text box under Tags.

- 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.

Evaluate new DATs and engines before distribution

You might want to test DAT and engine files on a few systems before deploying them to your entire organization. You can test update packages using the Evaluation branch of your Master Repository.

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.
- 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 McAfee Agent calls in to the server. The next time the agent updates, it retrieves them from the Evaluation branch.

- 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.

- 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.

Manage client tasks

Create and maintain client tasks.

Tasks

- [Create client tasks on page 218](#)
Use client tasks to automatically perform product updates. The process is similar for all client tasks.
- [Edit client tasks on page 219](#)
You can edit any previously configured client task settings or schedule information.
- [Delete client tasks on page 219](#)
You can delete any previously configured client tasks.
- [Compare client tasks on page 220](#)
Compare like client tasks using the **Client Task Comparison** tool. This allows you to determine which settings are different and which are the same.

Create client tasks

Use client tasks to automatically perform product updates. The process is similar for all client tasks.

In some cases, you must create a new client task assignment to associate a client task to a System Tree group.

For option definitions, click ? in the interface.

Task

- 1 Open the New Task dialog box.
 - a Select **Menu | Policy | Client Task Catalog**.
 - b Under Client Task Types, select a product.
 - c Click **New Task**.
- 2 Select a task type from the list, then click **OK**.

The Client Task Builder opens.
- 3 Type a name for the task, add a description, then configure the settings specific to the task type you are creating.



The configuration options change depending on the task type selected.

- 4 Review the task settings, then click **Save**.

The task is added to the list of client tasks for the selected client task type.

Edit client tasks

You can edit any previously configured client task settings or schedule information.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Client Task Catalog** and the Client Task Catalog dialog box appears.
- 2 Select the Client Task Type from the navigation tree on the left and the available client tasks appear in the window on the right.
- 3 Double-click the client task name and it appears in the Client Task Catalog dialog box.
- 4 Edit the task settings as needed, then click **Save**.

The managed systems receive these changes the next time the agents communicate with the server.

Delete client tasks

You can delete any previously configured client tasks.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Policy | Client Task Catalog** and the **Client Task Catalog** dialog box appears.
- 2 Select the **Client Task Type** from the navigation tree on the left and the available client tasks appear in the window on the right.
- 3 From the **Actions** column, click **Delete** next to the client task.
- 4 Click **OK**.

Compare client tasks

Compare like client tasks using the **Client Task Comparison** tool. This allows you to determine which settings are different and which are the same.

Many of the values and variables included on this page are specific to each product. For option definitions not included in the table, see the product documentation for the product that provides the Client Task you want to compare.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Client Task Comparison**, then select a **Product**, **Client Task Type**, and **Show** settings from the lists.

These settings populate the client tasks to compare in the **Client Task 1** and **Client Task 2** lists.

- 2 Select the client tasks to compare in the **Compare Client Tasks** row from the **Client Task 1** and the **Client Task 2** column lists.

The top two rows of the table display the number of settings that are different and identical. To reduce the amount of data that is displayed, you can also change the **Show** setting from **All Client Task Settings**, to **Client Task Differences** and **Client Task Matches**.

- 3 Click **Print** to open a printer-friendly view of this comparison.

18 Server tasks

Server tasks are configurable actions that run on McAfee ePO at scheduled times or intervals. Leverage server tasks to automate repetitive tasks.

McAfee ePO includes preconfigured server tasks and actions. Most of the additional software products you manage with McAfee ePO also add preconfigured server tasks.

Contents

- ▶ [Create a server task](#)
- ▶ [Accepted Cron syntax when scheduling a server task](#)
- ▶ [The Server Task Log](#)

Create a server task

Create server tasks to schedule a variety of actions to run on a specified schedule.

If you want McAfee ePO to run certain actions without manual intervention, a server task is the best approach.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.

The Server Tasks Builder opens to the Description page.

- 2 Give the task an appropriate name, and decide whether the task has a Schedule status. Click **Next**.



If you want the task to run automatically, set **Schedule status** to **Enabled**.

The Actions page appears.

- 3 Select and configure the action for the task, then click **Next**.

The Schedule page appears.

- 4 Choose the Schedule type (the frequency), Start date, End date, and Schedule time to run the task. Click **Next**.



The schedule information will only be used if you enable **Schedule status**.

The Summary page appears.

- 5 Click **Save** to save the server task.

The new task appears in the Server Tasks list.

Accepted Cron syntax when scheduling a server task

If you select the **Advanced** option when scheduling a server task, you can specify a schedule using Cron syntax.

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.

Field Name	Allowed Values	Allowed Special Characters
Seconds	0-59	, - * /
Minutes	0-59	, - * /
Hours	0-23	, - * /
Day of Month	1-31	, - * ? / L W C
Month	1-12, or JAN - DEC	, - * /
Day of Week	1-7, or SUN - SAT	, - * ? / L C #
Year (optional)	Empty, or 1970-2099	, - * /

Allowed special characters

- Commas (,) are allowed to specify more 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 Server Task Log

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 include details about:

- The success or failure of the task
- Any subtasks run when performing the scheduled task

You can also cancel a task that is in progress.

View server task information in the server task log

Examine the server task log for information about your server tasks. The server task log provides the status of the task and any errors that might have occurred.

- Access information about server tasks: click **Menu | Automation | Server Task Log**.

The following task information is displayed:

- 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 about any new packages that are being checked in to the master repository
- Status of task at each site (when expanded)
- Any errors or warnings, their codes, and the site to which they apply

Manage the Server Task Log

Open the Server Task Log to view, filter, and purge the task logs as needed.

The status of each server task appears in the **Status** column:

- **Waiting** — Task is waiting for another task to finish.
- **In Progress** — Task has started but not finished.
- **Paused** — Task was paused by a Server Task action.
- **Stopped** — Task was stopped by a Server Task action.
- **Failed** — Task was started but did not complete successfully.
- **Completed** — Task completed successfully.
- **Pending Termination** — A termination request has been sent.
- **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 Select one of these actions.

Action	Steps
View the server task log	<ol style="list-style-type: none"> 1 Click any of the column titles to sort the events. 2 Select any of the task logs, click Actions, then select one of the following to modify the server task log: <ul style="list-style-type: none"> • 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 which task log entries to delete, then click OK. • Terminate Task — Stop a task that is in progress.
Filter the server task log	Select a filter from the Filter drop-down list.
Purge the server task log	<ol style="list-style-type: none"> 1 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.

19 Managing SQL databases

Back up and restore, maintain, and manage your SQL Server databases.

Contents

- ▶ *Maintaining SQL databases*
- ▶ *Use a remote command to determine the Microsoft SQL database server and name*
- ▶ *Configure a snapshot and restore the SQL database*
- ▶ *Use a remote command to determine the Microsoft SQL database server and name*
- ▶ *Use Microsoft SQL Server Management Studio to find McAfee ePO server information*
- ▶ *The Threat Event Log*

Maintaining SQL databases

Your ePolicy Orchestrator databases require regular maintenance to promote optimal performance and to protect your data.

Use the Microsoft management tool appropriate for your version of SQL:

SQL version	Management tool
SQL 2008 and 2012	SQL Server Management Studio
SQL Express	SQL Server Management Studio Express

Depending on your deployment of the ePolicy Orchestrator software, plan on spending a few hours each week on regular database backups and maintenance. Perform these tasks regularly, either weekly or daily. However, these tasks are not the only maintenance tasks available. See your SQL documentation for details on what else you can do to maintain your database.

Use a remote command to determine the Microsoft SQL database server and name

The following ePolicy Orchestrator remote command is used to determine the Microsoft SQL database server and database name.

Task

For option definitions, click ? in the interface.

- 1 Type this remote command in your browser address bar:

```
https://localhost:8443/core/config
```

In this command:

- `localhost` — Is the name of your McAfee ePO server.
- `:8443` — Is the default McAfee ePO server port number. Your server might be configured to use a different port number.

2 Save the following information that appears in the **Configure Database Settings** page:

- Host name or IP address
- Database name

Configure a snapshot and restore the SQL database

To quickly reinstall a McAfee ePO server, configure a Disaster Recovery snapshot to save, or confirm a snapshot is being saved to the SQL database. Then back up that SQL database, which includes the snapshot, and copy the database backup file to a restore SQL Server.

A quick reinstallation of the McAfee ePO server requires these tasks.

Tasks

- [Configure Disaster Recovery Server Task on page 226](#)
Use the Disaster Recovery Snapshot Server Task to modify the scheduled automatic Snapshots of your McAfee ePO server configuration saved to the SQL database.
- [Use Microsoft SQL to backup and restore database on page 227](#)
To save the disaster recovery snapshot with the McAfee ePO server configuration information, use Microsoft SQL Server procedures.

Configure Disaster Recovery Server Task

Use the Disaster Recovery Snapshot Server Task to modify the scheduled automatic Snapshots of your McAfee ePO server configuration saved to the SQL database.

The preconfigured status of your Disaster Recovery Server Snapshot Task depends on the SQL database your McAfee ePO server uses. Disaster Recovery Snapshot is enabled, by default, on all Microsoft SQL Servers except the Express Edition.



McAfee does not recommend enabling Disaster Recovery Snapshot scheduling with the Microsoft SQL Server Express Editions because of the data file size limitations. The maximum data file size for Microsoft SQL Server 2005 Express Edition is only 4 GB and 10 GB for Microsoft SQL Server 2008 and 2012 Express Editions.

You can only run one Disaster Recovery Snapshot at a time. If you run multiple Snapshots, only the last Snapshot creates any output and the previous Snapshots are overwritten.

You can modify the default Disaster Recovery Server Task as needed.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Server Tasks**, select **Disaster Recovery Snapshot Server** from the Server Tasks list, and click **Edit**.
The Disaster Recovery Server Task wizard appears.
- 2 From the **Descriptions** tab **Schedule status**, click **Enabled** or **Disabled** as needed.

- From the **Schedule** tab, change the following settings as needed:
 - Schedule type** — Set the frequency when the Snapshot is saved.
 - Start Date** and **End Date** — Set the start and end dates the Snapshots are saved, or click **No End Date** to have the task run continuously.
 - Schedule** — Set the time when the Snapshot is saved. By default, the Snapshot task runs at 1:59 a.m. daily.



McAfee recommends that you run the Disaster Recovery Server Task during off hours to minimize the changes to the database during the Snapshot creation process.

- From the **Summary** tab, confirm the server task is configured correctly and click **Save**.

Use Microsoft SQL to backup and restore database

To save the disaster recovery snapshot with the McAfee ePO server configuration information, use Microsoft SQL Server procedures.

Before you begin

To complete this task you must have connectivity and authorization to copy files between your primary and restore McAfee ePO SQL servers. See *Appendix A: Maintaining ePolicy Orchestrator Databases* for details.

After you create a snapshot of the McAfee ePO server configuration, you must:

Task

- Create a Microsoft SQL Server backup of the database using:
 - Microsoft SQL Server Management Studio
 - Microsoft Transact-SQLSee your Microsoft SQL Server documentation for details to complete these processes.
- Copy the backup file created to your restore SQL server.
- Restore the backup of the primary SQL database that includes the disaster recovery snapshot records using:
 - Microsoft SQL Server Management Studio
 - Microsoft Transact-SQL

See your Microsoft SQL Server documentation for details to complete these processes.

This creates a duplicate SQL server ready for restoration, if needed, by connecting it to a new ePolicy Orchestrator software installation using the **Restore** option.

Use a remote command to determine the Microsoft SQL database server and name

The following ePolicy Orchestrator remote command is used to determine the Microsoft SQL database server and database name.

Task

For option definitions, click ? in the interface.

- 1 Type this remote command in your browser address bar:

`https://localhost:8443/core/config`

In this command:

- `localhost` — Is the name of your McAfee ePO server.
 - `:8443` — Is the default McAfee ePO server port number. Your server might be configured to use a different port number.
- 2 Save the following information that appears in the **Configure Database Settings** page:
 - Host name or IP address
 - Database name

Use Microsoft SQL Server Management Studio to find McAfee ePO server information

From the Microsoft SQL Server Management Studio, determine your existing McAfee ePO server information.

Task

- 1 Use a Remote Desktop Connection to log on to the host name or IP address of the Microsoft SQL database server.
- 2 Open the Microsoft SQL Server Management Studio and connect to the SQL server.
- 3 From the **Object Explorer** list, click **<Database Server Name> | Databases | <Database name> | Tables**.
- 4 Scroll down to find the **EPOServerInfo** table, right-click the table name and select **Edit top 200 Rows** from the list.
- 5 Find and save the information in these database records.
 - **ePOVersion** — For example, 5.1.0
 - **LastKnownTCPIP** — For example, 172.10.10.10
 - **DNSName** — For example, epo-2k8-epo51.server.com
 - **RmdSecureHttpPort** — For example, 8443
 - **ComputerName** — For example, EPO-2K8-EPO51

Make sure you have this information in case you ever need to restore your ePolicy Orchestrator software.

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.
- **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.
- **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.
- **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.

View and purge the Threat Event Log

You should periodically view and purge your threat events.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Threat Event Log**.
- 2 Select one of these actions.

Action	Steps
View Threat Event Log.	<ol style="list-style-type: none"> 1 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. 2 From the Available Columns list, select different table columns that meet your needs, then click Save. 3 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.
Purge Threat Events.	<ol style="list-style-type: none"> 1 Click Actions Purge. 2 In the Purge dialog box, next to Purge records older than, type a number and select a time unit. 3 Click OK. <p>Records older than the specified age are deleted permanently.</p>

Schedule purging the Threat Event Log

You can create a server task to automatically purge the Threat Event Log.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **New Task**.
- 2 Name and describe the task. Next to **Schedule Status**, select **Enabled**, then click **Next**.
- 3 Select **Purge Threat Event Log** from the drop-down list.
- 4 Select whether to purge by age or from a queries result. If you purge by query, you must pick a query that results in a table of events.
- 5 Click **Next**.

- 6 Schedule the task as needed, then click **Next**.
- 7 Review the task's details, then click **Save**.

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 20 *Dashboards and monitors*
 - Chapter 21 *Queries and reports*
 - Chapter 22 *Events and responses*
 - Chapter 23 *Issues*
 - Chapter 24 *Disaster Recovery*

20 Dashboards and monitors

Dashboards help you keep constant watch on your environment.

Dashboards are collections of monitors. Monitors condense information about your environment into easily understood graphs and charts. Usually, related monitors are grouped together on a specific dashboard. For example, the Threat Events dashboard contains four monitors that display information about threats to your network.

You must have the right permissions to view or modify dashboards and monitors.

