

McAfee ePolicy Orchestrator 4.5 Product Guide

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

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 MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

- Introducing ePolicy Orchestrator 4.5** **14**
 - Components and what they do. 14
 - Using this guide. 15
 - Audience. 15
 - Finding documentation for McAfee enterprise products. 15

- Getting Started with ePolicy Orchestrator 4.5** **17**
 - Logging on and off ePO servers. 17
 - Logging on to ePO servers. 17
 - Logging off ePO servers. 17
 - Viewing the server version number 18
 - How to navigate the ePO interface. 18
 - The Menu. 18
 - The navigation bar. 19
 - Setting up ePolicy Orchestrator. 19
 - Configure your ePO server. 20
 - Add systems to the System Tree. 20
 - Distribute agents to your systems. 21
 - Create repositories. 21
 - Configure your policies and client tasks. 22
 - Deploy your products and software. 22
 - Configure advanced features. 22

- Configuring ePolicy Orchestrator** **23**
 - ePO user accounts. 24
 - Global administrators. 24
 - Working with user accounts. 24
 - How permission sets work. 25
 - Working with permission sets. 26
 - Contacts. 28
 - Working with contacts. 28
 - Server settings and the behaviors they control. 29
 - Working with server settings. 30

Managing ePolicy Orchestrator users with Active Directory.	36
Configuring Windows authentication and authorization.	37
Registering servers for use with ePolicy Orchestrator.	39
What are registered servers.	39
Registering servers.	39
Security keys and how they work.	41
Backing up and restoring keys.	42
Master repository key pair.	44
Agent-server secure communication (ASSC) keys.	46
MyAvert Security Threats	50
Working with MyAvert Security Threats.	50
Agent Handlers and what they do.	52
How Agent Handlers work.	52
Handler groups and priority.	52
Working with Agent Handlers.	53
IPv6.	58
Exporting tables and charts to other formats.	59
Distributing Agents to Manage Systems.	60
About the McAfee Agent.	60
Agent-server communication	61
Wake-up calls and wake-up tasks.	62
SuperAgents and broadcast wake-up calls.	63
System requirements and supported operating systems and processors.	63
Installing the McAfee Agent.	65
Methods of agent deployment and installation.	65
Agent installation folder — Windows.	78
Agent installation folder — UNIX-based systems.	78
The agent installation package.	79
Agent installation command-line options.	80
Assigning values to custom properties.	81
Upgrading and Restoring Agents.	81
Upgrading agents using product deployment task.	82
Upgrading agents manually or with login scripts.	83
Restoring a previous version of the agent (Windows).	83
Restoring a previous version of the agent (UNIX).	83
Configuring Agent Policies.	83
About agent policy settings.	84

Proxy settings for the agent.	86
Retrieving system properties.	87
Scheduling a client task for a group.	87
Creating a new scheduled client task.	88
Configuring selected systems for updating.	89
Working with the agent from the ePO server.	89
Viewing agent and product properties.	89
Viewing system information.	90
Accessing settings to retrieve properties.	90
Windows system and product properties reported by the agent.	91
Sending manual wake-up calls to systems.	92
Sending manual wake-up calls to a group.	92
Making the system tray icon visible.	93
Locating inactive agents.	93
Running agent tasks from the managed system.	93
Running a manual update.	94
Enforcing policies.	94
Updating policies.	95
Sending properties to the ePO server.	95
Sending events to the ePO server immediately.	95
Using the icon option to update.	95
Forcing the agent to call in to the server.	96
Viewing version numbers and settings.	96
Agent command-line options.	97
Using the system tray icon.	97
What the system tray icon does.	97
Making the system tray icon visible.	98
Enabling user access to updating functionality.	98
Removing the McAfee Agent.	98
Running FrmInst.exe from the command line.	99
Removing agents when deleting systems from the System Tree.	99
Removing agents when deleting groups from the System Tree.	99
Removing agents from systems in query results.	100
Uninstalling from non-Windows operating systems.	100
Agent Activity Logs.	101
Viewing the agent activity log.	101

Organizing the System Tree	103
The System Tree	104
Considerations when planning your System Tree	105
Administrator access	105
Environmental borders and their impact on system organization	106
Subnets and IP address ranges	106
Tags and systems with similar characteristics	107
Operating systems and software	107
Tags and how they work	107
Active Directory and NT domain synchronization	108
Active Directory synchronization	108
NT domain synchronization	110
Criteria-based sorting	110
How settings affect sorting	111
IP address sorting criteria	111
Tag-based sorting criteria	111
Group order and sorting	112
Catch-all groups	112
How a system is first placed in the System Tree	112
Working with tags	113
Creating tags with the Tag Builder	113
Excluding systems from automatic tagging	114
Applying tags to selected systems	115
Applying criteria-based tags automatically to all matching systems	115
Creating and populating groups	116
Creating groups manually	118
Adding systems manually to an existing group	118
Importing systems from a text file	119
Sorting systems into criteria-based groups	121
Importing Active Directory containers	123
Importing NT domains to an existing group	125
Synchronizing the System Tree on a schedule	127
Updating the synchronized group with an NT domain manually	128
Moving systems manually within the System Tree	128
Transferring systems between ePO servers	129
Creating Repositories	130
Repository types and what they do	130

Types of distributed repositories.	132
Repository branches and their purposes.	133
Repository list file and its uses.	134
How repositories work together.	134
Ensuring access to the source site.	135
Configuring proxy settings.	135
Configuring proxy settings for the McAfee Agent.	135
Configuring proxy settings for MyAvert Security Threats.	136
Working with source and fallback sites.	137
Switching source and fallback sites.	137
Creating source sites.	137
Editing source and fallback sites.	138
Deleting source sites or disabling fallback sites.	139
Using SuperAgents as distributed repositories.	139
Creating SuperAgent repositories.	139
Selecting which packages are replicated to SuperAgent repositories.	140
Deleting SuperAgent distributed repositories.	141
Creating and configuring FTP, HTTP, and UNC repositories.	141
Creating a folder location on an FTP, HTTP server or UNC share.	141
Adding the distributed repository to ePolicy Orchestrator.	142
Avoiding replication of selected packages.	143
Disabling replication of selected packages.	144
Enabling folder sharing for UNC and HTTP repositories.	144
Editing distributed repositories	144
Deleting distributed repositories.	145
Working with the repository list files.	145
Exporting the repository list SiteList.xml file.	145
Exporting the repository list SiteMgr.xml file for backup or use by other servers.	146
Importing distributed repositories from the SiteMgr.xml file.	146
Importing source sites from the SiteMgr.xml file.	147
Changing credentials on multiple distributed repositories.	147
Managing your Network with Policies and Client Tasks.	148
Product extensions and what they do.	148
Policy management.	149
Policy application.	150
Creating Policy Management queries.	151
Client tasks and what they do.	152

Bringing products under management.	153
Viewing policy information.	153
Viewing groups and systems where a policy is assigned.	153
Viewing the settings of a policy.	154
Viewing policy ownership.	154
Viewing assignments where policy enforcement is disabled.	154
Viewing policies assigned to a group.	155
Viewing policies assigned to a specific system.	155
Viewing a group's policy inheritance.	155
Viewing and resetting broken inheritance.	155
Working with the Policy Catalog.	156
Creating a policy from the Policy Catalog page	156
Duplicating a policy on the Policy Catalog page.	157
Editing a policy's settings from the Policy Catalog.	157
Renaming a policy from the Policy Catalog.	158
Deleting a policy from the Policy Catalog.	158
Working with policies.	158
Changing the owners of a policy.	159
Moving policies between ePO servers.	159
Assigning a policy to a group of the System Tree.	160
Assigning a policy to a managed system.	160
Assigning a policy to multiple managed systems within a group.	161
Enforcing policies for a product on a group.	161
Enforcing policies for a product on a system.	162
Copying and pasting assignments.	162
Working with client tasks.	164
Creating and scheduling client tasks.	164
Editing client tasks.	164
Deleting client tasks.	165
Frequently asked questions.	165
Sharing policies among ePO servers.	166
Setting up policy sharing for multiple ePO servers.	166
How policy assignment rules work.	167
Policy assignment rule priority.	168
Working with policy assignment rules.	168
Deploying Software and Updates.	171
Deployment packages for products and updates.	171

Product and update deployment.	173
Deployment tasks.	173
Update tasks.	174
Global updating.	174
Pull tasks.	175
Replication tasks.	176
Repository selection.	177
Server task log.	177
Checking in packages manually.	178
Using the Product Deployment task to deploy products to managed systems.	179
Configuring the Deployment task for groups of managed systems.	179
Configuring the Deployment task to install products on a managed system.	180
Deploying update packages automatically with global updating.	181
Deploying update packages with pull and replication tasks.	183
Using pull tasks to update the master repository.	183
Replicating packages from the master repository to distributed repositories.	185
Configuring agent policies to use a distributed repository.	187
Using local distributed repositories that are not managed.	188
Checking in engine, DAT and ExtraDAT update packages manually.	189
Updating managed systems regularly with a scheduled update task.	190
Confirming that clients are using the latest DAT files.	190
Evaluating new DATs and engines before distribution.	191
Manually moving DAT and engine packages between branches.	192
Deleting DAT or engine packages from the master repository.	192
Reporting On System Status.	193
Queries.	193
Public and personal queries.	194
Query permissions.	194
Query Builder.	195
Working with queries.	196
Creating custom queries.	196
Running an existing query.	197
Running a query on a schedule.	197
Making a personal query group.	199
Making existing personal queries public.	200
Duplicating queries.	200
Sharing a query between ePO servers.	200

Exporting query results to other formats.	201
Multi-server rollup querying.	202
Preparing for rollup querying.	202
Creating a query to define compliance.	204
Generating compliance events.	204
The Audit Log.	205
Working with the Audit Log.	205
The Server Task log.	207
Working with the Server Task Log.	210
Allowed Cron syntax when scheduling a server task.	211
The Threat Event Log.	212
Working with the Threat Event Log.	213
Data exports from any table or chart.	214
Monitoring with Dashboards.	216
Default dashboards and their monitors.	216
Queries as dashboard monitors.	216
Default dashboards and their monitors.	216
Setting up dashboard access and behavior.	218
Giving users permissions to dashboards.	219
Configuring the refresh frequency of dashboards.	219
Working with Dashboards.	219
Creating dashboards.	220
Making a dashboard active.	220
Selecting all active dashboards.	220
Making a dashboard public.	221
Detecting Rogue Systems.	222
What are rogue systems.	223
How the Rogue System Sensor works.	223
Passive listening to layer-2 traffic.	223
Intelligent filtering of network traffic.	224
Data gathering and communications to the server.	224
Systems that host sensors.	225
How detected systems are matched and merged.	225
Rogue System Detection states.	226
Overall system status.	226
Rogue System Sensor status.	227
Subnet status.	228

Top 25 Subnets.....	228
Rogue Sensor Blacklist.....	229
Rogue System Detection policy settings.....	229
Considerations for policy settings.....	229
Rogue System Detection permission sets.....	231
Setting up Rogue System Detection.....	231
Configuring Rogue System Detection policy settings.....	232
Configuring server settings for Rogue System Detection.....	232
Editing Detected System Compliance.....	232
Editing Detected Systems Matching.....	233
Editing Rogue System Sensor settings.....	234
Editing Detected System Exception Categories.....	234
Editing Detected System OUIs.....	235
Working with detected systems.....	235
Adding systems to the Exceptions list.....	235
Adding systems to the Rogue Sensor Blacklist.....	236
Adding detected systems to the System Tree.....	236
Editing system comments.....	237
Exporting the Exceptions list.....	237
Importing systems to the Exceptions list.....	238
Merging detected systems.....	238
Pinging a detected system.....	238
Querying detected system Agents.....	239
Removing systems from the Detected Systems list.....	239
Removing systems from the Exceptions list.....	239
Removing systems from the Rogue Sensor Blacklist.....	240
Viewing detected systems and their details.....	240
Working with sensors.....	240
Changing the sensor-to-server port number.....	241
Installing sensors.....	241
Editing sensor descriptions.....	243
Removing sensors.....	243
Working with subnets.....	244
Adding subnets.....	244
Deleting subnets.....	244
Ignoring subnets.....	245
Including subnets.....	245

Renaming subnets.....	245
Viewing detected subnets and their details.....	246
Rogue System Detection command-line options.....	246
Default Rogue System Detection queries.....	247
Setting Up Automatic Responses.....	248
Automatic Responses and how it works.....	249
Throttling, aggregation, and grouping.....	249
Default rules.....	250
Planning.....	251
Determining how events are forwarded.....	251
Determining which events are forwarded immediately.....	251
Determining which events are forwarded.....	252
Configuring Automatic Responses.....	252
Assigning permission sets to access Automatic Responses.....	252
Working with SNMP servers.....	254
Working with registered executables and external commands.....	256
Creating and editing Automatic Response rules.....	258
Describing the rule.....	258
Setting filters for the rule.....	259
Setting thresholds of the rule.....	259
Configuring the action for Automatic Response rules.....	260
Frequently asked questions.....	261
Managing Issues and Tickets.....	263
Ways to manage issues.....	263
Creating, configuring, and managing issues.....	264
Creating basic issues manually.....	264
Configuring responses to automatically create issues.....	265
Managing issues.....	269
Purging closed issues.....	270
Purging closed issues manually.....	270
Purging closed issues on a schedule.....	270
Tickets and how they work.....	271
Ways to add tickets to issues.....	271
Assignment of ticketed issues to users.....	271
How tickets and ticketed issues are closed.....	271
Benefits of adding comments to ticketed issues.....	271
How tickets are reopened.....	272

Synchronization of ticketed issues.	272
Integration with ticketing servers.	272
Considerations when deleting a registered ticketing server.	273
Required fields for mapping.	273
Sample mappings.	273
Working with tickets.	276
Adding tickets to issues.	276
Synchronizing ticketed issues.	276
Synchronizing ticketed issues on a schedule.	277
Working with ticketing servers.	277
Installing extensions for ticketing server.	278
Registering and mapping a ticketing server.	281
Configuring the field mappings.	282
Upgrading a registered ticketing server.	284
Appendix: Maintaining ePolicy Orchestrator Databases.	285
Perform regular maintenance of SQL Server databases.	285
Backup and restore ePolicy Orchestrator databases.	286
Changing SQL Server information.	286

Introducing ePolicy Orchestrator 4.5

ePolicy Orchestrator 4.5 provides a scalable platform for centralized policy management and enforcement of your security products and the systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

Contents

- ▶ [Components and what they do](#)
- ▶ [Using this guide](#)
- ▶ [Finding documentation for McAfee enterprise products](#)

Components and what they do

The ePolicy Orchestrator software is comprised of these components:

- **ePO server** — The center of your managed environment. The server delivers security policies and tasks, controls updates, and processes events for all managed systems. The ePO server includes these subcomponents:
 - Application server — Auto Response, Registered Servers, and user interface
 - Agent Handler — Policies, tasks, and properties
 - Event parser — Threat events and client events
 - RSD server and data channel listener
- **Registered servers** — Used to register the ePO server with other servers. Registered server types include:
 - LDAP server — Used for Policy Assignment Rules and to enable automatic user account creation.
 - SNMP server — Used to receive an SNMP trap. You must add the SNMP server's information so that ePolicy Orchestrator knows where to send the trap.
 - Ticketing server — Before tickets can be associated with issues, you must have a registered Ticketing server configured. The system running the ticketing extension must be able to resolve the address of the Service Desk system.
- **Database** — The central storage component for all data created and used by ePolicy Orchestrator. You can choose whether to house the database on your ePO server or on a separate system, depending on the specific needs of your organization.
- **Master repository** — The central location for all McAfee updates and signatures, residing on the ePO server. Master repository retrieves user-specified updates and signatures from McAfee or from user-defined source sites.
- **Distributed repositories** — Placed strategically throughout your environment to provide managed systems access 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.

- **McAfee Agent** — A vehicle of information and enforcement between the 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 ePO server. A McAfee Agent can also be configured as a SuperAgent with the addition of a repository.
- **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 can help you manage the needs of large or complex network infrastructures by allowing you more control over agent-server communication.

NOTE: Depending on the needs of your organization and the complexity of your network, you might not need to use all of these components.

Using this guide

This guide provides information on configuring and using your product. For system requirements and installation instructions, see the *ePolicy Orchestrator Installation Guide*.

This material is organized in the order that McAfee recommends you set up ePolicy Orchestrator in a production environment for the first time, and is also accessible to anyone seeking specific topics.

This guide serves as a tool to help administrators set up their ePolicy Orchestrator environment for the first time, and as a reference tool for more experienced users.

Audience

This information is intended primarily for network administrators who are responsible for their company's security program, and assumes the customer has installed and used ePolicy Orchestrator in a lab environment.

Finding documentation for McAfee enterprise products

To access the documentation for your McAfee products, use the McAfee ServicePortal.

- 1 Go to the McAfee ServicePortal (<http://mysupport.mcafee.com>) and, under **Self Service**, click **Read Product Documentation**.
- 2 Select a **Product**.
- 3 Select a **Version**.
- 4 Select a product document

Product documentation by phase

McAfee documentation provides the information you need during each phase of product implementation, from installing a new product to maintaining existing ones. Depending on the product, additional documents might also be available. After a product is released, information

regarding the product is entered into the online KnowledgeBase, available through the McAfee ServicePortal.

Installation phase — Before, during, and after installation

- *Release Notes*
- *Installation Guide*

Setup phase — Using the product

- *Product Guide*
- *Online Help*

Maintenance phase — Maintaining the software

- *KnowledgeBase* (<http://mysupport.mcafee.com>)

Getting Started with ePolicy Orchestrator 4.5

This chapter provides a high-level overview of ePolicy Orchestrator and how it works. All of the concepts included here, along with their associated tasks, are discussed in greater detail in the chapters that comprise the rest of this guide.

Contents

- ▶ [Logging on and off ePO servers](#)
- ▶ [Viewing the server version number](#)
- ▶ [How to navigate the ePO interface](#)
- ▶ [Setting up ePolicy Orchestrator](#)

Logging on and off ePO servers

Use these tasks to log on to and off from ePO servers. Before using ePolicy Orchestrator, you must be logged on to the ePO server with valid account credentials.

Tasks

- ▶ [Logging on to ePO servers](#)
- ▶ [Logging off ePO servers](#)

Logging on to ePO servers

Use this task to log on to the ePO server. You must have valid credentials to do this. You can log on to multiple ePO servers by opening a new browser session for each ePO server.

Task

- 1 Open an Internet browser and go to the URL of the server to open the **Log On to ePolicy Orchestrator** dialog box.
- 2 Type the **User name** and **Password** of a valid account.
NOTE: Passwords are case-sensitive.
- 3 Select the **Language** you want the software to display.
- 4 Click **Log On**.

Logging off ePO servers

Use this task to log off from ePO servers. Log off from the ePO server whenever you finish using the software.

Task

- To log off from the server, click **Log Off** at the top of any page, or close the browser.

Viewing the server version number

You can view the version number, edition, and license information of the ePolicy Orchestrator server.

- To view the version number and edition of an ePO server, log on to the desired ePolicy Orchestrator server. This information appears in the title bar.

NOTE: For more specific information about the version of ePolicy Orchestrator:

- 1 Click **Menu | Software | Extensions**, then click **Server** in the McAfee category of the Extensions list.
 - 2 Scroll through the server extension to **ePO Core**.
- To view license information, go to the logon page.
 - To view detailed information about the extensions installed on your ePO server, click **Menu | Software | Extension**. Select a category from the Extensions list to view details.

How to navigate the ePO interface

Navigation in ePolicy Orchestrator 4.5 has been redesigned to make it faster and easier to find the features and functionality you need. The interface now uses a single menu for all top-level features of ePolicy Orchestrator, and a customizable navigation bar. Top-level features were previously displayed as tabs when selecting a section.

For example, in ePolicy Orchestrator 4.0, when the Reporting section was selected, the top-level features that were displayed included: Queries, Server Task Log, Audit Log, Event Log, and MyAvert.

In version 4.5, all of these top-level features are accessed from the **Menu**. The following table provides some examples of the change in navigation steps to arrive at a desired page.

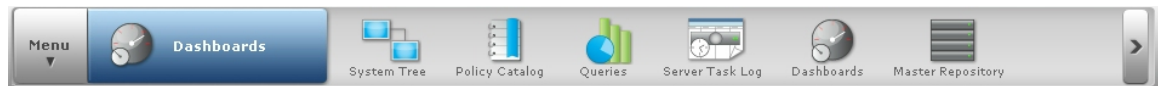
To get to...	in version 4.0	in version 4.5
The Audit Log	Click Menu Audit Log tab.	Click Menu and select User Management Audit Log .
The Policy Catalog	Click Menu Policy Catalog page.	Click Menu and select Policy Policy Catalog .

The Menu



The **Menu** is new in version 4.5 of ePolicy Orchestrator software. The Menu uses categories that comprise the various ePO features and functionalities. Each category contains a list of primary feature pages associated with a unique icon. The Menu and its categories replace static group of section icons used to navigate the 4.0 version of the interface. For example, in the 4.5 version, the Reporting category includes all of the pages included in the 4.0 version Reporting section, plus other commonly used reporting tools such as the Dashboards page. When an item in the Menu is highlighted, its choices appear in the details pane of the interface.

The navigation bar



In ePolicy Orchestrator 4.5, the navigation bar is customizable. In the 4.0 version of the interface, the navigation bar was comprised of a fixed group of section icons that organized functionality into categories. Now you can decide which icons are displayed on the navigation bar by dragging any Menu item on or off the navigation bar. When you navigate to a page in the Menu, or click an icon in the navigation bar, the name of that page is displayed in the blue box next to the Menu.

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

Setting up ePolicy Orchestrator

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

Process overview

- ▶ Configure your ePO server
- ▶ Add systems to the System Tree
- ▶ Distribute agents to your systems
- ▶ Create repositories
- ▶ Configure your policies and client tasks
- ▶ Deploy your products and software
- ▶ Configure advanced features

Configure your ePO server

To configure your ePO server, you'll need to:

- Set up user accounts
- Assign permission sets
- Configure ePO server settings

Set up user accounts

Set up user accounts for all of the users in your network who need to access and use the ePolicy Orchestrator software. You need to set up these accounts before assigning permission sets. For more information on setting up user accounts, see *ePO user accounts* in *Configuring ePolicy Orchestrator*.

To set up user accounts, click **Menu | User Management | Users**.

Assign permission sets

Assign permission sets for your ePO users. Permission sets allow you to define what users are allowed to do with the software. You can assign permission sets to individuals or to groups. For more information on assigning permission sets, see *How permission sets work* in *Managing User Roles and Permissions*.

To assign permission sets, click **Menu | User Management | Permissions Sets**.

Configure server settings

Configure server settings for your specific environment. You can change the server settings at any time. For more information on configuring server settings, see *Server settings and the behaviors they control* in *Managing User Roles and Permissions*.

To configure server settings, click **Menu | Configuration | Server Settings**.

Add systems to the System Tree

The System Tree allows you to organize and act on all systems you manage with ePolicy Orchestrator. Before setting up other features, you must create your System Tree. There are several ways you can add systems to the System Tree, including:

- Synchronize ePolicy Orchestrator with your Active Directory server.
- Browse to systems on your network individually.

- Add individual and groups of systems by importing a text (.txt) file containing a list of systems. For more information on all of the methods you can use to add systems, including detailed steps for each method, see *Organizing the System Tree*.

To begin adding systems to the System Tree, click **Menu | Systems | System Tree**.

Distribute agents to your systems

Each system you want to manage must have the McAfee Agent installed. You can install agents on Windows-based systems manually, or by using the ePO interface. You must install agents on non-Windows systems manually.

Once agents are installed on all of your systems, you can use ePolicy Orchestrator to manage, update, and report on these systems. For more information on distributing agents, see *Distributing Agents*.

To begin distributing agents to your systems, click **Menu | Systems | System Tree**.

Create repositories

Before deploying any products, components, or updates to your managed systems with ePolicy Orchestrator, you must configure repositories. There are two types of repositories you can use in your environment, master and distributed.

Master repository

The master repository is located on your ePO server. It is the location where products and updates that are pulled from the Source Site are saved. For more information about the master repository, see *Repository types and what they do* in *Creating Repositories*.

To start working with the master repository, click **Menu | Software | Master Repository**.

Distributed repositories

Distributed repositories are those that you place throughout your network. The placement and type of distributed repositories you use depend on the unique needs of your organization and environment. There are several ePO components and types you can use for distributed repositories, including:

- SuperAgents
- FTP
- HTTP
- UNC share
- Unmanaged

The complexity and size of your network are determining factors in which type and how many distributed repositories you use. For more information about distributed repositories, see *Repository types and what they do* in *Creating Repositories*.

To start working with distributed repositories, click **Menu | Software | Distributed Repository**.

Configure your policies and client tasks

McAfee recommends that you configure policy settings before deploying the respective product, component, or update to your managed systems. By doing so you can ensure that products and components have the desired settings as soon as possible.

Policies

A policy is a collection of settings that you create and configure. These policies are enforced by McAfee products. Policies ensure that the managed security products are configured and perform according to that collection of settings.

Once configured, policies can be enforced at any level of the System Tree, as well as on specific groups of users. System policies are inherited from their parent group in the System Tree. However, you can break inheritance at any location in the tree in order to enforce specific policies at a particular location. For more information about policies, see *Policy management and Policy application* in *Configuring Policies and Client Tasks*.

To start configuring policies for systems in the System Tree, click **Menu | Policy | Policy Catalog**, then select a product from the **Product** menu and click **Actions | New Policy**.

Client tasks

Client tasks are scheduled actions that run on managed systems that host any client-side software. You can define tasks for the entire System Tree, a specific group, or an individual system. Like policy settings, client tasks are inherited from parent groups in the System Tree. For more information about client tasks, see *Client tasks and what they do* in *Configuring Policies and Client Tasks*.

To start scheduling client tasks, click **Menu | Systems | System Tree | Client Tasks**, then click **Actions | New Task**.

Deploy your products and software

Once your repositories, policy settings, and client tasks are created and configured, you can deploy products, components, and updates to the desired systems with ePolicy Orchestrator. You can perform these actions as needed, or you can schedule them using server tasks. For more information, see *Deploying Software and Updates*.

To schedule these actions, click **Menu | Automation | Server Tasks**, then click **Actions | New Task**.

Configure advanced features

Once your managed environment is up and running, you can configure and implement the advanced features of ePolicy Orchestrator, including:

- Remote Agent Handlers
- Automatic Responses
- Issues and Ticketing

More information on these and all ePolicy Orchestrator features is available in the following chapters of this guide.

Configuring ePolicy Orchestrator

The ePO server is the center of your managed environment, providing a single location from which to administer system security throughout your network.

If your organization is very large or divided into multiple large sites, ePolicy Orchestrator 4.5 is scalable to allow you to customize how you set up your managed environment. You can:

- Install a separate ePO server at each site.
- Install remote Agent Handlers at each site, provided an ePO server is installed that you want to communicate with.

The option you choose depends on the needs of your environment. Using remote agent handlers allows you to reduce network traffic when managing agents and sending updates. Agent handlers can also serve as distributed repositories. Remote agent handlers help to load balance your network and increase fallback security, while passing all agent-server communication back to your ePO server and its database.

Using multiple ePO servers differs from using remote agent handlers because each ePO server maintains a separate database from which you can roll up information to your main ePO server and database. Both choices can help to limit the amount of network traffic created within a local LAN. Network traffic has a larger impact on your resources when this communication takes place across WAN, VPN, or other slower network connections typically found between remote sites.

Are you configuring the ePO server for the first time?

When configuring the ePO server for the first time:

- 1 Decide how to implement the flexibility of permission sets.
- 2 Create user accounts and permission sets, and assign the permission sets to the user accounts as needed.
- 3 Set up your contacts list and email server settings.

Contents

- ▶ [ePO user accounts](#)
- ▶ [How permission sets work](#)
- ▶ [Contacts](#)
- ▶ [Server settings and the behaviors they control](#)
- ▶ [Managing ePolicy Orchestrator users with Active Directory](#)
- ▶ [Registering servers for use with ePolicy Orchestrator](#)
- ▶ [Security keys and how they work](#)
- ▶ [MyAvert Security Threats](#)
- ▶ [Agent Handlers and what they do](#)
- ▶ [IPv6](#)

- ▶ [Exporting tables and charts to other formats](#)

ePO user accounts

User accounts provide a means for users to access and use the software. They are associated with permission sets, which define what users are allowed to do with the software.

You must create user accounts and permission sets to accommodate the needs of each user that logs on to the ePO server. You can create accounts for individual users, or you can create a permission set that maps to users or groups in your Active Directory/NT server.

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

Global administrators

Global administrators have read and write permissions and rights to all operations. When you install the server, a global administrator account is created with the user name admin.

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

Permissions exclusive to global administrators include:

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

Working with user accounts

Use these tasks to create and maintain user accounts.

Tasks

- ▶ [Creating user accounts](#)
- ▶ [Editing user accounts](#)
- ▶ [Deleting user accounts](#)

Creating user accounts

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Users**, then click **New User**. The New User page appears.
- 2 Type a user name.

- 3 Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization, you might want to disable it.
- 4 Select whether the new account uses **ePO authentication** or **Windows authentication**, and provide the required credentials.
- 5 Optionally, provide the user's full name, email address, phone number, and a description in the **Notes** text box.
- 6 Choose to make the user a global administrator, or select the appropriate permission sets for the user.
- 7 Click **Save** to save the current entries and return to the Users tab. The new user should appear in the Users list.

Editing user accounts

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

Task

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

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

Deleting user accounts

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

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

Task

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

- 1 Click **Menu | User Management | Users**.
- 2 From the Users list, select the user you want to delete, then click **Actions | Delete**.
- 3 Click **OK**.

How permission sets work

A permission set is a group of permissions that can be granted to users or Active Directory (AD) groups by assigning it to those users' accounts. One or more permission sets can be assigned to users who are not global administrators (global administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if

one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks. Consider this as you plan your strategy for granting permissions to the users in your environment.

When are permission sets assigned?

Global administrators can assign existing permission sets when they create or edit user accounts and when they create or edit permission sets.

What happens when I install new products?

When a new product extension is installed, it can add one or more groups of permissions to the permission sets. For example, when you install a VirusScan Enterprise extension, a VirusScan Enterprise section is added to each permission set. Initially, the newly added section is listed in each permission set with no permissions yet granted. The global administrators can then grant permissions to users through existing or new permission sets.

Default permission sets

ePolicy Orchestrator 4.5 ships with four default permission sets that provide permissions to ePolicy Orchestrator functionality. These are:

- **Executive Reviewer** — Provides view permissions to dashboards, events, contacts, and can view information that relates to the entire System Tree.
- **Global Reviewer** — Provides view access globally across functionality, products, and the System Tree, except for extensions, multi-server roll-up data, registered servers, and software.
- **Group Admin** — Provides view and change permissions across ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.
- **Group Reviewer** — Provides view permissions across ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.

Working with permission sets

Use these tasks to create and maintain permission sets.

Tasks

- ▶ [Creating permission sets for user accounts](#)
- ▶ [Duplicating permission sets](#)
- ▶ [Editing permission sets](#)
- ▶ [Deleting permission sets](#)

Creating permission sets for user accounts

Use this task to create a permission set.

Before you begin

You must be a global administrator to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Permission Sets**, then click **New Permission Set**.
- 2 Type a name for the permission set and select the users to which the set is assigned.
- 3 Select a server name from the drop-down list, or click **Add** if the server name you need does not appear in the server list.
- 4 Click **Save**. The Permission Sets page appears.
- 5 Select the new permission set from the Permission Sets list. Its details appear to the right.
- 6 Click **Edit** next to any section where you want to grant permissions.
- 7 On the Edit Permission Set page that appears, select the appropriate options, then click **Save**.
- 8 Repeat for all appropriate sections of the permission set.

Duplicating permission sets

Use this task to duplicate a permission set. Duplicating a permission set is useful when you want to change only a few of the settings for a new permission set. Only global administrators can duplicate permission sets.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Permission Sets**, then select the permission set you want to edit in the Permission Sets list. Its details appear to the right.
- 2 Click **Actions | Duplicate**, type a New name in the Duplicate dialog box, then click **OK**.
- 3 Select the new duplicate in the Permission Sets list. Its details appear to the right.
- 4 Click **edit** next to any section where you want to change permissions.
- 5 On the Edit Permission Set page that appears, select the appropriate options, then click **Save**.
- 6 Repeat for all sections of the permission set where you want to grant permissions.

Editing permission sets

Use this task to edit a permission set. Only global administrators can edit permission sets.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Permission Sets**, then select the permission set you want to edit in the Permission Sets list. Its details appear to the right.
- 2 Click **Edit** next to any section where you want to grant permissions.
- 3 On the Edit Permission Set page that appears, select the appropriate options, then click **Save**.
- 4 Repeat for all appropriate sections of the permission set.

Deleting permission sets

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

Task

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

- 1 Click **Menu | User Management | Permission Sets**, then select the permission set you want to delete in the Permission Sets list. Its details appear to the right.
- 2 Click **Actions | Delete**, then click **OK** in the Action pane. The permission set no longer appears in the Permission Sets list.

Contacts

The ePolicy Orchestrator software maintains a list of email addresses that it uses to send email messages to specified users in response to events. Currently this list is used by Automatic Responses, Queries, and export functionality.

Working with contacts

Use these tasks to create and maintain email address information of individuals who might receive email messages from ePolicy Orchestrator.

Tasks

- ▶ [Creating contacts](#)
- ▶ [Editing contacts](#)
- ▶ [Deleting contacts](#)

Creating contacts

Use this task to add email addresses to Contacts.

Task

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

- 1 Click **Menu | User Management | Contacts**, then click **Actions | New Contact**.
- 2 Type a first name, last name, and email address for the contact.
- 3 Click **Save**. The new contact appears on the Contacts page.

Editing contacts

Use this task to edit information in an existing entry on the Contacts page.

Task

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

- 1 Click **Menu | User Management | Contacts**, then select a contact.
- 2 Click **Actions | Edit**. The Edit Contact page appears.

- 3 Edit the information as desired.
- 4 Click **Save**.

Deleting contacts

Use this task to delete entries from the Contacts page.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Contacts**, then select a contact.
- 2 Click **Actions | Delete**, then click **OK** in the Action pane. The contact no longer appears in the list.

Server settings and the behaviors they control

Various settings control how the ePO server behaves. You can change most settings at any time. But, only global administrators can access the server settings.

Types of ePO server settings are:

- **Dashboards** — Specifies the default active dashboard that is assigned to new users' accounts at the time of account creation, if one has been defined.
- **Detected System Compliance** — Specifies the settings that affect how rogue systems in your network are identified and treated.
- **Detected System Exception Categories** — Specifies the categories that can be used to mark systems in your environment as exceptions.
- **Detected System Matching** — Specifies the settings used to match detected systems and system interfaces.
- **Detected System OUIs** — Specifies how your OUI (Organizationally Unique Identifier) list is updated, and when the last update occurred.
- **Email Server** — Specifies the email server that is used when ePolicy Orchestrator sends email messages.
- **Event Filtering** — Specifies which events are forwarded by the agent.
- **Event Notification** — Specifies the interval at which you want ePO Notification Events to be sent to Automatic Responses.
- **Global Updating** — Specifies whether and how global updating is enabled.
- **License Key** — Specifies the 25 digit license key you provide while installing ePolicy Orchestrator, via the hyperlink from the Log On to ePO page to an Enter License Key page, or via this Server Settings page. McAfee introduced license keys to help customers with license usage tracking needs and to be compliant with McAfee licensing terms.
- **MyAvert Security Threats** — Specifies the update frequency for the MyAvert Security Threats service. If proxy settings are entered in Proxy Settings, they are used while collecting MyAvert security threats.
- **Policy Maintenance** — Specifies whether policies for unsupported products are visible or hidden. This is needed only after ePolicy Orchestrator is upgraded to 4.5 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.
- **Proxy Settings** — Specifies the type of proxy settings configured for your ePO server.
- **Repository Packages** — Specifies whether any package can be checked in to any branch. Only agents later than version 3.6 can retrieve packages other than updates from branches other than Current.
- **Rogue System Sensor** — Specifies the settings that define behavior for Rogue System Sensors in your network.
- **Security Keys** — Specifies and manages the agent-server secure communication keys, and repository keys.
- **Server Certificate** — Specifies the server certificate that your ePO server uses for HTTPS communication with browsers.
- **System Tree Sorting** — Specifies whether and how System Tree sorting is enabled in your environment.
- **User Auto Creation** — Specifies whether ePO users are automatically created upon logon, based on AD (Active Directory) user profiles.
- **Windows Authentication** — Specifies the domain name and Active Directory servers configured. This is also used for user authentication. For example, Windows Authentication is used to determine if the password entered should allow the user to log on to ePolicy Orchestrator.
- **Windows Authorization** — Specifies the domain name and Active Directory servers configured for use with this ePO server. This is used while dynamically assigning permissions to the users who have logged on to ePolicy Orchestrator.

Working with server settings

Use these tasks to configure and maintain the server. Only general server settings are covered here. Feature-specific server settings are covered in the sections for those features. For example, System Tree sorting server settings are covered in *Organizing the Systems Tree*.

Tasks

- ▶ [Specifying an email server](#)
- ▶ [Replacing the server certificate](#)
- ▶ [Configuring the template and location for exported reports](#)
- ▶ [Determining which events are forwarded to the server](#)
- ▶ [Viewing and changing communication ports](#)

Specifying an email server

Use this task to specify an email server that ePolicy Orchestrator uses to send email messages.

Task

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

- 1 Click **Menu | Configuration | Server Settings**, then click **Email Server** in the Settings Categories list.
- 2 Click **Edit**. The Edit Email Server page appears.
- 3 Type the SMTP server name and SMTP server port.
- 4 Select whether to authenticate to the email server, and provide credentials if **Authenticate** is selected.
- 5 Type the email address that appears as the return address on messages sent from ePolicy Orchestrator.
- 6 Click **Save**, then select **Email Server**.
- 7 In the content area next to **Test email**, type a valid email address for receiving email messages, then click **Test** to validate the settings.

Replacing the server certificate

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

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**.

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

Configuring the template and location for exported reports

Use this task to define the appearance and storage location for tables and dashboards you export as documents. You can configure:

- Headers and footers, including a custom logo, name, page numbering, etc.
- Page size and orientation for printing.
- Directory where exported tables and dashboards are stored.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, then select **Printing and Exporting** in the Settings list.
- 2 Click **Edit**. The Edit Printing and Exporting page appears.
- 3 In the **Headers and footers for exported documents** section, click **Edit Logo** to open the Edit Logo page.

- a Select **Text** and type the text you want included in the document header, or do one of the following r:
 - Select **Image** and browse to the image file, such as your company logo.
 - Select the default McAfee logo.
 - b Click **OK** to return to the Edit Printing and Exporting page.
 - 4 From the drop-down lists, select any metadata that you want displayed in the header and footer.
 - 5 Select a **Page size** and **Page orientation**.
 - 6 Type a new location or except the default location where exported documents will be saved.
 - 7 Click **Save**.

Determining which events are forwarded to the server

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

Before you begin

You must be a global administrator to perform this task.

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 ePO server.

Enabling user autocreation

Use this task to enable user autocreation, which creates ePO user account records for Active Directory users when they first log on.

Before you begin

Configure the following prerequisites before enabling User Auto Creation,

- 1 Register the LDAP server containing the user accounts with your ePO server.
 - NOTE:** ePO 4.5 supports only Windows LDAP servers.
- 2 Edit Windows Authorization settings to map the corresponding domain and the registered LDAP server.
 - NOTE:** If the LDAP server is on a different domain, then specify the corresponding domain controller on the Windows Authentication settings. For more information on editing windows authentication settings, see *Configuring Windows authentication* section.
- 3 Create a new permission set and map the Active Directory groups.
 - NOTE:** Permission sets are assigned to users based on the Active Directory groups mapped to it. For example, User1 is a member of Group1 and Group2. P1 and P2 are permission

sets mapped to Group1 and Group2 respectively. In this case, User1 will have a combined permissions of P1 and P2 to the ePO server.

- 4 Add users to be created to the Active Directory group.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, then select **User Auto Creation** from the Settings Categories list.
- 2 Click **Edit**. The Edit User Auto Creation page opens.
- 3 Select **Automatically create ePO user records for Active Directory users at logon**, then click **Save**.

NOTE:

- Users are not automatically created if they do not belong to a group with at least one mapped permission set.
 - You cannot create a global administrator using user autocreation.
- 4 The user can log on to ePO server with Active Directory credentials.

Viewing and changing communication ports

Use this task to view the ports that ePolicy Orchestrator uses for communication with distributed components. These ports were originally configured during installation. After installation you can change only the two ports used for agent communication. If you need to change other ports, you must reinstall the server and reconfigure the ports in the installation wizard.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, select **Ports**, then click **Edit**. The Edit Ports page appears.
- 2 Change the agent-server communication port or agent broadcast communication port as necessary, then click **Save**.

NOTE: The agent-server communication port is used for agent-server communication; the agent broadcast port is used for SuperAgent wake-up calls. Any changes take effect during the next agent-server communication.

SSL certificates

The browsers supported by 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 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 ePO console. To stop this warning message from appearing you must do one of the following:

- Add the ePO server certificate to the collection of trusted certificates used by the browser.
NOTE: This must be done for every browser that interacts with ePO. If the browser certificate changes, you must add the 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 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.
NOTE: 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 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 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.

Installing a trusted security certificate for the ePO browser

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

Tasks

- ▶ [Installing the security certificate when using Internet Explorer 7](#)
- ▶ [Installing the security certificate when using Internet Explorer 8](#)
- ▶ [Installing the security certificate when using Firefox 3.0](#)

Installing the security certificate when using Internet Explorer 7

Use this task to install the security certificate when using Internet Explorer 7, so that the Certificate Error warning won't appear every time you log on.

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

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

- 5 Select the Certification Path tab, then select **Orion_CA_<servername>**, and click **View Certificate**. Another Certificate dialog box opens to the General tab, displaying the Certificate Information.
- 6 Click **Install certificate** to open the Certificate Import Wizard.
- 7 Click **Next** to specify where the certificate is stored.
- 8 Select **Place all certificates in the following store**, then click **Browse** to select a location.
- 9 Select the **Trusted Root Certificate Authorities** folder from the list, click **OK**, then click **Next**.
- 10 Click **Finish**. In the Security Warning that appears, click **Yes**.
- 11 Close the browser and restart ePolicy Orchestrator.

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

Installing the security certificate when using Internet Explorer 8

Use this task to install the security certificate when using Internet Explorer 8, so that the warning dialog box won't appear every time you log on.

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.
CAUTION: Do not click **Install Certificate** on the General tab. If you do, the process fails.
- 5 Select the Certification Path tab, then select **Orion_CA_<servername>**, and click **View Certificate**. Another Certificate dialog box opens to the General tab, displaying the Certificate Information.
- 6 Click **Install certificate** to open the Certificate Import Wizard.
- 7 Click **Next** to specify where the certificate is stored.
- 8 Select **Place all certificates in the following store**, then click **Browse** to select a location.
- 9 Select the **Trusted Root Certificate Authorities** folder from the list, click **OK**, then click **Next**.
- 10 Click **Finish**. In the Security Warning that appears, click **Yes**.
- 11 Close the browser and restart ePolicy Orchestrator.

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

Installing the security certificate when using Firefox 3.0

Use this task to install the security certificate when using Firefox 3.0, so that the warning dialog box won't appear every time you log on.

Task

- 1 From your browser, start ePolicy Orchestrator. The Secure Connection Failed page appears.
- 2 Click **Or you can add an exception** at the bottom of the page. The page now displays the Add Exception button.
- 3 Click **Add Exception**. The Add Security Exception dialog appears.
- 4 Click **Get Certificate**. The Certification Status information is populated and the Confirm Security Exception button is enabled.
- 5 Make sure that **Permanently store this exception** is selected, then click **Confirm Security Exception**.

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

Managing ePolicy Orchestrator users with Active Directory

ePolicy Orchestrator 4.5 offers the ability to dynamically create ePO users and assign permission sets to them by automatically creating users based on Windows authenticated user credentials. This process is accomplished by mapping ePO permission sets to Active Directory groups in your environment. This feature can reduce the management overhead when you have a large number of ePO users in your organization. To complete the configuration, you must work through the following process:

- 1 Configure user authentication.
- 2 Register LDAP servers.
- 3 Configure Windows authorization.
- 4 Assign permission sets to the Active Directory group.
- 5 Enable user autcreation.

User authentication

ePolicy Orchestrator users can be authenticated with ePO password authentication or Windows authentication. If you use Windows authentication, you can specify whether users authenticate:

- Against the domain that your ePO server is joined to (default).
- Against a list of one or more domain controllers.
- Using a WINS server to look up the appropriate domain controller.

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

Registered LDAP servers

It is necessary to register LDAP servers with your 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.

NOTE: Users trusted via one-way external trusts are not supported. Active Directory is the only LDAP server type supported at this time.

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.

NOTE: ePolicy Orchestrator can dynamically assign permission sets Windows Authenticated users even if user autocreation 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.

User autocreation

When you have configured the previously discussed sections, you can enable the User autocreation server setting. User autocreation 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.
- The domain used in the logon attempt maps to a domain listed in the windows authorization server setting.
- The Active Directory server mapped to the domain contains a record for the user.
- The user is a member of at least one group that maps to an ePO permission set.

Configuring Windows authentication and authorization

Use these tasks to set up automatic user creation.

Tasks

- ▶ [Configuring Windows authentication](#)
- ▶ [Registering LDAP servers](#)
- ▶ [Configuring Windows authorization](#)
- ▶ [Enabling user autocreation](#)

Configuring Windows authentication

Use this task to configure Windows authentication. How you configure these settings depends on several variables:

- Do you want to use a WINS server to look up which domain your users are authenticating against?
- Do you want to use multiple domain controllers?

By default, users can authenticate using Windows credentials for the domain that the ePO server is joined to. If you have multiple domains, or your ePO server is not located in the same domain as your users, you must configure Windows authentication

Before you begin

To access the Windows Authentication page in the server settings, you must stop the ePolicy Orchestrator application service using these steps:

- 1 From the server console, click **Start | Settings | Control Panel | Administrative Tools | Services**. The Services window opens.
- 2 Right-click **McAfee ePolicy Orchestrator Applications Server** and select **Stop**.
- 3 Rename the WinAuth.dll file to WinAuth.bak.

NOTE: In default installations, this file's location is C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin.

- 4 Restart the server.

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**. The Edit Windows Authentication page opens.
- 3 Specify whether to use Domain controllers or WINS server, using the DNS host name.

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

- 4 Click **Save**.

Configuring Windows authorization

Use this task to configure the Windows authorization settings that are used with your Active Directory servers. This is required to enable:

- Dynamic assignment of permission sets
- Automatic user account creation

Before you begin

You must register an LDAP server with your ePO server.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, click **Windows Authorization**, then click **Edit**. The Edit Windows Authorization page opens.
- 2 Select the **Default Active Directory Server** from the list.
- 3 Specify the **NetBIOS Domain Name** for your LDAP server, and select your **Active Directory Server** from the list, then click **Save**.

NOTE: You can add or remove multiple domains using + or -.

Registering servers for use with ePolicy Orchestrator

ePolicy Orchestrator 4.5 can be set up to work with a variety of servers that you might use in your network. Different types of servers are needed to support various functionalities of ePolicy Orchestrator and other McAfee and third-party products.

Contents

- ▶ [What are registered servers](#)
- ▶ [Registering servers](#)

What are registered servers

Registered servers are servers that work with your ePO server to support or add functionality. When you install ePolicy Orchestrator for the first time, no other servers are registered with your ePO server.

You can register several types of servers with your main ePO server, including:

- **ePolicy Orchestrator servers** — You can register additional ePO servers to use with your main ePO server.
- **LDAP servers** — Lightweight Directory Access Protocol (LDAP) servers can use ePO functionality, such as automatic user creation and Policy Assignment Rules.
- **SNMP servers** — Simple Network Management Protocol (SNMP) servers can enable the use of SNMP traps as Automatic Response actions.

Registering servers

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

Tasks

- ▶ [Registering ePO servers](#)
- ▶ [Registering LDAP servers](#)
- ▶ [Registering SNMP servers](#)

Registering ePO servers

Use this task to register additional ePO servers for use with your main ePO server.

Task

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

- 1 Click **Menu | Configuration | Registered Servers** and click **New Server**. The Registered Server Builder wizard opens.
- 2 From the Server type menu on the Description page, select **ePO 4.5**, specify a unique name and any notes, then click **Next**. The Details page opens.
- 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
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).
Password	Specifies the password for this server.
Policy sharing	Specifies whether to enable or disable policy sharing for this server.
SQL Server instance	Allows you to specify whether this is the default server or a specific instance, by providing the Instance name.
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	Verifies the connection for the detailed server.
Transfer systems	Specifies whether to enable or disable the ability to transfer systems for this server. When enabled, select Automatic sitelist import or Manual sitelist import .
Use NTLMv2	Optionally choose to use NT LAN Manager authentication protocol. Select this option when the server you are registering employs this protocol.
User name	Specifies the user name for this server.

4 Click **Save**.

Registering LDAP servers

Use this task to register an LDAP (Lightweight Directory Access Protocol) server. You must have a registered LDAP server to use Policy Assignment Rules, to enable dynamically assigned permission sets, and to enable automatic user account creation.

Before you begin

Make sure you have the appropriate rights to modify server settings, permission sets, users, and registered servers.

Task

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

1 Click **Menu | Configuration | Registered Servers**, then click **New Server**. The Registered Server Builder wizard opens.

- 2 From the Server type menu on the Description page, select **LDAP Server**, specify a unique name and any details, then click **Next**. The Details page appears.
- 3 Specify the **Server name**, **Username**, **Password**, then click **Save**.

NOTE: Default settings for the **Username Attribute**, **Group name Attribute**, and **Unique ID Attribute** are provided automatically. These default settings support standard Active Directory configurations. You should change these settings only if you have a custom configuration, and can verify that the correct settings are different than those provided.

Registering SNMP servers

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

Task

For option definitions click ? in the interface.

- 1 Click **Menu | Configuration | Registered Servers**, then click **New Server**. The Registered Server Builder wizard opens.
- 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**. The Details page appears.
- 3 From the URL drop-down list, select one of these types of server address, then enter the address:

Option	Definition
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 Server page.

Security keys and how they work

ePolicy Orchestrator relies on three security key pairs to:

- Authenticate agent-server communication.
- Verify the contents of local repositories.
- Verify the contents of remote repositories.

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

Agent-server secure communication (ASSC) keys

- The first time the agent communicates with the server, it sends its public key to the server.
- From then on, the server uses the agent public key to verify messages signed with the agent's secret key.
- The server uses its own secret key to sign its message to the agent.
- The agent uses the server's public key to verify the agent's message.
- You can have multiple secure communication key pairs, *but only one can be designated as the master key*.
- When the client agent key updater task runs (**ePO Agent Key Updater 3.5.5**), agents using different public keys receive the current public key.
- If you are upgrading from ePolicy Orchestrator 3.6 or earlier, a legacy key is retained. If you are upgrading from ePolicy Orchestrator 3.6.1, the legacy key is the master key by default. If you are upgrading from ePolicy Orchestrator 4.0, the master key is unchanged. Whether or not you upgrade from version 3.6.1 or 4.0, the existing keys are migrated to your ePO 4.5 server.

Local master repository key pairs

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

Other repository key pairs

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

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

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

Backing up and restoring keys

Use these tasks to back up and restore security keys.

Tasks

- ▶ [Backing up all security keys](#)
- ▶ [Restoring security keys](#)
- ▶ [Restoring security keys from a backup file](#)

Backing up all security keys

McAfee recommends periodically backing up all security keys, and always creating a backup before making any changes to the key management settings. Store the backup in a secure network location, so that the keys can be restored easily in the unexpected event any are lost from the ePO server.

Use this task to back up all security keys that are currently managed on this 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 Click **Back Up All** near the bottom of the page. The File Download dialog box appears.
- 3 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**.

Restoring security keys

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

Use this task to restore the security keys on the 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 Click **Restore All** near the bottom of the page. The Restore Security Keys page appears.
- 3 Browse to the zip file containing the security keys, select it, and click **Next**. The Restore Security Keys wizard opens to the Summary page.
- 4 Browse to the keys you want to replace your existing key with, then click **Next**.
- 5 Click **Restore**. The Edit Security Keys page reappears.
- 6 Browse to a secure network location to store the zip file, then click **Save**.

Restoring security keys from a backup file

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

Before you begin

You must have already created a backup zip file of all of your keys.

CAUTION: When you restore security keys, all existing keys are removed and replaced by the keys in the backup file. Ensure that the needed keys are in the backup file before overwriting all existing keys.

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 Click **Restore All** at the bottom of the page. The Restore Security Keys wizard opens.
- 3 Browse to and select the backup zip file, then click **Next**.
- 4 Verify that the keys in this file are the ones you want to overwrite your existing keys, then click **Restore All**.

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 ePO server. If the content is unsigned, or signed with an unknown repository private key, the downloaded content is considered invalid and deleted.

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

Other repository public keys

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

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

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

Working with repository keys

Use these tasks to work with and manage repository keys.

Tasks

- ▶ [Using one master repository key pair for all servers](#)
- ▶ [Using master repository keys in multi-server environments](#)

Using one master repository key pair for all servers

Use this task to ensure that all ePO servers and agents use the same master repository key pair in a multi-server environment. This consists of first exporting the key pair you want all servers to use, then importing the key pair into all other servers in your environment.

Task

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

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

- 2 Next to **Local master repository key pair**, click **Export Key Pair**. The Export Master Repository Key Pair dialog box appears.
- 3 Click **OK**. The File Download dialog box appears.
- 4 Click **Save**, browse to a location that is accessible by the other servers, where you want to save the zip file containing the secure-communication key files, then click **Save**.
- 5 Next to **Import and back up keys**, click **Import**. The Import Keys wizard opens.
- 6 Browse to the zip file containing the exported master repository key files, then click **Next**.
- 7 Verify that these are the keys you want to import, then click **Save**.

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

Using master repository keys in multi-server environments

Use this task to ensure that agents 3.6 and later can use content originating from any ePO server in your environment.

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

The master repository key pair is unique for each installation of ePolicy Orchestrator. If you use multiple servers, each uses a different key. If your agents can download content that originates from different master repositories, you must ensure that agents (version 4.0 and later) recognize the content as valid.

You can ensure this in two ways:

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

The following process exports the key pair from one ePO server to a target ePO server, then, at the target ePO server, imports and overwrites the existing key pair.

Before you begin

McAfee recommends that you back up the existing master repository key pair on the target ePO server before overwriting it with an imported master repository key pair.

You must have permission to access and write to the target ePO server before starting this process.

Task

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

- 1 On the ePO server with the master repository key pair, click **Menu | Configuration | Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**. The Edit Security Keys page appears.
- 2 Next to **Local master repository key pair**, click **Export Key Pair**. The Export Agent-Server Communication Keys dialog box appears.
- 3 Click **OK**. The File Download dialog box appears.
- 4 Click **Save**, then browse to a location on the target ePO server to save the zip file.

- 5 Change the name of the file if needed, then click **Save**.
- 6 On the target ePO server where you want to load the master repository key pair, click **Menu | Configuration | Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**. The Edit Security Keys page appears.
- 7 Next to **Import and back up keys**, click **Import**. The Import Keys dialog box appears.
- 8 Next to **Select file**, browse to and select the master key pair file you saved, then click **Next**. The summary dialog box appears.
- 9 If the summary information appears correct, click **Save**. The new master key pair appears in the list next to **Agent-server secure communication keys**.
- 10 From the list, select the file you imported in the previous steps and click **Make Master**. This changes the existing master key pair to the new key pair you just imported.
- 11 Click **Save** to complete the process.

Agent-server secure communication (ASSC) keys

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

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

NOTE: Windows agents older than version 3.6 are not supported.

Working with ASSC keys

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

Tasks

- ▶ [Deleting agent-server secure communication \(ASSC\) keys](#)
- ▶ [Generating and using new ASSC key pairs](#)
- ▶ [Designating an ASSC key pair as the master](#)
- ▶ [Exporting ASSC keys](#)
- ▶ [Importing ASSC keys](#)
- ▶ [Using the same ASSC key pair for all servers and agents](#)
- ▶ [Using a different ASSC key pair for each ePO server](#)
- ▶ [Viewing systems that use an ASSC key pair](#)

Deleting agent-server secure communication (ASSC) keys

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

CAUTION: Do not delete any keys that are currently in use by any agents. If you do, those agents cannot communicate with the server.

Before you begin

McAfee recommends backing up all keys before making any changes to the key management settings.

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 From the **Agent-server secure communication keys** list, select the key you want to remove, then click **Delete**. The Delete Key dialog box appears.
- 3 Click **OK** to delete the key pair from this server.

Exporting ASSC keys

Use this task to export agent-server secure communication keys from one ePO server to a different ePO server, to allow agents to access that new 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 In the **Agent-server secure communication keys** list, select a key, then click **Export**. The Export Agent-Server Communication Keys dialog box appears.
- 3 Click **OK**. Your browser prompts you to for action to download the sr<ServerName>.zip file to the specified location.

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

Importing ASSC keys

Use this task to import agent-server secure communication keys that were exported from a different ePO server. This procedure allows agents from that server to access this 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 Click **Import**. The Import Keys page appears.
- 3 Browse to and select the key from the location where you saved it (by default, on the desktop), then click **Open**.
- 4 Click **Next** and review the information on the Import Keys page.
- 5 Click **Save**.

Generating and using new ASSC key pairs

Use this task to generate new agent-server secure communication key pairs.

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 the **Agent-server secure communication keys** list, click **New Key**. In the dialog box, type the name of the security key.
- 3 If you want existing agents to use the new key, select the key in the list, then click **Make Master**.

Agents 3.6 and later begin using the new key at the first agent-server communication after their next update task is complete. For earlier versions of the agent, you must run a client product update task to push down the new key, using the agent updater 3.5.5 that is in the master repository.

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

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

Designating an ASSC key pair as the master

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

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 From the **Agent-server secure communication keys** list, select a key , then click **Make Master**.
- 3 Create an update task for the agents to run immediately, so that agents update after the next agent-server communication.

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

- 4 Back up all keys.

Using the same ASSC key pair for all servers and agents

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

Process overview

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

- 1 Create an agent update task.
- 2 Export the keys chosen from the selected 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.

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

Using a different ASSC key pair for each ePO server

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

NOTE: Agents can communicate with only one server at a time. The 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 ePO servers.

Task

For option definitions, click ? in the interface.

- 1 From each ePO server in your environment, export the master agent-server secure communication key pair to a temporary location to where? a location? a zip file?.
- 2 Import each of these key pairs into every ePO server.

Viewing systems that use an ASSC key pair

Use this task to view the systems whose agents use a specific agent-server secure communication key pair, which appears in the **Agent-server secure communication keys** list. After making a specific key pair the master, you might want to view the systems that are still using the previous key pair. Do not delete a key pair until you know that no agents are still using it.

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

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

MyAvert Security Threats

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

Protection status and risk assessment

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

Protection available

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

Protection pending on Medium-to-Low Risk Threats

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

Protection Pending on High-Risk Threats

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

Working with MyAvert Security Threats

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

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

Tasks

- ▶ [Configuring MyAvert update frequency](#)
- ▶ [Viewing threat notifications](#)
- ▶ [Deleting threat notifications](#)

Configuring MyAvert update frequency

Use this task to configure the update frequency for MyAvert Security Threats.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, select **MyAvert Security Threats**, then click **Edit**.
- 2 In the **Updating** option, chose one of the following:
 - **Update MyAvert Security Threats every** — Select, type a number, and select a unit of time from the list for the updates to occur.
 - **Do not update MyAvert Security Threats** — Select to stop updates.
- 3 Click **Save**.

Viewing threat notifications

Use this task to view threat notifications and mark threats as read or unread. You can filter threats by their importance, or whether they've been marked read, or unread.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | MyAvert**.



My Avert Security Threats					
	Threat ▲	Protection	Risk	Discovery Date	Type
<input checked="" type="checkbox"/>	W32/Netsky.b@MM	Protection Available	Medium	2004/02/18	Virus
<input checked="" type="checkbox"/>	W32/Sobig.e@MM	Protection Available	Medium	2003/06/25	Virus
<input type="checkbox"/>	W32/Bugbear.b@MM	Protection Available	Medium	2003/06/04	Virus
<input type="checkbox"/>	W32/Sobig.b@MM	Protection Available	Medium	2003/05/18	Virus
<input type="checkbox"/>	W32/Fizzer@MM	Protection Available	Medium	2003/05/08	Virus
<input type="checkbox"/>	W32/Sobig.a@MM	Protection Available	Medium	2003/01/09	Virus

Figure 1: MyAvert Security Threats page

- 2 To narrow the viewable notifications, select an option from the **Filter Options** drop-down list.
- 3 To mark notifications as read or unread, select the desired threats, then click **Actions | Mark Read** or **Mark Unread**, as needed. You might need to select **Read** or **Unread** from the **Filter** drop-down list to view the notifications you want to mark.

Deleting threat notifications

Use this task to delete threat notifications from the MyAvert page. You cannot delete any threat notifications for which protection is still pending.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | MyAvert**.
- 2 Select threat notifications for which protection is available, then click **Actions** and select **Delete**.

Agent Handlers and what they do

An Agent Handler is the component of ePolicy Orchestrator that handles communication between the agent and the ePO server. Each installation of ePolicy Orchestrator includes an Agent Handler. Beginning with version 4.5 of ePolicy Orchestrator, Agent Handlers can be installed independently of your main ePO server on systems throughout your network. Multiple remote handlers can help you address scalability and topology issues in your network. In some cases, using multiple Agent Handlers can limit or reduce the number of ePO servers you need in your environment. They can provide fault tolerant and load-balanced communication with a large number of agents, including geographically distributed agents.

How Agent Handlers work

Agent Handlers distribute network traffic, which is generated by an agent-to-server communication interval (ASCI), by assigning managed systems or groups of systems to report to a specific Agent Handler. Once assigned, a managed system performs regular agent-server communication to its Agent Handler instead of to the main ePO server.

The handler provides updated sitelists, policies, and policy assignment rules, just as the 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.

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

Multiple Agent Handlers

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

Handler groups and priority

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

Handler groups

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

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

- **Using multiple handlers for load balancing**

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

- **Setting up a fallback plan to ensure agent-server communication**

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

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

Sitelist files

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

Working with Agent Handlers

Use these tasks to configure and manage Agent Handlers.

Before you begin

You must have Agent Handlers installed in your network to complete these tasks. For information on Agent Handler installation, see the *McAfee ePolicy Orchestrator 4.5 Installation Guide*.

Tasks

- ▶ [Assigning agents to Agent Handlers](#)
- ▶ [Managing Agent Handler assignments](#)
- ▶ [Setting up Agent Handler groups](#)
- ▶ [Managing Agent Handler groups](#)

Assigning agents to Agent Handlers

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

Task

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

- 1 Click **Menu | Configuration | Agent Handlers**, then click **Actions | New Assignment**.
- 2 Specify a unique name for this assignment.
- 3 Specify the agents for this assignment using one or both of the following **Agent Criteria** options:
 - Browse to a **System Tree location**.
 - Type the IP address, IP range, or subnet mask of managed systems in the **Agent Subnet** field.
- 4 Specify **Handler Priority** by deciding whether to:
 - **Use all Agent Handlers** — Agents randomly select which handler to communicate with.
 - **Use custom handler list** — When using a custom handler list, select the handler or handler group from the drop-down menu.

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

Managing Agent Handler assignments

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

Task

For option definitions, click ? in the interface.

To do this...	Do this...
Delete a handler assignment	Click Delete in the selected assignment row.
Edit a handler assignment	Click Edit for the selected assignment. The Agent Handler Assignment page opens, where you can specify: <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. <p>TIP: Use the drag-and-drop handle to quickly change the priority of handlers in your custom handler list.</p>
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.

Setting up Agent Handler groups

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Agent Handlers**, then in **Handler Groups**, click **New Group**. The Add/Edit Group page appears.
- 2 Specify the group name and the **Included Handlers** details, including:
 - Click **Use load balancer** to use a third-party load balancer, then fill in 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.

NOTE: When using a custom handler list, select the handlers from the Included Handlers drop-down list. Use + and – to add and remove additional Agent Handlers to the list (an Agent Handler can be included in more than one group). Use the drag-and-drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.
- 3 Click **Save**.

Managing Agent Handler groups

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

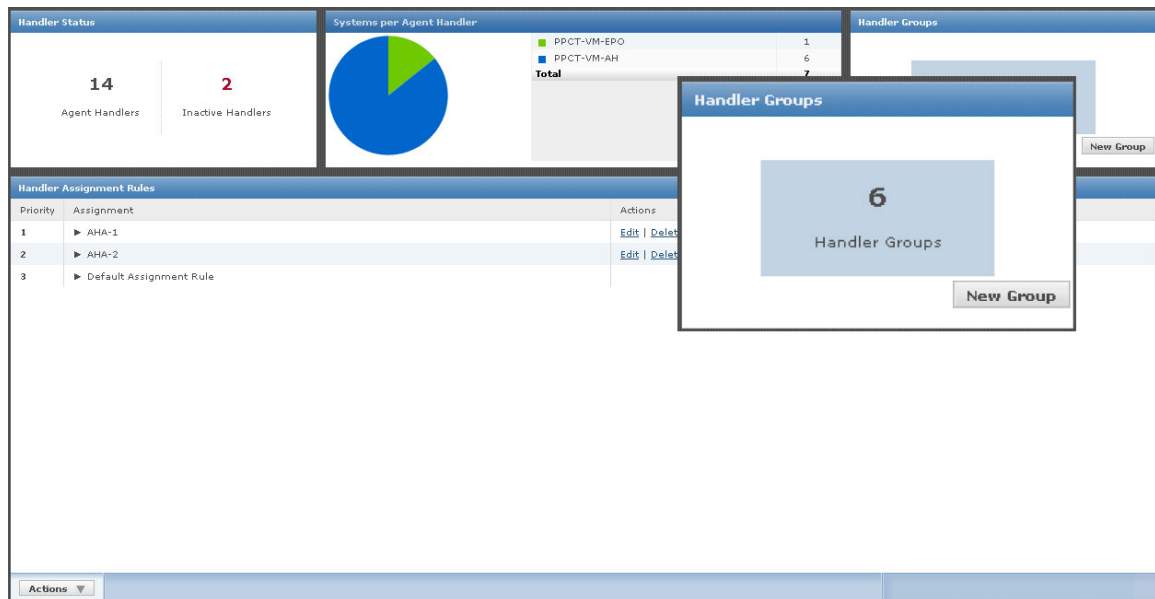


Figure 2: Handler Groups monitor

Task

For option definitions, click ? in the interface.

To do this...	Do this...
Delete a handler group	Click Actions Delete in the selected group row.
Edit a handler group	Click Actions Edit for the selected group. The Agent Handler Group Settings page opens, where you can specify: <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. <p>NOTE: Use a custom handler list to specify which handlers, and in what order, agents assigned to this group communicate with.</p>
Enable or disable a handler group	Click Actions Enable or Disable in the selected group row.

Moving agents between handlers

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

Tasks

- ▶ [Grouping agents by assignment rules](#)
- ▶ [Grouping agents by assignment priority](#)
- ▶ [Grouping agents using the System Tree](#)

Grouping agents by assignment rules

Use this task to assign agents to handlers using Agent Handler assignment rules. 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.

NOTE: When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

Task

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

- 1 Click **Menu | Configuration | Agent Handlers**, then click **Edit** in the Actions column of the Handler Assignment Rules table . The Agent Handler Assignment page appears.

NOTE: If the Default Assignment Rules is the only assignment in the list, you must create a new assignment. Refer to, *Assigning agents to Agent Handlers*.
- 2 Type a name for the **Assignment Name**.
- 3 You can configure **Agent Criteria** by System Tree locations, by agent subnet, or individually using the following:
 - System Tree Locations — Select the group from the **System Tree location**.

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

Grouping agents by assignment priority

Use this task to assign agents to handlers using Agent Handler 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.

NOTE: 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.
NOTE: 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**. The Edit Priority page appears.
NOTE: Moving one assignment to a priority lower than another assignment creates a hierarchy where the lower assignment is actually part of the higher assignment.
- 4** To change the priority of an assignment, which is shown in the Priority column on the left, do one of the following:
 - Use drag-and-drop — Use the drag-and-drop handle to drag the assignment row up or down to another position in the Priority column.
 - Click **Move to Top** — In the Quick Actions, click **Move to Top** to automatically move the selected assignment to the top priority.
- 5** When the priorities of the assignments are configured correctly, click **Save**.

Grouping agents using the System Tree

Use this task to assign agents to handlers 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.

NOTE: 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**.

IPv6

Internet Protocol version 6 (IPv6) is an Internet Layer protocol for packet-switched inter-networks. IPv6 has a much larger address space than IPv4. The larger address space provides flexibility in allocating addresses and routing traffic. The extended address length (128 bits) is intended to eliminate the need for network address translation, to prevent exhausting the number of unique IP addresses in your network. This also simplifies aspects of address assignment and renumbering when you change Internet connectivity providers.

McAfee ePolicy Orchestrator 4.5 is fully compatible with IPv6. The changeover from IPv4 to IPv6 will be gradual, and some organizations might use both protocols. To accommodate all instances, ePolicy Orchestrator 4.5 works 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 ePolicy Orchestrator works depends on the client network configuration. For example, if the client network is configured to use only IPv4 addresses, ePolicy Orchestrator works in Only IPv4 mode. Similarly, if the client network is configured to use both IPv4 and IPv6 addresses, ePolicy Orchestrator works in Mixed mode.

Until IPv6 is installed and enabled, ePolicy Orchestrator listens only on IPv4 addresses. When IPv6 is enabled, ePolicy Orchestrator works in the mode in which it is configured.

When the ePO server communicates with an Agent Handler or Rogue System Sensor on IPv6, address-related properties such as IP address, subnet address, and subnet mask are reported in IPv6 format. When transmitted between client and 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.

Exporting tables and charts to other formats

Use this task to export data various formats for uses such as reporting, importing into other ePO servers, backing up, etc.. You can export to HTML and PDF files for viewing formats, or to CSV or XML files for using and transforming the data in other applications.

Task

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

- 1** From the page displaying the data (tables or charts), select **Export Table** or **Export Data** from the **Options** menu. The **Export** page appears.
- 2** Select whether the data files are exported individually or in a single archive (zip) file.
- 3** Select the format of the exported file. If exporting to a PDF file, select the page size and orientation.
- 4** Select whether the files are emailed as attachments to selected recipients, or they are saved to a location on the server where a link is provided. You can open or save the file to another location by right-clicking it.

NOTE: When typing multiple email addresses for recipients, you must separate entries with a comma or semi-colon.

- 5** Click **Export**.

The files are created and either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.