Contents

- ▶ *Using dashboards and monitors*
- ▶ *Manage dashboards*
- ▶ *Export and import dashboards*
- ▶ *Manage dashboard monitors*
- ▶ *Move and resize dashboard monitors*
- ▶ *Default dashboards and their monitors*
- ▶ *Specify first-time dashboards and dashboard refresh intervals*

Using dashboards and monitors

Customize your dashboards and monitors so you get the information you need for your role and environment.

The McAfee ePO console has a default dashboard that appears the first time you log on. The next time you log on, the Dashboards page displays the last dashboard you used.

If you have deleted all the default dashboards, when you start McAfee ePO, this text appears in the middle of the dashboards page: No dashboards are configured. Create a new dashboard or import an existing dashboard. To create or import a dashboard, see either *Manage dashboards* or *Export and import dashboards*.

You can switch dashboards by selecting a different dashboard from the drop-down menu. There are three different kinds of dashboards you can choose from.

- 1 **McAfee Dashboards** — McAfee dashboards are not editable, and can be viewed by all users. You can duplicate a McAfee Dashboard as a starting point for your own customized dashboards.
- 2 **Public Dashboards** — Public dashboards are user-created dashboards that are shared across users.
- 3 **Private Dashboards** — These are the dashboards you've created for your own use. Private dashboards are not shared across users.

When you create a private or public dashboard, you can drag and drop the monitors you want from the Monitor Gallery to the new dashboard.

See also[Manage dashboards on page 236](#)[Manage dashboard monitors on page 238](#)

Manage dashboards

Create, edit, duplicate, delete, and assign permissions to dashboards.

Before you begin

You must have the correct permissions to modify a dashboard.




The default dashboards and predefined queries, shipped with ePolicy Orchestrator, cannot be modified or deleted. To change them, duplicate, rename, and modify the renamed dashboard or query.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Reporting | Dashboards**, to navigate to the **Dashboards** page.
- 2 Select one of these actions.

Action	Steps
Create a dashboard	<p>To create a different view on your environment, create a new dashboard.</p> <ol style="list-style-type: none"> 1 Click Dashboard Actions New. 2 Type a name, select a dashboard visibility option, and click OK. <p>A new blank dashboard is displayed. You can add monitors to the new dashboard as needed.</p>
Edit and assign permissions to a dashboard	<p>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.</p> <ol style="list-style-type: none"> 1 Click Dashboard Actions Edit. 2 Select a permission: <ul style="list-style-type: none"> • Do not share this dashboard • Share this dashboard with everyone • Share this dashboard with the following permission sets <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  With this option, you must also choose one or more permission sets. </div> 3 Click OK to change the dashboard. <p>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.</p>

Action	Steps
Duplicate a dashboard	<p>Sometimes the easiest way to create a new dashboard is to copy an existing one that's close to what you want.</p> <ol style="list-style-type: none">1 Click Dashboard Actions Duplicate.2 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 now opens. <p>The duplicate is an exact copy of the original dashboard including all permissions. Only the name is changed.</p>
Delete a dashboard	<ol style="list-style-type: none">1 Click Dashboard Actions Delete.2 Click OK to delete the dashboard. <p>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.</p>

See also

[Using dashboards and monitors on page 235](#)

Export and import dashboards

Once you have fully defined your dashboard and monitors, the fastest way to migrate them to other McAfee ePO servers is to export them and import them onto the other servers.

Before you begin

To import a dashboard, you must have access to a previously exported dashboard contained in an XML file.

A dashboard exported as an XML file can be imported to the same or a different system.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu** | **Reporting** | **Dashboards**.
- 2 Select one of these actions.

Action	Steps
Export dashboard	<ol style="list-style-type: none"> 1 Click Dashboard Actions Export. Your browser attempts to download an XML file according to your browser settings. 2 Save the exported XML file to an appropriate location.
Import dashboard	<ol style="list-style-type: none"> 1 Click Dashboard Actions Import. The Import Dashboard dialog box appears. 2 Click Browse and select the XML file containing an exported dashboard. Click Open. 3 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. 4 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.

Manage dashboard monitors

You can create, add, and remove monitors from dashboards.

Before you begin


You must have write permissions for the dashboard you are modifying.

If you lack the necessary rights or product licenses to view a monitor, or if the underlying query for the monitor is no longer available, you will see a message telling you so in place of the monitor.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu** | **Reporting** | **Dashboards**. Select a dashboard from the **Dashboard** drop-down list.
- 2 Select one of these actions.

Action	Steps
Add a monitor	<ol style="list-style-type: none"> 1 Click Add Monitor. The Monitor Gallery appears at the top of the screen. 2 Select a monitor category from the View drop-down list. The available monitors in that category appear in the gallery. 3 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. 4 Configure the monitor as needed (each monitor has its own set of configuration options), then click OK. 5 After you have added monitors to this dashboard, click Save Changes to save the newly configured dashboard. 6 When you have completed your changes, click Close. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  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. </div>
Edit a monitor	<p>Every monitor type supports different configuration options. For example, a query monitor allows the query, database, and refresh interval to be changed.</p> <ol style="list-style-type: none"> 1 Choose a monitor to manage, click the arrow in its top-left corner, and select Edit Monitor. The monitor's configuration dialog appears. 2 When you have completed modifying the monitor's settings, click OK. If you decide to not make changes, click Cancel. 3 If you decide to keep the resulting changes to the dashboard, click Save, otherwise click Discard.
Remove a monitor	<ol style="list-style-type: none"> 1 Choose a monitor to remove, click the arrow in its top-left corner, and select Remove Monitor. The monitor's configuration dialog appears. 2 When you are finished modifying the dashboard, click Save Changes. To revert the dashboard to its prior state, click Discard Changes.

See also

Using dashboards and monitors on page 235

Move and resize 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.

Task

For option definitions, click ? in the interface.

- 1 Move or resize a monitor:
 - To move a dashboard monitor:
 - 1 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.
 - 2 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:
 - 1 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.
 - 2 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.
- 2 Click **Save Changes**. To revert to the prior configuration, click **Discard Changes**.

Default dashboards and their monitors

ePolicy Orchestrator comes 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 administrator who installed McAfee ePO. The administrator who performed the installation must change the permissions on additional dashboards before other McAfee ePO users can view them.

Similarly, some monitors within a dashboard can require additional permissions to 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:

- **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 high-level reports on security threats, with links to more specific product McAfee information. The monitors included in this dashboard are:

- **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.

Getting Started with ePolicy Orchestrator dashboard

The Getting Started with ePolicy Orchestrator dashboard is a set of monitors where you can learn about McAfee ePO and create the product software installation URL. By default, the Getting Started with ePolicy Orchestrator dashboard is the one users see when they first log on to McAfee ePO. The monitors included in this dashboard are:

- **Welcome to ePolicy Orchestrator** — Displays a slide show to familiarize yourself with the software and how it works.
- **Getting Started** — Displays the list of products you can install on your managed computers.

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 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.

Specify first-time dashboards and dashboard refresh intervals

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

You can specify which dashboard a user sees when they log on for the first time by mapping the dashboard 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 perform the following actions:

- 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 affect available bandwidth. We recommend that you choose a refresh interval that is frequent enough to ensure accurate and timely information is displayed without consuming undue network resources. The default interval is five minutes.

For option definitions, click ? in the interface.

Task

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**.

21

Queries and reports

ePolicy Orchestrator comes with its own querying and reporting capabilities.

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

Contents

- ▶ *Query and report permissions*
- ▶ *About queries*
- ▶ *Query Builder*
- ▶ *Configuring queries and reports for the first time*
- ▶ *Work with queries*
- ▶ *Multi-server rollup querying*
- ▶ *About reports*
- ▶ *Structure of a report*
- ▶ *Work with reports*

Query and report permissions

Restrict access to queries and reports in a number of ways.

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 various 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.



The default dashboards and predefined queries, shipped with ePolicy Orchestrator, cannot be modified or deleted. To change them, duplicate, rename, and modify the renamed dashboard or query.

Query results are actionable

Query results are actionable. Query results displayed in tables (and drill-down tables) have various 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 these 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 webpage.
- **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.



Tables do not include drill-down tables.

Chart types include:

Table 21-1 Chart Type Groups

Type	Chart or Table
Bar	<ul style="list-style-type: none"> • Bar Chart • Grouped Bar Chart • Stacked Bar Chart
Pie	<ul style="list-style-type: none"> • Boolean Pie Chart • Pie Chart
Bubble	<ul style="list-style-type: none"> • Bubble Chart
Summary	<ul style="list-style-type: none"> • Multi-group Summary Table • Single Group Summary Table

Table 21-1 Chart Type Groups *(continued)*

Type	Chart or Table
Line	<ul style="list-style-type: none"> • Multi-line Chart • Single Line Chart
List	<ul style="list-style-type: none"> • Table

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.

Configuring queries and reports for the first time

Follow these high-level steps when configuring 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.

Work with queries

Queries can be run, exported, and more depending on your needs.

Tasks

- [Manage custom queries on page 247](#)
You can create, duplicate, edit, and delete queries as needed.
- [Run a query on page 248](#)
You can run saved queries on-demand.
- [Run a query on a schedule on page 248](#)
A server task is used to run a query on a regular basis. Queries can have sub-actions that allow you to perform a variety of tasks, such as emailing the query results or working with tags.
- [Create a query group on page 249](#)
Query groups allow you to save queries or reports without allowing other users access to them.
- [Move a query to a different group on page 249](#)
Change the permissions on a query by moving it to a different group.
- [Export and import queries on page 249](#)
Network information is highly structured. Exporting and importing queries from one server to another makes data retrieval consistent across all McAfee ePO servers.
- [Export query results to other formats on page 250](#)
Query results can be exported to these formats: HTML, PDF, CSV, and XML.




Manage custom queries

You can create, duplicate, edit, and delete queries as needed.

Task

For option definitions, click ? in the interface.

- 1 Open the Queries & Reports page: click **Menu** | **Reporting** | **Queries & Reports**.
- 2 Select one of these actions.

Action	Steps
Create custom query	<ol style="list-style-type: none"> 1 Click New Query, and the Query Builder appears. 2 On the Result Type page, select the Feature Group and Result Type for this query, then click Next. 3 Select the type of chart or table to display the primary results of the query, then click Next. <ul style="list-style-type: none">  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. <ul style="list-style-type: none">  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 action on items in any table or drill-down table. <ul style="list-style-type: none">  Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property. <ul style="list-style-type: none"> • 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 this query 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: <ul style="list-style-type: none"> • New Group — Type the new group name and select either: <ul style="list-style-type: none"> • Private group (My Groups) • Public group (Shared Groups) • Existing Group — Select the group from the list of Shared Groups. 7 Click Save. The new query appears in the Queries list.
Duplicate query	<ol style="list-style-type: none"> 1 From the list, select a query to copy, then click Actions Duplicate. 2 In the Duplicate dialog box, type a name for the duplicate and select a group to receive a copy of the query, then click OK. The duplicated query appears in the Queries list.

Action	Steps
Edit query	<ol style="list-style-type: none"> 1 From the list, select a query to edit, then click Actions Edit. 2 Edit the query settings and click Save when done. <p>The changed query appears in the Queries list.</p>
Delete query	<ol style="list-style-type: none"> 1 From the list, select a query to delete, then click Actions Delete. 2 When the confirmation dialog box appears, click Yes. <p>The query no longer appears in the Queries list. If any reports or server tasks used the query, they now appear as invalid until you remove the reference to the deleted query.</p>

Run a query

You can run saved queries on-demand.

For option definitions, click ? in the interface.

Task

- 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.

Run a query on a schedule

A server task is used to run a query on a regular basis. Queries can have sub-actions that allow you to perform a variety of tasks, such as emailing the query results or working with tags.

Task

For option definitions, click ? in the interface.

- 1 Open the Server Task Builder.
 - a From the Queries and Reports page, select a query.
 - b Select **Actions | Schedule**.
- 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 that you want to run.
- 5 Select the language for displaying the results.
- 6 From the **Sub-Actions** list, select an action to take based on the results. Available sub-actions depend on the permissions of the user, and the products managed by your McAfee ePO server.



You are not limited to selecting one action for the query results. Click the + button to add 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**.

- Schedule the task, then click **Next**.
- 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 when you click **Run** next to the task on the Server Tasks page.

Create 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.

For option definitions, click ? in the interface.

Task

- Click **Menu | Reporting | Queries & Reports**, then click **Group Actions | New Group**.
- In the **New Group** page, type a group name.
- 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.



Administrators have full access to all By permission set and Public queries.

- Click **Save**.

Move a query to a different group

Change the permissions on a query by moving it to a different group.

For option definitions, click ? in the interface.

Task

- Click **Menu | Reporting | Queries & Reports**. In the **Queries** list, select the query you want to move.
- Click **Actions** and select one of the following:
 - Move to Different Group** — Select the group from the **Select target group** menu.
 - Duplicate** — Specify a new name and select the group from the **Group to receive copy** menu.
- Click **OK**.

Export and import queries

Network information is highly structured. Exporting and importing queries from one server to another makes data retrieval consistent across all McAfee ePO servers.

Task

For option definitions, click ? in the interface.

- 1 Open the Queries tab by selecting **Menu | Reporting | Queries & Reports**.
- 2 Select one of these actions.

Action	Steps
Export a query	<ol style="list-style-type: none"> 1 Select the group containing the query that you want to export from the Groups list, then select the query you want to export. 2 Click Actions Export Queries. The McAfee ePO server sends an XML file to your browser. 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.
Import a query	<ol style="list-style-type: none"> 1 Click Import Queries. 2 Click Browse to navigate to and select the XML file containing the dashboard that you want to import. 3 Select a new or existing group for the query. <ul style="list-style-type: none"> • New — Give the name of the group and select whether it is private or public. • Existing — Select the group the imported query will join. 4 Click Save. A confirmation screen displays the information about the query as it exists in the XML file and how it is named after import. If there is no valid query in the selected file, an error message is displayed. 5 Click OK to finalize the import. The newly imported query acquires the permissions of the group where it was imported.

Export query results to other formats

Query results can be exported to these formats: 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.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Reporting | Queries & Reports**, select a query, then click **Run**.
- 2 After the query is run, click **Options | 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 webpage.
 - **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 this 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 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:

- Create a query to define compliance
- Generate a compliance event

Create a Rollup Data server task

Rollup Data server tasks draw data from multiple servers at the same time.

Before you begin

Register each McAfee ePO reporting server that you want to include in rollup reporting. Registering each server 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 to include its summary data in rollup reporting.



You can't roll up data from registered McAfee ePO servers at versions that are no longer supported. For example, you can't aggregate data from McAfee ePO servers at version 4.5 or earlier.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **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**, then 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**, click **Select**. Choose the servers you want data from in the **Select Registered Servers** dialog box, then click **OK**.
- 6 Select the data type to be rolled up, then click **Next**. To select multiple data types, click the + at the end of the table heading.