Distributing Agents to Manage Systems

Managing your network systems effectively is dependent on each system running an active, up-to-date agent.

There are several methods to distribute the agent. The ones you use depend on:

- Environmental settings and controls, such as the network configuration; the configuration of ePolicy Orchestrator; the requirements of third-party tools.
- Whether you are upgrading agents or distributing them for the first time.

Are you distributing agents for the first time?

When deploying agents throughout your environment for the first time:

- 1 Review the information in this chapter to understand the agent, its policies and tasks, and the methods to distribute it.
- 2 Configure agent policy settings for the systems where you are distributing agents.
- 3 Distribute agents with the chosen methods to the desired locations.

Contents

- ▶ [About the McAfee Agent](#)
- ▶ [Installing the McAfee Agent](#)
- ▶ [Upgrading and Restoring Agents](#)
- ▶ [Configuring Agent Policies](#)
- ▶ [Working with the agent from the ePO server](#)
- ▶ [Running agent tasks from the managed system](#)
- ▶ [Using the system tray icon](#)
- ▶ [Removing the McAfee Agent](#)
- ▶ [Agent Activity Logs](#)

About the McAfee Agent

The term *agent* is used in three different contexts:

- McAfee Agent
- SuperAgent
- Agent Handler

McAfee Agent

The McAfee Agent is the client-side component that provides secure communication between McAfee managed products and ePolicy Orchestrator. The agent also provides local services to

these products and to products developed by McAfee's Security Innovation Alliance partners. While enabling products to focus on enforcing their policies, the McAfee Agent delivers services that include updating, logging, reporting events and properties, task scheduling, communication and policy storage.

The agent is installed on the systems you intend to manage with ePolicy Orchestrator. Systems can only be managed by ePolicy Orchestrator with an agent installed.

While running silently in the background, the agent:

- Gathers information and events from managed systems and sends them to the ePO server.
- Installs products and upgrades on managed systems.
- Enforces policies and schedules tasks on managed systems and sends events back to the ePO server.
- Updates security content such as the DAT files associated with McAfee VirusScan.

SuperAgent

A SuperAgent is an agent that can broadcast wake-up calls to other ePO agents located on the same network broadcast segment (usually identical with a network subnet). Each SuperAgent then pings the agents in its subnet. Agents located in a segment with no SuperAgent do not receive the wake-up call. This is an alternative to sending ordinary agent wake-up calls to each agent in the network, and the advantage is that it can distribute network traffic.

SuperAgents can also serve as the repository of distributable software and updates for those agents in its broadcast segment. Additionally, the agent's global updating feature relies entirely upon SuperAgent wake-up calls to perform its function.

Agent Handler

An Agent Handler is the ePO component responsible for managing communication between agent and server. Beginning with ePolicy Orchestrator 4.5, Agent Handlers can be installed on other computers to provide fault tolerant and load-balanced communication to many agents, including geographically distributed agents.

Agent-server communication

During agent-server communication, the agent and server exchange information using a proprietary network protocol that ePolicy Orchestrator uses for secure network transmissions. At each communication, the agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the agent, and the repository list if it has changed since the last agent-server communication. The agent enforces the new policies locally on the managed system and applies any task or repository changes.

Agent-server communication can be initiated in these ways:

- Agent-to-server communication interval (ASCI) lapses.
- Agent-initiated communication upon agent startup.
- Agent wake-up calls from ePO or Agent Handlers.
- Communication initiated manually from the managed system (Windows only).

Agent-server communication interval

The agent-server communication interval (ASCI) is set on the General tab of the McAfee Agent policy page. This setting determines how often the agent calls in to the server. The default setting of 60 minutes means that the agent contacts the server once every hour.

When deciding whether to modify the interval, consider the following:

- At each ASCI, the following actions occur:
 - The agent collects and sends its properties to the server or Agent Handler.
 - The agent sends the events that have occurred since the last agent-server communication.
 - The server or Agent Handler sends new policies and tasks to the client. This action might dictate other resource-consuming actions, such as an immediate DAT download.
 - The agent enforces policies.
- Although these activities do not burden any one computer, the cumulative demand on the network, on ePO servers, or on Agent Handlers can be significant, considering these variables:
 - The number of systems being managed by ePolicy Orchestrator.
 - Your organization's threat response requirements.
 - The network or physical location of clients in relation to servers or Agent Handlers.
 - Available bandwidth.

In general, the more these variables reflect conditions that are likely to burden or slow down your network, the less frequently you want to perform an agent-server communication. For clients with critical functions, you might want to set a more frequent interval.

Agent-initiated communication after agent installation

After the agent is installed, it calls in to the server at a randomized interval within ten minutes. Thereafter, the agent calls in at each agent-server communication interval (ASCI). By default, agent-server communication occurs every 60 minutes.

You can force the agent to communicate with the server at any time after installation by clicking the McAfee system tray icon, (if it has been enabled), and selecting **McAfee Agent Status Monitor**. When the Monitor appears, clicking **Collect and Send Props** sends full or minimal properties as defined on the General page of the McAfee Agent Policy Catalog. Clicking **Send Events** transmits events to the server but does not transmit policies and tasks from the server.

NOTE: For information on enabling the system tray icon see *Using the system tray icon*.

If the system tray icon has not been enabled, you can access the status monitor at the command prompt. Set the working directory to the McAfee Common Framework folder (the default location is C:\Program Files\McAfee\Common Framework), then type this command:

```
CmdAgent.exe /s
```

Wake-up calls and wake-up tasks

Communication between the ePO server and the agent takes place at regular intervals set by the ePO administrator. The purpose of an agent wake-up call is to trigger an immediate agent-server communication rather than wait for the next agent-server communication, which is set at 60 minutes by default. There are two ways to issue a wake-up call:

- Directly from the server — This is the most common approach and requires the presence of an open port on the client.

- On a schedule set by the administrator — This approach is useful when agent-server communication has been disabled on the General tab of the McAfee Agent policy catalog. The administrator can create and deploy a wake-up *task*, which triggers a wake-up *call* on a schedule.

Some reasons for issuing an agent wake-up call are:

- There has been a change in policy that you want the agent to adopt immediately, without waiting for the next ASCII.
- You have created a new task that you want the agent to run immediately.
- A query has generated a report indicating that a client is out of compliance, and you want to test its status as part of a troubleshooting procedure.

If you are running Microsoft Windows and have converted a particular system to use as a SuperAgent, it can issue wake-up calls to designated network broadcast segments. SuperAgents distribute the bandwidth impact of the agent wake-up call, and help distribute network traffic.

SuperAgents and broadcast wake-up calls

If you operate in a Windows environment and plan to use agent wake-up calls to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent.

SuperAgents distribute the bandwidth load of concurrent wake-up calls. Instead of sending agent wake-up calls from the server to every agent, the server sends the SuperAgent wake-up call to SuperAgents in the selected System Tree segment. When SuperAgents receive this wake-up call, they send broadcast wake-up calls to all agents in their network broadcast segments.

The process is:

- 1 Server sends a wake-up call to all SuperAgents.
- 2 SuperAgents broadcast a wake-up call to all agents in the same broadcast segment.
- 3 All agents (regular agents and SuperAgents) exchange data with the server.
- 4 An agent without an operating SuperAgent on its broadcast segment is not prompted to communicate with the server.

To deploy enough SuperAgents to the appropriate locations, first determine the broadcast segments in your environment and select a system (preferably a server) in each segment to host a SuperAgent. Be aware that agents in broadcast segments without SuperAgents do not receive the broadcast wake-up call, so they do not call in to the server in response to a wake-up call.

Agent and SuperAgent wake-up calls use the same secure channels. Ensure that:

- The agent wake-up communication port (8081 by default) is not blocked.
- The agent broadcast communication port (8082 by default) is not blocked.

NOTE: Client firewalls might block communication from the ePO server. Ensure that the ports required for communication from the ePO server are not blocked by a firewall on the client.

System requirements and supported operating systems and processors

This section specifies the system requirements for McAfee Agent 4.5 and the operating systems and processors it supports.

System requirements

- Installed disk space — 14–19 MB, excluding log files
- Memory — 256 MB RAM
- Processor speed — 500 MHz minimum

Supported operating systems and processors

Operating systems	Processor
Apple Macintosh OS X Tiger	<ul style="list-style-type: none"> • Intel • PowerPC
HP-UX 11i v1 (build 11.11)	PA-RISC
HP-UX 11i v2 (build 11.23)	
IBM AIX 5.3 (TL8 or later)	Power 5
IBM AIX 6.1	Power 5
McAfee Email and Web Security 3100	Not applicable
McAfee Email and Web Security 3200	
Red Hat Linux Enterprise 4	x86, x64 or compatible
Red Hat Linux Enterprise 5	
Solaris 8; 32-bit or 64-bit	SPARC
Solaris 9; 32-bit or 64-bit	
Solaris 10; 64-bit	
SuSE Linux 8.2	x86, x64 or compatible
SuSE Enterprise Server 9	
SuSE Enterprise Server 10	
Windows 2003 Server R2; Enterprise Edition; 32-bit or 64-bit; SP 1 or 2	<ul style="list-style-type: none"> • Itanium 2 • Intel Pentium • Intel Celeron (recommended) or compatible • x86, x64 or compatible
Windows 2003 Server R2; Standard Edition; 32-bit or 64-bit; SP1 or 2	
Windows 2003 Server R2; Web Edition; 32-bit or 64-bit; SP1 or 2	
Windows Vista Home Premium; 32-bit or 64-bit; GA or SP1	<ul style="list-style-type: none"> • Intel Pentium • Intel Celeron (recommended) or compatible • x86, x64 or compatible
Windows Vista Home Basic; 32-bit or 64-bit; GA or SP1	
Windows Vista Business; 32-bit or 64-bit; GA or SP1	
Windows Vista Enterprise; 32-bit or 64-bit; GA or SP1	
Windows Vista Ultimate; 32-bit or 64-bit; GA or SP1	
Windows 2008 Server; Standard; 32-bit or 64-bit; GA	
Windows 2008 Server Enterprise; 32-bit or 64-bit; GA	
Windows 2008 Server Datacenter; 32-bit or 64-bit; GA	
Windows 2008 Server, Web; 32-bit or 64-bit; GA	
Windows 2008 Server, Core; 32-bit or 64-bit; GA	
Windows XP Home Edition; 32-bit or 64-bit; SP2 or 3	

Operating systems	Processor
Windows XP Professional; 32-bit or 64-bit; SP2 or 3	
Windows XP Tablet PC Edition; 32-bit or 64-bit; SP3	

NOTE: The agent is compatible with Windows operating systems that provide Data Execution Prevention (DEP).

Installing the McAfee Agent

The installation procedure for the McAfee Agent varies depending on:

- The operating system in use — Windows, Solaris, HB-Ux, Macintosh, or Linux.
- The type of installation — First-time installation or upgrade on a system already hosting an agent.
- The tools used to install — ePolicy Orchestrator native tools, login scripts, images, or none.

This section provides instructions on installing the agent in a variety of environments.

Methods of agent deployment and installation

The terms *deployment* and *installation* both describe the process of equipping one or more computers with the McAfee Agent. However, there is a difference:

- *Installation* means placing the agent on a computer where no agent is present. Administrator privileges are required to install the agent.
- *Deployment* means placing the agent, or managed products and their upgrades, on one or more computers where an agent is already present.

If you are operating in a Windows environment, you can push install or update the agent directly from the ePO console. Alternatively, you can copy the agent installation package onto removable media or into a network share for manual or login script installation on your Windows systems.

However, you cannot push the installation package to UNIX-based systems. Here, the agent must be installed manually using an installation script (`install.sh`) that ePO creates when you check in the agent to the ePO master repository and indicate the operating system in use. Once the agent is in place on the client computers, you can run an agent deployment task to schedule updates to the agent as well as deploy products for management by ePO.

NOTE: The procedure described for agent installation on UNIX-based systems can be used in Windows environments as well, if preferred

This table lists methods for installing and deploying the agent. The first three methods are installing the agent and might require the use of embedded credentials. The remaining five methods are deploying the agent and do not require embedded credentials.

Method	Action	Notes
Installing the agent		
Manually	The network administrator installs the agent on each managed system individually.	<ul style="list-style-type: none"> • Aside from using third-party deployment products, this is the only method available for the initial installation on UNIX systems. • Once the agent is installed, you can use ePolicy Orchestrator to

Method	Action	Notes
		upgrade products and update product content..
Using third-party software such as Microsoft Systems Management Server (SMS) or IBM Tivoli	Configure your third-party software to distribute the agent installation package, which is located on your ePO server.	<ul style="list-style-type: none"> The agent installation package contains necessary security keys and the site list. See third-party instructions.
Using login scripts (Windows only)	The network administrator creates an installation or upgrade script, which runs at each logon to a system.	<ul style="list-style-type: none"> The user must log on to the system to trigger the installation or upgrade. The installation package must be in a location accessible to the system.
<p>Deploying the agent: A deployment task is created in ePolicy Orchestrator and is sent to the client where it runs. If the repository contains a newer version of the agent, the deployment task pull down the newer version and installs it over the existing version.</p>		
Using ePolicy Orchestrator	The ePO administrator specifies the systems and selects Install Agent when adding a new system.	<ul style="list-style-type: none"> Selecting a large number of systems can temporarily affect network throughput. You must specify credentials with administrator rights to the target systems.
Upgrading agents using the deployment task	Use the ePO System Tree to upgrade the agent on selected target systems.	<ul style="list-style-type: none"> Requires that an agent is already present on the target system.
Deploying an image containing the agent (Windows)	Administrator creates an image that contains the agent and deploys the image. Before creating the image, the administrator removes the agent GUID and MAC address from the agent section of the registry.	<ul style="list-style-type: none"> Removing the GUID and MAC address allows the agent to generate a new GUID and MAC address upon the first agent-server communication. Failure to remove the GUID and MAC address results in "sequencing errors" from the multiple identical systems
Enabling the agent on unmanaged McAfee products (Windows)	Using the System Tree, the ePO administrator selects the systems to be converted from unmanaged status to managed status and selects Install agents .	<ul style="list-style-type: none"> Requires an agent on the target system in unmanaged mode.
Enabling the agent on unmanaged McAfee products (UNIX-based platforms)	Type the following command on the system containing the agent you want to enable: /opt/McAfee/cma/bin/msaconfig -m -d <Path of location containing srpubkey.bin , reqseckey.bin and SiteList.xml > [-nostart]	<ul style="list-style-type: none"> You must have root privileges to perform this action. You must use the srpubkey.bin, reqseckey.bin and SiteList.xml files from the ePO server.

Installing on Windows from ePolicy Orchestrator

You must have administrator privileges on the Windows system to perform this task. The agent extension must be installed on the ePolicy Orchestrator server before the agent is installed on any clients.

- 1 Download both the agent extension, **ePOAgentMeta.zip** and the agent package, **MA450Win.zip** to the system containing the ePO server.
- 2 Install the agent extension:
 - a Click **Menu | Software | Extensions**. The Extensions page opens.
 - b Click **Install Extension**.
 - c Browse to the location containing **ePOAgentMeta.zip**, select it and click **OK**. The Install Extensions summary page appears.
 - d Click **OK** to complete the installation of the extension.
- 3 Check in the agent package to the ePolicy Orchestrator repository.

NOTE: If installing on a computer running Common Management Agent 3.6, the package must be checked in to the **Current** repository branch.

 - a In ePolicy Orchestrator, click **Software**.
 - b Click **Check In Package**.
 - c Browse to **MA450Win.zip**, select it and click **Next**.
 - d If **Allow package check-in for any repository branch** has been enabled, place the package any branch. To enable this feature, click **Menu | Configuration | Server Settings**, then select **Repository Packages** from the list of Setting Categories. Click **Edit** to toggle from No to Yes.
 - e Click **Save**.
- 4 Push the agent to client systems by following these steps:
 - a Click **Menu | Systems | System Tree**.
 - b Select the target systems or groups.
 - c Click **Actions**, select **Agent** from the pop-up menu, then select **Deploy Agents** from the submenu. The Deploy McAfee Agent page appears.
 - d Select the version of the agent to be deployed.
 - e If needed, select installation options:
 - **Install only on systems that do not already have an agent managed by this ePO server**
 - **Force installation over existing version**(Not recommended)
 - f Define the installation path for the agent: select a prefix from the drop-down menu, then accept the folder name that appears or type a new one.
 - g Type valid credentials in the **Domain**, **User name**, and **Password** fields.
 - h Click **OK**.

Installing on Windows using third-party deployment methods

The agent extension must be installed on the ePO server before the agent is installed on any target systems. McAfee recommends that you refer to the release notes to verify that you are using the most current package and extension.

TIP: This task requires the creation of an agent installation package, FramePkg.exe (see Step 4). Installation of the package requires administrator credentials.

Task

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

- 1 Download both the agent extension, **ePOAgentMeta.zip**, and the agent package, **MA450Win.zip**, to the system containing the ePO server.
- 2 Install the agent extension:
 - a Click **Menu | Software | Extensions**. The Extensions page opens.
 - b Click **Install Extensions**.
 - c Browse to the location containing **ePOAgentMeta.zip**, select it and click **OK**. The Install Extensions summary page appears.
 - d Click **OK** to complete the installation of the extension.
- 3 Check in the agent package to one of the repository branches, **Current** (default), **Previous**, or **Evaluation**.
- 4 Create an installation package:
 - a Click **Menu | Systems | System Tree**. The System Tree page opens.
 - b Click **System Tree Actions**, then select **New Systems** from the drop-down menu.
 - c Select **Create and download agent installation package**.
 - d Deselect **Use Credentials**.

NOTE: If deselected, you receive the default package. If selected you can specify required credentials.
 - e Click **OK**. The Download file dialog box opens.
 - f Select **FramePkg.exe** and save it to the desktop.
- 5 To embed credentials, modify the local security policy on the target systems:
 - a Log on to the target system using an account with local administrator permissions.
 - b From the command line, run SECPOL.MSC to open the Local Security Settings dialog box.
 - c In the System Tree under **Security Settings | Local Policies**, select **User Rights Assignment**.
 - d In the Policy column of the details pane, double-click **Impersonate a client after authentication** to open the Local Security Policy Setting dialog box.
 - e Click **Add** to open the Select Users or Groups dialog box.
 - f Select the user or group that the user is likely to run as (for example, **Everyone** or **Users**), then click **Add**.
 - g Click **OK**. You are now ready to use your third-party software to distribute **FramePkg.exe**.

Installing the agent manually

Use these instructions to install agents manually.

Tasks

- ▶ [Installing on Windows manually](#)
- ▶ [Installing on UNIX-based operating systems](#)

Installing on Windows manually

This method is appropriate if your organization requires that software is installed on systems manually. You can install the agent on the system, or distribute the FramePkg.exe installer for

users to run the installation program themselves. If you want users (who have local administrator rights) to install the agent on their own systems, distribute the agent installation package file to them. You can attach it to an email message, copy it to media, or save it to a shared network folder.

After the agent is installed, it calls in to the server and adds the new system to the System Tree.

Task

For option definitions, click ? in the interface.

- 1 Distribute the agent installation package to the target system.
- 2 Double-click **FramePkg.exe** and wait a few moments while the agent is installed. Within ten minutes, the agent calls in to the ePO server for the first time.
- 3 As needed, bypass the ten-minute interval by forcing the agent to call. Use this command:
CMDAGENT /p

Installing on UNIX-based operating systems

Use this task to install the agent on AIX, HP-UX, Linux, Macintosh, and Solaris systems. The agent extension must be installed on the ePO server before the agent is installed on any target systems.

Before you begin

- You must have root privileges on the UNIX-based system to complete this task

Task

- 1 Download ePOAgentMeta.zip to a temporary location on the ePO server.
- 2 Open the ePOAgentMeta.zip and extract the agent package for the target operating system.

Operating system	File name
HP-UX	MA450HPX.zip
Linux	MA450LNX.zip
Macintosh	MA450MAC.zip
Solaris	MA450SLR.zip
AIX	MA450AIX.zip

- 3 Install the agent extension on the ePO server.
 - a Click **Menu | Software | Extensions**, then click **Install extension**.
 - b Browse to the location containing **ePOAgentMeta.zip**, select it and click **OK**. The Install Extensions summary page appears.
 - c Click **OK** to complete the installation of the extension.
- 4 Check in the agent package to one of the repository branches, **Current** (default), **Previous**, or **Evaluation**.

TIP: The path includes the name of the selected repository. For example, if checked in to the Current branch of the ePO software repository, the path of the required files is:

Operating System	Location
AIX	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT4000AIXX\Install\0409
HPUX	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT4000HPUX\Install\0409
Linux	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700LYNX\Install\0409
Macintosh	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700MACX\Install\0409
Solaris	C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700SLRS\Install\0409

- 5 From the selected repository branch, copy the **install.sh** file to the target systems.
- 6 Log on to the target system as "root."
- 7 Open **Terminal**, then switch to the location where you copied the install.sh file.
- 8 Run these commands:

```
chmod +x install.sh  
./install.sh -i
```

Creating custom agent installation packages

Use this task to create a custom agent installation package.

If you use a distribution method other than ePolicy Orchestrator deployment capabilities (such as login scripts or third-party deployment software), you can create a custom agent installation package (FramePkg.exe) with embedded administrator credentials. This is necessary in a Windows environment if users do not have local administrator permissions. The user account credentials you embed are used to install the agent.

NOTE: Microsoft Windows XP Service Pack 2 and later do not allow embedded administrator credentials until the package file name has been added to the exception list of the Windows firewall.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then from the System Tree Actions drop-down menu, click **New Systems**. The New Systems page appears.
- 2 Next to **How to add systems**, select **Create and download agent installation package**.
- 3 Select the appropriate operating system.
- 4 Type the appropriate **Credentials for agent installation**, then click **OK**.
- 5 When prompted, select the file to be downloaded. Click to open the file. Right-click to save the file.
- 6 Distribute the custom installation package file as needed.

Installing the agent with login scripts

Use this Windows only task to set up and use network login scripts to install the agent on Windows systems as they log on to the network.

Using network login scripts is a reliable method to make sure that every system logging on to your network is running an agent. You can create a login script to call a batch file that checks if the agent is installed on systems attempting to log on to the network. If no agent is present, the batch file installs the agent before allowing the system to log on. Within 10 minutes of being installed, the agent calls in to the server for updated policies and ePO tasks, and the system is added to the System Tree.

This method is appropriate when:

- Domain names or sorting filters are assigned to the segments of your System Tree.
- You already have a managed environment and want to ensure that new systems logging on to the network become managed as a result.
- You already have a managed environment and want to ensure that systems are running a current version of the agent.

Before you begin

- McAfee recommends first creating segments of your System Tree that use either network domain names or sorting filters that add the expected systems to the desired groups. If you don't, all systems are added to the Lost&Found group, and you must move them manually.
- Consult your operating system documentation for writing login scripts. The details of the login script depend on your needs. This task uses a basic example.
- Create a batch file (ePO.bat) that contains commands you want to execute on systems when they log on to the network. The content of the batch file depends on your needs, but its purpose is to check whether the agent has been installed in the expected location and, if not, run FramePkg.exe to install the agent. Below is a sample batch file that does this.

```
IF EXIST "C:\Program Files\McAfee\Common Framework\FRAMEWORKSERVICE.EXE" GOTO END_BATCH
\\MyServer\Agent\UPDATE$\FRAMEPKG.EXE /INSTALL=AGENT
:END_BATCH
```

NOTE: The installation folders for your distribution might be different than in this example, depending on where you have specified to install the agent.

This example checks:

- The default installation folder for an agent file and, if not present, installs the new agent.

Task

For option definitions, click ? in the interface.

- 1 Copy the agent installation package, FramePkg.exe, from your ePO server to a shared folder on a network server, where all systems have permissions.

Systems logging on to the network are automatically directed to this folder, to run the agent installation package and install the agent. The default location for the agent installation packages for Windows is: C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe

- 2 Create a custom agent installation package with embedded administrator credentials, which are required to install the agent on the system.

- 3 Save the batch file you created, ePO.bat, to the NETLOGON\$ folder of your primary domain controller (PDC) server. The batch file runs from the PDC every time a system logs on to the network.
- 4 Add a line to your login script that calls the batch file on your PDC server. The line would look similar to this example:
`CALL \\PDC\NETLOGON\EPO.BAT`
Each system runs the script when it logs on to the network and, if necessary, installs the agent.

Including the agent on an image

When you include the McAfee Agent on an image, you must remove its GUID from the registry. This allows subsequently installed agent images to generate their own GUID at their first agent-server communication.

CAUTION: If you don't follow this step, all deployed agent images have the same GUID, and must be changed manually. In a large organization, this is impractical. Although you can configure the ePO server to identify replicated GUIDs and assign a new GUID at the next agent-server communication, the action consumes considerable processing bandwidth. For information, see *Identifying and correcting a duplicate GUID*.

Task

On the imaged system, locate the registry key for the agent and remove it. The registry keys are located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent\AgentGUID
```

Identifying and correcting a duplicate GUID

If you deployed the agent on an image without first removing its GUID from the registry, multiple systems in your environment will have duplicate GUIDs. When these systems fail to communicate with the Agent Handler, they generate sequencing errors, which indicate a GUID problem. The Managed Systems query result type tracks the following information about these errors:

- The number of sequence errors for each system in the Managed Systems Sequence Errors property.
- The date and time of the last sequence error in the Managed Systems Last Sequence Error property.

The tracked information is incorporated into one or the other of the available pre-defined queries:

- Systems with High Sequence Errors
- Systems with no Recent Sequence Errors

Two predefined tasks help manage GUID problems.

- **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**

This task deletes the systems that have a large number of sequencing errors and classifies the agent GUID as problematic. As a result, the agent is forced to generate a new GUID. The threshold number of sequencing errors is set in the query Systems with High Sequence Errors.

- **Duplicate Agent GUID - Clear error count**

Sequencing errors can occur occasionally for inconsequential reasons. This task clears the count of sequencing errors in systems that have not had any recent sequencing errors. This

cleanup task does not remove any problematic GUIDs. The threshold value for defining *recent* is set in the query Systems with no Recent Sequence Errors

Use this task to identify computers with GUID problems and take corrective action.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks** to open the Server Tasks Builder.
- 2 Click **Edit** for one or the other of the following tasks.
 - **Duplicate Agent GUID - Clear error count**
 - **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**
- 3 In the Description page, select **Enabled**, then click either **Save** or **Next**.
 - If you click **Save**, the task runs with the default configuration displayed on the **Actions** and **Schedule** tabs. If you want to configure a schedule for this task, click **Next**. This allows you to review the Action settings and then set a schedule.
 - If you click **Next**, the Actions page appears. This page has been preconfigured to correspond to the requirements of the Duplicate Agent GUID task that you selected in Step 2. Ensure that the following settings are displayed:

	Duplicate Agent GUID - Clear error count	Duplicate Agent GUID - remove systems with potentially duplicated GUIDs
Actions	Run Query	Run Query
Query	Systems with no Recent Sequence Errors	Systems with High Sequence Errors
Sub-Actions	Clear Agent GUID Sequence Error Count	Move Agent GUID to Duplicate List and Delete Systems

- Click **Next** again to display the Schedule page. Specify the frequency, start and end dates, and time for running this query.
- 4 Click **Save**.

TIP: You can run either of the tasks immediately by selecting **Run** in the Actions column on the Server Tasks page.

Scheduling corrective action for a duplicate GUID

If you have deployed the agent on an image without first having removed its GUID from the registry, multiple systems in your environment will have duplicate GUIDs. When these systems fail to communicate with the Agent Handler, they generate sequencing errors, indicating a GUID problem.

Use this task to automatically identify duplicate agent GUIDs, and schedule their removal.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Edit** in the row labeled **Duplicate Agent GUID - remove systems**. The Server Task Builder wizard opens.
- 2 On the Description page, select **Enabled**.

- To run the task with the default configuration displayed on the Actions and Schedule tabs, click **Save**.
- To configure the Actions and Schedule tabs, click **Next**. The Actions page appears.
- 3** From the Actions drop-down menu, select **Run Query**.
- 4** From the Query drop-down menu, select one of these options, then click **OK**.
 - **System with high Sequence errors**
 - **Systems with no recent Sequence errors**
- 5** From the Sub-Actions drop-down menu, select one of these options, then click **Next**.
 - **Clear Agent GUID Sequence Error Count**
 - **Move Agent GUID to Duplicate List and Delete systems**
- 6** Set a schedule for running the task, then click **Next**.
- 7** Review your settings, then click **Save**.

Deploying the agent via push technology

Use this task to deploy agents to your Windows systems using ePolicy Orchestrator.

This method is recommended if large segments of your System Tree are already populated. For example, if you created System Tree segments by importing domains or Active Directory containers, and you chose not to deploy the agent during the import.

Before you begin

To use this method, these requirements must be met:

- Systems must already be added to the System Tree.

NOTE: If you have not yet created the System Tree, you can deploy the agent installation package to systems at the same time that you add groups and systems to the System Tree. However, McAfee does not recommend this procedure if you are importing large domains or Active Directory containers. Those activities generate significant network traffic.

- The account specified must have local administrator privileges on all target systems. Domain administrator rights are required on a system to access the default Admin\$ shared folder. The ePO server service requires access to this shared folder in order to install agents.
- The ePO server must be able to communicate with the desired systems.

Before beginning a large agent deployment, ping some targets by machine name to verify that the server can communicate with a few systems in each segment of your network. If the targeted systems respond to the ping, ePolicy Orchestrator can reach the segments.

NOTE: The ability to successfully use ping commands from the ePO server to managed systems is not required for the agent to communicate with the server. It is, however, a useful test to determine if you can deploy agents from the server.

- The Admin\$ share folder on target systems must be accessible from the ePO server. Verify that this is true on a sample of target systems. This test also validates your administrator credentials, because you cannot access remote Admin\$ shares without administrator rights. From the ePO server, click **Start | Run**, then type the path to the target system's Admin\$ share, specifying either system name or IP address.

If the systems are properly connected over the network, and your credentials have sufficient rights, and the Admin\$ share folder is present, a Windows Explorer dialog box appears.

- Network access must be enabled on Windows XP Home systems. Deploy the agent from ePolicy Orchestrator or install a custom agent installation package on systems running Windows XP Home.

To enable network access on Windows XP Home systems, click **Start | Control Panel | Performance and Maintenance | Administrative Tools | Local Security Policy | Security Settings | Local Policies | Security Options | Network access: Sharing and security model for local accounts**, then select **Classic - local users authenticate as themselves**.

Task

For option definitions, click ? in the interface.

- 1 Download the agent extension, **ePOAgentMeta.zip**, and the agent package, **MA450Win.zip**, to the system containing the ePO server.
- 2 Install the agent extension:
 - a Click **Menu | Software | Extensions**. The Extensions page opens.
 - b Click **Install Extensions**.
 - c Browse to the location containing **ePOAgentMeta.zip**, select it, then click **OK**. The Install Extensions summary page appears.
 - d Click **OK** to complete the installation of the extension.
- 3 Check in the agent package to the ePolicy Orchestrator repository.

NOTE: If installing on a computer running Common Management Agent 3.6, the package must be checked in to the Current repository branch.

 - a Click **Menu | Software | Master Repository**. A list of packages in the repository appears.
 - b Click **Actions**, then select **Check In Package** from the drop-down menu.
 - c Browse to **MA450Win.zip**, select it, then click **Next**.
 - d Ensure that **Current** is selected in the Branch field, then click **Save**.
- 4 Push the agent to target systems:
 - a Click **Menu | Systems | System Tree**, then select the groups or systems where you want to deploy the agent.
 - b Click **Actions**.
 - c Select **Agent** from the first pop-up menu, then select **Deploy Agents** from the second drop-down menu.
 - d From the drop-down list, select an **Agent version**.
 - e Type valid credentials in the **Domain**, **User name**, and **Password** fields.
 - f Click **OK**.
- 5 If you are deploying agents to a group, select whether to include systems from its subgroups.
- 6 If desired, select one of these options:
 - **Install only on systems that do not already have an agent managed by this ePO server**
 - **Force installation over existing version**

The force installation option is not available if **Install only on systems...** is selected.

NOTE: If you use the force installation option, the agent is removed in its entirety, including policies, tasks, events, and logs before the new agent is installed.

Enabling and disabling the agent on unmanaged McAfee products

Before acquiring ePolicy Orchestrator, you might have already been using McAfee products in your network. Some of the more recent McAfee products that use AutoUpdate, such as VirusScan Enterprise, are installed with the agent in *updater* mode. To start managing these products with ePolicy Orchestrator, you can enable the agent that is already on the system.

Enabling the agent on each system saves significant network bandwidth over deploying the agent installation package. However, existing McAfee products were probably installed with an older version of the agent, and these agents are *not* automatically upgraded to the latest version on the ePO server.

In some situations, you may want to convert a system that has been managed by ePolicy Orchestrator to updater (unmanaged) mode. Information is provided for converting from managed mode to unmanaged mode.

Use these tasks to enable agents on existing McAfee products in your environment so that they work with ePolicy Orchestrator or to disable management of systems by ePolicy Orchestrator.

Tasks

- ▶ [Converting the agent mode from unmanaged to managed mode in Windows](#)
- ▶ [Converting the agent mode from unmanaged to managed on UNIX-based platforms](#)
- ▶ [Converting the agent mode from managed to unmanaged mode in Windows](#)
- ▶ [Converting the agent mode from managed to unmanaged on UNIX-based platforms](#)

Converting the agent mode from unmanaged to managed mode in Windows

Use this task to convert the agent from unmanaged (updater) mode to managed mode in a Windows environment.

Before you begin

Before converting the agent mode, consider the following:

- By default, the FrmInst.exe file is installed in this location: C:\PROGRAM FILES\MCAFFEE\COMMON FRAMEWORK.
- You should not change the agent installation folder without removing and reinstalling the agent. Agents that you enable might be in a different folder than agents that you deploy in your network by another method.
- Assigning sorting filters or domain names to specific System Tree segments saves time. Without such designations, systems are placed in **Lost&Found** and you will have to move them from that location.
- You must copy the SiteList.xml (repository list file) from the ePO server to the target systems. The repository list contains network address and other information that the agent requires to call in to the server after being installed.
- SiteList.xml must be in the same location as srpubkey.bin and reqseseckey.bin.

Two methods for performing this task are provided.

Method A

This method, although simple and fast, involves sending a 5 MB file across the network.

- 1 Export Framepkg.exe to a temporary location on the target system, (that is, the system to be converted from unmanaged to managed mode.)
- 2 Run Framepkg.exe.

Method B

This method is complex and time consuming but involves using only 400 KB of network bandwidth.

- 1 Copy sitelist.xml, srpubkey.bin and reqseckey.bin to a temporary location on the target system.
- 2 Run frminst.exe on the target system.

Converting the agent mode from unmanaged to managed on UNIX-based platforms

Use this task to convert the agent from unmanaged (updater) mode to managed mode on a UNIX-based platform.

NOTE: This procedure can be used to change which ePO server or Agent Handler an agent communicates with.

Task

- 1 On the target system, locate the **msaconfig** file in the binaries subfolder of the **cma** folder. For example, on HP-UX, Linux, and Solaris systems, the location is `/opt/McAfee/cma/bin`. On Macintosh systems, the location is `/Library/McAfee/cma/bin`.
- 2 Run `/opt/McAfee/cma/bin/msaconfig -m -d <path of location containing srpubkey.bin, reqseckey.bin and SiteList.xml> [-nostart]`.

NOTE: Optional `-nostart` indicates that the agent does not restart after changing mode.

Converting the agent mode from managed to unmanaged mode in Windows

Use this task to convert the agent from managed mode to unmanaged (updater) mode in a Windows environment.

Task

- 1 Click **Menu | Systems | System Tree**.
- 2 Select the systems to convert.
- 3 From the Actions pop-up menu, select **Directory Management**, then select **Delete**.
- 4 Confirm the deletion. The selected system is no longer managed by ePolicy Orchestrator and now functions only as an updater.

Converting the agent mode from managed to unmanaged on UNIX-based platforms

Use this task to convert the agent from managed mode to unmanaged (updater) mode on a UNIX-based platform.

Task

- 1 On the target system, locate the **msaconfig** file in the binaries subfolder of the **cma** folder. For example, on HP-UX, Linux, and Solaris systems, the default location is `/opt/McAfee/cma/bin`. On Macintosh systems, the default location is `/Library/McAfee/cma/bin`.
- 2 Run `/opt/McAfee/cma/bin/msaconfig -u [-nostart]`.

NOTE: Optional `[-nostart]` indicates that the agent does not restart after changing mode.

Agent installation folder — Windows

The default location of the agent installation folder is the same on managed systems and on the ePO server.

- `<System_Drive>\Program Files\McAfee\Common Framework`

Agent installation folder — UNIX-based systems

Installation of the agent on UNIX-based operating systems generates files in these locations:

Operating system	Location	Contents
AIX	<code>/opt/McAfee/cma/</code>	All binaries, logs, agent working area
	<code>/etc/cma.d/</code>	Configuration and management information (including GUID and agent version) needed to manage point-products.
	<code>/etc/</code>	<code>cma.conf</code> Configuration and management information in xml format, allowing point-products to read.
	<code>/usr/sbin/</code>	<code>cma</code> Script for starting and stopping the agent, manually and when called by the system.
HP-UX	<code>/opt/McAfee/cma/</code>	All binaries, logs, agent working area.
	<code>/etc/cma.d/</code>	Configuration and management information (including GUID and agent version) needed to manage point-products.
	<code>/etc/</code>	<code>cma.conf</code> Configuration and management information in xml format, allowing point-products to read.
	<code>/sbin/init.d/cma</code>	<code>cma</code> Script for starting and stopping the agent, manually and when called by the system.
Linux	<code>/opt/McAfee/cma/</code>	All binaries, logs, agent working area.
	<code>/etc/cma.d/</code>	Configuration and management information (including GUID and agent version) needed to manage point-products.
	<code>/etc/</code>	<code>cma.conf</code>

Operating system	Location	Contents
		Configuration and management information in xml format, allowing point-products to read.
	/etc/init.d/	cma Script for starting and stopping the agent, manually and when called by the system.
Macintosh	/Library/McAfee/cma	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/Library/StartupItems/cma/	cma Script for starting and stopping the agent, manually and when called by the system.
Solaris	/opt/McAfee/cma/	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/etc/init.d/	cma Script for starting and stopping the agent, manually and when called by the system.

The agent installation package

A FramePkg.exe file is created when you install ePolicy Orchestrator and whenever you check in an agent package. It is a customized installation package for agents that report to your server. The package contains information necessary for the agent to communicate with the server. Specifically, this package includes:

- The agent installer
- SiteList.xml file
- srpubkey.bin (the server public key)
- reqseckey.bin (the initial request key)

By default, the path of the agent installation package on the server is:

```
C:\Program Files\McAfee\ePolicy
Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe
```

This is the installation package that the server uses to distribute and install agents. Other FramePkg.exe files are created when:

- Agent packages are checked in to any branch of the repository (Previous, Current, or Evaluation)

- Encryption key changes

The default agent installation package contains no embedded user credentials. When executed on the targeted system, the installation uses the account of the currently logged-on user.

Agent installation command-line options

Depending on whether the agent is already installed, you can use command-line options when you run the agent installation package (FramePkg.exe) or the agent framework installation (FrmInst.exe) program.

You can employ these command-line options when using the deployment task to upgrade to a new version of the agent.

This table describes all of the agent installation command-line options. These options are *not* case-sensitive, but their values are.

FramePkg.exe and FrmInst.exe command-line options

Command	Description
/DATADIR	Specifies the folder on the system to store agent data files. The default location is: <Documents and Settings>\All Users\Application Data\McAfee\Common Framework. If the operating system does not have a Documents and Settings folder, the default location is the Data folder within the agent installation folder. Sample: FRAMEPKG /INSTALL=AGENT /DATADIR=<AGENT DATA PATH>
/DOMAIN/ USERNAME/ PASSWORD	Specifies a domain, and account credentials used to install the agent. The account must have rights to create and start services on the desired system. If left unspecified, the credentials of the currently logged-on account are used. If you want to use an account that is local to the desired system, use the system's name as the domain. Sample: FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=jdoe /PASSWORD=password
/FORCEINSTALL	Specifies that the existing agent is uninstalled, then the new agent is installed. Use this option only to change the installation directory or to downgrade the agent. When using this option, McAfee recommends specifying a different directory for the new installation (/INSTDIR). Sample: FRAMEPKG /INSTALL=AGENT /FORCEINSTALL /INSTDIR=c:\newagentdirectory
/INSTALL=AGENT	Installs and enables the agent. Sample: FRAMEPKG /INSTALL=AGENT
/INSTALL=UPDATER	Enables the AutoUpdate 7.0 component if it has already been installed, and does not change whether the agent is enabled. This command-line option upgrades the agent. Sample: FRAMEPKG /INSTALL=UPDATER
/INSTDIR	Specifies the installation folder on the desired system. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default location is: <DRIVE>:\program files\mcafee\common framework Sample: FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent
/REMOVE=AGENT	Removes the agent if not in use. If in use, the agent changes to <i>updater</i> mode. Sample: FRMINST /REMOVE=AGENT

Command	Description
/SILENT or /S	Installs the agent in silent mode, hiding the installation from the end user. Sample: FRAMEPKG /INSTALL=AGENT /SILENT
/SITEINFO	Specifies the folder path to a specific repository list (SiteList.xml) file. Sample: FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\TMP\SITELIST.XML
/USELANGUAGE	Specifies the language version of the agent that you want to install. If you select 0409 or a locale other than the 12 languages with locale IDs, the software appears in English. If you install multiple language versions, the locale selected in operating system determines the language version that displays. Sample: FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404

Assigning values to custom properties

Use this task to specify up to four custom properties during installation of the agent at the command line. These values override values set by the ePO administrator.

Task

- At the command line, type the string that is appropriate for your operating system:
 - **Windows operating systems:** `FrmInst.exe /CustomProp1="Property 1" /CustomProp2="Property 2" /CustomProp3="Property 3" /CustomProp4="Property 4"`
NOTE: In Windows, custom property values are stored in the registry at `HKLM\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent\CustomProps\`
 - **UNIX-based operating systems:** `msaconfig -CustomProp1 "Property 1" -CustomProp2 "Property 2" -CustomProp3 "Property 3" -CustomProp4 "Property 4"`
NOTE: Custom property values are stored in `CustomProps.xml`, an editable file located at `/McAfee/cma/scratch/`.

Upgrading and Restoring Agents

Use these tasks to upgrade or restore existing agents in your environment.

If you have been using an older version of ePolicy Orchestrator and have previous agent versions in your environment, you can upgrade those agents once you've installed your new ePO server. The procedure for upgrading the agent depends on which agent version is running on your managed systems.

NOTE: Some previous agent versions do not support all functions in ePolicy Orchestrator 4.5. For full ePolicy Orchestrator functionality, upgrade to agent version 4.5 or later.

Tasks

- ▶ [Upgrading agents using product deployment task](#)
- ▶ [Upgrading agents manually or with login scripts](#)
- ▶ [Restoring a previous version of the agent \(Windows\)](#)
- ▶ [Restoring a previous version of the agent \(UNIX\)](#)

Upgrading agents using product deployment task

Use this task to deploy a newer version of the agent with the Product Deployment client task. This is the same task that is used to deploy products, such as VirusScan Enterprise, to systems that are already running agents.

Periodically, McAfee releases newer versions of the agent, which can be deployed and managed using ePolicy Orchestrator. When the agent installation package is available, you can download it from the McAfee download site, check it in to the master repository, then use the deployment task to upgrade the agent.

NOTE: The term *upgrading* is not the same as *updating*. *Upgrading* the agent means installing a newer version of the agent over an older version, for example, replacing McAfee Agent 4.0 with McAfee Agent 4.5. *Updating* means getting the most up-to-date DATs and signatures that products use to identify and disarm threats.

Before you begin

- If you use ePolicy Orchestrator to deploy agents in your network, the procedure differs slightly depending which previous version of the agent you are upgrading.
- If you are upgrading your agents and your network is very large, consider the size of the agent installation package file and your available bandwidth before deciding how many agents to upgrade at once. Consider using a phased approach. For example, upgrade one group in your System Tree at a time. In addition to balancing network traffic, this approach makes tracking progress and troubleshooting any issues easier.
- If you use a product deployment client task to upgrade agents, consider scheduling the task to run at different times for different groups in the System Tree.

Task

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

- 1** Ensure that the desired agent installation package is checked in to the desired branch of the master repository.
- 2** Click **Menu | Systems | System Tree**.
- 3** Click the **Client Tasks** tab.
- 4** Click **Actions**, then select **New Task** from the drop-down menu. The Client Task Builder wizard opens to the Description page.
- 5** Name the task, then select **Product Deployment** from the drop-down list and select whether the task should be sent to all computers or to tagged computers.
- 6** Click **Next**. The Configuration page appears.
- 7** Select the target platform.
- 8** Use the drop-down lists in the Products and Components area to specify the version of the agent to deploy and, if needed, additional command-line parameters.
- 9** If you are working in a Windows environment, select whether to run the task at each policy enforcement interval.
- 10** Click **Next** to open the Schedule page.
- 11** Schedule the task as needed, then click **Next**. The Summary page appears.
- 12** Verify the task's details, then click **Save**. The new deployment task is sent to the client computers at the next agent-server communication. Thereafter, every time the task executes, it checks to determine whether it should install the specified agent.

Upgrading agents manually or with login scripts

If you don't use ePolicy Orchestrator to deploy agents to managed systems, you can use your preferred agent distribution method to upgrade existing agents. Upgrading agents without using ePolicy Orchestrator, such as upgrading manually or using network login scripts, is the same as installing agents for the first time. You must distribute the FramePkg.exe installation file and launch it on the system using your preferred method.

Restoring a previous version of the agent (Windows)

Use this task to restore a previous version of the agent in a Windows environment. You might do this to test a new version of the agent.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then select the systems you want to downgrade.
- 2 From the Actions drop-down menu, select **Agent**, then select **Deploy Agents**. The Deploy Agent page appears.
- 3 From the drop-down list, select the agent you want to restore.
- 4 Select **Force installation over existing version**.
- 5 Specify the target location for the forced installation.
- 6 Enter user credentials for agent installation.
- 7 Provide the **Number of attempts**; **Retry interval**; and **Abort after** information.
- 8 Select whether the connection used for the deployment is to use a selected Agent Handler or all Agent Handlers.
- 9 Click **OK** to send the agent installation package to the selected systems.

Restoring a previous version of the agent (UNIX)

Use this task to restore a previous version of the agent in a UNIX environment. You might do this to test a new version of the agent.

Task

For option definitions, click ? in the interface.

- 1 Uninstall the currently installed version of the agent. For details, see *Uninstalling from UNIX-based operating systems*.
- 2 Install the earlier version of the agent. For details, see *Installing the agent manually*.

NOTE: Tasks, policies and other data are restored at the first agent-server communication following reinstallation.

Configuring Agent Policies

Agent policy general settings are specified on the Policy Catalog pages of the ePolicy Orchestrator console, including policies for events, logging, repositories, updates, and proxy.

- ▶ [About agent policy settings](#)
- ▶ [Proxy settings for the agent](#)
- ▶ [Retrieving system properties](#)
- ▶ [Scheduling a client task for a group](#)
- ▶ [Creating a new scheduled client task](#)
- ▶ [Configuring selected systems for updating](#)

About agent policy settings

Agent policy settings determine the performance and behavior of an agent in your environment. The interface provides 6 configuration pages for setting policy options:

- **General**, where the following policies are set:
 - Policy enforcement interval
 - Use of system tray icon
 - Agent wake-up call support in Windows environments
 - Where the agent goes for product and update packages
 - Creation of SuperAgents
 - Rebooting options
 - Agent-server communication
 - Sending full or minimal system properties and product properties
- **Events**, where priority event forwarding is set. (See topic entitled Priority event forwarding).
- **Logging**, where the following policies are set:
 - Enabling/disabling of logging
 - Level of logging detail
 - Setting remote access to logging
- **Repositories**, where repository selection variables are set. (See topic entitled Selecting a repository).
- **Updates**, where the following policies are set:
 - Identifying log file information
 - Specifying post-updating executables
 - Downgrading DAT files
 - Defining repository branches
- **Proxy**, where proxy settings are specified. (See topic Proxy settings for the agent).

Before distributing a large number of agents throughout your network, consider carefully how you want the agent to behave in the segments of your environment. Although you can configure agent policy settings after agents are distributed, McAfee recommends setting them prior to the distribution, to prevent unnecessary impact on your resources.

For complete descriptions of all options on the agent policy pages, click **?** on the page displaying the options.

Priority event forwarding

During normal operation, the agent and security software on the managed system generate software events regularly. These events can range from information about regular operation, such as when the agent enforces policies locally, to critical events, such as when a virus is detected and not cleaned. These events are uploaded to the server at each agent-server communication and are stored in the database. A typical deployment of agents in a large network can generate thousands of these events an hour.

You can configure the agent to forward events on a priority basis if they are equal to or greater than a specified severity. Specific event severities are determined by the product generating the events. If you plan to use Automatic Responses, McAfee recommends that you enable priority uploading of higher severity events for those features to function as intended.

You can enable priority uploading of events on the Events tab of the McAfee Agent policy pages.

Selecting a repository

Use this task to set the policy for repository selection. The agent can update from any repository in its repository list based on the policy setting. This repository management tool allows you to specify the most efficient means for designating a source repository for updates.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy Catalog**.
- 2 Select **McAfee Agent** from the Product drop-down menu and ensure that **General** is selected in the Category drop-down menu.
- 3 Click **Actions**, then select **New Policy** to create a new policy or **My Default** policy to edit your policy.
- 4 Type a name for the policy, then click **OK**.
- 5 On the Repositories tab, select whether to **Use this repository list** (the ePO-managed repository list, SiteList.xml), or **Use other repository list** (a locally controlled repository list that is not managed by ePolicy Orchestrator).
- 6 Choose a basis for selecting a repository:

Selection Method	Definition
Ping time	The shortest round-trip elapsed time between sending an echo request to a remote ICMP-enabled system and receiving a response from that system. Ping timeout can be used to control the maximum time taken. Minimum = 5 seconds; maximum = 60 seconds. The default is 30 seconds.
Subnet distance	The fewest hops an ICMP packet makes while traversing the network from a local system to a remote system. The maximum number of hops can be used to control the packet traversal.
Use order in repository list	A user-defined list of repositories based on locally determined preferences. You can sequence and enable or disable specific distributed repositories on the Repositories tab of the McAfee Agent policy pages. Allowing agents to update from any distributed repository ensures that they get the update from some location.

NOTE: The agent selects a repository each time a change occurs in the repository list, IP address, or policy option.

Proxy settings for the agent

To access the McAfee update sites, the agent must be able to access the Internet. Use the agent policy settings to configure proxy server settings for managed systems. The Proxy tab of the McAfee Agent policy pages includes these settings:

- **Do not use a proxy** (default setting)
- **Use Internet Explorer proxy settings** — This setting allows an agent in a Windows environment to use the proxy server and credential information currently configured for Internet Explorer. There are several methods to configure Internet Explorer for use with proxies. For information, see Internet Explorer Help.
NOTE: When this setting is selected, the fields for specifying user authentication for HTTP and FTP proxies become available, as well as the option **Allow user to configure proxy settings**. By selecting this option, the administrator grants permission to the user of a managed product to access additional update repositories that are configured behind the proxy server.
- **Configure the proxy settings manually** — When this setting is selected, the fields for specifying user authentication for HTTP and FTP proxies become available. This selection also allows the administrator to specify the HTTP and FTP locations using **DNS name**, **IPv4** address, or **IPv6** address.

Configuring proxy settings for the agent

Use this task to specify whether to use proxies.

Task

For option definitions, click ? in the interface.

- 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 From the list of policies select the **Edit Settings** link on the row labeled My Default, .
- 3 Click **Proxy**. The proxy settings page appears.
- 4 Select your preferred option:
 - If your agent does not require a proxy to access the Internet, select **Do not use a proxy**. This is the default selection.
 - On Windows systems you can select **Use Internet Explorer proxy settings** and if appropriate, select **Allow user to configure proxy settings**.
 - If you need a proxy other than Internet Explorer, select **Configure the proxy settings manually**.
- 5 Select a form for the address of the source HTTP or FTP location where the agent is to pull updates. The DNS Name drop-down menu includes the address options **DNS Name** (the fully-qualified domain name), **IPv4** and **IPv6** notation.
- 6 Type the DNS name or IP address and Port numbers of the HTTP and/or FTP source. If appropriate, select **Use these settings for all proxy types**.
- 7 Select **Specify exceptions** to designate systems that do not require access to the proxy.
- 8 Select **Use HTTP proxy authentication** and/or **Use FTP proxy authentication**, then provide a user name and credentials.
- 9 Click **Save**.

Retrieving system properties

Use this task to retrieve system properties from managed systems.

At each agent-server communication, the agent sends information to the ePO server about the managed computer, including information about the software products that are installed. The scope of the information depends on how you have configured:

- The agent policy that specifies whether to retrieve a full set of information about installed programs, or only a minimal set.
- The task setting that specifies whether to retrieve all properties defined by the agent policy, or only properties that have changed since the last agent-server communication. This setting is available when configuring an immediate or scheduled wake-up call.

For detailed information on how to access the configuration settings for retrieving properties of the managed system and of the products installed, see *Retrieving properties*. For a list of properties, see topic entitled *Windows system and product properties reported by the agent*.

Task

NOTE: Use the agent **General** policy page to set minimal or full product properties

To retrieve system properties <i>plus...</i>	Do this. . .
Minimal product properties that have changed since the last agent-server communication	<ol style="list-style-type: none">1 Set the agent policy to send minimal product properties.2 Set the wake-up task to send only properties that have changed since the last communication.
Full product properties that have changed since the last agent-server communication	<ol style="list-style-type: none">1 Set the agent policy to send full product properties.2 Set the wake-up task to send only properties that have changed since the last communication.
Minimal product properties whether or not they have changed since the last agent-server communication	<ol style="list-style-type: none">1 Set the agent policy to send minimal product properties.2 Set the wake-up task to send all properties, as defined by the agent policy.
Full product properties whether or not they have changed.	<ol style="list-style-type: none">1 Set the agent policy to send full properties.2 Set the wake-up task to send all properties, as defined by the agent policy.

Scheduling a client task for a group

Use this task to schedule a client task for a group.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Client Tasks**.
- 2 In the System Tree, select the group to be configured.

- 3 In the Actions field, click **Edit Settings** for the task to be configured. The Client Task Builder wizard opens.
- 4 Break inheritance.
- 5 On the **Schedule** page:
 - a Enable the task.
 - b Set the schedule, frequency, and options for the task.
 - c Click **Next** to review your settings.
- 6 Click **Save**. At the next agent-server communication, the task is sent to the group's members.

Creating a new scheduled client task

Use this task to create a new client task that runs on a schedule, such as a mirror task, update task, and McAfee Agent wake-up task.

Task

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

- 1 Click **Menu | Systems | System Tree**.
- 2 Select **Client Tasks**, then click **Actions** and select **New Task** from the drop-down menu. The Client Task Builder wizard opens.
- 3 On the **Description** page:
 - a Type a name for the task and any notes that might be useful.
 - b From the drop-down menu, select the kind of task you are creating.
 - c Indicate whether to send the task to all systems or to only systems that have certain tags or have no tags.
 - d Click **Next**.
- 4 On the **Configuration** page:
 - For a mirror task, type the location on the managed systems where you want to replicate contents from the repository. The repository is selected based on policy selections on the Repositories tab of the agent policy pages.
 - For an update task, indicate if the update progress dialog box is visible on managed systems and if users can postpone the update. You can also indicate if all packages in the repository are included or only selected packages.
 - For an agent wake-up task, indicate whether to send only properties that have changed since the last agent-server communication, or all properties defined by the agent policy.
- 5 Click **Next**.
- 6 On the **Schedule** page:
 - a Enable the task.
 - b Set the schedule, frequency, and options for the task.
 - c Click **Next** to review your settings.
- 7 Click **Save**.

Configuring selected systems for updating

Use this task to specify which update packages are updated immediately when Update Now is selected. 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 that have been deployed previously

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the systems to be updated.
- 2 From the Actions menu, select **Agent**, then select **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.
- 3 Click **OK**.

Working with the agent from the ePO server

The ePO interface includes pages where agent tasks and policies can be configured, and where agent properties can be viewed.

Use these tasks when working with the agent from the ePO server.

Tasks

- ▶ [Viewing agent and product properties](#)
- ▶ [Viewing system information](#)
- ▶ [Accessing settings to retrieve properties](#)
- ▶ [Windows system and product properties reported by the agent](#)
- ▶ [Sending manual wake-up calls to systems](#)
- ▶ [Sending manual wake-up calls to a group](#)
- ▶ [Making the system tray icon visible](#)
- ▶ [Locating inactive agents](#)

Viewing agent and product properties

Use this task to verify that the properties match the policy changes you have made. This is useful for troubleshooting. The available properties depend on whether you configured the agent to send full or minimal properties on the McAfee Agent policy pages.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**.
- 2 Select a system. Information about the system's properties, installed products, and agent appear.

Viewing system information

Use this task to view information about a selected system, including a list of its managed products.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**.
- 2 Click the system whose information you want to view. The System Details page appears.
- 3 Scroll through the list of available information, including a field labeled **Installed Products**.
- 4 Click the **More** link to see detailed properties for each installed product.

Accessing settings to retrieve properties

Use these tasks to access the settings used for retrieving properties.

Task

For option definitions, click ? in the interface.

To do this...	Do this...
Set agent policy	<ol style="list-style-type: none"> 1 Click Menu Systems System Tree Assigned Policies <Product = McAfee Agent> Edit Assignment Edit Policy. 2 Select or deselect Send full product properties in addition to system properties. If deselected, only minimal product properties are sent in addition to system properties.
Send an immediate agent wake-up call	<ol style="list-style-type: none"> 1 Click Menu Systems System Tree <select target systems> Actions Agent Wake Up Agents. 2 Select Get full product properties in addition to system properties if you need them.
Set the scheduled wake-up call	<ol style="list-style-type: none"> 1 Click Menu Systems System Tree Client Tasks <select a wake-up task or create a New Task> Type = McAfee Agent Wakeup Next. 2 Select Send all properties defined by the agent policy or Send only properties that have changed since the last agent-server communication. 3 Set the Schedule.

Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

Agent Version	IPX Address	Subnet Address
CPU Serial Number	Is 64 Bit OS	Subnet Mask
CPU Speed (MHz)	Last Communication	System Description
CPU Type	MAC Address	System Location
Custom Props 1-4	Managed State	System Name
Default Language	Number Of CPUs	System Tree Sorting
Description	Operating System	Tags
DNS Name	OS Build Number	Time Zone
Domain Name	OS OEM Identifier	Total Disk Space
Free Disk Space	OS Platform	Total Physical Memory
Free Memory	OS Service Pack Version	User Name
Installed Products	OS Type	
IP Address	OS Version	

Product properties

Each McAfee product designates the properties it reports to ePolicy Orchestrator and, of those, which are included in a set of minimal properties. This list shows the kinds of product data that are reported to ePolicy Orchestrator by the McAfee software installed on your system. If you find errors in the reported values, review the details of your products before concluding that they are incorrectly reported.

- Agent Wake-Up Communication Port
- Agent-to-Server Communication Interval
- DAT Version
- Engine Version
- HotFix/Patch Version
- Language
- License Status
- Policy Enforcement Interval
- Product Version
- Service Pack

Sending manual wake-up calls to systems

Use this task to manually send an agent or SuperAgent wake-up call to systems in the System Tree. This is useful when you make policy changes and you want agents to call in for an update before the next agent-server communication.

Before you begin

Before sending the agent wake-up call to systems, make sure that **Enable agent wake-up call support** is enabled and applied on the General tab of the McAfee Agent policy pages. It is enabled by default.

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 from the **Actions** drop-down menu, select **Agent**, then select **Wake Up Agents** from the submenu. The Wake Up McAfee Agent page appears.
- 3 Ensure that the systems you selected appear in the Target section.
- 4 Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call**.
- 5 Accept the default **Randomization** (0 - 60 minutes) or type a different value. Consider the number of systems that are receiving the wake-up call, and how much bandwidth is available. If you type 0, agents respond immediately.
- 6 During regular communication, the agent sends only properties that have changed since the last agent-server communication. This task is set by default to **Get full product properties**. To send the complete properties as a result of this wake-up call, ensure that this is option selected.
- 7 Click **OK** to send the agent or SuperAgent wake-up call.

Sending manual wake-up calls to a group

Use this task to manually send an agent or SuperAgent wake-up call to a System Tree group. This is useful when you have made policy changes and want agents to call in for an update.

Before you begin

Make sure that wake-up support for the targeted group is enabled and applied on the General tab of the McAfee Agent policy pages. It is enabled by default.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**.
- 2 Click **Group Details**, then select the target group from the System Tree.
- 3 From the Actions drop-down menu, select **Wake Up Agents**. The Wake Up McAfee Agent page appears.
- 4 Verify that the group appears next to **Target group**.

- 5 Select whether to send the agent wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.
- 6 Next to **Type**, select whether to send an **Agent wake-up call** or **SuperAgent wake-up call**.
- 7 Accept the default **Randomization** (0 - 60 minutes), or type a different value. If you type 0, agents awaken immediately.
- 8 During regular communication, the agent sends only properties that the point-products designate as important. This task is set by default to **Get full product properties**. To send the complete properties as a result of this wake-up call, ensure that this is option selected.
- 9 Click **OK** to send the agent or SuperAgent wake-up call.

Making the system tray icon visible

Use this task to make the McAfee system tray icon visible on managed computers.

Task

- 1 Click **Menu | Systems | System Tree | Assigned Policies | <Product = McAfee Agent>**.
- 2 Click a policy, for example **McAfee Default**. The McAfee Agent General tab for the selected policy opens.
- 3 Select **Show the McAfee system tray icon (Windows only)**.
You can also select **Allow end users to update security from the McAfee system tray menu**. When selected, users who are running McAfee Agent 4.5 can choose **Update Security** from the McAfee system tray icon to update all products for which an update package is present in the repository.
- 4 When you have completed your changes to the default configuration, click **Save**.

Locating inactive agents

An inactive agent is one that has not communicated with the ePO server within a user-specified time period. Some agents might become disabled or be uninstalled by users. In other cases, the system hosting the agent might have been removed from the network. McAfee recommends performing regular weekly searches for systems with these inactive agents.

To perform the search, run the ePolicy Orchestrator query named **Managed Inactive Agents**. (For information on queries, see *Queries* in the ePolicy Orchestrator Product Guide.) The default configuration of this query reports systems that have not communicated with the ePO server in the last month. You can specify hours, days, weeks, quarters or years.

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication. The query results allow you take a variety of actions with respect to the systems identified, including ping, delete, wake up, re-deploy an agent, etc.

CAUTION: If you force install a new agent, all previous policies and settings are lost.

Running agent tasks from the managed system

Use these tasks to perform selected procedures from the system where the agent is installed.

If you can access the managed system where the agent is installed, you can view and manage some features of the agent.

NOTE: The agent interface is available on the managed system only if you selected **Show McAfee system tray icon** on the General tab of the McAfee Agent policy pages.

Tasks

- ▶ [Running a manual update](#)
- ▶ [Enforcing policies](#)
- ▶ [Updating policies](#)
- ▶ [Sending properties to the ePO server](#)
- ▶ [Sending events to the ePO server immediately](#)
- ▶ [Using the icon option to update](#)
- ▶ [Forcing the agent to call in to the server](#)
- ▶ [Viewing version numbers and settings](#)
- ▶ [Agent command-line options](#)

Running a manual update

Use this Windows-only task to run an update manually from the managed system.

Task

- 1 On the managed system, right-click the McAfee system tray icon.
- 2 Select **Update Security**. The agent performs an update from the repository defined in the agent policy.

Product updates can include:

- Patch releases
- Legacy product plug-in (.DLL) files
- Service pack releases
- SuperDAT (SDAT*.EXE) packages
- Supplemental detection definition (ExtraDAT) files
- Detection definition (DAT) files
- Anti-virus engines
- Managed-product signatures

Enforcing policies

Use this Windows-only task to prompt an agent to enforce all configured policies on the managed system.

Task

- 1 On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.
- 2 Click **Enforce Policies**. The policy enforcement activity is displayed in the Agent Status Monitor.

Updating policies

Use this Windows-only task to prompt the agent on the managed system to call in to the server to update policy settings.

Task

- 1 On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.
- 2 Click **Check New Policies**. The policy-checking activity is displayed in the Agent Status Monitor.

Sending properties to the ePO server

Use this Windows-only task to send properties to the ePO server from the managed system.

Task

- 1 On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.
- 2 Click **Collect and Send Props**. A record of the property collection activity is added to the list of activities in the Agent Status Monitor.

NOTE: The agent policy controls whether full or incremental properties are sent.

Sending events to the ePO server immediately

Use this Windows-only task to send events to the server immediately from the managed system.

Task

- 1 On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | Status Monitor**.
- 2 Click **Send Events**. A record of the sending-events activity is added to the list of activities in the Agent Status Monitor.

NOTE: This action sends all events to ePolicy Orchestrator irrespective of their severity.

Using the icon option to update

For the administrator to control what is updated and when, the Windows-only option for users to **Update Security** is disabled by default. If you want to allow Windows users to update all McAfee products on their managed systems, you must enable this functionality. See *Configuring selected systems for updating* for more information. The icon cannot be used to update applications selectively. The user can update all the items in the repository, or none of them.

When the user selects **Update Security**, all of the following items are updated with the contents of the designated repository:

- Patch releases
- Legacy product plug-in (.DLL) files
- Service pack releases

- SuperDAT (SDAT*.EXE) packages
- Supplemental detection definition (ExtraDAT) files
- Detection definition (DAT) files
- Anti-virus engines
- Managed-product signatures

Forcing the agent to call in to the server

Use this Windows-only task to force the new agent to call in to the ePO server immediately. You can do this from any system on which an agent has just been installed. This is useful after installing the agent manually.

Task

- 1 On the system where you installed the agent, open a DOS command window by selecting **Start | Run**, type `cmd`, and press **Enter**.
- 2 In the command window, navigate to the agent installation folder containing the `CmdAgent.exe` file.
- 3 Type this command:
`CMDAGENT /p`
- 4 Press **Enter**. The agent calls into the server immediately.

When the agent calls in to the server for the first time, the system is added to the System Tree as a managed system. If you configured criteria-based sorting for the System Tree, the system is added to the location appropriate for its IP address or tags. Otherwise, the system is added to the Lost&Found group. Once the system is added to the System Tree, you can manage its policies through ePolicy Orchestrator.

Viewing version numbers and settings

Use this task to view the agent settings from the managed system and to look up the version numbers of the agent and product from the managed system. This is useful for troubleshooting when installing new agent versions, or to confirm that the installed agent is the same version as the one displayed in the agent properties on the server.

Task

- 1 On the managed system, right-click the McAfee system tray icon.
- 2 Select **About** to view information about the agent:
 - Computer name
 - Agent version number
 - DNS Name
 - IP Address
 - Port Number
 - Agent ID (GUID)
 - Date and time of last security update
 - Time lapse since last agent-to-server communication
 - Agent-to-server communication interval

- Policy enforcement interval
- Management state (managed or unmanaged)

In addition, information identifies the McAfee products installed and under management by ePolicy Orchestrator.

Agent command-line options

Use the Windows-only Command Agent (CmdAgent.exe) tool to perform selected agent tasks from the managed system. CmdAgent.exe is installed on the managed system at the time of agent installation. Perform this task locally on managed systems using this program or the McAfee system tray icon.

The CmdAgent.exe file is located in the agent installation folder. By default, this location is:

C:\PROGRAM FILES\MCAFFEE\COMMON FRAMEWORK

Command-line parameters

Parameter	Description
/C	Checks for new policies. The agent contacts the ePO server for new or updated policies, then enforces them immediately upon receipt.
/E	Prompts the agent to enforce policies locally.
/P	Sends properties and events to the ePO server.
/S	Displays the Agent Monitor and its options.

Using the system tray icon

In a Windows environment, if the agent policy has been set to show the McAfee icon in the system tray of the managed system, the user can access shortcuts to information and functionality of managed products.

- ▶ [What the system tray icon does](#)
- ▶ [Making the system tray icon visible](#)
- ▶ [Enabling user access to updating functionality](#)

What the system tray icon does

Option	Function
About...	Displays system and product information for products installed on the system, including the agent, the ePO server with which the agent communicates, and the software products being managed.
Quick Settings	Links to product menu items that are frequently used.
Manage Features	Displays links to the administrative console of managed products.
Update Security	Triggers immediate updating of all installed McAfee software products. This includes application of patches and hotfixes, as well as DAT and signature updates. NOTE: This feature is available only if specifically enabled in the agent policy.

Option	Function
Scan Computer for	Launches McAfee programs, such as VirusScan, that scan systems on-demand and detect unwanted malicious software.
View Security Status	Displays the current system status of managed McAfee products, including current events.
McAfee Agent Status Monitor	Triggers the Agent Status Monitor, which: <ul style="list-style-type: none">• Displays information on the collection and transmission of properties.• Sends events.• Downloads and enforces policies.

Making the system tray icon visible

Use this task to make the McAfee system tray icon visible on managed computers.

Task

- 1 Click **Menu | Systems | System Tree | Assigned Policies | <Product = McAfee Agent>**.
- 2 Click a policy, for example **McAfee Default**. The McAfee Agent General tab for the selected policy opens.
- 3 Select **Show the McAfee system tray icon (Windows only)**. You can also select **Allow end users to update security from the McAfee system tray menu**. When selected, users who are running McAfee Agent 4.5 can choose **Update Security** from the McAfee system tray icon to update all products for which an update package is present in the repository.
- 4 When you have completed your changes to the default configuration, click **Save**.

Enabling user access to updating functionality

Use this task to allow users to update through the system tray icon.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Policy Catalog | <Product = McAfee Agent>**.
- 2 Click **Edit Settings** in the row containing the policy to be modified. The McAfee Agent General tab for the selected policy opens.
- 3 Select **Allow end users to run update security from the McAfee system tray menu**.
- 4 When you have completed your changes to the default configuration, click **Save**.

Removing the McAfee Agent

Use these tasks to remove agents from systems.

NOTE: You cannot remove the agent using the Product Deployment task, which can remove products such as VirusScan Enterprise.

Tasks

- ▶ Running FrmInst.exe from the command line
- ▶ Removing agents when deleting systems from the System Tree
- ▶ Removing agents when deleting groups from the System Tree
- ▶ Removing agents from systems in query results
- ▶ Uninstalling from non-Windows operating systems

Running FrmInst.exe from the command line

Use this task to remove the agent from a system by running the agent installation program, FrmInst.exe, from the command line.

NOTE: If there are point-products installed on a system from which the agent has been removed, the now unmanaged agent continues in updater mode.

Task

- Run the agent installation program, FrmInst.exe, from the command line with the /REMOVE=AGENT option. The default location of this file is:
C:\PROGRAM FILES\MCAFFEE\COMMON FRAMEWORK

Removing agents when deleting systems from the System Tree

Use this task to remove agents from systems when you delete those systems from the System Tree.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then select the group with the systems you want to delete.
- 2 Select the systems from the list, then click **Actions**.
- 3 Select **Directory Management** from the drop-down menu, then select **Delete** from the submenu.
- 4 Confirm the deletion, then click **OK**.

The selected systems are deleted from the System Tree and their agents are removed at their next agent-server communication, unless point products continue to reside on those systems.

Removing agents when deleting groups from the System Tree

Use this task to remove agents from all systems in a group when you delete that group from the System Tree.

CAUTION: When you delete a group, all of its child groups and systems are also deleted.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then select a group to be deleted.

- 2 At the bottom of the System Tree panel, click **System Tree Actions** then select **Delete Group**.
- 3 Select **Remove agent from all systems**, then click **OK**.

The systems in the selected group are deleted from the System Tree, and their agents are removed at their next agent-server communication, unless point-products reside on those systems.

Removing agents from systems in query results

Use this Windows-only task to remove agents from systems listed in the results of a query (for example, the Agent Versions Summary query).

Task

For option definitions, click ? in the interface.

- 1 Run the desired query, then, from the results page, select the systems to be deleted.
- 2 Select **Directory Management** from the drop-down menu, then select **Delete** from the submenu.
- 3 Confirm the deletion, then click **OK**.

The agents are uninstalled after the next agent-server communication.

Uninstalling from non-Windows operating systems

Use this task to remove the agent from HP-UX, Linux, Macintosh, and Solaris systems. The task involves:

- Removing the agent from the system.
- Removing the system name from the ePO System Tree.

Task

- 1 Log on as "root" to the system where you want to remove the agent.
- 2 Run the command appropriate for your operating system.

Operating System	Commands
AIX	rpm -e MFEcma
HP-UX	swremove MFEcma
Linux	rpm -e MFEcma rpm -e MFErt NOTE: Be certain to follow the order listed here.
Macintosh	/Library/McAfee/cma/uninstall.sh
Solaris	pkgrm MFEcma

- 3 Click **Menu | Systems | System Tree**, then select the systems you have uninstalled.

- 4 From the Actions drop-down menu, select **Directory Management**, then select **Delete** from the submenu.

Agent Activity Logs

The agent log files are useful for determining agent status or for troubleshooting. Two log files record agent activity and are located in the agent installation folders on the managed system.

Agent activity log

This log file records agent activity related to things such as policy enforcement, agent-server communication, and event forwarding. You can define a size limit of this log file. On the Logging tab of the McAfee Agent policy pages, you can configure the level of agent activity that is recorded.

The agent activity log is an XML file named agent_<system>.xml, where <system> is the NetBIOS name of the system where the agent is installed.

Detailed agent activity log

In addition to the information stored in the agent activity log, the detailed activity log contains troubleshooting messages. This file has a 1 MB default size limit. When this log file reaches 1 MB, a backup copy is made (agent_<system>_backup.log).

On Windows systems, the detailed agent activity log is named agent_<system>.log file, where <system> is the NetBIOS name of the system on which the agent is installed.

On UNIX-based systems, the detailed log files are found in the folder /opt/McAfee/cma/scratch/etc and they are named log, log.1, log.2,..., log.5. The higher the log number, the older the file.

Viewing the agent activity log

Use these tasks to view the agent activity log. This log file records an agent's activity. The amount of detail depends on the policy settings you select on the Logging tab of the McAfee Agent policy pages.

These log files can be viewed from the managed system or from the ePO interface.

Tasks

- ▶ [Viewing the agent activity log from the managed system](#)
- ▶ [Viewing the agent activity log from the ePO server](#)

Viewing the agent activity log from the managed system

Use this task to view the agent activity log from the system where the agent is installed.

Task

NOTE: The agent icon is available in the system tray only if the **Show McAfee system tray icon (Windows only)** option is selected on the General tab of the McAfee Agent policy pages. If it is not visible, select this option and apply it. When you finish viewing the log file content, you can hide the icon again by deselecting the option and applying the change.

- 1 On the managed system, right-click the McAfee Agent icon in the system tray, then select **Status Monitor**. The Status Monitor displays the agent activity log.
- 2 When finished viewing the agent activity log, close the Status Monitor.

Viewing the agent activity log from the ePO server

Use this task to view the agent activity log of a system from the ePO server.

Before you begin

Be sure that the McAfee Agent policy settings are set to the following:

- Accept connection only from ePO server is unchecked (McAfee Agent policy pages, General tab)
- Enable remote access to log is checked (McAfee Agent policy pages, Logging tab)

Task

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

- 1 Click **Menu | Systems | System Tree**, then select the system.
- 2 From the Actions drop-menu, select **Agent**, then select **Show Agent Log**.
- 3 To view the backup copy of the detailed log, click **previous**.

Organizing the System Tree

In ePolicy Orchestrator, the System Tree is the starting point for organizing your managed environment.

- **System Tree** — The System Tree allows for easy management of policies and tasks, and organization of systems and groups.
- **Tags** — Tags allow you to create labels that can be applied to systems manually or automatically, based on criteria assigned to the tag. You can sort systems into groups based on tags (like IP address sorting), send client tasks to computers based on tags, or use tags for criteria in queries.
- **NT Domain and Active Directory synchronization** — This feature now allows for:
 - True synchronization of the Active Directory structure.
 - Control of potential duplicate system entries in the System Tree.
 - Control of systems in the System Tree when they are deleted from the domain or container.
- **Sorting systems into groups automatically** — You can now use tags as sorting criteria, in addition to the previous functionality provided by IP address sorting. Each type of sorting criteria can be used alone or in combination.

The System Tree contains all of the systems managed by ePolicy Orchestrator; it is the primary interface for managing policies and tasks on these systems. You can organize systems into logical groups (for example, functional department or geographic location), and sort them by IP address, subnet masks, or tags. You can manage policies (product configuration settings) and schedule tasks (for example, updating virus definition files) for systems at any level of the System Tree.

Before configuring ePolicy Orchestrator to deploy or manage the security software in your environment, you must plan how to best organize systems for management and select the methods to bring into and keep systems in the System Tree.

TIP: Many factors can influence how you should create and organize your System Tree. McAfee recommends taking time to review this entire guide before you begin creating your System Tree.

Are you setting up the System Tree for the first time?

When setting up the System Tree for the first time:

- 1 Evaluate the methods of populating the System Tree with your systems, and keeping it up-to-date. For example, through Active Directory synchronization, or criteria-based sorting.
- 2 Create and populate the System Tree.

Contents

- ▶ [The System Tree](#)
- ▶ [Considerations when planning your System Tree](#)

- ▶ [Tags and how they work](#)
- ▶ [Active Directory and NT domain synchronization](#)
- ▶ [Criteria-based sorting](#)
- ▶ [How a system is first placed in the System Tree](#)
- ▶ [Working with tags](#)
- ▶ [Creating and populating groups](#)
- ▶ [Moving systems manually within the System Tree](#)

The System Tree

The System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions.

Groups

The System Tree is a hierarchical structure that allows you to combine your systems within units called *groups*.

Groups have these characteristics:

- Groups can be created by global administrators or users with the appropriate permissions.
- A group can include both systems and other groups.
- Groups are administered by a global administrator or a user with appropriate permissions.

Grouping systems with similar properties or requirements into these units allows you to manage policies for systems in one place, rather than setting policies for each system individually.

As part of the planning process, consider the best way to organize systems into groups prior to building the System Tree.

Lost&Found group

The System Tree root (My Organization) includes a Lost&Found group. Depending on the methods for creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined.

The Lost&Found group has these characteristics:

- It can't be deleted.
- It can't be renamed.
- Its sorting criteria can't be changed from being a catch-all group (although you can provide sorting criteria for the subgroups you create within it.)
- It always appears last in the list and is not alphabetized among its peers.
- Users must be granted permissions to the Lost&Found group to see the contents of Lost&Found.
- When a system is sorted into Lost&Found, it is placed in a subgroup named for the system's domain. If no such group exists, one is created.

CAUTION: If you delete systems from the System Tree, be sure you select the option to remove their agents. If the agent is not removed, deleted systems reappear in the Lost&Found group because the agent continues to communicate to the server.

Inheritance

Inheritance is an important property that simplifies policy and task administration. Because of inheritance, child groups in the System Tree hierarchy inherit policies set at their parent groups. For example:

- Policies set at the My Organization level of the System Tree are inherited by groups below it.
- Group policies are inherited by subgroups or individual systems within that group.

Inheritance is enabled by default for all groups and individual systems that you add to the System Tree. This allows you to set policies and schedule client tasks in fewer places.

To allow for customization, however, inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions). You can lock policy assignments to preserve inheritance.

Considerations when planning your System Tree

An efficient and well-organized System Tree can simplify maintenance. Many administrative, network, and political realities of each environment can affect how your System Tree is structured. Plan the organization of the System Tree before you build and populate it. Especially for a large network, you want to build the System Tree only once.

Because every network is different and requires different policies — and possibly different management — McAfee recommends planning your System Tree before implementing the ePO software.

Regardless of the methods you choose to create and populate the System Tree, consider your environment while planning the System Tree.

Administrator access

When planning your System Tree organization, consider the access requirements of those who must manage the systems.

For example, you might have very decentralized network administration in your organization, where different administrators have responsibilities over different parts of the network. For security reasons, you might not have a global administrator account that can access every part of your network. In this scenario, you might not be able to set policies and deploy agents using a single global administrator account. Instead, you might need to organize the System Tree into groups based on these divisions and create accounts and permission sets.

Consider these questions:

- Who is responsible for managing which systems?
- Who requires access to view information about the systems?
- Who should not have access to the systems and the information about them?

These questions impact both the System Tree organization, and the permission sets you create and apply to user accounts.

Environmental borders and their impact on system organization

How you organize the systems for management depends on the borders that exist in your network. These borders influence the organization of the System Tree differently than the organization of your network topology.

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

Topological borders

Your network is already defined by NT domains or Active Directory containers. The better organized your network environment, the easier it is to create and maintain the System Tree with the synchronization features.

Geographic borders

Managing security is a constant balance between protection and performance. Organize your System Tree to make the best use of limited network bandwidth. Consider how the server connects to all parts of your network, especially remote locations that are often connected by slower WAN or VPN connections, instead of faster LAN connections. You may want to configure updating and agent-server communication policies differently for remote sites to minimize network traffic over slower connections.

Grouping systems first by geography provides several advantages for configuring policies:

- You can configure update policies for the group so that all systems update from one or more distributed software repositories located nearby.
- You can schedule client tasks to run at times better suited to the site's location.

Political borders

Many large networks are divided by individuals or groups responsible for managing different portions of the network. Sometimes these borders do not coincide with topological or geographic borders. Who accesses and manages the segments of the System Tree affects how you structure it.

Functional borders

Some networks are divided by the roles of those using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you may need to organize segments of the System Tree by functionality if different groups require different policies.

A business group may run specific software that requires special security policies. For example, arranging your email Exchange Servers into a group and setting specific exclusions for VirusScan Enterprise on-access scanning.

Subnets and IP address ranges

In many cases, organizational units of a network use specific subnets or IP ranges, so you can create a group for a geographic location and set IP filters for it. Also, if your network isn't spread out geographically, you can use network location, such as IP address, as the primary grouping criterion.

TIP: If possible, consider using sorting criteria based on IP address information to automate System Tree creation and maintenance. Set IP subnet masks or IP address range criteria for

applicable groups within the System Tree. These filters automatically populate locations with the appropriate systems.

Tags and systems with similar characteristics

You can use tags for automated sorting into groups. Tags identify systems with similar characteristics. If you can organize your groups by characteristics, you can create and assign tags based on that criteria, then use these tags as group sorting criteria to ensure systems are automatically placed within the appropriate groups.

If possible, consider using tag-based sorting criteria to automatically populate groups with the appropriate systems.

Operating systems and software

Consider grouping systems with similar operating systems to manage operating system-specific products and policies more easily. If you have legacy systems, you can create a group for them and deploy and manage security products on these systems separately. Additionally, by giving these systems a corresponding tag, you can automatically sort them into a group.

Tags and how they work

Tags are like labels that you can apply to one or more systems, automatically (based on criteria) or manually. Once tags are applied, you can use them to organize systems in the System Tree or run queries that result in an actionable list of systems. Therefore, with tags as organizational criteria, you can apply policies, assign tasks, and take a number of actions on systems with the same tags.

Traits of tags

With tags, you can:

- Apply one or more tags to one or more systems.
- Apply tags manually.
- Apply tags automatically, based on user-defined criteria, when the agent communicates with the server.
- Exclude systems from tag application.
- Run queries to group systems with certain tags, then take direct action on the resulting list of systems.
- Base System Tree sorting criteria on tags to group systems into desired System Tree groups automatically.

Who can use tags

Users with appropriate permissions can:

- Create and edit tags and tag criteria.
- Apply and remove existing tags to systems in the groups where they have access.
- Exclude systems from receiving specific tags.
- Use queries to view and take actions on systems with certain tags.

- Use scheduled queries with chained tag actions to maintain tags on specific systems within the parts of the System Tree where they have access.
- Configure sorting criteria based on tags to ensure that systems stay in the appropriate groups of the System Tree.

Types of tags

ePolicy Orchestrator uses two types of tags:

- **Tags without criteria.** These tags can be applied only to selected systems in the System Tree (manually) and systems listed in the results of a query.
- **Criteria-based tags.** These tags are applied to all non-excluded systems at each agent-server communication. Such tags use criteria based on any properties sent by the agent. They can also be applied to non-excluded systems on demand.

Active Directory and NT domain synchronization

ePolicy Orchestrator 4.5 can integrate with Active Directory and NT domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

Active Directory synchronization

If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain part or all of the System Tree with Active Directory synchronization settings. Once defined, the System Tree is updated with any new systems (and subcontainers) in your Active Directory.

Active Directory integration allows you to:

- Synchronize with your Active Directory structure, by importing systems and the Active Directory subcontainers (as System Tree groups) and keeping them up-to-date with Active Directory. At each synchronization, both systems and the structure are updated in the System Tree to reflect the systems and structure of Active Directory.
- Import systems as a flat list from the Active Directory container (and its subcontainers) into the synchronized group.
- Control what to do with potential duplicate systems.
- Use the system description, which is imported from Active Directory with the systems.

In previous versions of ePolicy Orchestrator, there were the two tasks: Active Directory Import and Active Directory Discovery. Now, use this process to integrate the System Tree with your Active Directory systems structure:

- 1** Configure the synchronization settings on each group that is a mapping point in the System Tree. At the same location, you can configure whether to:
 - Deploy agents to discovered systems.
 - Delete systems from the System Tree when they are deleted from Active Directory.
 - Allow or disallow duplicate entries of systems that already exist elsewhere in the System Tree.
- 2** Use the Synchronize Now action to import Active Directory systems (and possibly structure) into the System Tree according to the synchronization settings.

- 3 Use an NT Domain/Active Directory Synchronization server task to regularly synchronize the systems (and possibly the Active Directory structure) with the System Tree according to the synchronization settings.

Types of Active Directory synchronization

There are two types of Active Directory synchronization (*systems only* and *systems and structure*). Which one you use depends on the level of integration you want with Active Directory.

With each type, you control the synchronization by selecting whether to:

- Deploy agents automatically to systems new to ePolicy Orchestrator. You may not want to set this on the initial synchronization if you are importing a large number of systems and have limited bandwidth. The agent MSI is about 6 MB in size. However, you might want to deploy agents automatically to any new systems that are discovered in Active Directory during subsequent synchronization.
- Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.
- Prevent adding systems to the group if they exist elsewhere in the System Tree. This ensures that you don't have duplicate systems if you manually move or sort the system to another location.
- Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

Systems and structure

When using this synchronization type, changes in the Active Directory structure are carried over into your System Tree structure at the next synchronization. When systems or containers are added, moved, or removed in Active Directory, they are added, moved, or removed in the corresponding locations of the System Tree.

When to use this synchronization type

Use this to ensure that the System Tree (or parts of it) look exactly like your Active Directory structure.

If the organization of Active Directory meets your security management needs and you want the System Tree to continue to look like the mapped Active Directory structure, use this synchronization type with subsequent synchronization.

Systems only

Use this synchronization type to import systems from an Active Directory container, including those in non-excluded subcontainers, as a flat list to a mapped System Tree group. You can then move these to appropriate locations in the System Tree by assigning sorting criteria to groups.

If you choose this synchronization type, be sure to select not to add systems again if they exist elsewhere in the System Tree. This prevents duplicate entries for systems in the System Tree.

When to use this synchronization type

Use this synchronization type when you use Active Directory as a regular source of systems for ePolicy Orchestrator, but the organizational needs for security management do not coincide with the organization of containers and systems in Active Directory.

NT domain synchronization

Use your NT domains as a source for populating your System Tree. When you synchronize a group to an NT domain, all systems from the domain are put in the group as a flat list. You can manage these systems in the single group, or you can create subgroups for more granular organizational needs. Use a method, like automatic sorting, to populate these subgroups automatically.

If you move systems to other groups or subgroups of the System Tree, be sure to select to not add the systems when they already exist elsewhere in the System Tree. This prevents duplicate entries for systems in the System Tree.

Unlike Active Directory synchronization, only the system names are synchronized with NT domain synchronization; the system description is not synchronized.

Criteria-based sorting

As in past releases of ePolicy Orchestrator, you can use IP address information to automatically sort managed systems into specific groups. You can also create sorting criteria based on tags, which are like labels assigned to systems. You can use either type of criteria or both to ensure systems are where you want them in the System Tree.

Systems only need to match one criterion of a group's sorting criteria to be placed in the group.

After creating groups and setting your sorting criteria, perform a **Test Sort** action to confirm that the criteria and sorting order achieve the desired results.

Once you have added sorting criteria to your groups, you can run the **Sort Now** action. The action moves selected systems to the appropriate group automatically. Systems that do not match the sorting criteria of any group are moved to **Lost&Found**.

New systems that call in to the server for the first time are added automatically to the correct group. However, if you define sorting criteria after the initial agent-server communication, you must run the **Sort Now** action on those systems to move them immediately to the appropriate group, or wait until the next agent-server communication.

Sorting status of systems

On any system or collection of systems, you can enable or disable System Tree sorting. If you disable System Tree sorting on a system, it is excluded from sorting actions, except when the **Test Sort** action is performed. When a test sort is performed, the sorting status of the system or collection is considered and can be moved or sorted from the **Test Sort** page.

System Tree sorting settings on the ePO server

For sorting to take place, sorting must be enabled on the server and on the systems. By default, sorting systems once enabled. As a result, systems are sorted at the first agent-server communication (or next, if applying changes to existing systems) and are not sorted again.

Test sorting systems

Use this feature to view where systems would be placed during a sort action. The **Test Sort** page displays the systems and the paths to the location where they would be sorted. Although this page does not display the sorting status of systems, if you select systems on the page (even ones with sorting disabled), clicking **Move Systems** places those systems in the location identified.

How settings affect sorting

You can choose three server settings that determine whether and when systems are sorted. Also, you can choose whether any system can be sorted by enabling or disabling System Tree sorting on selected systems in the System Tree.

Server settings

The server has three settings:

- **Disable System Tree sorting** — If criteria-based sorting does not meet your security management needs and you want to use other System Tree features (like Active Directory synchronization) to organize your systems, select this setting to prevent other ePO users from mistakenly configuring sorting criteria on groups and moving systems to undesirable locations.
- **Sort systems on each agent-server communication** — Systems are sorted again at each agent-server communication. When you change sorting criteria on groups, systems move to the new group at their next agent-server communication.
- **Sort systems once** — Systems are sorted at the next agent-server communication and marked to never be sorted again at agent-server communication, as long as this setting is selected. You can still sort such a system, however, by selecting it and clicking **Sort Now**.

System settings

You can disable or enable System Tree sorting on any system. If disabled on a system, that system will not be sorted, regardless of how the sorting action is taken. However, performing the Test Sort action will sort this system. If enabled on a system, that system is sorted always for the manual Sort Now action, and can be sorted at agent-server communication, depending on the server settings for System Tree sorting.

IP address sorting criteria

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. If IP address organization coincides with your needs, consider using this information to create and maintain parts or all of your System Tree structure by setting IP address sorting criteria for such groups.

In this version of ePolicy Orchestrator, this functionality has changed, and now allows for the setting of IP sorting criteria randomly throughout the tree. You no longer need to ensure that the sorting criteria of the child group's IP address is a subset of the parent's, as long as the parent has no assigned criteria. Once configured, you can sort systems at agent-server communication, or only when a sort action is manually initiated.

CAUTION: IP address sorting criteria should not overlap between different groups. Each IP range or subnet mask in a group's sorting criteria should cover a unique set of IP addresses. If criteria does overlap, the group where those systems end up depends on the order of the subgroups on the **System Tree | Groups Details** tab. You can check for IP overlap using the Check IP Integrity action in the Group Details tab

Tag-based sorting criteria

In addition to using IP address information to sort systems into the appropriate group, you can define sorting criteria based on the tags assigned to systems.

Tag-based criteria can be used with IP address-based criteria for sorting.

Group order and sorting

To provide additional flexibility with System Tree management, you can configure the order of a group's subgroups, and therefore the order by which they are considered for a system's placement during sorting. When multiple subgroups have matching criteria, changing this order can change where a system ends up in the System Tree.

Additionally, if you are using catch-all groups, they must be the last subgroup in the list.

Catch-all groups

Catch-all groups are groups whose sorting criteria is set to **All others** on the Sorting Criteria page of the group. Only subgroups at the last position of the sort order can be catch-all groups. These groups receive all systems that were sorted into the parent group, but were not sorted into any of the catch-all's peers.

How a system is first placed in the System Tree

When the agent communicates with the server for the first time, the server uses an algorithm to place the system in the System Tree. When it cannot find an appropriate location for a system, it puts the system in the Lost&Found group.

At the first agent-server communication

On each agent-server communication, the server attempts to locate the system in the System Tree by agent GUID (only systems whose agents have already called into the server for the first time have an agent GUID in the database). If a matching system is found, it is left in 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.

Remember, the order that subgroups are placed in the **Group Details** tab determines the order that subgroups are considered by the server when it searches for a group with matching criteria.

- 1 The server searches for a system without an agent GUID (its agent has never called in before) with a matching name in a group with the same name as the domain. If found, the system is placed in that group. This can happen after the first Active Directory or NT domain synchronization, or when you have manually added systems to the System Tree.
- 2 If a matching system is still not found, the server searches for a group of the same name as the domain where the system originates. If such a group is not found, one is created under the Lost&Found group, and the system is placed there.
- 3 Properties are updated for the system.
- 4 The server applies all criteria-based tags to the system if the server is configured to run sorting criteria at each agent-server communication.
- 5 What happens next depends on whether System Tree sorting is enabled on both the server and the system.

- If System Tree sorting is disabled on either the server or the system, the system is left where it is.
 - If System Tree sorting is enabled on the server and system, the system is moved based on the sorting criteria in the System Tree groups.
- NOTE:** 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.

NOTE: 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.

NOTE: 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.

Working with tags

Use these tasks to create and apply tags to systems.

Tasks

- ▶ [Creating tags with the Tag Builder](#)
- ▶ [Excluding systems from automatic tagging](#)
- ▶ [Applying tags to selected systems](#)
- ▶ [Applying criteria-based tags automatically to all matching systems](#)

Creating tags with the Tag Builder

Use this task to create a tag with the New Tag Builder wizard. Tags can use criteria that's evaluated against every system:

- Automatically at agent-server communication.
- When the Run Tag Criteria action is taken.
- Manually on selected systems, regardless of criteria, with the Apply Tag action.

Tags without criteria can only be applied manually to selected systems.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Tag Catalog**, then click **Tag Actions | New Tag**. The Tag Builder wizard opens.
- 2 On the Description page, type a name and meaningful description, then click **Next**. The Criteria page appears.
- 3 Select and configure the desired criteria, then click **Next**. The Evaluation page appears.

NOTE: 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.

NOTE: 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**.

NOTE: If the tag has criteria, this page displays the number of systems that will receive this tag when evaluated against its criteria.

The tag is added to the list of tags on the Tag Catalog page.

Excluding systems from automatic tagging

Use this task to exclude systems from having specific tags applied. Alternatively, you can use a query to collect systems, then exclude the desired tags from those systems from the query results.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the group that contains the systems in the System Tree.
- 2 Select one or more systems in the Systems table, then click **Actions | Tag | Exclude Tag**.
- 3 In the Exclude Tag dialog box, select the desired tag to exclude from the selected systems from the drop-down list, then click **OK**.
- 4 Verify the systems have been excluded from the tag:
 - a Click **Menu | Systems | Tag Catalog**, then select the desired tag in the list of tags.
 - b Next to **Systems with tag** in the details pane, click the link for the number of systems excluded from criteria-based tag application. The Systems Excluded from the Tag page appears.

- c Verify the desired systems are in the list.

Applying tags to selected systems

Use this task to apply a tag manually to selected systems in the System Tree.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the group that contains the desired system.
- 2 Select the desired systems, then click **Actions | Tag | Apply Tag**.
- 3 In the **Apply Tag** dialogue box, select the desired tag from the drop-down list to apply to the selected systems, then click **OK**.
- 4 Verify the tags have been applied:
 - a Click **Menu | Systems | Tag Catalog** select, then select the desired tag in the list of tags.
 - b Next to **Systems with tag** in the details pane, click the link for the number of systems tagged manually. The Systems with Tag Applied Manually page appears.
 - c Verify the desired systems are in the list.

Applying criteria-based tags automatically to all matching systems

Use these tasks to apply criteria-based tags automatically to all systems that match its criteria.

Tasks

- ▶ [Applying criteria-based tags to all matching systems](#)
- ▶ [Applying criteria-based tags on a schedule](#)

Applying criteria-based tags to all matching systems

Use this task to apply a criteria-based tag to all systems that match the criteria, except for those that have been excluded from the tag.

Task

For option definitions, click ? in the interface.

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

NOTE: This removes the tag from systems that don't match the criteria and applies the tag to systems which match criteria but were excluded from receiving the tag.
- 4 Click **OK**.
- 5 Verify the systems have the tag applied:
 - a Click **Menu | Systems | Tag Catalog**, then select the desired tag in the list of tags.

- b** Next to **Systems with tag** in the details pane, click the link for the number of systems with tag applied by criteria. The Systems with Tag Applied by Criteria page appears.
- c** Verify the desired systems are in the list.

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

Applying criteria-based tags on a schedule

Use this task to schedule a regular task that applies a tag to all systems that match its criteria.

Task

For option definitions, click ? in the interface.

- 1** Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder page appears.
- 2** On the Description page, name and describe the task and select whether the task is enabled once it is created, then click **Next**. The Actions page appears.
- 3** Select **Run Tag Criteria** from the drop-down list, then select the desired tag from the Tag drop-down list.

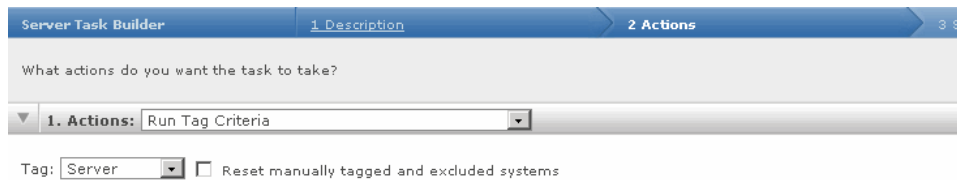


Figure 3: Run Tag Criteria server task action

- 4** Select whether to reset manually tagged and excluded systems.
NOTE: This removes the tag on systems that don't match the criteria and applies the tag to systems that match criteria but were excluded from receiving the tag.
- 5** Click **Next**. The Schedule page appears.
- 6** Schedule the task as desired, then click **Next**. The Summary page appears.
- 7** Review the task settings, then click **Save**.

The server task is added to the list on the Server Tasks page. If you selected to enable the task in the Server Task Builder wizard, it runs at the next scheduled time.

Creating and populating groups

Use these tasks to create and populate groups. You can populate groups with systems, either by typing NetBIOS names for individual systems or by importing systems directly from your network. You can also populate groups using drag-and-drop by dragging the selected systems and dragging them into any group in the System Tree. Drag-and-drop also allows you to move groups and subgroups within the System Tree.

There is no single way to organize a System Tree, and because every network is different, your System Tree organization can be as unique as your network layout. Although you won't use each method offered, you can use more than one.

For example, if you use Active Directory in your network, consider importing your Active Directory containers rather than your NT domains. If your Active Directory or NT domain organization does not make sense for security management, you can create your System Tree in a text file and import it into your System Tree. If you have a smaller network, you can create your System Tree by hand and add each system manually.

Best practices

While you won't use all of the System Tree creation methods, you also probably won't use just one. In many cases, the combination of methods you choose balances ease of creation with the need for additional structure to make policy management efficient.

For example, you might create the System Tree in two phases. First, you can create 90% of the System Tree structure by importing whole NT domains or Active Directory containers into groups. Then, you can manually create subgroups to classify systems together that may have similar anti-virus or security policy requirements. In this scenario, you could use tags, and tag-based sorting criteria on these subgroups to ensure they end up in the desired groups automatically.

If you want all or part of your System Tree to mirror the Active Directory structure, you can import and regularly synchronize the System Tree to Active Directory.

If one NT domain is very large or spans several geographic areas, you can create subgroups and point the systems in each to a separate distributed repository for efficient updating. Or, you can create smaller functional groupings, such as for different operating system types or business functions, to manage unique policies. In this scenario, you could also use tags and tag-based sorting criteria to ensure the systems stay in the group.

If your organization's IP address information coincides with your security management needs, consider assigning IP address sorting criteria to these groups before agent distribution, to ensure that when agents check into the server for the first time, the systems are automatically placed in the correct location. If you are implementing tags in your environment, you can also use tags as sorting criteria for groups, or even a combination of IP address and tag sorting criteria.

Although you can create a detailed System Tree with many levels of groups, McAfee recommends that you create only as much structure as is useful. In large networks, it is not uncommon to have hundreds or thousands of systems in the same container. Assigning policies in fewer places is easier than having to maintain an elaborate System Tree.

Although you can add all systems into one group in the System Tree, such a flat list makes setting different policies for different systems very difficult, especially for large networks.

Tasks

- ▶ [Creating groups manually](#)
- ▶ [Adding systems manually to an existing group](#)
- ▶ [Importing systems from a text file](#)
- ▶ [Sorting systems into criteria-based groups](#)
- ▶ [Importing Active Directory containers](#)
- ▶ [Importing NT domains to an existing group](#)
- ▶ [Synchronizing the System Tree on a schedule](#)
- ▶ [Updating the synchronized group with an NT domain manually](#)

Creating groups manually

Use this task to create groups manually. You can populate these groups with systems by typing NetBIOS names for individual systems or by importing systems directly from your network.

Task

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

- 1 Select the desired group in the System Tree under which to create a subgroup. Then:
 - From the Group Details page (**Menu | Systems | System Tree | Group Details**) click **Actions | New Subgroup**.
 - From the System Tree page (**Menu | Systems | System Tree**) click **System Tree Actions | New Subgroup**.
- 2 The New Subgroup dialog box appears.

TIP: You can create more than one subgroup at a time.
- 3 Type the desired name then click **OK**. The new group appears in the System Tree.
- 4 Repeat as necessary until you are ready to populate the groups with the desired systems. Add systems to the System Tree and ensure they get to the desired groups by:
 - Typing system names manually.
 - Importing them from NT domains or Active Directory containers. You can regularly synchronize a domain or a container to a group for ease of maintenance.
 - Setting up IP address-based or tag-based sorting criteria on the groups. When agents check in from systems with matching IP address information or matching tags, they are automatically placed in the appropriate group.

Adding systems manually to an existing group

Use this task to import systems from your Network Neighborhood to groups. You can also import a network domain or Active Directory container.

Task

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

- 1 Click **Menu | Systems | System Tree**, then in the **System Tree Actions** menu click **New Systems**. The New Systems page appears.

Figure 4: New Systems page

- 2 Select whether to deploy the agent to the new systems, and whether the systems are added to the selected group or to a group according to sorting criteria.
- 3 Next to **Systems to add**, 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 If you selected **Push agents and add systems to the current group**, you can enable automatic System Tree sorting. Do this to apply the sorting criteria to these systems. Specify the following options:

Option	Action
Agent version	Select the agent version to deploy.
Installation path	Configure the agent installation path or accept the default.
Credentials for agent installation	Type valid credentials to install the agent.
Number of attempts	Type an integer, using zero for continuous attempts.
Retry interval	Type the number seconds between retries.
Abort After	Type the number of minutes before aborting the connection.
Connect using	Select either a specific Agent Handler or all Agent Handlers.

- 5 Click **OK**.

Importing systems from a text file

Use these tasks to create a text file of systems and groups to import into the System Tree.

Tasks

- ▶ [Creating a text file of groups and systems](#)
- ▶ [Importing systems and groups from a text file](#)

Creating a text file of groups and systems

Use this task to create a text file of the NetBIOS names for your network systems that you want to import into a group. You can import a flat list of systems, or organize the systems into groups, then add the specified systems to them. You can create the text file by hand. In large networks, use other network administration tools to generate a text file list of systems on your network.

Define the groups and their systems by typing the group and system names in a text file. Then import that information into ePolicy Orchestrator. You must have network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate complete text files containing complete lists of the systems on your network. Once you have the text file, edit it manually to create groups of systems, and import the entire structure into the System Tree.

Regardless of how you generate the text file, you must use the correct syntax before importing it.

Task

For option definitions, click ? in the interface.

- 1 List each system separately on its own line. To organize systems into groups, type the group name followed by a backslash (\), then list the systems belonging to that group beneath it, each on a separate line.

```
GroupA\system1
```

```
GroupA\system2
```

```
GroupA\GroupB\system3
```

```
GroupC\GroupD
```

- 2 Verify the names of groups and systems, and the syntax of the text file, then save the text file to a temporary folder on your server.

Importing systems and groups from a text file

Use this task to import systems or groups of systems into the System Tree from a text file you have created and saved.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then click **System Tree Actions** and select **New Systems**. The New Systems page appears.
- 2 Select **Import systems from a text file into the selected group, but do not push agents**.
- 3 Select whether the import file contains:
 - **Systems and System Tree Structure**
 - **Systems only (as a flat list)**
- 4 Click **Browse**, then select the text file.

- 5 Select what to do with systems that already exist elsewhere in the System tree.
- 6 Click **OK**.

The systems are imported to the selected group in the System Tree. If your text file organized the systems into groups, the server creates the groups and imports the systems.

Sorting systems into criteria-based groups

Use these tasks to configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled on the server and the desired systems, and sorting criteria and the sorting order of groups must be configured.

Tasks

- ▶ [Adding sorting criteria to groups](#)
- ▶ [Enabling System Tree sorting on the server](#)
- ▶ [Enabling and disabling System Tree Sorting on Systems](#)
- ▶ [Sorting systems manually](#)

Adding sorting criteria to groups

Use this task to configure sorting criteria for a group. Sorting criteria can be based on IP address information or tags.

Task

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

- 1 Click **Menu | Systems | System Tree | Group Details** and select the group in the System Tree.
- 2 Next to **Sorting criteria** click **Edit**. The **Sorting Criteria** page for the selected group appears.
- 3 Select **Systems that match any of the criteria below**, then the criteria selections appear.
NOTE: Although you can configure multiple sorting criteria for the group, a system only has to match a single criterion to be placed in this group.
- 4 Configure the criterion. Options include:
 - **IP addresses** — Use this text box to define an IP address range or subnet mask as sorting criteria. Any system whose address falls within it is sorted into this group.
 - **Tags** — Add specific tags to ensure systems with such tags that come into the parent group are sorted into this group.
- 5 Repeat as necessary until sorting criteria reconfigured for the group, then click **Save**.

Enabling System Tree sorting on the server

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, then select **System Tree Sorting** in the Setting Categories list and click **Edit**.
- 2 Select whether to sort systems only on the first agent-server communication or on each agent-server communication.

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

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

Enabling and disabling System Tree Sorting on Systems

Use this task to 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. Alternatively, 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.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the desired systems.
- 2 Click **Actions | Directory Management | Change Sorting Status**, then select whether to enable or disable System Tree sorting on selected systems.
- 3 In the Change Sorting Status dialog box select whether to disable or enable system tree sorting on the selected system.

NOTE: Depending on the server setting for System Tree sorting, these systems are sorted on the next agent-server communication. Otherwise, they can only be sorted with the Sort Now action.

Sorting systems manually

Use this task to sort selected systems into groups with criteria-based sorting enabled.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems** and select the group that contains the desired systems.
- 2 Select the systems then click **Actions | Directory Management | Sort Now**. The Sort Now dialog box appears.

NOTE: If you want to preview the results of the sort before sorting, click **Test Sort** instead. (However, if you move systems from within the **Test Sort** page, all selected systems are sorted, even if they have System Tree sorting disabled.)

- 3 Click **OK** to sort the systems.

Importing Active Directory containers

Use this task to import systems from your network's Active Directory containers directly into your System Tree by mapping Active Directory source containers to the groups of the System Tree. Unlike previous versions, you can now:

- Synchronize the System Tree structure to the Active Directory structure so that when containers are added or removed in Active Directory, the corresponding group in the System Tree is added or removed also.
- Delete systems from the System Tree when they are deleted from Active Directory.
- Prevent duplicate entries of systems in the System Tree when they already exist in other groups.

Before you begin

You must have appropriate permissions to perform this task.

Best practices

Implementation of this feature depends on whether you are creating the System Tree for the first time or if you upgrading from a previous version with an existing System Tree structure with which you are not using Active Directory integration.

If you have been using a previous version of ePolicy Orchestrator and already have a fully-populated System Tree, you can still take advantages of Active Directory integration by mapping your System Tree groups to Active Directory containers. You can use this feature to create mapping points between Active Directory containers and System Tree groups to import any new systems found in Active Directory to the appropriate location of the System Tree.

Task

For option definitions, click ? in the interface.

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

NOTE: You cannot synchronize the Lost&Found group of the System Tree.

Synchronization Settings for My Organization > North America	
Synchronization type:	<input type="radio"/> None <input type="radio"/> NT Domain <input checked="" type="radio"/> Active Directory
Synchronize:	<input checked="" type="radio"/> Systems and container structure <input type="radio"/> Systems only (as a flat list)
Systems that exist elsewhere in the System Tree:	<input type="radio"/> Add systems to the synchronized group and leave them in their current System Tree location (creates duplicate entries) <input type="radio"/> Leave systems in their current System Tree location only <input checked="" type="radio"/> Move systems from their current System Tree location to the synchronized group
Active Directory domain:	<input type="text" value="example.ad.domain"/>

Figure 5: Synchronization Settings page

- 2 Next to **Synchronization type**, click **Edit**. The Synchronization Settings page for the selected group appears.

- 3** Next to **Synchronization type**, select **Active Directory**. The Active Directory synchronization options appear.
- 4** Select the type of Active Directory synchronization you want to occur between this group and the desired Active Directory container (and its subcontainers):
 - **Systems and container structure** — Select this option if you want this group to truly reflect the Active Directory structure. When synchronized, the System Tree structure under this group is modified to reflect that of the Active Directory container it's mapped to. When containers are added or removed in Active Directory, they are added or removed in the System Tree. When systems are added, moved, or removed from Active Directory, they are added, moved, or removed from the System Tree.
 - **Systems only** — Select this option if you only want the systems from the Active Directory container (and non-excluded subcontainers) to populate this group, and this group only. No subgroups are created when mirroring Active Directory.
- 5** Select whether a duplicate entry for the system will be created for a system that already exists in another group of the System Tree.

TIP: McAfee does not recommend selecting this option, especially if you are only using the Active Directory synchronization as a starting point for security management and use other System Tree management functionality (for example, tag sorting) for further organizational granularity below the mapping point.
- 6** In **Active Directory domain** you can:
 - Type the fully-qualified domain name of your Active Directory domain.
 - Select from a list of already registered LDAP servers.
- 7** Next to **Container**, click **Browse** 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 **Exclusions** and select a subcontainer to exclude, then click **OK**.
- 9** Select whether to deploy agents automatically to new systems. If you do, be sure to configure the deployment settings.

TIP: McAfee recommends that you do not deploy the agent during the initial import if the container is large. Deploying the 3.62 MB agent package to many systems at once may cause network traffic issues. Instead, import the container, then deploy the agent to groups of systems at a time, rather than all at once. Consider revisiting this page and selecting this option after the initial agent deployment, so that the agent is installed automatically on new systems added to Active Directory.
- 10** Select whether to delete systems from the System Tree when they are deleted from the Active Directory domain. Optionally choose whether to remove agents from the deleted systems.
- 11** To synchronize the group with Active Directory immediately, click **Synchronize Now**. Clicking **Synchronize Now** saves any changes to the synchronization settings before synchronizing the group. If you have an Active Directory synchronization notification rule enabled, an event is generated for each system added or removed (these events appear in the Audit Log, and are queryable). If you deployed agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the

Last Synchronization time is updated, displaying the time and date when the synchronization finished, not when any agent deployments completed.

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

12 When the synchronization completes, view the results with the System Tree.

Once the systems are imported, distribute agents to them if you did not select to do so automatically. Also, consider setting up a recurring NT Domain/Active Directory Synchronization server task to keep your System Tree up to date with any new systems or organizational changes in your Active Directory containers.

Importing NT domains to an existing group

Use this task to import systems from an NT domain to a group you created manually.

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

If the domain is very large, you can create subgroups to assist with policy management or System Tree organization. To do this, first import the domain into a group of your System Tree, then manually create logical subgroups.

TIP: To manage the same policies across several domains, import each of the domains into a subgroup under the same group, on which you can set policies that inherit into each of the subgroups.

When using this method:

- Set up IP address or tag sorting criteria on subgroups to automatically sort the imported systems.
- Schedule a recurring NT Domain/Active Directory Synchronization server task for easy maintenance.

Task

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

- 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.

Synchronization Settings for My Organization > North America	
Synchronization type:	<input type="radio"/> None <input checked="" type="radio"/> NT Domain <input type="radio"/> Active Directory
Systems that exist elsewhere in the System Tree:	<input type="radio"/> Add systems to the synchronized group and leave them in their current System Tree location <input checked="" type="radio"/> Leave systems in their current System Tree location only <input type="radio"/> Move systems from their current System Tree location to the synchronized group
Domain:	<input type="text"/> * <input type="button" value="Browse..."/>
Agent deployment:	<input type="checkbox"/> Deploy agents to new systems when they are discovered Deployment settings: Not configured <input type="button" value="Configure Settings"/>

Figure 6: Synchronization Settings page

- 3 Next to **Synchronization type**, select **NT Domain**. The domain synchronization settings appear.
- 4 Next to **Systems that exist elsewhere in the System Tree**, select what to do with systems that would be added during synchronization already exist in another group of the System Tree.

NOTE: McAfee does not recommend selecting **Add systems to the synchronized group and leave them in their current System Tree location**, especially if you are only using the NT domain synchronization as a starting point for security management and use other System Tree management functionalities (for example, tag sorting) for further organizational granularity below the mapping point.

- 5 Next to **Domain**, click **Browse** and select the NT domain to map to this group, then click **OK**. Alternatively, you can type the name of the domain directly in the text box.

NOTE: When typing the domain name, do not use the fully-qualified domain name.

- 6 Select whether to deploy agents automatically to new systems. If you do so, be sure to configure the deployment settings.

TIP: McAfee recommends that you do not deploy the agent during the initial import if the domain is large. Deploying the 3.62 MB agent package to many systems at once may cause network traffic issues. Instead, import the domain, then deploy the agent to smaller groups of systems at a time, rather than all at once. However, once you've finished deploying agents, consider revisiting this page and selecting this option after the initial agent deployment, so that the agent is installed automatically on any new systems that are added to the group (or its subgroups) by domain synchronization.

- 7 Select whether to delete systems from the System Tree when they are deleted from the NT domain. You can optionally choose to remove agents from deleted systems.
- 8 To synchronize the group with the domain immediately, click **Synchronize Now**, then wait while the systems in the domain are added to the group.

NOTE: Clicking **Synchronize Now** saves changes to the synchronization settings before synchronizing the group. If you have an NT domain synchronization notification rule enabled, an event is generated for each system added or removed. (These events appear in the Audit Log, and are queryable). If you selected to deploy agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the

Last Synchronization time is updated. The time and date are when the synchronization finished, not when any agent deployments completed.

- 9 If you want to synchronize the group with the domain manually, click **Compare and Update**. The Manually Compare and Update page appears.

NOTE: Clicking **Compare and Update** saves any changes to the synchronization settings.

- a If you are going to remove any systems from the group with this page, select whether to remove their agents when the system is removed.
- b Select the systems to add to and remove from the group as necessary, then click **Update Group** to add the selected systems. The Synchronize Setting page appears.

- 10 Click **Save**, then view the results in the System Tree if you clicked **Synchronize Now** or **Update Group**.

Once the systems are added to the System Tree, distribute agents to them if you did not select to deploy agents as part of the synchronization. Also, consider setting up a recurring NT Domain/Active Directory Synchronization server task to keep this group up-to-date with new systems in the NT domain.

Synchronizing the System Tree on a schedule

Use this task to schedule a server task that updates the System Tree with changes in the mapped domain or Active Directory container. Depending on a group's synchronization settings, this task:

- Adds new systems on the network to the specified group.
- Adds new corresponding groups when new Active Directory containers are created.
- Deletes corresponding groups when Active Directory containers are removed.
- Deploys agents to new systems.
- Removes systems that are no longer in the domain or container.
- Applies policies and tasks of the site or group to new systems.
- Prevents or allows duplicate entries of systems that still exist in the System Tree that you've moved to other locations.

NOTE: The agent cannot be deployed to all operating systems in this manner. You might need to distribute the agent manually to some systems.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder opens.
- 2 On the Description page, name the task and choose whether it is enabled once it is created, then click **Next**. The Actions page appears.
- 3 From the drop-down list, select **Active Directory Synchronization/NT Domain**.
- 4 Select whether to synchronize all groups or selected groups. If you are synchronizing only some synchronized groups, click **Select Synchronized Groups** and select specific ones.

- 5 Click **Next**. The Schedule page appears.
- 6 Schedule the task, then click **Next**. The Summary page appears.
- 7 Review the task details, then click **Save**.

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

Updating the synchronized group with an NT domain manually

Use this task to update a synchronized group with its mapped NT domain, including:

- Add systems currently in the domain.
- Remove systems from your System Tree that are no longer in the domain.
- Remove agents from all systems that no longer belong to the specified domain.

Task

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

- 1 Click **Menu | Systems | System Tree | Group Details**, then select the group that is mapped to the NT domain.
- 2 Next to **Synchronization type**, click **Edit**. The Synchronization Settings page appears.
- 3 Near the bottom of the page, click **Compare and Update**. The Manually Compare and Update page appears.
- 4 If you are removing systems from the group, select whether to remove the agents from systems that are removed.
- 5 Click **Add All** or **Add** to import systems from the network domain to the selected group. Click **Remove All** or **Remove** to delete systems from the selected group.
- 6 Click **Update Group** when finished.

Moving systems manually within the System Tree

Use this task to move systems from one group to another in the System Tree. You can move systems from any page that displays a table of systems, including the results of a query.

NOTE: 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**.

Transferring systems between ePO servers

Use this task to transfer systems between ePO servers.

Before you begin

Configure the following requirements before transferring systems between ePO servers:

- Interchange the agent-server secure communication key between the servers:

NOTE: The following steps accommodate two-way transfer. If you prefer to enable only one-way transfers you do not need to import the key from the target server into the main server.

- 1 Export the agent-server secure communication key from both the servers. See *Exporting ASSC keys* for more information.
 - 2 Import the agent-server secure communication key from server A to server B. See *Importing ASSC keys* for more information.
 - 3 Import the agent-server secure communication key from server B to server A.
- Register the server that you want to transfer the system to.

NOTE: Be sure to enable Transfer Systems on the Details page of the Registered Server Builder wizard.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**, then select the systems you want to transfer.
- 2 Click **Actions | Agent | Transfer Systems**. The Transfer Systems dialog box appears.
- 3 Select the desired server from the drop-down menu and click **OK**.

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

Creating Repositories

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.

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

Are you creating repositories for the first time?

When creating and setting up repositories for the first time:

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

Contents

- ▶ [Repository types and what they do](#)
- ▶ [How repositories work together](#)
- ▶ [Ensuring access to the source site](#)
- ▶ [Working with source and fallback sites](#)
- ▶ [Using SuperAgents as distributed repositories](#)
- ▶ [Creating and configuring FTP, HTTP, and UNC repositories](#)
- ▶ [Working with the repository list files](#)
- ▶ [Changing credentials on multiple distributed repositories](#)

Repository types and what they do

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

Master repository

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

The master repository is configured when ePolicy Orchestrator is installed. However, you must ensure that proxy server settings are configured correctly. By default, ePolicy Orchestrator uses Microsoft Internet Explorer proxy settings.

Distributed repositories

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

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

Replication can occur:

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

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

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

CAUTION: 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 McAfeeHttp update site, but you can change the source site or create multiple source sites if you require. McAfee recommends using the McAfeeHttp or McAfeeFtp update sites as your source site.

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

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

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

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

Fallback site

The fallback site is a source site that's been enabled as the backup site, from which managed systems can retrieve updates when their usual repositories are inaccessible. For example, when network outages or virus outbreaks occur, accessing the established location might be difficult.

Therefore, managed systems can remain up-to-date in such situations. The default fallback site is the McAfeeHttp update site. You can enable only one fallback site.

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

Types of distributed repositories

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

SuperAgent repositories

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

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

TIP: Although functionality of SuperAgent broadcast wake-up calls requires a SuperAgent in each broadcast segment, this is not a requirement for functionality of the SuperAgent repository. Managed systems only need to "see" the system hosting the repository.

FTP repositories

You can use an FTP server to host a distributed repository. Use FTP server software, such as Microsoft Internet Information Services (IIS), to create a new folder and site location for the distributed repository. See your web server documentation for details.

HTTP repositories

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

UNC share repositories

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

Unmanaged repositories

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

If a distributed repository is not managed, a local administrator must keep it up-to-date manually.

Once the distributed repository is created, use ePolicy Orchestrator to configure managed systems of a specific System Tree group to update from it.

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

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

Repository branches and their purposes

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

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

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

Current branch

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

Evaluation branch

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

Previous branch

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

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

Repository list file and its uses

The repository list (SiteList.xml and SiteMgr.xml) file contains the names of all the repositories you are managing. The repository list includes the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository list to the agent during agent-server communication.

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

Use an exported SiteList.xml file to:

- Import to an agent during installation.

Use an exported SiteMgr.xml file to:

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

How repositories work together

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

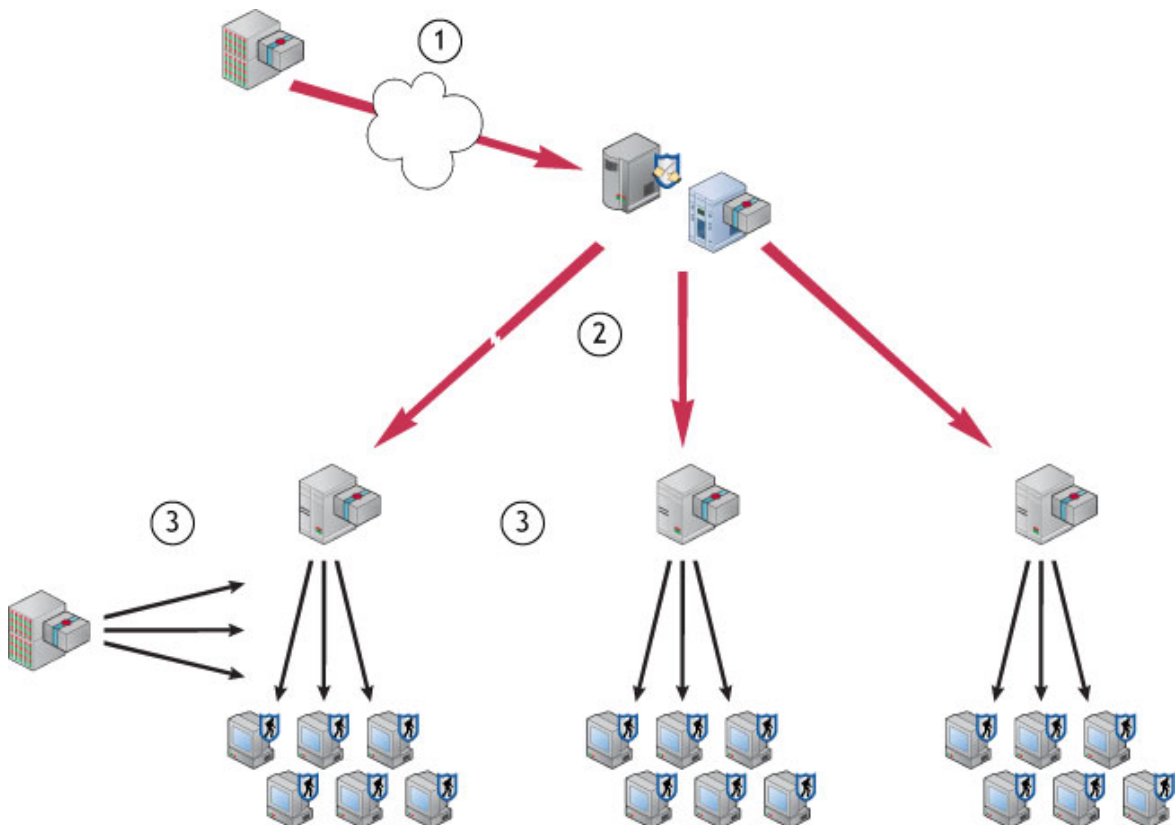


Figure 7: Sites and repositories delivering packages to systems

- 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.

Ensuring access to the source site

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

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

Tasks

- ▶ [Configuring proxy settings](#)
- ▶ [Configuring proxy settings for the McAfee Agent](#)
- ▶ [Configuring proxy settings for MyAvert Security Threats](#)

Configuring proxy settings

Use this task to configure proxy settings to pull DATs for updating your repositories and to update MyAvert security threats.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**. The Server Settings page appears.
- 2 From the list of setting categories, select **Configure Proxy Settings**, then click **Edit**. The Edit Configure Proxy Settings page appears.
- 3 Select **Configure the proxy settings manually**.
- 4 Next to **Proxy server**, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Then type the IP address or fully-qualified domain name and the **Port** number of the proxy server.
NOTE: If you are using the default source and fallback sites, or if you configure another HTTP source site and FTP fallback site (or vice versa), configure both HTTP and FTP proxy authentication information here.
- 5 Next to **Proxy authentication**, configure the settings as appropriate, depending on whether you pull updates from HTTP repositories, FTP repositories, or both.
- 6 Next to **Exclusions**, select **Bypass Local Addresses**, then specify distributed repositories the server can connect to directly by typing the IP addresses or fully-qualified domain name of those systems, separated by semi-colons.
- 7 Click **Save**.

Configuring proxy settings for the McAfee Agent

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

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 **General**. A list of agents configured for the 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.

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

- 5 Select **Configure the proxy settings manually** to configure the proxy settings for the agent manually.
- 6 Type the IP address or fully-qualified domain name and the port number of the HTTP and/or FTP source where the agent pulls updates. Select **Use these settings for all proxy types** to make these the default settings for all the proxy types.
- 7 Select **Specify exceptions** to designate systems that do not require access to the proxy. Use a semicolon to separate the exceptions.
- 8 Select **Use HTTP proxy authentication** and/or **Use FTP proxy authentication**, then provide a user name and credentials.
- 9 Click **Save**.

Configuring proxy settings for MyAvert Security Threats

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**.
- 2 Select **Configure Proxy Settings** and click **Edit**. The Edit Configure Proxy Settings page appears.
- 3 Select **Configure the proxy settings manually**.
- 4 Next to **Proxy server**, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Then type the IP address or fully-qualified domain name and the **Port** number of the proxy server.

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

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

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

Working with source and fallback sites

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

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

Tasks

- ▶ [Switching source and fallback sites](#)
- ▶ [Creating source sites](#)
- ▶ [Editing source and fallback sites](#)
- ▶ [Deleting source sites or disabling fallback sites](#)

Switching source and fallback sites

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

Before you begin

You must have appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Software | Source sites**. A list appears with all sites that can be used as the source or fallback.
- 2 From the list, locate the site that you want to set as fallback, then click **Enable Fallback**.

Creating source sites

Use this task to create a new source site.

Before you begin

You must have appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Software | Source Sites**, then click **Actions | New Source Site**. The Source Site Builder wizard opens.

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

- 4 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.

- 5 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.

- 6 Click **Next**.

- 7 Review the Summary page, then click **Save** to add the site to the list.

Editing source and fallback sites

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

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Source Sites**. A list appears with all sites that can be used as the source or fallback.
- 2 Locate the site in the list, then click **Edit Settings**. The Source Site Builder wizard opens.
- 3 Edit the settings on the wizard pages as needed, then click **Save**.

Deleting source sites or disabling fallback sites

Use this task to delete source sites or disable fallback sites.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Source Sites**, then click **Delete** next to a source site. The Delete Source Site dialog box appears.
- 2 Click **OK**.

The site is removed from the Source Sites page.

Using SuperAgents as distributed repositories

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

Tasks

- ▶ [Creating SuperAgent repositories](#)
- ▶ [Selecting which packages are replicated to SuperAgent repositories](#)
- ▶ [Deleting SuperAgent distributed repositories](#)

Creating SuperAgent repositories

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

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

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 **General**. A list of agents configured for the ePO server appears.

- 2 Create a new policy, duplicate an existing one, or open one that's already applied to systems that host a SuperAgent where you want to host SuperAgent repositories.
 - 3 Select the **General** tab, then ensure **Convert agents to SuperAgents** is selected.
 - 4 Select **Use systems running SuperAgents as distributed repositories**, then type a folder path location for the repository. This is the location where the master repository copies updates during replication. You can use standard Windows variables, such as <PROGRAM_FILES_DIR>.
- NOTE:** Managed systems updating from this SuperAgent repository are able to access this folder. You do not need to manually enable file sharing.
- 5 Click **Save**.
 - 6 Assign this policy to each system that you want to host a SuperAgent repository.

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

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

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

If you do not want to wait for the next agent-server communication, you can send an agent wake-up call to the systems.

Selecting which packages are replicated to SuperAgent repositories

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Distributed Repositories**. A list of all distributed repositories appears.
 - 2 Locate the desired SuperAgent repository, then click **Edit Settings**. The Distributed Repository Builder wizard opens.
 - 3 On the Package Types page, select the required package types.
- NOTE:** Ensure that all packages required by any managed system using this repository are selected. Managed systems go to one repository for all packages — the task fails for systems that are expecting to find a package type that is not present. This feature ensures packages that are used only by a few systems are not replicated throughout your entire environment.
- 4 Click **Save**.

Deleting SuperAgent distributed repositories

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

Task

For option definitions, click ? in the interface.

- 1 Open the desired McAfee Agent policy pages (in edit mode) from the desired assignment point in the System Tree or from the **Policy Catalog** page.
- 2 On the **General** tab, deselect **Use systems running SuperAgents as distributed repositories**, then click **Save**.

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

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

Creating and configuring FTP, HTTP, and UNC repositories

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

Tasks

- ▶ [Creating a folder location on an FTP, HTTP server or UNC share](#)
- ▶ [Adding the distributed repository to ePolicy Orchestrator](#)
- ▶ [Enabling folder sharing for UNC and HTTP repositories](#)
- ▶ [Editing distributed repositories](#)
- ▶ [Deleting distributed repositories](#)

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

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

Task

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

Adding the distributed repository to ePolicy Orchestrator

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Distributed Repositories**, then click **Actions | New Repository**. The Distributed Repository Builder wizard opens.
- 2 On the Description page, type a unique name and select **HTTP, UNC, or FTP**, then click **Next**. The name of the repository does not need to be the name of the system hosting the repository.
- 3 On the Server page, provide the web address and port information of the site.

HTTP or FTP server type:

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

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.
- Specify the Replication UNC path for your HTTP folder.

UNC server type:

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

- 4 Click **Next**.

- 5 On the Credentials page:

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

HTTP or FTP server type:

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

UNC server type:

- Select **Use credentials of logged-on account** to use the credentials of the currently logged-on user.
 - Select **Enter the download credentials**, then enter domain and user account information.
- b Click **Test Credentials**. After a few seconds, a confirmation message appears, stating that the site is accessible to systems using the authentication information. If credentials are incorrect, check the following:
 - User name and password

- URL or path on the previous panel of the wizard
 - HTTP, FTP, or UNC site on the system
- 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. I , then click **Next**.
 - If you choose the **Selected packages** option, you must manually select the **Signatures and engines** and **Products, patches, service packs, etc.** you want to replicate.
 - Optionally select to **Replicate legacy DATs**.

NOTE: 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 are used by only a few systems are not replicated throughout your entire environment.
 - 9** Review the Summary page, then click **Save** to add the repository. ePolicy Orchestrator adds the new distributed repository to its database.

Avoiding replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default.

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

Before you begin

Disable any replication tasks scheduled to replicate the selected package. For more information, see *Disabling replication of selected packages*.

Task

For option definitions, click ? in the interface.

- 1** Click **Menu | Software | Distributed Repositories**, then select **Edit Settings** next to the desired repository. The Distributed Repository Builder wizard opens.
- 2** On the Package Types page, deselect the package that you want to avoid being replicated.
- 3** Click **Save**.

Disabling replication of selected packages

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

Use this task to disable replication before checking in the new package.

Task

For option definitions, click ? in the interface.

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

Enabling folder sharing for UNC and HTTP repositories

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

Task

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

Editing distributed repositories

Use this task to edit a distributed repository.

Task

For option definitions, click ? in the interface.

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

Deleting distributed repositories

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

Before you begin

You must have appropriate permissions to perform this task.

Task

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

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

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

Working with the repository list files

Use these tasks to export repository list files:

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

Tasks

- ▶ [Exporting the repository list SiteList.xml file](#)
- ▶ [Exporting the repository list SiteMgr.xml file for backup or use by other servers](#)
- ▶ [Importing distributed repositories from the SiteMgr.xml file](#)
- ▶ [Importing source sites from the SiteMgr.xml file](#)

Exporting the repository list SiteList.xml file

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

Before you begin

You must have appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Software | Master Repository**, then click **Actions | Export Sitelist**. The File Download dialog box appears.
- 2 Click **Save**, browse to the location to save the SiteList.xml file, then click **Save**.

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

You can also distribute the repository list to managed systems, then apply the repository list to the agent.

Exporting the repository list SiteMgr.xml file for backup or use by other servers

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

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

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

Importing distributed repositories from the SiteMgr.xml file

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

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Distributed Repositories**, then click **Actions | Import Repositories**. The Import Repositories dialog box appears.
- 2 Browse to select the exported SiteMgr.xml file, then click **OK**. The Import Repositories page appears.
- 3 Select the desired distributed repositories to import into this server, then click **OK**.

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

Importing source sites from the SiteMgr.xml file

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

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Source Sites**, then click **Actions | Import Source Sites**. The Import Source Sites dialog box appears.
- 2 Browse to and select the exported SiteMgr.xml file, then click **OK**. The Import Source Sites page appears.
- 3 Select the desired source sites to import into this server, then click **OK**.

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

Changing credentials on multiple distributed repositories

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

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Distributed Repositories**. The Distributed Repositories page appears.
- 2 Click **Actions** and select **Change Credentials**. The Change Credentials wizard opens to the Repository Type page.
- 3 Select the type of distributed repository for which you want to change credentials, then click **Next**. The Repository Selection page appears.
- 4 Select the desired distributed repositories, then click **Next**. The Credentials page appears.
- 5 Edit the credentials as needed, then click **Next**. The Summary page appears.
- 6 Review the information, then click **Save**.

Managing your Network with Policies and Client Tasks

Managing products from a single location is a central feature of ePolicy Orchestrator and is accomplished through the combination of product policies and client tasks. Policies ensure a product's features are configured correctly, while client tasks are the scheduled actions that run on the managed systems hosting any client-side software.

Are you configuring policies and tasks for the first time?

When configuring policies and tasks for the first time:

- 1 Plan product policies and client tasks for the segments of your System Tree.
- 2 Create and assign policies to groups and systems.
- 3 Create and assign client tasks to groups and systems.

Contents

- ▶ [Product extensions and what they do](#)
- ▶ [Policy management](#)
- ▶ [Policy application](#)
- ▶ [Creating Policy Management queries](#)
- ▶ [Client tasks and what they do](#)
- ▶ [Bringing products under management](#)
- ▶ [Viewing policy information](#)
- ▶ [Working with the Policy Catalog](#)
- ▶ [Working with policies](#)
- ▶ [Working with client tasks](#)
- ▶ [Frequently asked questions](#)
- ▶ [Sharing policies among ePO servers](#)
- ▶ [How policy assignment rules work](#)

Product extensions and what they do

Extensions are zip files you install on the ePO server to manage another security product in your environment. The extensions contain the files, components, and information necessary to manage such a product. Extensions replace the NAP files of previous releases.

Functionality that extensions add

When a managed product extension is installed, added functionality can include:

- Policy pages
- Server tasks
- Client tasks
- Default queries
- New result types, chart types, and properties to select with the Query Builder wizard
- Default Dashboards and dashboard monitors
- Feature permissions that can be assigned to user accounts
- Additional product-specific functionality

Where extension files are located

Some product extensions are installed automatically when ePolicy Orchestrator is installed. For products whose extensions are not installed by default, see the product documentation for the extension name and location on the product CD or in the product download.

Policy management

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

Some policy settings are the same as the settings you configure in the interface of the product installed on the managed system. Other policy settings are the primary interface for configuring the product or component. The ePolicy Orchestrator console allows you to configure policy settings for all products and systems from a central location.

Policy categories

Policy settings for most products are grouped by *category*. Each policy category refers to a specific subset of policy settings. Policies are created by category. In the **Policy Catalog** page, policies are displayed by product and category. When you open an existing policy or create a new policy, the policy settings are organized across tabs.

Where policies are displayed

To see all of the policies that have been created per policy category, click **Menu | Policy | Policy Catalog**, then select a **Product** and **Category** from the drop-down lists. On the Policy Catalog page, users can see only policies of the products to which they have permissions.

To see which policies, per product, are applied to a specific group of the System Tree, click **Menu | Systems | System Tree | Assigned Policies** page, select a group, then select a **Product** from the drop-down list.

NOTE: A McAfee Default policy exists for each category. You cannot delete, edit, export or rename these policies, but you can copy them and edit the copy.

How policy enforcement is set

For each managed product or component, choose whether the agent enforces all or none of its policy selections for that product or component.

From the Assigned Policies page, choose whether to enforce policies for products or components on the selected group.

In the Policy Catalog page, you can view policy assignments, where they are applied, and if they are enforced. You can also lock policy enforcement to prevent changes to enforcement below the locked node.

NOTE: If policy enforcement is turned off, systems in the specified group do not receive updated sitelists during an agent-server communication. As a result, managed systems in the group might not function as expected. For example, you might configure managed systems to communicate with Agent Handler A, but with policy enforcement turned off, the managed systems won't receive the new sitelist with this information, so they report to a different Agent Handler listed in an expired sitelist.

When policies are enforced

When you reconfigure policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication. The frequency of this communication is determined by the **Agent-to-server-communication interval** (ASCI) settings on the **General** tab of the **McAfee Agent** policy pages, or the McAfee Agent Wakeup client task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Once the policy settings are in effect on the managed system, the agent continues to enforce policy settings locally at a regular interval. This enforcement interval is determined by the **Policy enforcement interval** setting on the **General** tab of the **McAfee Agent** policy pages. This interval is set to occur every five minutes by default.

Policy settings for McAfee products are enforced immediately at the policy enforcement interval, and at each agent-server communication if policy settings have changed.

NOTE: For Symantec AntiVirus products, there is a delay of up to three minutes after the interval before policies are enforced. The agent first updates the GRC.DAT file with policy information, then the Symantec AntiVirus product reads the policy information from the GRC.DAT file, which occurs approximately every three minutes.

Exporting and importing policies

If you have multiple servers, you can export and import policies between them via XML files. In such an environment, you only need to create a policy once.

You can export and import individual policies, or all policies for a given product.

This feature can also be used to back up policies if you need to reinstall the server.

Policy sharing

Policy sharing is another way to transfer policies between servers. Sharing policies allows you to manage policies on one server, and use them on many additional servers all through the ePO console. For more information, see *Sharing policies among ePO servers*.

Policy application

Policies are applied to any system by one of two methods, *inheritance* or *assignment*.

Inheritance