The data types Threat Events, Client Events, and Applied Policies can be further configured to include the properties Purge, Filter, and Rollup Method. To do so, click **Configure** in the row that describes the available properties.

- 7 Schedule the task, then click **Next**.

The Summary page appears.



If you are reporting on rolled-up compliance history data, make sure 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.

- 8 Review the settings, 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, use, and events, for example — 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 a McAfee ePO 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 queries, drawing 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 by using groups and permission sets in 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

Work with reports

You can create, edit, and manage reports that combine queries and other elements into detailed PDF documents.

These documents can provide a large amount of useful data, but there are some tasks to complete to create a collection of reports that are useful to you.

Tasks

- [Create a report on page 254](#)
You can create reports and store them in McAfee ePO.
- [Edit an existing report on page 255](#)
You can modify an existing report's contents or the order of presentation.
- [View report output on page 259](#)
View the last run version of every report.
- [Group reports together on page 259](#)
Every report must be assigned to a group.
- [Run reports on page 260](#)
Reports must be run before examining their results.
- [Run a report on a schedule on page 260](#)
Create a server task to run a report automatically.
- [Export and import reports on page 261](#)
Reports can contain highly structured information, so exporting and importing them from one server to another makes data retrieval and reporting consistent across all McAfee ePO servers.
- [Configure the template and location for exported reports on page 261](#)
You can define the appearance and storage location for tables and dashboards you export as documents.
- [Delete reports on page 262](#)
You can delete reports that are no longer being used.

Create a report

You can create reports and store them in McAfee ePO.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries & Reports**, then select the **Report** tab.
- 2 Click **New Report**.
- 3 Click **Name, Description and Group**. Name the report, describe it, and select an appropriate group. Click **OK**.

- 4 You can now add, remove, rearrange elements, customize the header and footer, and change the page layout. At any point, click **Run** to check your progress.
- 5 When you are finished, click **Save**.

Edit 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

- [Add elements to a report on page 255](#)
You can add new elements to an existing report.
- [Configure image report elements on page 256](#)
Upload new images and modify the images used within a report.
- [Configure text report elements on page 256](#)
You can insert static text within a report to explain its contents.
- [Configure query table report elements on page 257](#)
Some queries are better displayed as a table when inside a report.
- [Configure query chart report elements on page 257](#)
Some queries are better displayed as a chart when inside a report.
- [Customize report headers and footers on page 258](#)
Headers and footers provide information about the report.
- [Remove elements from a report on page 258](#)
You can remove elements from a report if no longer needed.
- [Reorder elements within a report on page 259](#)
You can change the order in which elements appear within a report.

Add 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 wanted 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**.

Configure image report elements

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.

For option definitions, click ? in the interface.

Task

- 1 To configure an image already in a report, click the arrow at the top left corner of the image. Click **Configure**.

This displays the **Configure Image** page. If you are adding an image to the report, the **Configure Image** page appears immediately after you drop the **Image** element onto the report.

- 2 To use an existing image, select it from the gallery.
- 3 To use a new image, click **Browse** and select the image from your computer. Click **OK**.
- 4 To specify a specific image width, enter it in the **Image Width** field.

By default, the image is displayed in its existing width without resizing unless that width is wider than the available width on the page. In that case, it is resized to the available width keeping aspect ratio intact.

- 5 Select if you want the image aligned left, center, or right.
- 6 Click **OK**.

Configure 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 12 pt 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.

Configure 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 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**.

Configure 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 displays the **Configure Query Chart** page. If you are adding a 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 8 pt type.

- 6 Select the chart image height in pixels.
The default is one-third the page height.
- 7 Click **OK**.

Customize 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.

Remove 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**.

Reorder 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, then 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 appears 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.

View report output

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.

For option definitions, click ? in the interface.

Task

- 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.

A PDF opens within your browser, and your browser behaves as you have configured it for that file type.

Group 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.

For option definitions, click ? in the interface.

Task

- 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 appears in the report list.

Run 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.

Run a report on a schedule

Create a server task to run a report automatically.

If you want a report to be run without manual intervention, a server task is the best approach. This task creates a server task allowing for automatic, scheduled runs of a given report.

Task

For option definitions, click ? in the interface.

- 1 Open the Server Task Builder.
 - a On the Queries and Reports page, select a report.
 - b Select **Actions | Schedule**.
- 2 Name the task, describe it, and assign a schedule status, then click **Next**.

If you want the task to be run automatically, set the **Schedule status** to **Enabled**.

- 3 From the **Actions** drop-down list, select **Run Report**. Select the report to run and the target language, then click **Next**.
- 4 Choose a schedule type (frequency), dates, and time to run the report, then click **Next**.
The schedule information is used only if you enable **Schedule status**.
- 5 Click **Save** to save the server task.

The new task now appears in the **Server Tasks** list.

Export and import reports

Reports can contain highly structured information, so exporting and importing them from one server to another makes data retrieval and reporting consistent across all McAfee ePO servers.

Task

For option definitions, click ? in the interface.

- 1 Open the **Reports** page: select **Menu | Reporting | Queries & Reports**, then select the **Reports** tab.
- 2 Select one of these actions.

Action	Steps
Export a report	<ol style="list-style-type: none"> 1 Select the group that contains the report that you want to export from the Groups list. 2 Select the report that you want to export, then click Actions Export Reports. The McAfee ePO server sends an XML file to your browser. 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, and graphics.
Import a report	<ol style="list-style-type: none"> 1 From the Report page, click Import Reports. 2 Click Browse to navigate to and select the XML file containing the report that you want to import. 3 Select a new or existing group for the report. <ul style="list-style-type: none"> • New — Give the name of the group and select whether it is private or public. • Existing — Select the group the imported report will join. 4 Click OK. 5 Click Import to finalize the import. The newly imported report acquires the permissions of the group where it was imported.

Configure 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, and so on.
- 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 to save exported documents.
- 7 Click **Save**.

Delete 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.

22 Events and responses

Configure your McAfee ePO server to trigger an action in response to threat, client, or server events.

Contents

- ▶ *Using automatic responses*
- ▶ *Throttling, aggregation, and grouping*
- ▶ *Default rules*
- ▶ *Response planning*
- ▶ *Configuring responses for the first time*
- ▶ *Determine how events are forwarded*
- ▶ *Configure Automatic Responses*
- ▶ *Determine which events are forwarded to the server*
- ▶ *Choose a notification event interval*
- ▶ *Create and edit Automatic Response rules*
- ▶ *Event and response questions*

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 McAfee ePO 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 conditions 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 McAfee ePO server events. For example, a repository update or a replication task failed.

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

Enable the default ePolicy Orchestrator rules 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.

Table 22-1 Default notification rules

Rule name	Associated events	Configurations
Distributed repository update or replication failed	Distributed repository update or replication failed	Sends a notification message when any update or replication fails.
Malware detected	Any events from any unknown products	Sends a notification message: <ul style="list-style-type: none"> • When the number of events is at least 1,000 within an hour. • At most, once every two hours. • With the source system IP address, actual threat names, and actual product information, if available, and many other parameters. • When the number of selected distinct value is 500.
Master repository update or replication failed	Master repository update or replication failed	Sends a notification message when any update or replication fails.
Non-compliant computer detected	Non-Compliant Computer Detected events	Sends a notification message when any events are received from the Generate Compliance Event server task.

Response planning

Before creating rules that send notifications, save time by planning.

Make sure you have a plan in place for the following items.

- 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.

Configuring responses for the first time

Follow these high-level steps when you are configuring events and automatic responses 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.
 - **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.

Determine how events are forwarded

Determine when events are forwarded and which events are forwarded immediately.

The server receives event notifications from agents. You can configure McAfee Agent policies to forward events either immediately to the server or only at agent-server communication intervals.

If you choose to send events immediately (as set by default), the McAfee 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 McAfee 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

- [Determine which events are forwarded immediately on page 266](#)
Determine whether events are forwarded immediately or only during agent-server communication.
- [Determine which events are forwarded on page 267](#)
Use the **Server Settings** page to determine which events are forwarded to the server.

Determine which events are forwarded immediately

Determine whether events are forwarded immediately or only during agent-server communication.

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 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**.

Determine which events are forwarded

Use the **Server Settings** page 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 events, then click **Save**.

These settings take effect once all agents have called in.

Configure Automatic Responses

Configure the necessary resources to fully leverage Automatic Responses.

Tasks

- [Assign permissions to notifications on page 267](#)
Notifications permissions enable users to view, create, and edit registered executables.
- [Assign permissions to Automatic Responses on page 268](#)
Responses permissions enable users to create response rules for different event types and groups.
- [Manage SNMP servers on page 268](#)
Configure responses to use your SNMP (Simple Network Management Protocol) server.
- [Manage registered executables and external commands on page 270](#)
The registered executables you configure are run when the conditions of a rule are met.
Automatic responses trigger the registered executable commands to run.

Assign permissions to notifications

Notifications permissions enable users to view, create, and edit registered executables.
For option definitions, click ? in the interface.


Task

- 1 Click **Menu | User Management | Permission Sets**, then either create a permission set or select an existing one.
- 2 Next to **Event Notifications**, click **Edit**.
- 3 Select the notifications permission you want:
 - **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 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 notifications permissions you want, then click **Save**.

Assign permissions to Automatic Responses

Responses permissions enable users to create response rules for different event types and groups.

 Users need permissions for the following features to create a response rule.

- Threat Event Log
- System Tree
- Server Tasks
- Detected Systems

For option definitions, click ? in the interface.


Task

- 1 Click **Menu | User Management | Permission Sets**, then create a permission set or select an existing one.
- 2 Next to **Automatic Response**, click **Edit**.
- 3 Select an **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 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 **Automatic Response** permissions you want, then click **Save**.

Manage SNMP servers

Configure responses to use your SNMP (Simple Network Management Protocol) server.

You can configure responses to send SNMP 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

- [Edit SNMP servers on page 269](#)
Edit existing SNMP server entries.
- [Delete an SNMP server on page 269](#)
Delete an SNMP server from the **Registered Servers** list.

Edit SNMP servers

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 servers, select an SNMP server, then click **Actions | Edit**.
- 3 Edit the server information as needed, then click **Save**.

Delete an SNMP server

Delete an SNMP server from the **Registered Servers** list.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Configuration | Registered Servers**.
- 2 From the list of registered servers, select an SNMP server, then click **Actions | Delete**.
- 3 When prompted, click **Yes**.

The SNMP server is removed from the **Registered Servers** list.

Import .MIB files

Import .mib files before you set up rules to send notification messages to an SNMP server using 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.
- **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.

Manage registered executables and external commands

The registered executables you configure are run when the conditions of a rule are met. Automatic responses trigger the registered executable commands to run.



You can run registered executable commands only on console applications.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Configuration | Registered Executables**.
- 2 Select one of these actions.

Action	Steps
Add a registered executable	<ol style="list-style-type: none"> 1 Click Actions Registered Executable . 2 Type a name for the registered executable. 3 Type the path and select the registered executable that you want a rule to execute when triggered. 4 Modify the user credentials, if needed. 5 Test the executable and confirm it worked using the Audit Log. 6 Click Save. <p>The new registered executable appears in the Registered Executables list.</p>
Edit a registered executable.	<ol style="list-style-type: none"> 1 Find the registered executable to edit in the Registered Executable page, then click Edit. 2 Change the information as needed and click Save.
Duplicate a registered executable.	<ol style="list-style-type: none"> 1 Find the registered executable to duplicate in the Registered Executable page, then click Duplicate. 2 Type a name for the registered executable, then click OK. <p>The duplicated registered executable appears in the Registered Executables list.</p>
Delete a registered executable.	<ol style="list-style-type: none"> 1 Find the registered executable to delete in the Registered Executable page, then click Delete. 2 When prompted, click OK. <p>The deleted registered executable no longer appears in the Registered Executables list.</p>

Determine which events are forwarded to the server

You can determine which events are forwarded to the server using server settings and event filtering.

Before you begin



These settings impact 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.

Choose a notification event interval

This setting determines how often ePO notification events are sent to the Automatic Response system.

There are three types of 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.

For option definitions, click ? in the interface.

Task

- 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**.

Create and edit Automatic Response rules

Define when and how a response can be taken on an event occurring at the server or at a managed system.



Automatic Response rules do not have a dependency order.

Tasks

- [Describe a rule on page 272](#)
When creating a new rule, you can add a description, specify the language, specify the event type and group that triggers the response, and enable or disable the rule.
- [Set filters for the rule on page 272](#)
Set the filters for the response rule on the **Filters** page of the **Response Builder** wizard.
- [Set thresholds for the rule on page 272](#)
Define when the event triggers the rule on the **Aggregation** page of the **Response Builder** wizard.
- [Configure the action for Automatic Response rules on page 273](#)
Configure the responses that are triggered by the rule on the **Responses** page of the **Response Builder** wizard.

Describe a rule

When creating a new rule, you can add a description, specify the language, specify the event type and group that triggers the response, and 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.
- 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 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**.

Set filters for the rule

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 a 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**.

Set thresholds for the rule

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.



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**.

Configure the action for Automatic Response rules


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 definitions, 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 an 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**
-  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 **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.

Event and response 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. ePolicy Orchestrator notifications support any combination of the following notification targets for each rule:

- Email (including standard SMTP, SMS, and text pager)
- SNMP servers (using SNMP traps)
- Any external tool installed on the McAfee ePO server
- Issues
- Scheduled server tasks

23 Issues

Issues are action items that can be prioritized, assigned, and tracked.

Contents

- ▶ [Issues and how they work](#)
- ▶ [Work with issues](#)
- ▶ [Purge closed issues](#)

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.

Work with issues

You can create, assign, view details of, edit, delete, and purge issues.

Tasks

- [Create basic issues manually on page 277](#)
Basic issues can be created manually. Non-basic issues must be created automatically.
- [Configure responses to automatically create issues on page 278](#)
Use responses to automatically create issues when certain events occur.
- [Manage issues on page 279](#)
You can add comments, assign, delete, edit, and view details of issues.

Create 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.

Use this...	To do this...
Name	Type a meaningful name for the issue.
Description	Type a meaningful description of the issue.
State	Assign a state to the issue: <ul style="list-style-type: none"> • Unknown • New • Assign • Resolved • Closed
Priority	Assign a priority to the issue: <ul style="list-style-type: none"> • Unknown • Lowest • Low • Medium • High • Highest
Severity	Assign a severity to the issue: <ul style="list-style-type: none"> • Unknown • Lowest • Low • Medium • High • Highest
Resolution	Assign a resolution to the issue. The issue resolution can be assigned once the issue is processed: <ul style="list-style-type: none"> • 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**.

Configure responses to automatically create issues

Use responses to automatically create issues when certain events occur.

Task

For option definitions, click ? in the interface.

- 1 Open the Response Builder.
 - a Select **Menu | Automation | Automatic Responses**.
 - b Click **New Response**.
- 2 Complete the fields, then click **Next**.
- 3 Select properties to narrow the events that trigger the response, then click **Next**.
- 4 Specify these additional details, then click **Next**.
 - The frequency of events required to generate a response.
 - A method to group events.
 - The maximum time period that you want this response to occur.
- 5 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.
- 6 Type a name and description for the issue. Optionally, select one or more variables for the name and description.
This feature provides a number of variables providing information to help fix the issue.
- 7 Type or select any additional options for the response, then click **Next**.
- 8 Review the details for the response, then click **Save**.

Manage issues

You can add comments, assign, delete, edit, and view details of issues.
For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Automation | Issues**.
- 2 Perform the tasks that you want.

Option	Definition
Adding comments to issues	<ol style="list-style-type: none"> 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.
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.
Deleting issues	<ol style="list-style-type: none"> 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.

Option	Definition
Editing issues	<ol style="list-style-type: none"> 1 Select the checkbox next to an issue, then click Edit. 2 Edit the issue as needed. 3 Click Save.
Exporting the list of issues	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).
Viewing issue details	<p>Click an issue.</p> <p>The Issue Details page appears. This page shows all of the settings for the issue as well as the Issues Activity Log.</p>

Purge closed issues

You can purge closed issues from the database to delete them permanently.

Tasks

- [Purge closed issues manually on page 280](#)
Periodically purging closed issues from the database keeps it from getting too full.
- [Purge closed issues on a schedule on page 280](#)
You can schedule a task to periodically purge the database of closed issues. Purging closed issues keeps the database smaller.

Purge 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.



This function affects all closed issues; not just those in the current view.

Purge closed issues on a schedule

You can schedule a task to periodically purge the database of closed issues. Purging closed issues keeps the database smaller.

Task

For option definitions, click ? in the interface.

- 1 Open the **Server Task Builder**.
 - a Select **Menu | Automation | Server Tasks**.
 - b Click **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**.
- 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.

24 Disaster Recovery

Disaster Recovery helps you quickly recover, or reinstall your ePolicy Orchestrator software. **Disaster Recovery** uses a Snapshot feature that periodically saves your ePolicy Orchestrator configuration, extensions, keys, and more to Snapshot records in the ePolicy Orchestrator database.

Contents

- ▶ *What is Disaster Recovery*
- ▶ *Disaster Recovery components*
- ▶ *How Disaster Recovery works*
- ▶ *Create Snapshot*
- ▶ *Configure Disaster Recovery server settings*

What is Disaster Recovery

The ePolicy Orchestrator Disaster Recovery feature uses a Snapshot process to save specific McAfee ePO server database records to the ePolicy Orchestrator Microsoft SQL database.

The records saved by the Snapshot contain the entire ePolicy Orchestrator configuration at the specific time the Snapshot is taken. Once the Snapshot records are saved to the database, you can use the Microsoft SQL backup feature to save the entire ePolicy Orchestrator database and restore it to another SQL server for an ePolicy Orchestrator restore.

Restore SQL database connection examples

Using the restored ePolicy Orchestrator SQL database server, that includes the Disaster Recovery Snapshot, you can connect it to:

- Restored McAfee ePO server hardware with the original server name and IP address — This allows you to recover from, for example, a failed ePolicy Orchestrator software upgrade.
- New McAfee ePO server hardware with the original server name and IP address — This allows you to upgrade, or restore, your server hardware and quickly resume managing your network systems.
- New McAfee ePO server hardware with a new server name and IP address — This allows you to, for example, move your server from one domain to another.



This example can provide a temporary network management solution while you rebuild and reinstall your McAfee ePO server hardware and software back to its original domain.

- Restored or new McAfee ePO server hardware with multiple network interface cards (NICs) — You must confirm the correct IP address is configured for the McAfee ePO server NIC.

The Snapshot is configured, depending on your SQL database version, to automatically run every day. If you configure a script to automatically run the SQL Backup and to copy the SQL backup file to your restore SQL database server, then you can more easily restore your McAfee ePO server. In addition, you can manually take a Snapshot or run your scripts to quickly save and backup particularly complex or important ePolicy Orchestrator changes.



The Disaster Recovery Snapshot monitor, found on your ePolicy Orchestrator dashboard, allows you to manage and monitor your Snapshots in one place.

Disaster Recovery components

Using Disaster Recovery to restore your ePolicy Orchestrator software requires certain hardware, software, access privileges, and information.

You need two hardware server platforms:

- Your existing McAfee ePO server hardware, referred to as your "primary" McAfee ePO server.
- Duplicate SQL server hardware, referred to as your "restore" server, running Microsoft SQL that matches your primary McAfee ePO server database. This restore server should be kept up to date with the latest primary McAfee ePO SQL database server configuration using Snapshot and Microsoft SQL backup processes.



To avoid backup and restore problems, your primary and restore server hardware and SQL versions should closely match.

Snapshot Dashboard monitor

The Server Snapshot monitor, found on your ePolicy Orchestrator dashboard, allows you to manage and monitor your Snapshots in one place.



If the Snapshot monitor does not appear in your Dashboard, create a new dashboard and add the Disaster Recovery monitor.

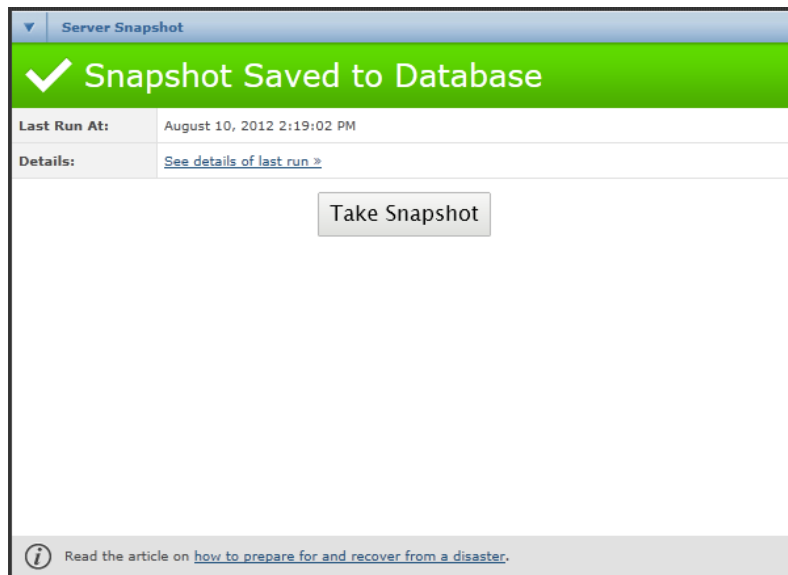


Figure 24-1 Disaster Recovery dashboard Snapshot monitor

Using the Server Snapshot monitor allows you to:

- Click **Take Snapshot** to manually save a McAfee ePO server Snapshot.
- Click **See details of last run** to open the **Server Task Log Details** page. This page displays information and log messages about the most recent Snapshot saved.
- Confirm the date and time the last Snapshot was saved to the SQL database, next to **Last Run At**.
- Click the **Disaster Recovery** link to launch the Help page with Disaster Recovery information.

The color and title of the Snapshot monitor tells you the status of your latest Snapshot. For example:

- **Blue, Saving Snapshot to Database** — Snapshot process is in progress.
- **Green, Snapshot Saved to Database** — Snapshot process completed successfully and it is up to date.
- **Red, Snapshot Failed** — An error occurred during the Snapshot process.
- **Grey, No Snapshot Available** — No Disaster Recovery Snapshot has been saved.
- **Orange, Snapshot Out of Date** — Changes to the configuration have occurred and a recent Snapshot has not been saved. Changes that trigger a Snapshot Out of Date status include:
 - Any extension changed. For example updated, removed, deleted, upgraded, or downgraded
 - The "Keystore" folder changed.
 - The "conf" folder changed.
 - The Disaster Recovery passphrase changed in Server Settings.

Disaster Recovery Snapshot Server Task

You can use the Disaster Recovery Snapshot Server Task to disable and enable the Snapshot server task schedule.



The Snapshot server task schedule is enabled, by default, for the Microsoft SQL Server database and disabled, by default, for the Microsoft SQL Server Express Edition database.

Disaster Recovery requirements

To use Disaster Recovery you need the hardware, software, and information listed in the following table.

Requirement	Description
Hardware requirements	
Primary McAfee ePO server hardware	The server hardware requirements are determined by the number of systems managed. <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> You could have the McAfee ePO server and SQL Server database installed on the same or separate server hardware. See <i>ePolicy Orchestrator 5.1.0 Software Installation Guide</i> for detailed hardware requirements. </div>
Restore McAfee ePO server hardware	This server hardware should closely mirror your primary McAfee ePO server hardware.
Primary McAfee ePO server	This primary server should be up and running correctly with a recent Snapshot saved in the SQL database.
Primary SQL database	The primary SQL database, stores the McAfee ePO server configuration, client information, and Disaster Recovery Snapshot records.
Software requirements	

Requirement	Description
Backup file of primary SQL database	Using either the Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line, you can create a backup file of the primary database including the Snapshot records.
Restore SQL database software	Using either the Microsoft SQL Server Management Studio or the RESTORE (Transact-SQL) command-line, you can restore the primary database including the Snapshot records on the restore SQL database server to duplicate the configuration of the primary SQL database.
ePolicy Orchestrator software	This software, downloaded from the McAfee website, is used to install and configure the restore McAfee ePO server.
Information requirements	
Disaster Recovery Keystore encryption passphrase	This passphrase was added during the initial installation of the ePolicy Orchestrator software and decrypts sensitive information stored in the Disaster Recovery Snapshot.
Administrator privileges	You must be able to access both the primary and restore servers and the SQL database as, for example, DBOwner and DBCreator.
Last known IP address, DNS name, or NetBIOS name of the primary McAfee ePO server	If you change any one of these during the McAfee ePO server restore, ensure that the McAfee Agents have a way to locate the server. The easiest way to do this is to create a Canonical Name (CNAME) record in DNS that points requests from the old IP address, DNS name, or NetBIOS name of the primary McAfee ePO server to the new information for the restore McAfee ePO server.

How Disaster Recovery works

To quickly reinstall the ePolicy Orchestrator software requires periodic snapshots of the ePolicy Orchestrator configuration. You must then back up and restore the database to a restore server, and reinstall the ePolicy Orchestrator software using the **Restore** option.

Disaster Recovery Snapshot and backup overview

The Disaster Recovery Snapshot, SQL database backup, and copying processes create a duplicate ePolicy Orchestrator database on a restore SQL database server.

This is an overview of the Disaster Recovery Snapshot, SQL database backup, and copying processes. For details, see:

- *Create Snapshot*
- *Use Microsoft SQL to backup and restore database*

The following figure is an overview of the ePolicy Orchestrator software Disaster Recovery process and the hardware involved.



In this figure the SQL database is installed on the same server hardware as the McAfee ePO server. The McAfee ePO server and SQL database could be installed on different server hardware.

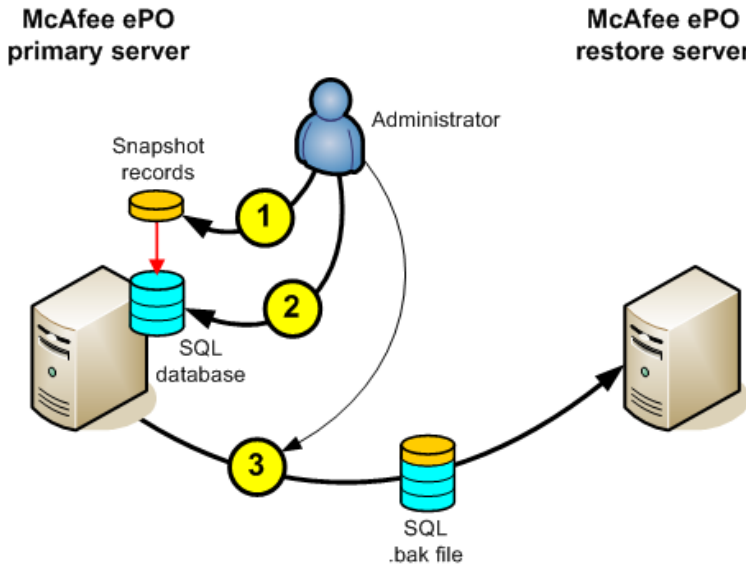


Figure 24-2 McAfee ePO server Disaster Recovery Snapshot and backup

The ePolicy Orchestrator software Disaster Recovery configuration includes these general steps performed on the McAfee ePO primary server:

- 1 Take a Snapshot of the McAfee ePO server configuration and save it to the primary SQL database. This can be done manually or via a default server task provided for this purpose.

When the Snapshot is taken, these are the database files saved:

- C:\Program Files\McAfee\ePolicy Orchestrator\Server\extensions — The default path to ePolicy Orchestrator software extension information.
- C:\Program Files\McAfee\ePolicy Orchestrator\Server\conf — The default path to required files used by the ePolicy Orchestrator software extensions.
- C:\Program Files\McAfee\ePolicy Orchestrator\Server\keystore — These keys are specifically for ePolicy Orchestrator agent-server communication and the repositories.

- C:\Program Files\McAfee\ePolicy Orchestrator\Server\DB\Keystore — The default path to the McAfee product installation server certificates.
- C:\Program Files\McAfee\ePolicy Orchestrator\Server\DB\Software — The default path to the McAfee product installation files.

The Disaster Recovery Snapshot records saved include the paths you have configured for your registered executables. The registered executable files are not backed up and you must replace those executable files when you restore the McAfee ePO server. After you restore the McAfee ePO server, any registered executables with broken paths are red on the Registered Executables page.



You should test your registered executable paths after you restore your McAfee ePO server. Some registered executable paths might not appear red, but still fail because of dependency issues related to the registered executables.

- 2 Backup the SQL database using either the Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line process.
- 3 Copy the SQL database backup file, created in step 2, to the duplicate restore SQL server.



It is critical you complete steps 2 and 3 to copy your snapshots from your primary SQL server to your restore SQL server in order to use the Disaster Recovery feature.

This completes the McAfee ePO server Disaster Recovery Snapshot and backup process. You do not need to continue with the following McAfee ePO server recovery installation unless you are reinstalling the ePolicy Orchestrator software.

McAfee ePO server recovery installation overview

Reinstalling the ePolicy Orchestrator software is the last step in quickly restoring the McAfee ePO server.

This is an overview of reinstalling the ePolicy Orchestrator software on the restore McAfee ePO server. For details, see the *Installation Guide*.

The following figure provides an overview of the McAfee ePO server reinstallation.

i In this figure the SQL database is installed in the same server hardware as the McAfee ePO server. The McAfee ePO server and SQL database could be installed on different server hardware.