Inheritance determines whether the policy settings and client tasks for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree.

When you break this inheritance by assigning a new policy anywhere in the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment

You can assign any policy in the Policy Catalog to any group or system, provided you have the appropriate permissions. Assignment allows you to define policy settings once for a specific need, then apply the policy to multiple locations.

When you assign a new policy to a particular group of the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment locking

You can lock the assignment of a policy on any group or system, provided you have the appropriate permissions. Assignment locking prevents other users:

- With appropriate permissions at the same level of the System Tree from inadvertently replacing a policy.
- With lesser permissions (or the same permissions but at a lower level of the System Tree) from replacing the policy.

Assignment locking is inherited with the policy settings.

Assignment locking is valuable when you want to assign a certain policy at the top of the System Tree and ensure that no other users replace it anywhere in the System Tree.

Assignment locking only locks the assignment of the policy, but does not prevent the policy owner from making changes to its settings. Therefore, if you intend to lock a policy assignment, make sure that you are the owner of the policy.

Policy ownership

All policies for products and features to which you have permissions are available from the **Policy Catalog** page. To prevent any user from editing other users' policies, each policy is assigned an owner — the user who created it.

Ownership provides that no one can modify or delete a policy except its creator or a global administrator. Any user with appropriate permissions can assign any policy in the **Policy Catalog** page, but only the owner or a global administrator can edit it.

If you assign a policy that you do not own to managed systems, be aware that if the owner of the named policy modifies it, all systems where this policy is assigned receive these modifications. Therefore, if you wish to use a policy owned by a different user, McAfee recommends that you first duplicate the policy, then assign the duplicate to the desired locations. This provides you ownership of the assigned policy.

TIP: You can specify multiple non-global administrator users as owners of a single policy.

Creating Policy Management queries

Use this task to create either of the following Policy Management queries:

- **Applied Policies** query — Retrieves policies assigned to a specified managed systems.
- **Broken Inheritance** query — Retrieves information on policies that are broken in the system hierarchy.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**, then click **Actions | New Query**. The Query Wizard opens.
- 2 On the Result Type page, select **Policy Management** from the Feature Group list.
- 3 Under Result Types, select one of these options, then click **Next** and the Chart page appears:
 - **Applied Policies**
 - **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.

NOTE: If you select **Boolean Pie Chart**, you must configure the criteria you want to include in the query.

- 5 Select the columns to be included in the query, then click **Next**. The Filter page appears.
- 6 Select properties to narrow the search results, then click **Run**. The Unsaved Query page displays the results of the query, which is actionable. You can take any available actions on items in any tables or drill-down tables.

NOTE: Selected properties appear in the content pane with operators that can specify criteria, which narrows the data that is returned for that property.

- If the query didn't return the expected results, click **Edit Query** to go back to the Query Builder and edit the details of this query.
 - If you don't need to save the query, click **Close**.
 - If you want to use again this query again, click **Save** and continue to the next step.
- 7 In 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**.
 - 8 Click **Save**.

Client tasks and what they do

ePolicy Orchestrator allows you to create and schedule client tasks that run on managed systems. You can define tasks for the entire System Tree, for a specific group, or for an individual system. Like policy settings, client tasks are inherited from parent groups in the System Tree.

Which extension files are installed on your ePO server determines which client tasks are available.

Client tasks are commonly used for:

- Product deployment

- Product functionality (for example, the VirusScan Enterprise On-Demand Scan task)
- Upgrades and updates

See the product documentation for your managed products for information and instructions.

Bringing products under management

Use this task to install an extension (zip) file. A product's extension must be installed before ePolicy Orchestrator can manage the product.

Before you begin

You must have appropriate permissions to perform this task.

Task

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

- 1 Ensure that the extension file is in an accessible location on the network.
- 2 Click **Menu | Software | Extensions | Install Extension**. The Install Extension dialog box appears.
- 3 Browse to and select the desired extension (zip) file, then click **OK**.
- 4 Verify that the product name appears in the **Extensions** list.

Viewing policy information

Use these tasks to view detailed information about the policies, their assignments, inheritance, and their owners.

Tasks

- ▶ [Viewing groups and systems where a policy is assigned](#)
- ▶ [Viewing the settings of a policy](#)
- ▶ [Viewing policy ownership](#)
- ▶ [Viewing assignments where policy enforcement is disabled](#)
- ▶ [Viewing policies assigned to a group](#)
- ▶ [Viewing policies assigned to a specific system](#)
- ▶ [Viewing a group's policy inheritance](#)
- ▶ [Viewing and resetting broken inheritance](#)

Viewing groups and systems where a policy is assigned

Use this task to view the groups and systems where a policy is assigned. This list shows the assignment points only, not each group or system that inherits the policy.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the selected category appear in the details pane.

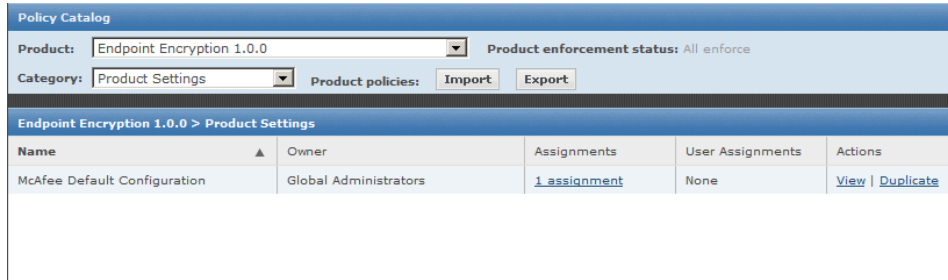


Figure 8: Policy Catalog page

- 2 Under **Assignments** on the row of the desired policy, click the link that indicates the number of groups or systems the policy is assigned to (for example, **6 assignments**).

On the Assignments page, each group or system where the policy is assigned appears with its **Node Name** and **Node Type**.

Viewing the settings of a policy

Use this task to view the specific settings of a policy.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the selected category appear in the details pane.
- 2 Click **Edit Settings** next to the desired policy. The policy pages and their settings appear.

NOTE: You can also view this information when accessing the assigned policies of a specific group. To access this information click **Menu | Systems | System Tree | Assigned Policies**, then click the link for the selected policy in the Policy column.

Viewing policy ownership

Use this task to view the owners of a policy.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the selected category appear in the details pane.
- 2 The owners of the policy are displayed under **Owner**.

Viewing assignments where policy enforcement is disabled

Use this task to view assignments where policy enforcement, per policy category, is disabled.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the selected category appear in the details pane.
- 2 Click the link next to **Product enforcement status**, which indicates the number of assignments where enforcement is disabled, if any. The **Enforcement for <policy name>** page appears.
- 3 Click any item in the list to go to its **Assigned Policies** page.

Viewing policies assigned to a group

Use this task to view the policies assigned to a group.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select a group in the System Tree. All assigned policies, organized by product, appear in the details pane.
- 2 Click any policy to view its settings.

Viewing policies assigned to a specific system

Use this task to view the policies assigned to a specific system.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the desired group in the System Tree. All systems belonging to the group appear in the details pane.
- 2 Select the system, then click **Actions | Agent | Modify Policies on a Single System**.
- 3 Select the product. The product's policies assigned to this system appear.
- 4 Click any policy to view its settings.

Viewing a group's policy inheritance

Use this task to view the policy inheritance of a specific group.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**. All assigned policies, organized by product, appear in the details pane.
- 2 The desired policy row, under **Inherit from**, displays the name of the group from which the policy is inherited.

Viewing and resetting broken inheritance

Use this task to view where policy inheritance is broken.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**. All assigned policies, organized by product, appear in the details pane.
- 2 The desired policy row, under **Broken Inheritance**, displays the number of groups and systems where this policy's inheritance is broken.
NOTE: 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.
- 3 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.
- 4 To reset the inheritance of any of these, select the checkbox next to the name, then click **Actions** and select **Reset Inheritance**.

Working with the Policy Catalog

Use these tasks to create and maintain policies from the Policy Catalog page.

Tasks

- ▶ [Creating a policy from the Policy Catalog page](#)
- ▶ [Duplicating a policy on the Policy Catalog page](#)
- ▶ [Editing a policy's settings from the Policy Catalog](#)
- ▶ [Renaming a policy from the Policy Catalog](#)
- ▶ [Deleting a policy from the Policy Catalog](#)

Creating a policy from the Policy Catalog page

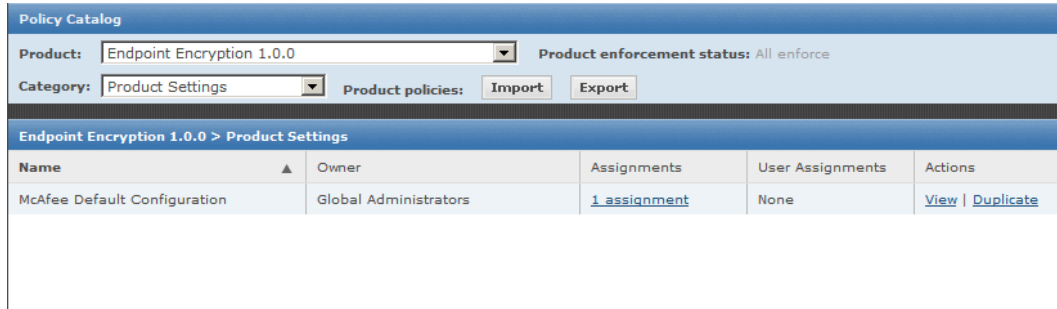
Use this task to create a new policy from the Policy Catalog. By default, policies created here are not assigned to any groups or systems. When you create a policy here, you are adding a custom policy to the Policy Catalog.

You can create policies before or after a product is deployed.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.



- 2 Click **Actions | New Policy**. The Create New Policy dialog box appears.
- 3 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
- 4 Type a name for the new policy and click **OK**. The Policy Settings wizard opens.
- 5 Edit the policy settings on each tab as needed.
- 6 Click **Save**.

Duplicating a policy on the Policy Catalog page

Use this task to create a new policy based on an existing one. For example, if you already have a policy that is similar to one you want to create, you can duplicate the existing one, then make the desired changes.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.
- 2 Locate the policy to duplicate, then click **Duplicate** in that policy's row. The Duplicate Existing Policy dialog box appears.
- 3 Type the name of the new policy in the field (for example, Sales Europe), then click **OK**. The new policy appears on the Policy Catalog page.
- 4 Click **Edit Settings** next to the new policy's name in the list.
- 5 Edit the settings as needed, then click **Save**.

Editing a policy's settings from the Policy Catalog

Use this task to modify the settings of a policy. Your user account must have appropriate permissions to edit policy settings for the desired product.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.
- 2 Locate the desired policy, then click **Edit Settings** next to it.
- 3 Edit the settings as needed, then click **Save**.

Renaming a policy from the Policy Catalog

Use this task to rename a policy. Your user account must have appropriate permissions to edit policy settings for the desired product.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.
- 2 Locate the desired policy, then click **Rename/Modify** in the desired policy's row. The Rename/Modify Policy dialog box appears.
- 3 Type a new name for the existing policy, then click **OK**.

Deleting a policy from the Policy Catalog

Use this task to delete a policy from the Policy Catalog. When you delete a policy, all groups and systems where it is currently applied inherit the policy of their parent group. Before deleting a policy, review the groups and systems where it is assigned. If you don't want the group or system to inherit the policy from the parent group, assign a different policy.

If you delete a policy that is applied to the My Organization group, the McAfee Default policy of this category is assigned.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.
- 2 Locate the desired policy, then click **Delete** in the policy's row.
- 3 Click **OK** when prompted.

Working with policies

Use these tasks to assign and manage the policies in your environment.

Tasks

- ▶ [Changing the owners of a policy](#)
- ▶ [Moving policies between ePO servers](#)
- ▶ [Assigning a policy to a group of the System Tree](#)
- ▶ [Assigning a policy to a managed system](#)
- ▶ [Assigning a policy to multiple managed systems within a group](#)
- ▶ [Enforcing policies for a product on a group](#)
- ▶ [Enforcing policies for a product on a system](#)
- ▶ [Copying and pasting assignments](#)

Changing the owners of a policy

Use this task to change the owners of a policy. By default, ownership is assigned to the user that created the policy. This task can only be performed by global administrators.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category**. All created policies for the selected category appear in the details pane.
- 2 Locate the desired policy, then click on the Owner of the policy. The Policy Ownership page appears.
- 3 Select the desired owners of the policy from the list, then click **OK**.

Moving policies between ePO servers

Use these tasks to move policies between servers. To do this, you must export the policy to an XML file from the Policy Catalog page of the source server, then import it to the Policy Catalog page on the target server.

Tasks

- ▶ [Exporting a single policy](#)
- ▶ [Exporting all policies of a product](#)
- ▶ [Importing policies](#)

Exporting a single policy

Use this task to export a policy to an XML file. Use this file to import the policy to another ePO server, or to keep as a backup of the policy.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.
- 2 Locate the desired policy, then click **Export** next to the policy. The Download File 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 ePO server, ensure that this location is accessible to the target ePolicy Orchestrator server.

Exporting all policies of a product

Use this task to export all policies of a product to an XML file. Use this file to import the policy to another ePO server, or to keep as a backup of the policies.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** . All created policies for the selected category appear in the details pane.
- 2 Click **Export** next to **Product policies**. The Download File 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 ePO server, ensure that this location is accessible to the target ePolicy Orchestrator server.

Importing policies

Use this task to import a policy XML file. Regardless of whether you exported a single policy or all named policies, the import procedure is the same.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Policy Catalog**, then click **Import** next to **Product policies**.
- 2 Browse to and select the desired policy XML file, then click **OK**.
- 3 Select the policies you want to import and click **OK**. The policies are added to the policy catalog.

Assigning a policy to a group of the System Tree

Use this task to assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select the desired **Product**. Each assigned policy per category appears in the details pane.
- 2 Locate the desired policy category, then click **Edit Assignment**. The Policy Assignment page appears.
- 3 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from**.
- 4 Select the desired policy from the **Assigned policy** drop-down list.

NOTE: From this location, you can also edit the selected policy's settings, or create a new policy.

- 5 Choose whether to lock policy inheritance. Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.
- 6 Click **Save**.

Assigning a policy to a managed system

Use this task to assign a policy to a specific managed system. You can assign policies before or after a product is deployed.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the desired group under System Tree. All the systems within this group (but not its subgroups) appear in the details pane.
- 2 Select the desired system, then click **Actions | Agent | Modify Policies on a Single System**. The Policy Assignment page for that system appears.
- 3 Select the desired **Product**. The categories of selected product are listed with the system's assigned policy.
- 4 Locate the desired policy category, then click **Edit Assignments**.
- 5 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from**.
- 6 Select the desired policy from the **Assigned policy** drop-down list.
NOTE: From this location, you can also edit settings of the selected policy, or create a new policy.
- 7 Choose whether to lock policy inheritance. Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.
- 8 Click **Save**.

Assigning a policy to multiple managed systems within a group

Use this task to assign a policy to multiple managed systems within a group. You can assign policies before or after a product is deployed.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the desired group in the System Tree. All the systems within this group (but not its subgroups) appear in the details pane.
- 2 Select the desired systems, then click **Actions | Agent | Set Policy & Inheritance**. The Assign Policies page appears.
- 3 Select the **Product, Category, and Policy** from the drop-down lists, then click **Save**.

Enforcing policies for a product on a group

Use this task to enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select the desired group in the System Tree.
- 2 Select the desired **Product**, then click the link next to **Enforcement Status**. The Enforcement page appears.

- 3 To change the enforcement status you must first select **Break inheritance and assign the policy and settings below**.
- 4 Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.
- 5 Choose whether to lock policy inheritance. Locking inheritance for policy enforcement prevents breaking enforcement for groups and systems that inherit this policy.
- 6 Click **Save**.

Enforcing policies for a product on a system

Use this task to enable or disable policy enforcement for a product on a system. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the group under **System Tree** where the system belongs. The list of systems belonging to this group appears in the details pane.
- 2 Select the desired system, then click **Actions | Modify Policies on a Single System**. The Policy Assignment page appears.
- 3 Select the desired **Product**, then click **Enforcing** next to **Enforcement status**. The Enforcement page appears.
- 4 If you want to change the enforcement status you must first select **Break inheritance and assign the policy and settings below**.
- 5 Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.
- 6 Click **Save**.

Copying and pasting assignments

Use these tasks to copy and paste policy assignments from one group or system to another. This is an easy way to share multiple assignments between groups and systems from different portions of the System Tree.

Tasks

- ▶ [Copying policy assignments from a group](#)
- ▶ [Copying policy assignments from a system](#)
- ▶ [Pasting policy assignments to a group](#)
- ▶ [Pasting policy assignments to a specific system](#)

Copying policy assignments from a group

Use this task to copy policy assignments from a group in the System Tree.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select the desired group in the System Tree.

- 2 Click **Actions | Copy Assignments**.
- 3 Select the products or features for which you want to copy policy assignments, then click **OK**.

Copying policy assignments from a system

Use this task to copy policy assignments from a specific system.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the desired group in the System Tree. The systems belonging to the selected group appear in the details pane.
- 2 Select the desired system, then click **Actions | Agent | Modify Policies on a Single System**.
- 3 Click **Actions | Copy Assignments**, select the desired products or features for which you want to copy policy assignments, then click **OK**.

Pasting policy assignments to a group

Use this task to paste policy assignments to a group. You must have already copied policy assignments from a group or system.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Assigned Policies**, then select the desired group in the System Tree.
- 2 In the details pane, click **Actions** and select **Paste Assignments**. If the group already has policies assigned for some categories, the Override Policy Assignments page appears.
NOTE: When pasting policy assignments, an extra policy appears in the list (Enforce Policies and Tasks). This policy controls the enforcement status of other policies.
- 3 Select the policy categories you want to replace with the copied policies, then click **OK**.

Pasting policy assignments to a specific system

Use this task to paste policy assignments to a specific system. You must have already copied policy assignments from a group or system.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the desired group in the System Tree. All of the systems belonging to the selected group appear in the details pane.
- 2 Select the system where you want to paste policy assignments, then click **Actions | Agent | Modify Policies on a Single System**.

- 3 In the details pane, click **Actions | Paste Assignment**. If the system already has policies assigned for some categories, the Override Policy Assignments page appears.

NOTE: When pasting policy assignments, an extra policy appears in the list (Enforce Policies and Tasks). This policy controls the enforcement status of other policies.

- 4 Confirm the replacement of assignments.

Working with client tasks

Use these tasks to create and maintain client tasks.

Tasks

- ▶ [Creating and scheduling client tasks](#)
- ▶ [Editing client tasks](#)
- ▶ [Deleting client tasks](#)

Creating and scheduling client tasks

Use this task to create and schedule a client task. The process is similar for all client tasks.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Client Tasks**, select the desired group in the System Tree, then click **Actions | New Task**. The Client Task Builder wizard opens.
- 2 Type a name for the task you are creating, add any notes, then select the product task type from the drop-down lists, for example, **Product Update**.
- 3 Specify any tags to use with this task and click **Next**.
- 4 Configure the settings, then click **Next**. The Schedule page appears.
- 5 Configure the schedule details as needed, then click **Next**.
- 6 Review the task settings, then click **Save**. The task is added to the list of client tasks for the selected group and any group that inherits the task.

Editing client tasks

Use this task to edit a client task's settings or to schedule information for any existing task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Client Tasks**, then select the group where the desired client task was in the System Tree.
- 2 Click **Edit Settings** next to the task. The Client Task Builder wizard opens.
- 3 Edit the task settings as needed, then click **Save**.

The managed systems receive these changes the next time the agents communicate with the server.

Deleting client tasks

Use this task to delete unneeded client tasks. You can delete any client task you have created.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Client Tasks**, then select the group where the desired client task was created in the System Tree.
- 2 Click **Delete** next to the desired client task.
- 3 Click **OK**.

Frequently asked questions

What is a policy?

A policy is a customized subset of product settings that correspond to a policy category. You can create, modify, or delete as many named policies as needed for each policy category.

What are the McAfee Default and My Default policies?

Upon installation, each policy category contains at least two policies. These are named McAfee Default and My Default. These are the only policies present for first-time installations. The configurations for both, initially, are the same.

The McAfee Default named policies cannot be edited, renamed, or deleted. The My Default policies can be edited, renamed, and deleted.

What happens to the child groups and systems of the group where I assigned a new policy?

All child groups and systems that are set to inherit the specific policy category, inherit the policy applied to a parent group.

How are the groups and systems where a policy is applied affected when the policy is modified in the Policy Catalog?

All groups and systems where a policy is applied receive any modification made to the policy at the next agent-server communication. The policy is then enforced at each policy enforcement interval.

I assigned a new policy, but it's not being enforced on the managed systems. Why?

New policy assignments are not enforced until the next agent-server communication.

I pasted policy assignments from one group or system (source) to another (target), but the policies assigned to the target location are not the same as the source location. Why not?

When you copy and paste policy assignments, only true assignments are pasted. If the source location was inheriting a policy that you selected to copy, it is the inheritance characteristic that was pasted to the target, so the target then inherits the policy (for that particular policy category)

from its parent, which might be a different policy than the one that was inherited onto the source.

Sharing policies among ePO servers

Policy sharing allows the administrator to designate policies that are developed on one server to be transmitted to other servers for implementation. In earlier versions of ePolicy Orchestrator, sharing was possible only by exporting a policy from the source server and importing it to the target servers one at a time.

The process has been simplified and automated. Now the administrator needs only to:

- 1 Designate the policy for sharing.
- 2 Register the servers that will share the policy.
- 3 Schedule a server task to distribute the shared policy.

Setting up policy sharing for multiple ePO servers

Use these tasks to configure policy sharing for use with multiple ePO servers. McAfee recommends completing these tasks in the sequence listed here.

NOTE: 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

- ▶ [Designating policies for sharing](#)
- ▶ [Registering servers for policy sharing](#)
- ▶ [Scheduling server tasks to share policies](#)

Designating policies for sharing

Use this task to designate a policy to be shared among multiple ePO servers.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then click **Product** menu and select the product whose policy you want to share.
- 2 In the **Actions** column for the policy to be shared, click **Share**.

Registering servers for policy sharing

Use this task to register the servers that will share a policy.

Before you begin

McAfee recommends that you set up policy sharing in a specific sequence. If you have not already designated the policies you want to share, see *Designating a policy for sharing* before completing this task.

Task

For option definitions, click ? in the interface.

- 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 4.5**, 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**.

Scheduling server tasks to share policies

Use this task to schedule a server task so that policies are shared among multiple ePO servers.

Before you begin

McAfee recommends that you set up policy sharing in a specific sequence. Before completing this task, be sure that you have completed these tasks:

- 1 *Designating policies for sharing*
- 2 *Registering servers for policy sharing*

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder wizard opens.
- 2 On the Description page, specify the name of the task and any notes, then click **Next**. The Actions page appears.
NOTE: New server tasks are enabled by default. If you do not want this task to be enabled, select **Disabled** in the **Schedule status** field.
- 3 From the Actions drop-down menu, select **Share Policies**, then click **Next**. The Schedule page appears.
- 4 Specify the schedule for this task, then click **Next**. The Summary page opens.
- 5 Review the summary details, then click **Save**.

How policy assignment rules work

Policy assignment rules give you the ability to create user-specific policy assignments. These assignments are enforced at the target system when a user logs on. On a managed system, the agent keeps a record of the users who log on to the network. The policy assignments you create for each user are pushed down to the system they log on to, and are cached during each agent-server communication. The agent applies the policies that you have assigned to each user.

NOTE: When a user logs on to a managed system for the first time, there can be a slight delay while the agent contacts its assigned server for the policy assignments specific to this user. During this time, the user has access only to that functionality allowed by the default machine policy, which typically is your most secure policy.

Policy assignment rules reduce the overhead of managing numerous policies for individual users, while maintaining more generic policies across your System Tree. 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. This level of granularity in policy assignment limits the instances of broken inheritance in the System Tree needed to accommodate the policy settings that particular users require to perform special functions.

Policy assignment rule priority

Policy assignment rules can be prioritized to simplify maintenance of policy assignment management. When you set priority to a rule, it is enforced before other assignments with a lower priority. In some cases, the outcome can be that some rule settings are overridden.

For example, consider a user who is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included users unrestricted access to internet content. Rule B has priority level 2, and heavily restricts the same user's access to internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the user has unrestricted access to internet content.

How multi-slot policies work with policy assignment rule priority

Priority of rules is not considered for multi-slot policies. When a single rule containing multi-slot policies of the same product category is applied to a user, all settings of the multi-slot policies are combined. Similarly, if multiple rules applied to a user contain multi-slot policy settings, all settings from each multi-slot policy are combined. As a result, the user gets a policy that combines the settings of each individual rule.

For example, consider the previous example where a user is included in two policy assignment rules with different assigned priorities. When these rules consist of multi-slot policy assignments, the settings for both policies are applied without regard to priority. You can prevent application of combined settings from multi-slot policies across multiple policy assignment rules by excluding a user (or other Active Directory objects such as a group or organizational unit) when creating the policy assignment rule. For more information on using multi-slot policies with policy assignment rules, refer to the product documentation for the managed product you are using.

Working with policy assignment rules

Use these tasks to configure and manage policy assignment rules. With these tasks you can set up, create, and manage policy assignment rules in your network.

Tasks

- ▶ [Creating policy assignment rules](#)
- ▶ [Managing policy assignment rules](#)

Creating policy assignment rules

Use this task to create policy assignment rules. Policy assignment rules allow you to enforce permissions and criteria based policies for individual users accessing your network.

Before you begin

To complete this task you must:

- Have a registered LDAP server. For more information, see *Registering LDAP servers*.
- Set up Windows Authorization for your registered LDAP server. For more information, see *Configuring Windows Authorization*.

to assign policy assignment rules

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Policy Assignment Rules**, then click **Actions | New Assignment Rule**. The Policy Assignment Builder wizard opens to the Details page.
- 2 Specify a unique **Name** and **Description** for this policy assignment rule, then click **Next**. The Selection Criteria page opens.

NOTE: By default, the priority for new policy assignment rules is assigned sequentially based on the number of existing rules. You can edit the priority of this and any rule by clicking **Edit Priority** on the Policy Assignment Rules page.

- 3 Specify the System property details for this rule. You can apply additional Available Properties to this policy assignment rule. The available properties include:
 - **Group Membership** — Specifies the group to which a user is assigned.
 - **Organizational Unit** — Specifies the Organizational Unit (OU) to which a user belongs.
 - **User** — Specifies a unique user name to which this policy will be assigned.
- 4 Click **Next**. The Assigned Policies page opens. Click **Add** to select the policies that you want to be enforced by this policy assignment rule. You can also **Edit** or **Remove** assigned policies from this page.
- 5 Review the summary and click **Save**.

Managing policy assignment rules

Use this table to perform common management tasks when working with policy assignment rules. To perform these actions, click **Menu | Policy | Policy Assignment Rules**. Select the action to perform from the **Actions** menu or the **Actions** column.

To do this...	Do this...
Delete a policy assignment rule	Click Delete in the selected assignment row.
Edit a policy assignment rule	Click Edit Settings for 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	Click Export . The Download Policy Assignment Rules page opens, where you can view or download the PolicyAssignmentRules.xml file.
Import policy assignment rules	Click Import . The Import Policy Assignment Rules dialog box opens, from which you can browse to a previously downloaded PolicyAssignmentRules.xml file. You are prompted to choose which rules included in the file to import. You can select which rules to import and, if any rules in the file have the same name as those already in your Policy Assignment Rules list, you can select which to retain.
Edit the priority of a policy assignment rule	Click Edit Priority . The Policy Assignment Rule Edit Priority page opens, where you change the priority of policy assignment rules using the drag-and-drop handle.

To do this...	Do this...
View the summary of a policy assignment rule	Click > in the selected assignment row.

Deploying Software and Updates

In addition to managing security products, ePolicy Orchestrator can deploy products to your network systems. Use ePolicy Orchestrator to deploy products and their updates.

Are you deploying products for the first time?

When deploying products for the first time:

- 1 Configure pull and replication tasks.
- 2 Check in product and update packages to the master repository.
- 3 Configure deployment and update tasks.

Contents

- ▶ [Deployment packages for products and updates](#)
- ▶ [Product and update deployment](#)
- ▶ [Checking in packages manually](#)
- ▶ [Using the Product Deployment task to deploy products to managed systems](#)
- ▶ [Deploying update packages automatically with global updating](#)
- ▶ [Deploying update packages with pull and replication tasks](#)
- ▶ [Configuring agent policies to use a distributed repository](#)
- ▶ [Using local distributed repositories that are not managed](#)
- ▶ [Checking in engine, DAT and ExtraDAT update packages manually](#)
- ▶ [Updating managed systems regularly with a scheduled update task](#)
- ▶ [Confirming that clients are using the latest DAT files](#)
- ▶ [Evaluating new DATs and engines before distribution](#)
- ▶ [Manually moving DAT and engine packages between branches](#)
- ▶ [Deleting DAT or engine packages from the master repository](#)

Deployment packages for products and updates

The ePolicy Orchestrator deployment infrastructure supports deploying products and components, as well as updating both.

Each McAfee product that ePolicy Orchestrator can deploy provides a product deployment package zip file. The zip file contains product installation files, which are compressed in a secure format. ePolicy Orchestrator can deploy these packages to any of your managed systems, once they are checked in to the master repository.

These zip files are used for both detection definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. McAfee recommends configuring policy settings before deploying the product to network systems. This saves time and ensures that your systems are protected as soon as possible.

These package types can be checked in to the master repository with pull tasks, or manually.

Supported package types

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, McAfee recommends 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 ePolicy Orchestrator. 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 the installation software of a McAfee product.	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.
Agent language packages File type: zip	An agent language package contains files necessary to display agent information in a local language.	Master repository — Checked in at installation. For future versions of the agent, you must check 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 ePolicy Orchestrator when they are checked in.

Digital signatures guarantee that packages originated from McAfee or were checked in by you, and that they have not been tampered with or corrupted. The agent only trusts package files signed by ePolicy Orchestrator or McAfee. This protects your network from receiving packages from unsigned or untrusted sources.

Package ordering and dependencies

If one product update is dependent on another, you must check in the update packages to the master repository in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them in again, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.

Product and update deployment

The ePO repository infrastructure allows you to deploy product and update packages to your managed systems from a central location. Although the same repositories are used, there are differences.

Comparison of product deployment and update packages

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 distributed repositories and installed automatically on managed systems using a deployment task.	Can be replicated to the distributed repositories 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:
 - Using global updating — Nothing else is required for systems on the network. You should, however, create and schedule an update task for laptop systems that leave the network.
 - Not using global updating — Use a replication task to copy the contents of the master repository to the distributed repositories, then create and schedule an update task for agents to retrieve and install the update on managed systems.

Deployment tasks

Once you have checked in the product deployment package, use the Product Deployment client task to install the product on managed systems. The task installs any product that is deployable through ePolicy Orchestrator and has been checked in to the master repository.

Best practices

You can run the Product Deployment task for any group or individual system. When deciding how to stage your product deployment, McAfee recommends considering the size of the package and the available bandwidth between the master or distributed repositories and the managed systems. In addition to potentially overwhelming the ePO server or your network, deploying products to many systems can make troubleshooting problems more complicated.

Consider a phased rollout to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred clients at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

If you are deploying McAfee products or components that are installed on a subset of your managed systems:

- 1 Use a tag to identify these systems.
- 2 Move the tagged systems to a group.
- 3 Configure a Product Deployment client task for the group.

Update tasks

Once an update package has been checked in to the master repository and replicated to the distributed repositories, the agents on the managed systems still need to know when to go to the distributed repositories for updates. If you are using global updating, this is not necessary.

You can create and configure update client tasks to control when and how managed systems receive update packages. If you are not using global updating, creating these tasks are the only way you can control client updating with ePolicy Orchestrator.

If you are using global updating, this task is not necessary, although you can create a daily task for redundancy.

Considerations when creating update client tasks

Consider the following when scheduling client update tasks:

- Create a daily Update client task that the highest level of the System Tree that is inherited by all systems. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact. Also, for large networks with offices in different time zones, help balance network load by running the task at the local system time on the managed system, rather than at the same time for all systems.
- Schedule the task at least an hour after the scheduled replication task, if you are using scheduled replication tasks.
- Run update tasks for DAT and engine files at least once a day. Managed systems might be logged off from the network and miss the scheduled task. Running the task frequently ensures these systems receive the update.
- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one task to update only DAT files, then create another to update both DAT and engine files weekly or monthly (engine packages are released less frequently).
- Create and schedule additional tasks to update products that do not use the agent for Windows.
- Create a task to update your main workstation applications, such as VirusScan Enterprise, to ensure they all receive the update files. Schedule it to run daily or several times a day.

Global updating

McAfee recommends using global updating as part of your updating strategy. Global updating automates replication to your distributed repositories and keeping your managed systems up-to-date. Replication and update tasks are not required. Checking contents in to your master repository initiates a global update. The entire process should finish within an hour in most environments.

Additionally, you can specify which packages and updates initiate a global update. However, when you only specify that certain content initiates a global update, ensure that you create a replication task to distribute content that was not selected to initiate a global update.

NOTE: When using global updating, McAfee recommends scheduling a regular pull task (to update the master repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update.

Global updating process

Most environments can be updated within an hour using this Global updating process:

- 1 Contents are checked in to the master repository.
- 2 The server performs an incremental replication to all distributed repositories.
- 3 The server issues a SuperAgent wake-up call to all SuperAgents in the environment.
- 4 The SuperAgent broadcasts a global update message to all agents within the SuperAgent subnet.
- 5 Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed for updating.
- 6 The agent searches the distributed repositories for a site that has this minimum catalog version.
- 7 Once a suitable repository is found, the agent runs the update task.

If the agent does not receive the broadcast for any reason, such as when the client computer is turned off, or there are no SuperAgents, at the next ASCI, the minimum catalog version is supplied, which starts the process.

NOTE: If the agent receives notification from a SuperAgent, the agent is supplied with the list of updated packages. If the agent finds the new catalog version at the next ASCI, it is not supplied with the list of packages to update, and therefore updates all packages available.

Requirements

These requirements must be met to implement global updating:

- A SuperAgent must use the same agent-server secure communication (ASSC) key as the agents that receive its wake-up call.
- A SuperAgent is installed on each broadcast segment. Managed systems cannot receive a SuperAgent wake-up call if there is no SuperAgent on the same broadcast segment. Global updating uses the SuperAgent wake-up call to alert agents that new updates are available.
- Distributed repositories are set up and configured throughout your environment. McAfee recommends SuperAgent repositories, but they are not required. Global updating functions with all types of distributed repositories.
- If using SuperAgent repositories, managed systems must be able to "see" the repository from which it updates. Although a SuperAgent is required on each broadcast segment for systems to receive the wake-up call, SuperAgent repositories are not required on each broadcast segment. The managed systems, however, must "see" the SuperAgent repository from which to update.

Pull tasks

Use pull tasks to update your master repository with DAT and engine update packages from the source site. DAT and engine files must be updated often. McAfee releases new DAT files

daily, and engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.

With this release, you can specify which packages are copied from the source site to the master repository.

NOTE: 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.

NOTE: 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.

TIP: 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 ePolicy Orchestrator.

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 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.

NOTE: 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.

Server task log

The server task log provides information about your pull and replication tasks, in addition to all server tasks. This provides the status of the task and any errors that might have occurred.