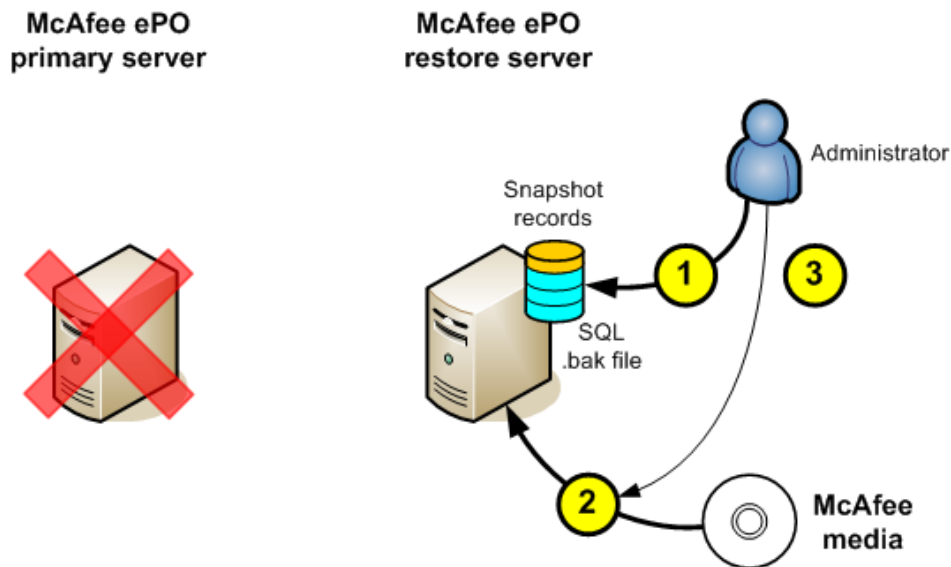


Figure 24-3 McAfee ePO server recovery installation

The ePolicy Orchestrator software installation using the Disaster Recovery Snapshot file includes these general steps performed on the McAfee ePO restore server:

- 1 Find the SQL database backup file, copied in step 3, of the previous section, and use either the Microsoft SQL Server Management Studio or the RESTORE (Transact-SQL) command-line process to restore the primary SQL server configuration to the restore SQL server.
- 2 During the ePolicy Orchestrator database software installation:
 - a On the Software Welcome dialog box, click **Restore ePO from an existing Disaster Recovery database Snapshot**.
 - b Select **Microsoft SQL Server** to link the ePolicy Orchestrator software to the restore SQL database that had the primary McAfee ePO server configuration restored in step 1.

After the ePolicy Orchestrator software installation is started, the database records saved during the Snapshot process are used in the software configuration instead of creating new records in the database.

- 3 If you changed the last known IP address, DNS name, or NetBIOS name of the primary McAfee ePO server, when creating the restore McAfee ePO server the McAfee Agents will not be able to connect to the restored McAfee ePO server. The easiest way to do this is to create a CNAME record in DNS that points requests from the old IP address, DNS name, or NetBIOS name of the primary McAfee ePO server to the new information for the restore McAfee ePO server.

i See *What is Disaster Recovery* for various server examples of restoring the SQL database connection to the McAfee ePO server.

Now the McAfee ePO restore server is running with the exact same configuration as the primary server. The clients can connect to the restore server and you can manage them exactly as before the primary McAfee ePO server was removed.

Create Snapshot

Creating frequent Disaster Recovery Snapshots of your primary McAfee ePO server is the first step in quickly restoring a McAfee ePO server.

After you make many configuration changes to the McAfee software, you should take a Disaster Recovery Snapshot manually using any of the following tasks.



Create a Disaster Recovery Snapshot Server task to automate server snapshots.

Tasks

- [Create Snapshot from Dashboard on page 290](#)
Use the ePolicy Orchestrator Dashboard to take Disaster Recovery Snapshots of your primary McAfee ePO server and to monitor the Snapshot process as the Dashboard status changes.
- [Create Snapshot from Web API on page 290](#)
Use the ePolicy Orchestrator Web API to take Disaster Recovery Snapshots of your primary McAfee ePO server. Doing so enables you to use one command string to complete the process.

Create Snapshot from Dashboard

Use the ePolicy Orchestrator Dashboard to take Disaster Recovery Snapshots of your primary McAfee ePO server and to monitor the Snapshot process as the Dashboard status changes.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Dashboards** to see the **ePO Server Snapshot** monitor.



If needed click **Add Monitor** and select **ePO Server Snapshot** from the list and drag it to the dashboard.

- 2 Click **Take Snapshot** to start saving the McAfee ePO server configuration.

During the Snapshot process the **Snapshot Monitor** title bar changes to indicate the status of the process. See *Snapshot Dashboard monitor* for Snapshot monitor status indicators.



The Snapshot process could take from 10 minutes to more than an hour to complete, depending on the complexity and size of your ePolicy Orchestrator managed network. This process should not affect your McAfee ePO server performance.

- 3 If needed, click **See details of current run** to open the **Server Task Log Details** of the last saved Snapshot.



After the Snapshot process is complete, you click **See details of current run** to open the **Server Task Log Details** of the last saved Snapshot.

The latest Disaster Recovery Snapshot is saved to the McAfee ePO server primary SQL database. The database is now ready to backup and copy to the restore SQL database server.

Create Snapshot from Web API

Use the ePolicy Orchestrator Web API to take Disaster Recovery Snapshots of your primary McAfee ePO server. Doing so enables you to use one command string to complete the process.

All the commands described in this task are typed in your web browser address bar to access your McAfee ePO server remotely.



You are prompted for the administrator username and password before the output is displayed.

See the *McAfee ePolicy Orchestrator 5.1.0 Scripting Guide* for detailed Web API use and examples. For option definitions, click ? in the interface.

Task

- 1 Use the following ePolicy Orchestrator Web API Help command to determine the parameters needed to run the Snapshot:

```
https://localhost:8443/remote/core.help?command=scheduler.runServerTask
```

In the previous command:

- localhost: — The name of your McAfee ePO server name.
- 8443 — Destination port, identified as "8443" (the default), in this example.
- /remote/core.help?command= — Calls the Web API Help
- scheduler.runServerTask — Calls the specific server task Help



The runServerTask command is case sensitive

The previous example command returns this help.

```
OK:
scheduler.runServerTask taskName
Runs a server task and returns the task log ID. Use task log ID with the
'tasklog.listTaskHistory' command to view the running task's status. Returns the
task log ID or throws on error.
Requires permission to run server tasks.
Parameters:
[taskName (param 1) | taskId] - The unique id or name of the task
```

- 2 Use the following command to list all the server tasks and determine the taskName parameter needed to run the Snapshot server task:

```
https://localhost:8443/remote/scheduler.listAllServerTasks?:output=terse
```

The previous example command returns a list that looks similar to the following. The exact list displayed depends on your permissions and the extensions installed.

```
OK:
ID Name                                                                                               Next Run
-----
14 Update Master Repository                                                                           8/1/12 at 2:17 AM
7 Synchronize Shared Tasks                                                                           None
6 Synchronize Shared Policies                                                                       None
11 RSD: Update Sensor Deployment Client Tasks                                                       None
10 RSD: Default Delete Detected Systems Task                                                         None
12 Roll Up Data (Local ePO Server)                                                                    None
8 Purge Threat and Client Events Older than 90 Days                                                 None
3 Issue synchronization                                                                              None
15 Inactive Agent Cleanup Task                                                                        None
13 Generate Records for McAfee Agent Compliance History Reporting                                     None
4 Duplicate Agent GUID - remove systems with potentially duplicated GUIDs                            None
5 Duplicate Agent GUID - clear error count                                                            None
9 Download Software Product List                                                                      8/1/12 at 2:09 AM
2 Disaster Recovery Snapshot Server                                                                    8/1/12 at 1:59 AM
```

- 3 Using the task name, `Disaster Recovery Snapshot Server` found in the previous step, run the Snapshot server task using the following command:

```
https://localhost:8443/remote/scheduler.runServerTask?taskName=Disaster%20Recovery%20Snapshot%20Server
```

If the task is successful, output similar to the following appears.

```
OK:
102
```



The Snapshot process could take from 10 minutes to more than an hour to complete, depending on the complexity and size of your ePolicy Orchestrator managed network. This process should not affect your McAfee ePO server performance.

- 4 Confirm the Web API server task Snapshot ran successfully.
- a Use the following command to find the Disaster Recovery Snapshot Server task log ID:

```
https://localhost:8443/remote/tasklog.listTaskHistory?taskName=Disaster%20Recovery%20Snapshot%20Server
```

This command displays all of the Disaster Recovery Snapshot Server tasks. Find the most recent task and note the ID number. For example, ID: 102 in the following:

```
ID: 102
Name: Disaster Recovery Snapshot Server
Start Date: 8/7/12 11:00:34 AM
End Date: 8/7/12 11:01:18 AM
User Name: admin
Status: Completed
Source: scheduler
Duration: Less than a minute
```

- b Use the following command and that Task ID number 102 to display all task log messages.

```
https://localhost:8443/remote/tasklog.listMessages?taskLogId=102
```

Scroll to the end of the messages and find the following:

```
OK:
Date: 8/7/12 11:00:34 AM
Message: Snapshot Server to Database

Date: 8/7/12 11:00:34 AM
Message: Starting to save server snapshot to the datatabase...

. . .

Date: 8/7/12 11:01:18 AM
Message: Successfully saved server snapshot to the database

Date: 8/7/12 11:01:18 AM
Message: Snapshot Server to Database
```

Configure Disaster Recovery server settings

You can change the Keystore encryption passphrase used when you installed the ePolicy Orchestrator software and link it to an SQL database restored with Disaster Recovery Snapshot records.

Before you begin

You must have administrator rights to change the Keystore encryption passphrase.

Using Disaster Recovery to create an McAfee ePO server Snapshot provides you with a quick recovery method for the McAfee ePO server.



As an administrator, this setting is helpful if you have lost, or forgotten, the Keystore encryption passphrase configured during the ePolicy Orchestrator software installation. You can change the existing passphrase without knowing the previously configured passphrase.

For option definitions, click ? in the interface.

Task

- 1 Click **Menu | Configuration | Server Settings**, select **Disaster Recovery** from the **Setting Categories**, then click **Edit**.
- 2 From **Keystore encryption passphrase**, click **Change passphrase** and type the new passphrase and confirm it.



The Keystore encryption passphrase is used to encrypt and decrypt the sensitive information stored in the server Snapshot. This passphrase is required during the McAfee ePO server recovery process. Make note of this passphrase.



The ePolicy Orchestrator database must be periodically copied to a restore Microsoft SQL Database server to create an actual backup database. See *Configure Snapshot and restore SQL database* for database server backup and restore processes.

A

Ports overview

Follow these port guidelines when you need to customize the ports the McAfee ePO server uses.

Contents

- ▶ *Change console-to-application server communication port*
- ▶ *Change agent-server communication port*
- ▶ *Ports required for communicating through a firewall*
- ▶ *Traffic quick reference*

Change console-to-application server communication port

If the McAfee ePO console-to-application server communication port is in use by another application, follow these steps to specify a different port.

Before you begin



This topic contains information about opening or modifying the registry. This information is intended for use by network and system administrators only.

- We strongly recommend that you back up your registry and understand the restore process. For more information, see the Microsoft documentation.
- Make sure that you run only `.reg` files that are not confirmed to be genuine registry import files.



Registry modifications are irreversible and can cause system failure if done incorrectly.

Task

For option definitions, click ? in the interface.

- 1 Stop the McAfee ePO services:
 - a Close all McAfee ePO consoles.
 - b Click **Start | Run**, type `services.msc`, then click **OK**.
 - c Right-click each of these services and select **Stop**:
 - McAfee ePolicy Orchestrator Application Server
 - McAfee ePolicy Orchestrator Event Parser
 - McAfee ePolicy Orchestrator Server

- 2 In the registry editor, select this key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{53B73DFD-AFBE-4715-88A1-777FE404B6AF}]
```

- 3 In the right pane, double-click **TomcatSecurePort.SQL** and change the value data to reflect the required port number (default is 8443).

- 4 Open a text editor and paste this line into a blank document:

```
UPDATE EPOServerInfo SET rmdSecureHttpPort =8443
```

Change **8443** to the new port number.

- 5 Name the file `TomcatSecurePort.sql` and save it to a temporary location on the SQL Server.
- 6 Use Microsoft SQL Server Management Studio to install the `TomcatSecurePort.SQL` file that you created.
 - a Click **Start | All Programs | Microsoft SQL Server Management Studio**.
 - b On the Connect to Server dialog box, click **Connect**.
 - c Expand **Databases**, then select **ePO database**.
 - d From the toolbar, select **New Query**.
 - e Click **File | Open | File...**, then browse to the `TomcatSecurePort.sql` file.
 - f Select the file, click **Open | Execute**.
- 7 In Windows Explorer, browse to this directory:
`\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\conf\`
- 8 In Notepad, open `Server.xml` and replace all entries for port 8443 with the new port number.
- 9 Click **Start | Run**, type `services.msc`, then click **OK**.
- 10 Right-click each of these services and select **Start**:
 - **McAfee ePolicy Orchestrator Application Server**
 - **McAfee ePolicy Orchestrator Event Parser**
 - **McAfee ePolicy Orchestrator Server**

Change agent-server communication port

Follow these steps to change the agent-server communication port.

Before you begin



This topic contains information about opening or modifying the registry. This information is for network and system administrators only.

- We strongly recommend that you back up your registry and understand the restore process. For more information, see the Microsoft documentation.
- Make sure that you run only .REG files that are confirmed to be genuine registry import files.



Registry modifications are irreversible and can cause system failure if done incorrectly.

Task

For option definitions, click ? in the interface.

- 1 Stop the McAfee ePO services:
 - a Close all McAfee ePO consoles.
 - b Click **Start | Run**, type `services.msc`, then click **OK**.
 - c Right-click each of these services and select **Stop**:
 - **McAfee ePolicy Orchestrator Application Server**
 - **McAfee ePolicy Orchestrator Event Parser**
 - **McAfee ePolicy Orchestrator Server**
- 2 Modify the port value in the registry:
 - a Click **Start | Run**, type `regedit`, then click **OK**.
 - b Navigate to the key that corresponds to your McAfee ePO 5.3.0:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ 53B73DFD-AFBE-4715-88A1-777FE404B6AF}]
- 3 Modify the string value `AgentPort` to reflect the appropriate port, then close the registry editor. The default value for this port is 80.
- 4 Modify the value in the McAfee ePO database:
 - a Open a text editor, and add these lines to the blank document:

```
UPDATE EPOServerInfo SET  
  
ServerHTTPPort=80
```
 - b Save the file as **DefaultAgentPort.SQL** in a temporary location on the SQL Server.
 - c Click **Start | All Programs | Microsoft SQL Server Management Studio** to use Microsoft SQL Server Management Studio to install the `DefaultAgentPort.sql` file.
 - d On the **Connect to Server** dialog box, click **Connect**.
 - e Expand **Databases**, then select **ePO database**.
 - f From the toolbar, select **New Query**.
 - g Click **File | Open | File**, browse to and select the `DefaultAgent.SQL` file, then click **Open | Execute..**
- 5 Paste this line into a blank document:

```
UPDATE EPOServerInfo SET rmdSecureHttpPort =8443
```

Change 8443 to the new port number.

- 6 Name the file `TomcatSecurePort.SQL` and save it to a temporary location on the SQL Server.
- 7 Use Microsoft SQL Server Management Studio to install the `TomcatSecurePort.SQL` file.
 - a Click **Start | All Programs | Microsoft SQL Server Management Studio**.
 - b On the **Connect to Server** dialog box, click **Connect**.
 - c Expand **Databases**, then select **ePO database**.
 - d From the toolbar, select **New Query**.
 - e Click **File | Open | File**, browse to and select the `TomcatSecurePort.SQL` file, then click **Open | Execute..**
- 8 Modify the port value in the McAfee ePO configuration files:
 - a Navigate to `C:\Program Files (x86)\McAfee\Policy Orchestrator\DB\...`
 - b Using a text editor, open `Server.ini` and change the value for `HTTPPort=80` to reflect the new number, then save the file.
 - c Using a text editor, open `Siteinfo.ini` and change the value for `HTTPPort=80` to reflect the new number, then save the file.
 - d Navigate to `C:\Program Files (x86)\McAfee\Policy Orchestrator\Apache2\conf\...`, open `httpd.conf` and change these lines to reflect the new port number:

```
Listen 80
```

```
ServerName<YourServerName>: 80
```

- 9 If using `VirtualHosts`, change:

```
NameVirtualHost *:80
```

```
<VirtualHost *:80>
```

- 10 Save the file and exit the text editor.
- 11 Restart the McAfee ePO services:
 - a Click **Start | Run**, type `services.msc`, and click **OK**.
 - b Right-click each of these services and select **Stop**:
 - **McAfee ePolicy Orchestrator Event Parser**
 - **McAfee ePolicy Orchestrator Server**
- 12 (Optional) Modify settings on remote Agent Handlers:
 - a Make sure that all McAfee ePO consoles are closed, then click **Start | Run**, type `services.msc` and click **OK**.
 - b Right-click each of these services and select **Stop**:
 - **McAfee ePolicy Orchestrator Event Parser**
 - **McAfee ePolicy Orchestrator Server**



This server might be listed as `MCAFEEOAPACHESRV` if the server wasn't restarted since the Agent Handler was installed.

- 13 Navigate to `C:\Program Files (x86)\McAfee\Policy Orchestrator\Apache2\conf\...`, using a text editor open `httpd.conf` and change these lines to reflect the new port number:

```
Listen 80
```

```
ServerName<YourServerName>: 80
```

If using `VirtualHosts`, change:

```
NameVirtualHost *:80
```

```
<VirtualHost *:80>
```

- 14 Save the file and exit the text editor.
- 15 Click **Start | Run**, type `services.msc`, then click **OK**.
- 16 Right-click each of these services and select **Stop**.
- **McAfee ePolicy Orchestrator Event Parser**
 - **McAfee ePolicy Orchestrator Server**



This server might be listed as `MCAFEEMPACHESRV` if the server has not been restarted since the Agent Handler was installed.

If you previously deployed agents to clients, reinstall the agent on all clients using the `/forceinstall` switch to overwrite the existing `Sitelist.xml` file. For more information about specific McAfee Agent versions that allow the `/forceinstall` switch to work successfully, see McAfee KnowledgeBase article [KB60555](#).

Ports required for communicating through a firewall

Use these ports to configure a firewall to allow traffic to and from your McAfee ePO server.

Relevant terms

- *Bidirectional* — The connection can be initiated from either direction.
- *Inbound* — The connection is initiated by a remote system.
- *Outbound* — The connection is initiated by a local system.

Table A-1 McAfee ePO server

Port	Default	Description	Traffic direction
Agent-server communication port	80	TCP port opened by the McAfee ePO server service to receive requests from agents.	Bidirectional between the Agent Handler and the McAfee ePO server and inbound from McAfee Agent to Agent Handlers and McAfee ePO server.
Agent communicating over SSL (4.5 and later agents only)	443	By default, 4.5 agents must communicate over SSL (443 by default). This port is also used for the remote Agent Handler to communicate with the McAfee ePO master repository.	Inbound connection to the McAfee ePO server from agents or Agent Handlers to the master repository. Inbound connection: <ul style="list-style-type: none"> • Agent to McAfee ePO • Agent Handler to master repository • McAfee ePO to master repository • Agent to Agent Handler
Agent wake-up communication port SuperAgent repository port	8081	TCP port opened by agents to receive agent wake-up requests from the McAfee ePO server. TCP port opened to replicate repository content to a SuperAgent repository.	Outbound connection from the McAfee ePO server and Agent Handler to the McAfee Agent.
Agent broadcast communication port	8082	UDP port opened by SuperAgent to forward messages from the McAfee ePO server and Agent Handler.	Outbound connection from the SuperAgent to other Agents.
Console-to-application server communication port	8443	HTTPS port opened by the McAfee ePO Application Server service to allow web browser console access.	Inbound connection to the McAfee ePO server from the McAfee ePO console.
Client-to-server authenticated communication port	8444	Used by the Agent Handler to communicate with the McAfee ePO server to get required information (for example, LDAP servers).	Outbound connection from remote Agent Handlers to the McAfee ePO server.
SQL Server TCP port	1433	TCP port used to communicate with the SQL Server. This port is specified or determined automatically during the setup process.	Outbound connection from the McAfee ePO server and Agent Handler to the SQL Server.
SQL Server UDP port	1434	UDP port used to request the TCP port that the SQL instance hosting the McAfee ePO database is using.	Outbound connection from the McAfee ePO server and Agent Handler to the SQL Server.
Default LDAP server port	389	LDAP connection to look up computers, users, groups, and Organizational Units for User-Based Policies.	Outbound connection from the McAfee ePO server and Agent Handler to an LDAP server.
Default SSL LDAP server port	636	User-Based Policies use the LDAP connection to look up users, groups, and Organizational Units.	Outbound connection from the McAfee ePO server and Agent Handler to an LDAP server.

Traffic quick reference

Use this port and traffic direction information to configure a firewall to allow traffic to and from your McAfee ePO server.

Relevant terms

- *Bidirectional* — The connection can be initiated from either direction.
- *Inbound* — The connection is initiated by a remote system.
- *Outbound* — The connection is initiated by a local system.

Table A-2 Agent Handler

Default port	Protocol	Traffic direction on McAfee ePO server	Traffic direction on Agent Handler
80	TCP	Bidirectional connection to and from McAfee ePO server.	Bidirectional connection to and from Agent Handler.
389	TCP	Outbound connection from McAfee ePO server.	Outbound connection from Agent Handler.
443	TCP	Inbound connection to McAfee ePO server.	Inbound connection to the Agent Handler.
636	TCP	Outbound connection from McAfee ePO server.	Outbound connection from Agent Handler.
1433	TCP	Outbound connection from McAfee ePO server.	Outbound connection from Agent Handler.
1434	UDP	Outbound connection from McAfee ePO server.	Outbound connection from Agent Handler.
8081	TCP	Outbound connection from McAfee ePO server.	
8443	TCP	Outbound connection from McAfee ePO server.	Outbound connection from Agent Handler.
8444	TCP	Inbound connection to McAfee ePO server.	Outbound connection from Agent Handler.

Table A-3 McAfee Agent



Default port	Protocol	Traffic direction
80	TCP	Outbound connection to McAfee ePO server and Agent Handler.
443	TCP	Outbound connection to the McAfee ePO server and Agent Handler.
8081	TCP	Inbound connection from the McAfee ePO server and Agent Handler.
		 If the agent is a SuperAgent repository, the inbound connection is from other agents.
8082	UDP	Inbound connection to agents.
		 Inbound and outbound connection is from or to a SuperAgent.

Table A-4 SQL Server

Default port	Protocol	Traffic direction
1433	TCP	Inbound connection from McAfee ePO server and Agent Handler.
1434	UDP	Inbound connection from McAfee ePO server and Agent Handler.

B

Opening a remote console connection

Using your McAfee ePO server name, or IP address, and the server communication port number you can connect and configure ePolicy Orchestrator from any supported Internet browser.



When you connect to ePolicy Orchestrator using a remote connection, some configuration changes are not allowed. For example, you can't run registered executables from a remote connection.

To configure a remote connection you must determine your McAfee ePO server name, or IP address, and the server communication port number. When you open ePolicy Orchestrator, while logged into your physical McAfee ePO server, notice the address that appears in your browser. It should be similar to:

```
https://win-2k8-epo51:8443/core/orionSplashScreen.do
```

In this example URL:

- win-2k8-epo51 — Is the name of the McAfee ePO server
- :8443 — Is the console-to-application server communication port number used by ePolicy Orchestrator.



The default port number is "8443" unless you changed it.

Task

- 1 Open any ePolicy Orchestrator supported Internet browser. See *McAfee ePolicy Orchestrator Software Installation Guide* for a list of supported browsers.
- 2 In the browser address bar type either of the following, and click **Enter**:

```
https://<servername>:8443
```



```
https://<ipaddress_of_server>:8443
```


For example,

```
https://win-2k8-epo51:8443
```
- 3 Log into ePolicy Orchestrator and you have established a remote console connection.

See the *ePolicy Orchestrator Scripting Guide* for examples of expanded commands you can run from a remote console connection.

Index

A

- about this guide [11](#)
- access requirements for System Tree [104](#)
- accounts
 - user types [39](#)
- Active Directory
 - applying permission sets [42](#)
 - configuring Windows authorization [44](#)
 - containers, mapping to System Tree groups [116](#)
 - implementation strategies [42](#)
 - systems only synchronization [107](#)
 - user logon [41](#)
- Active Directory synchronization
 - borders and [104](#)
 - deleting systems [106](#)
 - duplicate entry handling [106](#)
 - Synchronize Now action [106](#)
 - systems and structure [107](#)
 - tasks [106](#)
 - to System Tree structure [116](#)
 - types [106](#)
- adding comments to issues [279](#)
- administrators
 - about [57](#)
 - creating groups [103](#)
 - managing user accounts [39](#)
 - permissions [57](#)
 - source sites, configuring [66](#)
- agent
 - configuring policies to use repositories [70](#)
 - configuring proxy settings for [69](#)
 - convert to SuperAgent [139](#)
 - first call to server [109](#)
 - grouping [96](#)
 - grouping by assignment rules [96](#)
 - GUID and System Tree location [109](#)
 - maintenance [135](#)
 - McAfee Agent, ePolicy Orchestrator components [15](#)
 - queries provided by [151](#)
 - relay capability [142](#)
 - relay capability, disable [143](#)
 - relay capability, enable [144](#)
 - responses and event forwarding [266](#)
 - wake-up calls [137](#)
- agent communication port [153](#)
- agent deployment credentials [152](#)
- Agent Handlers
 - about [91](#)
 - assigning agents [94](#)
 - assignment priority [97](#)
 - authentication modes [91](#)
 - configuring and managing [93](#)
 - how they work [91](#)
 - moving agents between [96](#)
 - multiple [91](#)
 - priority in sitelist file [93](#)
 - scalability [28](#)
 - when not to use [28](#)
 - when to use [28](#)
- agent-server communication
 - about [135](#)
 - managing [152](#)
 - secure communication keys (ASSC) [158](#)
 - System Tree sorting [108](#)
- agent-server secure communication (ASSC)
 - about [155](#)
 - using different key pairs for servers [161](#)
 - using one key pair [160](#)
 - viewing systems that use a key pair [160](#)
 - working with keys [158](#)
- agent-server secure communication keys
 - export and import keys [123](#)
 - with Transfer Systems [121](#)
- aggregation, *See* notifications
- Applied Policies
 - creating queries [199](#)
- Apply Tag action [127](#)
- ASCII (See agent-server communication interval) [136](#)
- ASSC keys, *See* agent-server secure communication keys [121](#)
- assigning issues [279](#)
- assignment rules
 - agents and handlers [96](#)
- Audit Log
 - about [45](#)
 - purging automatically [46](#)
 - used with Product Deployment [173](#)
 - viewing and purging action history [45](#)

- authentication
 - configuring for Windows [44](#)
 - authentication, configuring for Windows [41](#)
 - authorization
 - strategies [42](#)
 - automatic responses [147](#), [263](#)
- B**
- backup and restore process
 - for SQL database [227](#)
 - bandwidth
 - considerations for event forwarding [271](#)
 - considerations for pull tasks [81](#)
 - distributed repositories and [61](#)
 - replication tasks and [81](#)
 - best practices
 - agent-server communication interval [135](#)
 - duplicating policies before assigning [187](#)
 - importing Active Directory containers [116](#)
 - policy assignment locking [187](#)
 - product deployment [210](#)
 - System Tree creation [111](#)
 - borders (See System Tree organization) [104](#)
 - branches
 - Change Branch action [218](#)
 - Current [183](#)
 - deleting DAT and engine packages [182](#)
 - Evaluation [218](#)
 - manually moving packages between [182](#)
 - Previous [182](#)
 - types of, and repositories [64](#)
 - Broken Inheritance
 - creating queries [199](#)
- C**
- catch-all groups [109](#)
 - certificate authentication
 - convert PVK to PEM file [56](#)
 - creating a self-signed certificate [53](#)
 - modify server certificate authentication [48](#)
 - signed by third-party certificate authority [53](#)
 - update CRL file [49](#)
 - using OpenSSL commands [55](#)
 - Change Branch action [218](#)
 - charts (See queries) [245](#)
 - Check IP Integrity action [109](#)
 - client certificate authentication
 - configuring ePolicy Orchestrator [47](#)
 - configuring users [49](#)
 - disabling [48](#)
 - enabling [48](#)
 - introduction to [46](#)
 - strategies for use [47](#)
 - troubleshooting [50](#)
 - client tasks
 - about [209](#)
 - client task catalog [209](#)
 - compared with product deployment projects [170](#)
 - comparing [220](#)
 - creating [218](#)
 - deleting [219](#)
 - editing settings for [219](#)
 - objects [209](#)
 - run immediately [149](#)
 - sharing [209](#)
 - view [216](#)
 - working with [218](#)
 - client tasks, on-demand [149](#)
 - cloud management
 - how the software works [16](#)
 - compare client tasks [220](#)
 - compare policies [204](#)
 - compliance
 - creating a query for [200](#)
 - generating events [200](#)
 - components
 - Disaster Recovery [284](#)
 - ePolicy Orchestrator, about [15](#)
 - McAfee ePO server, about [15](#)
 - repositories, about [61](#)
 - configuration
 - essential features [34](#)
 - overview [31](#)
 - system list on tag groups [130](#)
 - contacts
 - responses and [273](#)
 - conventions and icons used in this guide [11](#)
 - convert agents to SuperAgents [139](#)
 - creating issues [277](#)
 - credentials
 - caching deployment [152](#)
 - modifying database registrations [88](#)
 - criteria-based tags
 - applying [132](#)
 - sorting [115](#)
 - CRL file, update in Certificate Based Authentication [49](#)
 - Current branch
 - checking in update packages [183](#)
 - defined [64](#)
 - custom login messages [41](#)
- D**
- dashboard monitors
 - configuring [238](#)
 - moving and resizing [239](#)
 - dashboards [88](#)
 - configuring for exported reports [261](#)
 - configuring monitors [238](#)
 - create Snapshot [290](#)

- dashboards [88](#) (*continued*)
 - default monitors [240](#)
 - descriptions [240](#)
 - first-time [242](#)
 - granting permissions to [236](#)
 - import and export [237](#)
 - included monitors [240](#)
 - introduction [235](#)
 - managing [236](#)
 - McAfee [235](#)
 - moving and resizing monitors [239](#)
 - private [235](#)
 - public [235](#)
 - refresh intervals [242](#)
 - server settings [242](#)
 - DAT file updating
 - checking in manually [183](#)
 - considerations for creating tasks [215](#)
 - daily task [217](#)
 - deployment [212](#)
 - from source sites [66](#)
 - in master repository [64](#)
 - scheduling a task [217](#)
 - DAT files
 - See also* detection definition files
 - deleting from repository [182](#)
 - evaluating [218](#)
 - repository branches [182](#)
 - Data Migration Tool
 - used for product compatibility check [165](#)
 - Data Rollup server task [252](#)
 - database
 - restoring the SQL [226](#)
 - database servers
 - about using [87](#)
 - editing registrations [88](#)
 - registering [87](#)
 - removing [88](#)
 - databases
 - backup and restore process [227](#)
 - Disaster Recovery [284](#)
 - multi-server querying [251](#)
 - overview of backup [286](#)
 - overview of recovery [288](#)
 - ports and communication [20](#)
 - queries and retrieving data [244](#)
 - scheduling Snapshot [226](#)
 - deleting issues [279](#)
 - deployment
 - checking in packages manually [182](#)
 - global updating [178](#)
 - installing products [213](#), [214](#)
 - new product example [176](#)
 - package security [210](#)
 - deployment (*continued*)
 - product and update, first time [212](#)
 - products and updates [212](#)
 - supported packages [210](#)
 - tasks [210](#)
 - tasks, for managed systems [213](#)
 - view [173](#)
 - view assigned client task [216](#)
 - detection definition files [15](#)
 - Directory (See System Tree) [116](#)
 - disable agent relay capability [143](#)
 - Disaster Recovery
 - components [284](#)
 - configuring snapshots [226](#)
 - information needed for [228](#)
 - Keystore encryption passphrase [284](#)
 - overview [286](#)
 - server settings [292](#)
 - server task [226](#)
 - Snapshot [283](#)
 - what it is [283](#)
 - distributed repositories
 - about [61](#), [63](#)
 - adding to ePolicy Orchestrator [73](#)
 - creating and configuring [73](#)
 - deleting [76](#)
 - deleting SuperAgent repositories [72](#)
 - editing existing [76](#)
 - enabling folder sharing [76](#)
 - ePolicy Orchestrator components [15](#)
 - folder, creating [73](#)
 - how agents select [82](#)
 - limited bandwidth and [61](#)
 - replicating packages to SuperAgent repositories [72](#)
 - SuperAgent, tasks [71](#)
 - types [63](#)
 - unmanaged [63](#)
 - unmanaged, copying content to [78](#)
 - documentation
 - audience for this guide [11](#)
 - product-specific, finding [12](#)
 - typographical conventions and icons [11](#)
 - domain synchronization [104](#)
 - duplicate entries in the System Tree [118](#)
- ## E
- editing database server registrations [88](#)
 - editing issues [279](#)
 - email servers
 - configuring responses [267](#)
 - enable agent relay capability [144](#)
 - enforcement (See policy enforcement) [193](#)
 - engine updating
 - from source sites [66](#)
 - in master repository [64](#)

- engine updating (*continued*)
 - scheduling a task [217](#)
- Engine updating
 - checking in manually [183](#)
 - deployment packages [212](#)
- engines
 - deleting from repository [182](#)
 - repository branches [182](#)
- ePolicy Orchestrator
 - essential features [34](#)
 - how the software works [16](#)
 - introduction [13](#)
 - log on and log off [19](#)
 - remote console connection [303](#)
- ePolicy Orchestrator software
 - about [15](#)
- Evaluation branch
 - defined [64](#)
 - using for new DATs and engine [218](#)
- evaluation mode [37](#)
- events
 - compliance events [200](#)
 - determining which are forwarded [271](#)
 - filtering, server settings [20](#)
 - forwarding and notifications [266](#)
 - notification intervals [271](#)
 - system list on tag groups [130](#)
- executables
 - managing [270](#)
- exporting
 - client task objects [88](#)
 - dashboards [88](#)
 - permission sets [58](#)
 - policies [88](#)
 - policy assignments [88](#)
 - queries [88](#)
 - reports [261](#)
 - repositories [88](#)
 - responses [88](#), [268](#)
 - systems [88](#)
 - tags [88](#)
 - tasks [88](#)
- exporting systems [113](#)
- extension files
 - installing [181](#)

F

- fallback to your original server [288](#)
- fallback sites
 - about [61](#)
 - configuring [66](#)
 - deleting [68](#)
 - edit existing [67](#)
 - switching to source [67](#)

- features, ePolicy Orchestrator
 - components [15](#)
- filters
 - Event Filtering settings [20](#)
 - for server task log [223](#)
 - list [23](#)
 - query results [245](#)
 - setting for response rules [272](#)
- FTP repositories
 - about [63](#)
 - creating and configuring [73](#)
 - editing [76](#)
 - enabling folder sharing [76](#)

G

- geographic borders, advantages of [104](#)
- global administrators
 - permission needed for Disaster Recovery [284](#)
- global unique identifier (GUID) [109](#)
- global updates
 - contents [70](#)
- global updating
 - enabling [178](#)
 - process description [177](#)
 - requirements [177](#)
- grouping, *See* notifications
- groups
 - catch-all [109](#)
 - configuring criteria for sorting [115](#)
 - controlling access [57](#)
 - creating manually [112](#)
 - criteria-based [109](#)
 - defined [103](#)
 - importing NT domains [118](#)
 - moving systems manually [121](#)
 - operating systems and [105](#)
 - pasting policy assignments to [195](#)
 - policies, inheritance of [103](#)
 - policy enforcement for a product [193](#)
 - sorting criteria [114](#)
 - sorting, automated [105](#)
 - updating manually with NT domains [120](#)
 - using IP address to define [105](#)
 - viewing policy assignment [203](#)

H

- handler assignment
 - editing priority [94](#), [97](#)
 - managing [94](#)
 - viewing summary [94](#)
- handler groups
 - about [93](#)
 - creating [95](#)
 - deleting [95](#)

handler groups (*continued*)
 editing settings 95

handlers
 creating groups 95
 grouping agents 98
 moving agents between 96
 priority 93

hierarchy of SuperAgents 141, 142

HTTP repositories
 about 63
 creating and configuring 73
 editing 76
 enabling folder sharing 76

I

importing
 basics 89
 client task objects 88
 dashboards 88
 permission sets 58
 policies 88
 policy assignments 88
 queries 88
 reports 261
 repositories 88
 responses 88, 268
 systems 88
 tags 88
 tasks 88

inactive agents 149

inheritance
 and policy settings 187
 broken, resetting 203
 defined 103
 viewing for policies 203

installation
 planning 27

interface
 favorites bar 19
 menu 19
 navigation 19

interface,
 Menu 19

Internet Explorer
 configuring proxy settings 69

intervals
 between notifications 271

IP address
 as grouping criteria 105
 checking IP overlap 109
 IPv6 28
 range, as sorting criteria 115
 sorting 109
 sorting criteria 111, 115

IP address (*continued*)
 subnet mask, as sorting criteria 115

issue management 277

issues
 about 277
 adding comments 279
 assigning 279
 creating 277
 creating automatically from responses 278
 deleting 279
 editing 279
 managing 277
 viewing details 279
 working with 277

issues, purging
 closed issues 280
 closed issues on a schedule 280

K

keys, *See* security keys

Keystore encryption passphrase
 Disaster Recovery 284
 setting 292

L

LAN connections and geographical borders 104

language packages (*See* agent) 104

LDAP servers
 authentication strategies 42

LDAP servers, registering 85

license key 37

lists
 filtering 23
 searching 23

lists, working with 22

local distributed repositories 78

log files
 server task log 222

login messages 41

Lost and found group 102

M

managed systems
 agent-server communication 135
 deployment tasks for 213
 global updating and 61
 installing products on 214
 policy assignment 203
 policy management on 185
 rollup querying 251
 sorting, criteria-based 107
 tasks for 213

master repositories
 about 61

- master repositories (*continued*)
 - communicating with source sites [68](#)
 - configuring proxy settings [68](#)
 - using replication tasks [81](#)
 - master repository
 - checking in packages manually [183](#)
 - ePolicy Orchestrator components [15](#)
 - key pair for unsigned content [156](#)
 - security keys in multi-server environments [157](#)
 - updating with pull tasks [81](#)
 - McAfee Agent
 - properties, viewing [151](#)
 - statistics [146](#)
 - McAfee Agent (see agent) [15](#)
 - McAfee Default policy
 - frequently asked questions [206](#)
 - McAfee Links, default monitor [240](#)
 - McAfee Product Improvement Program
 - configuring [37](#)
 - removing the program [37](#)
 - McAfee recommendations
 - create a Rollup Data server task [252](#)
 - deploy agents when importing large domains [118](#)
 - duplicate policies before assignment [187](#)
 - evaluate borders for organization [104](#)
 - phased rollout for Product Deployment [210](#)
 - schedule replication tasks [81](#)
 - System Tree planning [103](#)
 - use global updating [177](#)
 - use IP addresses for sorting [105](#)
 - use tag-based sorting criteria [105](#)
 - McAfee ServicePortal, accessing [12](#)
 - Menu
 - navigating in the interface [20](#)
 - menu-based navigation [19](#)
 - message
 - custom login [41](#)
 - Microsoft Internet Information Services (IIS) [63](#)
 - Microsoft Windows Resource Kit [113](#)
 - monitors [235](#)
 - configuring [238](#)
 - included in dashboards [240](#)
 - monitors, Disaster Recovery
 - Snapshot status [284](#)
 - multiple McAfee ePO servers
 - policy sharing [205](#)
 - My Default policy
 - frequently asked questions [206](#)
 - My Organization group of System Tree [102](#)
- N**
- navigation
 - menu-based [19](#)
 - navigation,
 - Menu [19](#)
 - navigation, (*continued*)
 - menu-based [19](#)
 - navigation bar [20](#)
 - NETDOM.EXE utility, creating a text file [113](#)
 - network bandwidth (See System Tree organization) [104](#)
 - New Group wizard
 - creating new groups [249](#)
 - Notification event interval [271](#)
 - notification rules
 - defaults [125](#), [264](#)
 - importing .MIB files [269](#)
 - notifications
 - assigning permissions [267](#)
 - event forwarding [266](#), [267](#)
 - how they work [124](#)
 - recipients [124](#)
 - registered executables, managing [270](#)
 - SNMP servers [86](#), [269](#)
 - throttling, aggregation, and grouping [124](#), [264](#)
 - NT domains
 - importing to manually created groups [118](#)
 - synchronization [107](#), [118](#)
 - updating synchronized groups [120](#)
- O**
- operating systems
 - filters for response rule [272](#)
 - grouping [105](#)
 - legacy systems (Windows 95, Windows 98) [105](#)
- P**
- packages
 - checking in manually [182](#)
 - configuring deployment task [214](#)
 - moving between branches in repository [182](#)
 - security for [210](#)
 - passwords
 - changing on user accounts [39](#)
 - supported formats [40](#)
 - peer-to-peer; best practice [145](#)
 - permission sets [88](#)
 - applying to Active Directory groups [42](#)
 - assigning to reports [259](#)
 - example [57](#)
 - interaction with users and groups [57](#)
 - mapping to Active Directory groups [41](#)
 - System Tree [104](#)
 - Permission Sets
 - exporting and importing [58](#)
 - managing [58](#)
 - permissions
 - administrator [57](#)
 - assigning for notifications [267](#)
 - assigning for responses [268](#)

- permissions (*continued*)
 - for queries [243](#)
 - to dashboards [236](#)
- policies [88](#)
 - about [185](#)
 - assigning and managing [189](#)
 - automatic response [147](#)
 - broken inheritance, resetting [203](#)
 - categories [185](#)
 - changing the owner [190](#)
 - comparing [204](#)
 - configuring [189](#)
 - controlling on Policy Catalog page [188](#)
 - frequently asked questions [206](#)
 - group inheritance, viewing [203](#)
 - how they are applied to systems [187](#)
 - importing and exporting [185](#), [191](#)
 - inheritance [187](#)
 - managing, on Policy Catalog page [188](#)
 - ownership [187](#), [202](#)
 - responding to events [147](#)
 - settings, viewing [202](#)
 - sharing between McAfee ePO servers [190](#)
 - using tags to assign [198](#)
 - verifying changes [151](#)
 - viewing [185](#), [201](#)
 - working with Policy Catalog [187](#)
- policy assignment
 - copying and pasting [194](#), [195](#)
 - disabled enforcement, viewing [202](#)
 - group, assigning to [192](#)
 - locking [187](#)
 - Policy Catalog [187](#)
 - systems, assigning to [192](#), [193](#)
 - viewing [202](#), [203](#)
- policy assignment rules [196](#)
 - about [196](#)
 - and multi-slot policies [196](#)
 - creating [198](#)
 - deleting and editing [198](#)
 - editing priority [198](#)
 - importing and exporting [198](#)
 - priority [196](#)
 - rule criteria [196](#)
 - system-based [196](#)
 - system-based policies [197](#)
 - user-based [196](#)
 - user-based policies [197](#)
 - viewing summary [198](#)
- Policy Catalog
 - page, viewing [185](#)
 - working with [187](#)
- policy enforcement
 - enabling and disabling [193](#)
 - for a product [193](#)
- policy enforcement (*continued*)
 - viewing assignments where disabled [202](#)
 - when policies are enforced [185](#)
- policy events
 - responding to [147](#)
- policy management
 - creating queries [199](#)
 - using groups [103](#)
 - working with client tasks [218](#)
- policy sharing
 - assign [204](#)
 - designating [205](#)
 - multiple McAfee ePO servers [205](#)
 - registering server [204](#)
 - using registered server [205](#)
 - using server tasks [204](#), [205](#)
- ports
 - agent communication [153](#)
 - server settings [20](#)
 - server settings and communication [20](#)
- Previous branch
 - defined [64](#)
 - moving DAT and engine packages to [182](#)
 - saving package versions [182](#)
- Product Compatibility List
 - configuring download source [166](#)
 - overview [165](#)
- product deployment
 - about monitoring and modifying [172](#)
 - compared with client task deployment method [170](#)
 - creating [174](#)
 - methods [169](#)
 - monitoring and modifying [175](#)
 - projects [170](#)
 - view [173](#)
 - view assigned client task [216](#)
- product deployment packages
 - checking in [182](#)
 - checking in manually [183](#)
 - security and package signing [210](#)
 - supported packages [210](#)
 - updates [210](#)
- product improvement program
 - configuring [37](#)
 - removing the program [37](#)
- product installation
 - configuring deployment tasks [213](#), [214](#)
 - installing extension files [181](#)
- product properties [150](#)
- product updates
 - checking in packages manually [182](#)
 - deploying [212](#)
 - package signing and security [210](#)
 - process description [212](#)
 - source sites and [61](#)

- product updates (*continued*)
 - supported package types [210](#)
- properties
 - McAfee Agent, viewing from the console [151](#)
 - product [150](#)
 - system [150](#)
 - verifying policy changes [151](#)
- proxy settings
 - agent [69](#)
 - configuring for master repository [68](#)
 - server settings [36](#)
- pull tasks
 - considerations for scheduling [81](#)
 - server task log [223](#)
 - updating master repository [81](#)
- purging closed issues [280](#)
 - manually [280](#)

Q

- queries [88](#)
 - about [244](#)
 - actions on results [244](#)
 - agent [151](#)
 - changing groups [249](#)
 - chart types [245](#)
 - configuring [246](#)
 - creating a compliance query [200](#)
 - custom, managing [247](#)
 - exported as reports [244](#)
 - exporting to other formats [250](#)
 - filters [245](#)
 - permissions [243](#)
 - personal query group [249](#)
 - report formats [244](#)
 - result type [251](#)
 - results as dashboard monitors [244](#)
 - results as tables [245](#)
 - rollup, from multiple servers [251](#)
 - run existing [248](#)
 - scheduled [248](#)
 - sub-action [248](#)
 - system list on tag groups [130](#)
 - using in a server task [200](#)
 - using results to exclude tags on systems [130](#)
 - working with [246](#)
- Query Builder
 - about [245](#)
 - creating custom queries [243](#), [247](#)
 - result types [245](#)
- Quick Find [23](#)
- Quick System Search, default monitor [240](#)

R

- registered servers
 - adding SNMP servers [86](#)
 - enabling policy sharing [205](#)
 - LDAP servers, adding [85](#)
 - registering [83](#)
 - supported by ePolicy Orchestrator [83](#)
- registering database servers [87](#)
- relay capability [142](#)
- relay capability, disable [143](#)
- relay capability, enable [144](#)
- remote console connection [303](#)
- removing database server registrations [88](#)
- replication
 - avoiding for selected packages [75](#)
 - disabling of selected packages [76](#)
- replication tasks
 - full vs. incremental [81](#)
 - server task log [223](#)
 - updating master repository [81](#)
- Report Builder
 - creating custom reports [243](#)
- report elements
 - configuring charts [257](#)
 - configuring images [256](#)
 - configuring tables [257](#)
 - configuring text [256](#)
 - removing [258](#)
 - reordering [259](#)
- reports [233](#)
 - about [253](#)
 - adding elements [255](#)
 - adding to a group [259](#)
 - configuring [246](#)
 - configuring chart elements [257](#)
 - configuring image elements [256](#)
 - configuring table elements [257](#)
 - configuring template and location for [261](#)
 - configuring text elements [256](#)
 - creating [243](#), [254](#)
 - deleting [262](#)
 - editing existing [255](#)
 - exported query results [244](#)
 - exporting and importing [261](#)
 - formats [244](#)
 - headers and footers [258](#)
 - removing elements [258](#)
 - reordering elements [259](#)
 - running [260](#)
 - running with a server task [260](#)
 - scheduling [260](#)
 - structure and page size [253](#)
 - viewing output [259](#)
 - working with [254](#)

- repositories 88
 - arrange SuperAgent hierarchy 141, 142
 - branches 64, 182, 218
 - concept 61
 - creating SuperAgent repository 71
 - how they work together 65
 - importing from repository list files 80
 - master, configuring proxy settings for 68
 - replication and selection of 82
 - security keys 155, 157
 - source site 61
 - types of 61
 - UNC 77
 - unmanaged, copying content to 78
 - repository list files
 - about 65
 - adding distributed repository to 73
 - exporting to 79, 80
 - importing from 80
 - priority of Agent Handlers 93
 - SiteList.xml, uses for 65
 - working with 79
 - Response Builder wizard 273
 - response rules
 - creating and editing 271
 - Description page 272
 - setting filters for 272
 - setting thresholds 272
 - responses 88, 268
 - assigning permissions 268
 - configuring 265, 267, 270, 273
 - configuring to automatically create issues 278
 - contacts for 273
 - event forwarding 266
 - frequently asked questions 274
 - planning 265
 - rules that trigger 273
 - SNMP servers 268, 269
 - rules
 - configuring contacts for responses 273
 - defaults for notifications 125, 264
 - setting up for notifications, SNMP servers 269
 - Run Tag Criteria action 127
- S**
- scalability
 - about 27
 - horizontal 27
 - planning 27
 - using Agent Handlers 28
 - using multiple servers 27
 - vertical 27
 - schedule server task
 - for policy sharing 205
 - scheduling
 - applying criteria-based tags 132
 - Disaster Recovery Snapshot 226
 - server tasks with Cron syntax 222
 - security certificate
 - certificate authority (CA) 50
 - creating a self-signed certificate 53
 - installing 52
 - security keys
 - agent-server secure communication (ASSC) 155, 158
 - ASSC, working with 158
 - for content from other repositories 156
 - general 155
 - managing 156
 - master keys in multi-server environments 157
 - private and public 156
 - server settings 20
 - using one master key 157
 - security management 99
 - selected packages
 - avoid replication of 75
 - disabling replication of 76
 - server certificate
 - removing 48
 - replacing 51
 - server settings
 - dashboards 20
 - default categories 20
 - Disaster Recovery 292
 - global updates 70
 - global updating 178
 - Internet Explorer 69
 - notifications 125, 264
 - ports and communication 20
 - proxy settings 36
 - proxy, and master repositories 61
 - SSL certificates 50
 - types of 20
 - Server Task Builder wizard 132
 - server task log
 - about 223
 - view, filter, and purge tasks 223
 - server tasks
 - about 221
 - allowing Cron syntax 222
 - create 221
 - Data Rollup 252
 - Disaster Recovery 226
 - for policy sharing 204
 - log file, purging 223
 - query with a sub-action 248
 - replacing server certificate 51
 - running reports 260
 - scheduling a query 248
 - scheduling with Cron syntax 222

- server tasks (*continued*)
 - server task log 222
 - Synchronize Domain/AD 106
- server types
 - supported by ePolicy Orchestrator 83
- servers
 - backup and restore process 227
 - configuration overview 31
 - database 87
 - Disaster Recovery 228, 284
 - hardware upgrade using Disaster Recovery 283
 - importing and exporting queries 249
 - importing policies from 191
 - LDAP servers, registering 85
 - master repository key pair 156
 - McAfee ePO server, components 15
 - overview of backup 286
 - overview of recovery 288
 - registering additional servers 83
 - settings and controlling behavior 20
 - sharing objects between 88
 - sharing policies 190
 - SNMP, and notifications 269
 - SNMP, and responses 268
 - supported server types 83
 - transferring systems 122
 - types you can register 83
 - when to use more than one 27
- ServicePortal, finding product documentation 12
- setup 25
- sitelist files 93
- sites
 - deleting source or fallback 68
 - editing existing 67
 - fallback 61, 66
 - switching source and fallback 67
- Snapshot
 - create from Dashboard 290
 - create from Web API 290
 - creating 290
 - Dashboard monitor 284
 - overview 286
 - part of Disaster Recovery 283
 - records saved to database 286
 - scheduling defaults 226
 - Server Task Log Details 290
- snapshots
 - configuring 226
- SNMP servers
- See also* responses
- registering 86
- software manager 163 (*continued*)
 - product compatibility 165
- Software Manager
 - checking in extensions 164
 - checking in packages 164
 - evaluation software 164
 - licensed software 164
 - removing extensions 164
 - removing packages 164
- Sort Now action 107
- sorting criteria
 - configuring 115
 - for groups 115
 - groups, automated 105
 - IP address 109
 - IP address-based 115
 - sorting systems into groups 107
 - tag-based 105, 109, 115
- source sites
 - about 61
 - configuring 66
 - creating 66
 - deleting 68
 - editing existing 67
 - fallback 61
 - importing from SiteMgr.xml 80
 - product updates and 61
 - switching to fallback 67
 - update packages and 212
- SPIPE 135
- SQL database
 - backup and restore process 227
 - Disaster Recovery 284
 - overview of backup 286
 - overview of recovery 288
 - restoring the database 226
 - scheduling Snapshot 226
- SQL servers, *See* databases
- SSL certificates
 - about 50
- subgroups
 - and policy management 118
 - criteria-based 109
- subnets, as grouping criteria 105
- SuperAgent repositories
 - about 63
 - creating 71
 - deleting 72
 - global updating requirements 177
 - replicating packages to 72
 - tasks 71
- SuperAgents
 - about 138
 - caching 140
 - convert agents 139

- SuperAgents (*continued*)
 - distributed repositories [63](#)
 - hierarchy [141](#), [142](#)
 - wake-up calls [137](#), [139](#)
 - wake-up calls to System Tree groups [138](#)
 - synchronization
 - Active Directory and [107](#)
 - defaults [109](#)
 - deploying agents automatically [106](#)
 - excluding Active Directory containers [106](#)
 - NT domains [107](#)
 - preventing duplicate entries [107](#)
 - scheduling [119](#)
 - Synchronize Now action [106](#)
 - systems and structures [107](#)
 - systems only, with Active Directory [107](#)
 - System Tree
 - access requirements [104](#)
 - assigning policies to a group [192](#)
 - child groups and inheritance [103](#)
 - creation, automated [105](#)
 - criteria-based sorting [107](#)
 - defined [103](#)
 - deleting systems from [103](#)
 - grouping agents [98](#)
 - groups and manual wake-up calls [138](#)
 - Lost and found group [102](#)
 - My Organization level [102](#)
 - parent groups and inheritance [103](#)
 - permission sets [104](#)
 - populating groups [111](#)
 - structure [101](#)
 - System Tree organization
 - add systems to groups [112](#)
 - borders in your network [104](#)
 - creating groups [111](#)
 - duplicate entries [118](#)
 - importing Active Directory containers [116](#)
 - importing systems and groups [114](#)
 - mapping groups to Active Directory containers [116](#)
 - moving systems to groups manually [121](#)
 - network bandwidth [104](#)
 - operating systems [105](#)
 - planning considerations [103](#)
 - text files, importing systems and groups [113](#)
 - using subgroups [118](#)
 - System Tree sorting
 - default settings [109](#)
 - enabling [115](#), [116](#)
 - IP address [109](#)
 - on agent-server communication [108](#)
 - ordering subgroups [109](#)
 - server and system settings [20](#), [108](#)
 - sort systems once [108](#)
 - tag-based criteria [109](#)
 - System Tree synchronization
 - scheduling [119](#)
 - to Active Directory structure [116](#)
 - system-based policies
 - about [197](#)
 - criteria [197](#)
 - systems [88](#)
 - assigning policies to [192](#), [193](#)
 - exporting from the Systems Tree [113](#)
 - pasting policy assignments to [195](#)
 - policy enforcement for a product [193](#)
 - properties [150](#)
 - sorting into groups [116](#)
 - viewing policy assignment [203](#)
- T**
- table row, select checkboxes [23](#)
 - tables, working with [22](#)
 - Tag Builder wizard [127](#)
 - Tag Catalog [127](#)
 - tag-based sorting criteria [105](#), [109](#)
 - tags [88](#)
 - applying [132](#)
 - create, delete, and modify subgroups [129](#)
 - creating with Tag Builder wizard [127](#)
 - criteria-based [107](#)
 - criteria-based sorting [115](#)
 - edit, delete, export, and move [128](#)
 - excluding systems from automatic tagging [130](#)
 - group sorting criteria [105](#)
 - manual application of [131](#)
 - tags, subgroups
 - create, delete, and modify [129](#)
 - technical support, finding product information [12](#)
 - Test Sort action [107](#)
 - Threat Event Log
 - about [228](#)
 - viewing and purging [230](#)
 - throttling, *See* notifications
 - troubleshooting
 - client certificate authentication [50](#)
 - product deployment [210](#)
 - verifying properties of the McAfee Agent and products [151](#)
- U**
- UNC share repositories
 - about [63](#)
 - creating and configuring [73](#)
 - editing [76](#)
 - enabling folder sharing [76](#)
 - using
 - recommendations [77](#)
 - unmanaged repositories [63](#)

updates

- checking in manually [182](#)
- client tasks [215](#)
- considerations for creating tasks [215](#)
- deployment packages [212](#)
- for selected systems [147](#)
- package signing and security [210](#)
- packages and dependencies [210](#)
- scheduling an update task [217](#)
- source sites and [61](#)

updating

- automatically, with global updating [178](#)
- DATs and Engine [212](#)
- deployment tasks [210](#)
- global, process [177](#)
- process description [212](#)
- scheduling an update task [217](#)

user accounts

- changing passwords [39](#)
- managing [39](#)
- types [39](#)

user-based policies

- about [197](#)
- criteria [197](#)

users

- permission sets and [57](#)

utilities

- NETDOM.EXE, creating a text file [113](#)

V

- viewing issue details [279](#)
- VirusScan Enterprise example
 - deployment [176](#)
- VPN connections and geographical borders [104](#)

W

- wake-up calls
 - about [137](#)
 - manual [137](#)
 - SuperAgents and [137](#), [139](#)
 - tasks [137](#)
 - to System Tree groups [138](#)
- WAN connections and geographical borders [104](#)
- Windows
 - authentication, configuring [41](#), [44](#)
 - Authorization, configuring [44](#)
- Windows authentication
 - enabling [43](#)
 - strategies [42](#)