Replication task information in the server task log

Click **Menu | Automation | Server Task Log** to access the following information for replication tasks:

- Start date and task duration
- Status of task at each site (when expanded)
- Any errors or warnings, their codes, and the site to which they apply

Pull task information in the server task log

Click **Menu | Automation | Server Task Log** to access the following information for pull tasks:

- Start date and task duration
- Any errors or warnings and their codes
- Status of each package that is checked in to the master repository
- Information regarding any new packages that are being checked in to the master repository

Checking in packages manually

Use this task to manually check in the deployment packages to the master repository so that ePolicy Orchestrator can deploy them.

Before you begin

You must have the appropriate permissions to perform this task.

NOTE: You cannot check in packages while pull or replication tasks are running.

Task

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

- 1 Click **Menu | Software | Master Repository**, then click **Actions | Check In Package**. The Check In Package wizard opens.
- 2 Select the package type, then browse to and select the desired package file.
- 3 Click **Next**. The Package Options page appears.
- 4 Confirm or configure the following:
 - **Package info** — Confirm this is the correct package.
 - **Branch** — Select the desired branch. If there are requirements in your environment to test new packages before deploying them throughout the production environment, McAfee recommends using the Evaluation branch whenever checking in packages. Once you finish testing the packages, you can move them to the Current branch by clicking **Menu | Software | Master Repository**.
 - **Options** — Select whether to:
 - **Move the existing package to the Previous branch** — When selected, moves packages in the master repository from the Current branch to the Previous branch when a newer package of the same type is checked in. Available only when you select Current in Branch.
 - **Add this package to the global update list** — Adds the package to the Distributed repository. A SuperAgent call also occurs, forcing the package to be installed on all the managed systems.
 - **Package signing** — Specifies if the package is signed by McAfee or is third-party package.
- 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 tab.

Using the Product Deployment task to deploy products to managed systems

Use these tasks to deploy products to managed systems with the Product Deployment client task. ePolicy Orchestrator 4.5 allows you to create this task for a single system, or for groups of the System Tree.

Tasks

- ▶ [Configuring the Deployment task for groups of managed systems](#)
- ▶ [Configuring the Deployment task to install products on a managed system](#)

Configuring the Deployment task for groups of managed systems

Use this task to configure the Product Deployment task to deploy products to groups of managed systems in the System Tree.

Task

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

- 1 Click **Menu | Systems | System Tree | Client Tasks**, then select a group in the System Tree.
- 2 Click **Actions | New Task**. The Client Task Builder wizard opens.
- 3 Type the name of the task and add any descriptive information to the **Notes** field.
The information you add here is visible only when you open the task at this group, or at a child group that inherits the task from this group.
- 4 Select **Product Deployment (McAfee Agent)** from the **Type** drop-down menu.
- 5 Next to **Tags**, select the desired platforms to which you are deploying the packages:
 - **Send this task to all computers.**
 - **Send this task to only computers that have the following criteria** — Use one of the **edit** links to configure the criteria.
- 6 Click **Next**. The Configuration page appears.
- 7 Next to **Target platforms**, select the type(s) of platform to use the deployment.
- 8 Next to **Products and components**, set the following:
 - Select the desired product from the first drop-down menu. The products listed are those for which you have already checked in a package to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product's package.
 - Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
 - To specify command-line installation options, type the desired command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

NOTE: You can click **+** or **-** to add or remove products and components from the displayed list.

- 9 Next to **Options**, select if you want to run this task for every policy enforcement process (Windows only).
- 10 Click **Next**. The Schedule page appears.
- 11 Schedule the task as needed, then click **Next**. The Summary page appears.
- 12 Review and verify the details of the Product Deployment task, then click **Save**.

Configuring the Deployment task to install products on a managed system

Use this task to deploy products to a single system using the Product Deployment task. Create a Product Deployment client task for a single system when that system requires:

- A product installed that other systems within the same group do not require.
- A different schedule than other systems in the group. For example, if a system is located in a different time zone than its peers.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Systems**, then select the group in the System Tree that contains the desired system.
- 2 Select the checkbox next to the desired system.
- 3 Click **Actions | Agent | Modify Tasks on a Single System**. A list of client tasks assigned to this system appears.
- 4 Click **Actions | New Task**. The Client Task Builder wizard opens.
- 5 Type the name of the task and add any descriptive information to the **Notes** field.
The information you add here is visible only when you open the task at this group. or at a child group that inherits the task from this group.
- 6 Select **Product Deployment** from the **Type** drop-down menu.
- 7 Next to **Tags**, select the desired platforms to which you are deploying the packages:
 - **Send this task to all computers.**
 - **Send this task to only computers that have the following criteria** — Use one of the **edit** links to configure the criteria.
- 8 Click **Next**. The Configuration page appears.
- 9 Next to **Target platforms**, select the type(s) of platform to use the deployment.
- 10 Next to **Products and components** set the following:
 - Select the desired product from the first drop-down list. The products listed are those for which you have already checked in a package to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product's package.
 - Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.

- To specify command-line installation options, type the desired command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

NOTE: You can click **+** or **-** to add or remove products and components from the list displayed.

- 11** Next to **Options**, select if you want to run this task for every policy enforcement process (Windows only).
- 12** Click **Next**. The Schedule page appears.
- 13** Schedule the task as needed, then click **Next**. The Summary page appears.
- 14** Review and verify the details of the Product Deployment task, then click **Save**.

Deploying update packages automatically with global updating

Use this task to enable global updating on the server. Global updating automatically deploys user-specified update packages to managed systems.

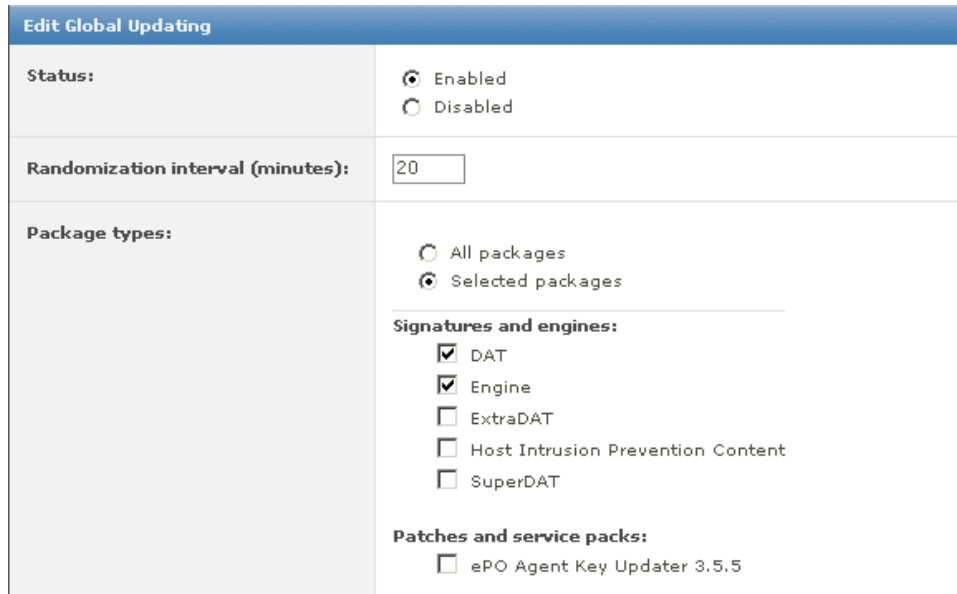
Before you begin

- Repositories must be created and available to all agents that receive the SuperAgent wake-up call.
- There must be a SuperAgent in each broadcast segment that you want to receive the SuperAgent wake-up call.
- Only global administrators can perform this task.

Task

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

- 1 Click **Menu | Configuration | Server Settings**, select **Global Updating**, then click **Edit** at the bottom of the page.



Edit Global Updating	
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Randomization interval (minutes):	<input type="text" value="20"/>
Package types:	<input type="radio"/> All packages <input checked="" type="radio"/> Selected packages
Signatures and engines:	
<input checked="" type="checkbox"/> DAT	
<input checked="" type="checkbox"/> Engine	
<input type="checkbox"/> ExtraDAT	
<input type="checkbox"/> Host Intrusion Prevention Content	
<input type="checkbox"/> SuperDAT	
Patches and service packs:	
<input type="checkbox"/> ePO Agent Key Updater 3.5.5	

Figure 9: Edit Global Updating page

- 2 On the Edit Global Updating page next to **Status**, select **Enabled**.
- 3 Edit the **Randomization interval**, if desired. The default is **20 minutes**.

Each client update occurs at a randomly selected time within the randomization interval, which helps distribute network load. 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 **Packages 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.

NOTE: 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.

NOTE: 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.

Deploying update packages with pull and replication tasks

Use these tasks to implement a task-based updating strategy once you have created your repository infrastructure. You must rely on these tasks if you are not using global updating in your environment.

Before you begin

Make sure that repositories are created and in locations available to managed systems.

Tasks

- ▶ [Using pull tasks to update the master repository](#)
- ▶ [Replicating packages from the master repository to distributed repositories](#)

Using pull tasks to update the master repository

Use either of these tasks to update the contents of the master repository from the McAfee update site or from a user-configured source site.

You can schedule pull tasks or run them immediately.

Before you begin

Ensure that proxy settings are configured so that the master repository can access the source site.

Tasks

- ▶ [Running a pull task on a schedule](#)
- ▶ [Running a Pull Now task](#)

Running a pull task on a schedule

Use this task to schedule a recurring pull task that updates the master repository from the source site. Pull tasks now provide the ability to select which packages are copied from the source site.

Before you begin

You must have the appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Software | Master Repository**, then click **Actions | Schedule Pull**. The Server Task Builder wizard opens.
- 2 On the Description page, name and describe the task.
- 3 Choose whether to enable or disable the task, then click **Next**. The Actions page appears.
Disabled tasks can be run manually, but do not run at scheduled times.
- 4 From the **Actions** menu, select **Repository Pull**.

- 5 Select the source site from which to pull contents into the master repository.
- 6 Select one of the following branches to receive the packages:
 - **Current** — Use the packages without testing them first.
 - **Evaluation** — Used to test the packages in a lab environment first.
 - **Previous** — Use the previous version to receive the package.
- 7 Select **Move existing packages of the same type to the Previous branch** to move the current package versions saved in the Current branch to the Previous branch.
- 8 Select whether to pull:
 - **All packages.**
 - **Selected packages** — If you select this option, you must click **Select Packages** and choose the packages to pull from the source site when this task runs.

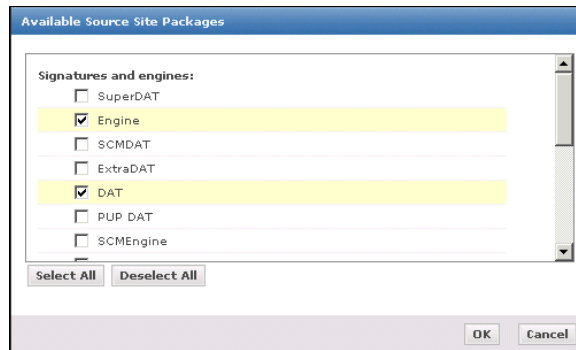


Figure 10: Available Source Site Packages dialog box

- 9 Click **Next**. The Schedule page of the wizard appears.
- 10 Schedule the task as needed, then click **Next**. The Summary page appears.

NOTE: The Schedule page provides more flexibility than the scheduling functionality of previous versions. In addition to more granular scheduling in all of the schedule types, you can use cron syntax by selecting the **Advanced** schedule type.
- 11 Review the summary information, then click **Save**.

The scheduled Repository Pull task is added to the task list on the Server Tasks page.

Running a Pull Now task

Use this task to initiate a pull task that updates the master repository from the source site immediately. With this release, you can select which packages in the source site are copied to the master repository.

Before you begin

- You must have the appropriate software permissions to perform this task.
- Proxy settings must be configured to allow the master repository to access the source site.

Task

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

- 1 Click **Menu | Software | Master Repository**, then click **Actions | Pull Now**. The Pull Now wizard opens.

- 2 Select the source site from the list of available repositories.
- 3 Select one of the following branches to receive the packages:
 - **Current** — Use the packages without testing them first.
 - **Evaluation** — Used to test the packages in a lab environment first.
 - **Previous** — Use the previous version to receive the package.
- 4 Select **Move existing packages of the same type to the Previous branch** to move the current package versions saved in the Current branch to the Previous branch.
- 5 Click **Next**. The Package Selection page appears.
- 6 Select which packages to copy from the source site, then click **Next**. The Summary page appears.
- 7 Verify the task details, then click **Start Pull** to begin the pull task. The Server Task Log page appears, where you can monitor the status of the task until it finishes.

Replicating packages from the master repository to distributed repositories

Use one of these tasks to replicate contents of the master repository to distributed repositories. You can schedule a Repository Replication server task that occurs regularly, or run a Replicate Now task for immediate replication.

Tasks

- ▶ [Running a Repository Replication server task on a schedule](#)
- ▶ [Running a Replicate Now task](#)
- ▶ [Avoiding replication of selected packages](#)

Running a Repository Replication server task on a schedule

Use this task to create a scheduled Repository Replication server task.

Before you begin

- You must have appropriate permissions to perform this task.
- Your distributed repositories must be set up and added to this ePO server.

Task

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

- 1 Click **Menu | Software | Distributed Repositories**, then click **Actions | Schedule Replication**. The Server Task Builder wizard opens.
- 2 On the Description page, name and describe the task.
- 3 Choose whether to enable or disable the task, then click **Next**. The Actions page appears.
Disabled tasks can be run manually, but do not run at scheduled times.

4 Select **Repository Replication** from the drop-down menu.

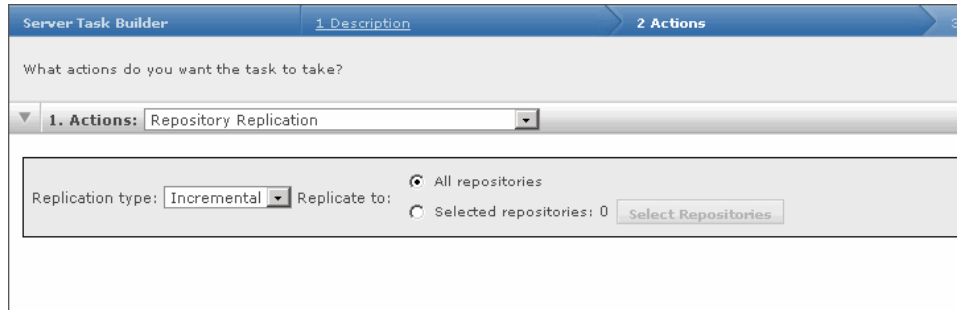


Figure 11: Repository Replicator server task action

5 From the **Replication type** drop-down menu, select one:

- **Incremental** Replicates only the differences between the master and distributed repositories.
- **Full** — Replicates all contents of the master repository to the distributed repositories.

6 Next to **Replicate to**, select **All repositories** or **Selected repositories**.

NOTE: If you select **Selected repositories**, you must click **Select Repositories** to choose which distributed repositories receive packages when this task is initiated.

7 Click **Next**. The Schedule page of the wizard appears.

8 Schedule the task as desired, then click **Next**. The Summary page appears.

NOTE: The Schedule page provides more flexibility than the scheduling functionality of previous versions. In addition to more granular scheduling in all of the schedule types, you can use cron syntax by selecting the **Advanced** schedule type.

9 Review the summary information, then click **Save**.

The scheduled Repository Pull task is added to the task list on the Server Tasks page.

Running a Replicate Now task

Use this task to replicate contents from the master repository to distributed repositories immediately.

Before you begin

- You must have appropriate permissions to perform this task.
- Any distributed repositories participating in the replication must be set up and added to ePolicy Orchestrator.

Task

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

- 1** Click **Menu | Software | Distributed Repositories**, then click **Actions | Replicate Now**. The Replicate Now wizard opens.
- 2** On the Repositories page, select which distributed repositories participate in the replication, then click **Next**.

If you are not sure which distributed repositories need to be updated, replicate to them all.

- 3 On the Replication Type, select **Incremental replication** or **Full replication**, then click **Next**.

NOTE: If this is the first time you are replicating to a distributed repository, it is a full replication even if you select incremental replication.

- 4 On the Summary page, review the details then click **Start Replication**. The Server Task Log page displays the status of the task until it is complete. Replication time depends on the changes to the master repository and the number of distributed repositories to which you are replicating.

After the task is complete, you can initiate an immediate client update task so that managed systems in other locations can get updates from the distributed repositories.

Avoiding replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default.

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

Before you begin

Disable any replication tasks scheduled to replicate the selected package. For more information, see *Disabling replication of selected packages*.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Distributed Repositories**, then select **Edit Settings** next to the desired repository. The Distributed Repository Builder wizard opens.
- 2 On the Package Types page, deselect the package that you want to avoid being replicated.
- 3 Click **Save**.

Configuring agent policies to use a distributed repository

Use this task to customize how agents select distributed repositories.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Policy | Policy Catalog**, then click **Product | McAfee Agent**.
- 2 Click **Edit Settings** of an 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.
NOTE: 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 up** or **Move down** to specify the order in which you want client systems to select distributed repositories.
 - 8 Click **Save** when finished.

Using local distributed repositories that are not managed

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

Task

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

- 1 Copy all files and subdirectories in the master repository folder from the server. By default, this is in the following location on your server:
C:\Program Files\McAfee\ePO\4.0.0\DB\Software
- 2 Paste the copied files and subfolders in your repository folder on the distributed repository system.
- 3 Configure an agent policy for managed systems to use the new unmanaged distributed repository:
 - a Click **Menu | Policy | Policy Catalog**, then click **Product | McAfee Agent**.
 - b Click **Edit Settings** of an existing agent policy, or create a new agent policy.
CAUTION: Policy inheritance cannot be broken for tabs of a policy. Therefore, when you apply this policy to systems, ensure that only the desired systems receive and inherit the policy to use the unmanaged distributed repository.
 - c On the Repositories tab, click **Add**. The Add Repository window appears.
 - d Type a name in the **Repository Name** text field. The name does not have to be the name of the system hosting the repository.
 - e Under **Retrieve Files From**, select the type of repository.
 - f Under **Configuration**, type the location you created using the 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 ePolicy Orchestrator. When a nonmanaged 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.

Checking in engine, DAT and ExtraDAT update packages manually

Use this task to manually check in the update packages to the master repository, to deploy them using ePolicy Orchestrator. Some packages can only be checked in manually.

Before you begin

You must have appropriate permissions to perform this task.

NOTE: You cannot check in packages while pull or replication tasks are running.

Task

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

- 1 Click **Menu | Software | Master Repository**, then click **Actions | Check In Package**. The Check In Package wizard opens.
- 2 Select the package type, then browse to and select the desired package file.
- 3 Click **Next**. The Package Options page appears.
- 4 Select a branch:
 - **Current** — Use the packages without testing them first.
 - **Evaluation** — Used to test the packages in a lab environment first.
NOTE: Once you finish testing the packages, you can move them to the Current branch by clicking **Menu | Software | Master Repository**.
 - **Previous** — Use the previous version to receive the package.
- 5 Next to **Options**, select whether to:
 - **Move the existing package to the Previous branch** — Select this option to move the existing package (of the same type that you are checking in) to the Previous branch.
- 6 Click **Save** to begin checking in the package. Wait while the package is checked in.

The new package appears in the Packages in Master Repository list on the Master Repository page.

Updating managed systems regularly with a scheduled update task

Use this task to create and configure update tasks. If you are not using global updating, McAfee recommends using a daily Update client task to ensure systems are up-to-date with the latest DAT and engine files.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree | Client Tasks**. Select the desired group in the System Tree where you want the task to apply, then click **Actions | New Task**. The Client Task Builder wizard opens.
- 2 On the Description page, type the name and describe the task.
- 3 Select **Product Update** from the **Type** drop-down list.
- 4 Next to **Tags**, select the desired platforms to which you are deploying the packages.:
 - **Send this task to all computers**
 - **Send this task to only computers that have the following criteria** — Use one of the **edit** links to configure the criteria.
- 5 Click **Next**. The **Configuration** page appears.
- 6 Next to the **Update in Progress Dialog Box** select if you want the users to be aware an update is in process and if you want to allow them to postpone the process.
- 7 Next to **Package types** select one of the following:
 - **All packages**.
 - **Selected packages** — If selected, you must configure which of the following to include:
 - **Signatures and engines**
NOTE: When configuring individual signatures and engines, if you select **Engine** and deselect **DAT** when the new engine is updated a new DAT is automatically updated to ensure complete protection.
 - **Patches and service packs**
 - **Others**
- 8 Click **Next**. The Schedule page appears.
- 9 Schedule the task as desired, then click **Next**. The Summary page appears.
- 10 Review the details of the task, 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.

Confirming that clients are using the latest DAT files

Use this task to check the version of DAT files on managed systems.

Task

For option definitions, click ? in the interface.

- Click **Menu | Reporting | Queries**, select **VSE: DAT Deployment** in the Queries list, then click **Actions | Run**.

NOTE: See the VirusScan Enterprise documentation for more information on this query.

Evaluating new DATs and engines before distribution

Use this task to test update packages using the Evaluation branch. You might want to test DAT and engine files on a few systems before deploying them to your entire organization.

ePolicy Orchestrator provides three repository branches for this purpose.

Task

For option definitions, click ? in the interface.

- 1** Create a scheduled Repository Pull task that copies update packages in the Evaluation branch of your master repository. Schedule it to run after McAfee releases updated DAT files. For additional information, see *Deploying update packages with pull and replication tasks*.
- 2** Create or select a group in the System Tree to serve as an evaluation group, and create a McAfee Agent policy for the systems to use only the Evaluation branch (in the **Repository Branch Update Selection** section of the **Updates** tab). For additional information, see *Configuring the Deployment task for groups of managed systems*.

The policies take affect the next time the agent calls in to the server. The next time the agent updates, it retrieves them from the Evaluation branch.

- 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. For additional information, see *Updating managed systems regularly with a scheduled update task*.

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. For additional information, see *Checking in packages manually*. 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.

Manually moving DAT and engine packages between branches

Use this task to move packages manually between the Evaluation, Current, and Previous branches after they are checked in to the master repository.

Task

For option definitions, click ? in the interface.

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

NOTE: If you have NetShield for NetWare in your network, select **Support NetShield for NetWare**.

- 5 Click **OK**.

Deleting DAT or engine packages from the master repository

Use this task to delete packages from the master repository. As you check in new update packages regularly, they replace the older versions or move them to the Previous branch, if you are using the Previous branch. However, you might want to manually delete DAT or engine packages from the master repository.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Software | Master Repository**. The Packages in Master Repository table appears.
- 2 In the row of the desired package, click **Delete**. The Delete Package dialog box appears.
- 3 Click **OK**.

Reporting On System Status

ePolicy Orchestrator 4.5 ships with its own querying and reporting capabilities. These are highly customizable, flexible and easy to use. Included is the **Query Builder** wizard, which creates and runs queries that result in user-configured data in user-configured charts and tables. In addition to the querying system, you can use the following logs to gather information about activities that occur on your ePO server and throughout your network:

- Audit log
- Server Task log
- Threat Event log

To get you started, McAfee includes a set of default queries that provide the same information as the default reports of previous versions.

Are you setting up queries for the first time?

When setting up queries for the first time:

- 1 Understand the functionality of queries and the **Query Builder** wizard.
- 2 Review the default queries, and edit any to your needs.
- 3 Create queries for any needs that aren't met by the default queries.

Contents

- ▶ [Queries](#)
- ▶ [Query Builder](#)
- ▶ [Working with queries](#)
- ▶ [Multi-server rollup querying](#)
- ▶ [The Audit Log](#)
- ▶ [The Server Task log](#)
- ▶ [The Threat Event Log](#)
- ▶ [Data exports from any table or chart](#)

Queries

Queries are configurable objects that retrieve and display data from the database. The results of queries are displayed in charts and tables. Any query's results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitors.

Query results are actionable

Query results are now actionable. Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. For example, you can deploy agents to systems in a table of query results. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV — Use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Transform the data for other purposes.
- HTML — View the exported results as a web page.
- PDF — Print the results.

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.

Public and personal queries

Queries can be personal (private) or public. Private queries exist in the user's **My Groups** list, and are available only to their creator. Public queries exist in the **Shared Groups** list, and are available to everyone who has permissions to use public queries.

By default, all of ePolicy Orchestrator default queries are public. However, not all users have permission to view queries automatically. Additionally, users must have permissions to view queries to be able to view all of the default dashboards, because some of the monitors on these dashboards are created by queries.

Only users with appropriate permissions can make their personal queries public ones.

NOTE: If migrating from ePolicy Orchestrator 4.5, any queries that were private in version 4.0 remain private in this version. These private queries are located in the **Migrated Queries** group inside the **My Groups** list. Public queries that are migrated are located in the **Shared Groups** list in the **Migrated Queries** group.

Query permissions

Use query permissions to assign specific levels of query functionality to permission sets, which are assigned to individual users.

To run most queries, you also need permissions to the feature sets associated with their result types. In a query's results pages, the available actions to take on the resulting items depend on the feature sets a user has permission to.

Available permissions include:

- **No permissions** — The Query tab is unavailable to a user with no permissions.
- **Use public queries** — Grants permission to use any queries that have been made public.
- **Use public queries; create and edit personal queries** — Grants permission to use any queries that have been made public, as well as the ability to use the Query Builder wizard to create and edit personal queries.
- **Edit public queries; create and edit personal queries; make personal queries public** — Grants permission to use and edit any public queries, create and edit any personal queries, as well as the ability to make any personal query available to anyone with access to public queries.

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 selection you make in the Query Builder wizard is a result type from a feature group. This selection identifies 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.

NOTE: Tables do not include drill-down tables.

Chart types include:

Chart Type Groups
Pie: <ul style="list-style-type: none">• Boolean Pie Chart• Pie Chart
Bar: <ul style="list-style-type: none">• Grouped Bar Chart• Single Group Bar Chart• Stacked Bar Chart
Summary: <ul style="list-style-type: none">• Multi-group Summary Table• Single Group Summary Table
Line: <ul style="list-style-type: none">• Multi-line Chart

Chart Type Groups
<ul style="list-style-type: none">• 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.

Working with queries

Use these tasks to create, use, and manage queries.

Tasks

- ▶ [Creating custom queries](#)
- ▶ [Running an existing query](#)
- ▶ [Running a query on a schedule](#)
- ▶ [Making existing personal queries public](#)
- ▶ [Duplicating queries](#)
- ▶ [Sharing a query between ePO servers](#)

Creating custom queries

Use this task to create custom queries with the Query Builder wizard. You can query on system properties, product properties, many of the log files, repositories, and more.

Task

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

- 1 Click **Menu | Reporting | Queries**, then click **Actions | New Query**. The Query Builder wizard opens.
- 2 On the Result Type page, select the **Feature Group** and **Result Type** for this query, then click **Next**. The Chart page appears.
NOTE: This choice determines the options available on subsequent pages of the wizard.
- 3 Select the type of chart or table to display the primary results of the query, then click **Next**. The Columns page appears.

NOTE: If you select Boolean Pie Chart, you must configure the criteria to include in the query.

- 4 Select the columns to be included in the query, then click **Next**. The Filter page appears.

NOTE: If you selected **Table** on the Chart page, the columns you select here are the columns of that table. Otherwise, these are the columns that make up the query details table.

- 5 Select properties to narrow the search results, then click **Run**. The Unsaved Query page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.

NOTE: Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property.

- If the query didn't appear to return the expected results, click **Edit Query** to go back to the Query Builder and edit the details of this query.
 - If you don't need to save the query, click **Close**.
 - If this is a query you want to use again, click **Save** and continue to the next step.
- 6 The Save Query page appears. Type a name for the query, add any notes, and select one of the following:
 - **New Group** — Type the new group name and select either:
 - **Private group (My Groups)**
 - **Public group (Shared Groups)**
 - **Existing Group** — Select the group from the list of **Shared Groups**.
 - 7 Click **Save**.

Running an existing query

Use this task to run an existing query from the Queries page.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**, then select a query from the Queries list.
- 2 Click **Actions | Run**. The query results appear. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.
- 3 Click **Close** when finished.

Running a query on a schedule

Use this task to create and schedule a server task that runs a table-based (list chart type) query and takes actions on the query results.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder wizard opens.
- 2 On the Description page, name and describe the task, then click **Next**. The Actions page appears.
- 3 From the **Actions** drop-down menu, select **Run Query**.

- 4 In the **Query** field, browse to the table-based query you want to run.
- 5 Select the language in which to display the results.
- 6 From the **Sub-Actions** list, select an action to take based on the results. Available actions depend on the permissions of the user, and include:
 - **Add to System Tree** — Specifies the systems selected from the query to be added to the System Tree.
 - **Apply Tag** — Applies a specified tag to all systems (that are not excluded from the tag) in the query results. This option is valid only for queries that result in a table of systems.
 - **Assign Policy** — Assigns a specified policy to all systems in the query results. This option is valid only for queries that result in a table of systems.
 - **Change Sorting Status** — Enables or disables System Tree sorting on all systems in the query results. This option is valid only for queries that result in a table of systems.
 - **Clear Agent GUID Sequence Error Count** — Clears the agent GUID sequence count found by the query.
 - **Clear Tag** — Removes a specified tag from all systems in the query results. This option is valid only for queries that result in a table of systems.
 - **Delete Sensor** — Specifies the sensor selected from the query to be deleted.
 - **Delete Systems** — Specifies the systems selected from the query to be deleted.
 - **Detected System Exceptions** — Specifies what to do with the system exceptions detected by the query.
 - **Email File** — Sends the results of the query to a specified recipient, in a user-configured format (PDF, XML, CSV, or HTML).
 - **Exclude Tag** — Excludes a specified tag from all systems in the query results. This option is valid only for queries that result in a table of systems.
 - **Export to File** — Exports the query results to a specified format. The exported file is placed in a location specified in the Printing and Exporting server settings.
 - **Generate Compliance Event** — Generates an event based on a percentage or actual number threshold of systems that do not match the criteria in the query. This action is intended for compliance-based Boolean pie chart queries that retrieve data on managed systems (for example, the McAfee Agent and VirusScan Enterprise Compliance Summary default queries).
 - **Install Rogue Sensor** — Specifies when to install a Rogue System Sensor when the query detects the system.
 - **Move Agent GUID to Duplicate List** — Moves an agent GUID to the duplicate list when it is discovered by the query.
 - **Move System to Another Group** — Moves all systems in the query results to a group in the System Tree. This option is valid only for queries that result in a table of systems.
 - **Push Agents for Windows** — Uses push technology to move agents for Windows that are detected by the query.
 - **Remove Rogue Sensor** — Removes the Rogue System Sensor detected by the query.
 - **Repository Replication** — Replicates master repository contents to the distributed repositories in the query results. This is valuable for queries that return a list of out-of-date repositories (for example, the Distributed Repository Status default query). This option is valid only for queries that result in a table of distributed repositories.
 - **Resort Systems** — Resorts the systems found by the query.

- **Sensor Blacklist Management** — Allows editing of the sensor blacklist systems detected by the query.
- **Set System Description** — Allows adding a description and four custom fields.
- **Transfer Systems** — Allows moving systems detected by the query within the System Tree.
- **Update Agents** — Distributes and updates agents detected by the query.
- **Wake Up Agents** — Sends a wake-up call to specified systems.

NOTE: 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 ensure you place the actions in the order you want them to be taken on the query results.

- 7 Click **Next**. The Schedule page appears.
- 8 Schedule the task as desired, then click **Next**. The Summary page appears.
- 9 Verify the configuration of the task, then click **Save**.

The task is added to the list on the Server Tasks page. If the task is enabled (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.

Making a personal query group

Use this task to make personal query groups that allow you to save personal queries that you create.

NOTE: You can also create personal query groups during the process to save a custom query. See *Creating custom queries*.

Before you begin

You must have appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Reporting | Queries**, then click **Group Actions | New Group**. The New Group page appears.
- 2 Type a group name.
- 3 From **Group Visibility**, select one of the following:
 - **Private group** — Adds the new group under My Groups.
 - **Public group** — Adds the new group under Shared Groups.
 - **By permission** — Adds the new group under Shared Groups. Users with the following default permissions can view the results:
 - **Executive Reviewer** — Only users designated as an Executive Reviewer can view the results.
 - **Global Reviewer** — Only users designated as a Global Reviewer can view the results.
 - **Group Admin** — Only users designated as a Group Admin can view the results.

- **Group Reviewer** — Only users designated as a Group Reviewer can view the results.

NOTE: Global Administrators have full access to all **By permission** queries.

TIP: You can also specify any custom user permission sets in your environment.

- 4 Click **Save**.

Making existing personal queries public

Use this task to make personal queries public. All users with permissions to public queries have access to any personal queries you make public.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**. In the **Queries** list, select the query you want to make public and click **Actions** and select either:
 - **Move to Different Group** — Select the desired shared group from the **Select target group** menu.
 - **Duplicate** — Specify a new name and select the desired share group from the **Group to receive copy** menu.

NOTE: The public group must be created before performing this task.

- 2 Click **OK**.

Duplicating queries

Use this task to create a query based on an existing query.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**. From the list, select a query to duplicate and click **Actions | Duplicate**. The Duplicate dialog box appears.
- 2 Type a name for the duplicate and select a group to receive a copy of the query, then click **OK**.

Sharing a query between ePO servers

Use these tasks to import and export a query for use among multiple servers.

Tasks

- ▶ [Exporting queries for use by another ePO server](#)
- ▶ [Importing queries](#)

Exporting queries for use by another ePO server

Use this task to export a query to an XML file, which can be imported to another ePO server.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**, then select a query from the Queries list.
- 2 Click **Actions | Export Query Definition**. The File Download dialog box appears.
- 3 Click **Save File**, select the desired location for the XML file, then click **OK**.

Importing queries

Use this task to import a query that was exported from another ePO server.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**, then click **Actions | Import Query**. The Import Query wizard opens.
- 2 Next to **File to Import**, browse to the XML file to import.
- 3 Select the group where you want the imported file saved, then click **Save**. The summary of the import process is displayed.
- 4 Click **OK**.

The query is added to the group you selected from the list.

Exporting query results to other formats

Use this task to export query results for other purposes. You can export to HTML and PDF files for viewing formats, or to CSV or XML files for using and transforming the data in other applications.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries** then select the query or multiple queries to export.

NOTE: You can also, run the query from the Queries page and click **Options | Export Data** from the query results page to access the Export page.

- 2 Click **Actions | Export Data**. The Export page appears.
- 3 Select what to export. For chart-based queries, select either **Chart data only** or **Chart data and drill-down tables**.
- 4 Select whether the data files are exported individually or in a single archive (zip) file.
- 5 Select the format of the exported file. If exporting to a PDF file, configure the following:

- Select the **Page size** and **Page orientation**.

Optionally select:

- **Show filter criteria**.
- **Include a cover page with these text** and include the needed text.

- 6 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.

NOTE: When typing multiple email addresses for recipients, you must separate entries with a comma or semicolon.

- 7 Click **Export**.

The files are created and either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.

Multi-server rollup querying

ePolicy Orchestrator 4.5 includes the ability to run queries that report on summary data from multiple ePO 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.

NOTE: As a prerequisite to running a Rolled-Up Compliance History query, you must take two preparatory actions on each server whose data you want to include:

- Creating a query to define compliance
- Generating a compliance event

Preparing for rollup querying

Use these tasks to ensure the EPORollup_ tables on the reporting server are populated and ready for using queries based on the Rolled-Up query result types. These tasks should be performed for each server whose data will be included in the query results.

Before you begin

Using the **Rolled-Up Compliance History** result type requires:

- A Boolean pie chart query based on managed systems be created on each server.

- A Run Query server task be created on each server, which uses the subaction Generate Compliance Event. Be sure to specify the previously mentioned Boolean pie chart query as the input for this subaction.
- Schedule the task for the time interval needed for Compliance History reporting. For example, if compliance must be collected on a weekly basis, then schedule the task to run weekly.

Tasks

- ▶ [Registering ePO servers](#)
- ▶ [Creating a Rollup Data server task](#)

Registering ePO servers

Use this task to register each ePO server with the reporting server that you want to include in rollup reporting. Registering ePO servers is required to collect summary data from those servers to populate the EPORollup_ tables of the rollup reporting server.

NOTE: The reporting server must be registered as well if its summary data is to be included in rollup reporting.

Task

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

- 1 Click **Menu | Configuration | Registered Servers**, then click **New Server**. The Registered Server Builder wizard opens.
- 2 On the Descriptions page, select **ePO 4.5** from the server type menu, specify a name and description, then click **Next**. The Details page appears.
- 3 Provide the details of the server, its database server, and the credentials to access the server, then click **Save**.

Creating a Rollup Data server task

Use this task to create a Rollup Data server task that populates the necessary tables on the reporting server with summary data from registered servers.

Best practices

Depending on the size of your network and the number of managed systems you have, performing the Rollup Data server task can be time intensive. McAfee recommends performing this task during off-peak hours, and using the incremental rollup option whenever possible.

Task

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

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder wizard opens.
- 2 On the Description page, type a name and description for the task, and select whether to enable it, then click **Next**. The Actions page appears.
- 3 Click **Actions** and select **Roll Up Data**.
- 4 From the **Roll up data from:** drop-down menu, select **All registered servers** or **Select registered servers**. If you choose **Select registered servers**, a browse button appears labeled **Select**.

- 5 Select the data type to be rolled up. You can select multiple data types.
NOTE: The data types Threat Events, Client Events, and Applied Policies can be further configured to include the additional properties Purge, Filter and Rollup Method. To do so, click **Configure** in the row that describes the additional properties available.
- 6 Click **Next**. The Schedule page appears.
- 7 Schedule the task, then click **Next**. The Summary page appears.
NOTE: If you are reporting on rolled-up compliance history data, ensure that the time unit of the Rolled-Up Compliance History query matches the schedule type of the Generate Compliance Event server tasks on the registered servers.
- 8 Review the settings, then click **Save**.

Creating a query to define compliance

Use this task to specify the properties to be included in a query to define compliance for Compliance History reporting.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**, then click **Actions | New Query**. The Query Builder wizard opens.
- 2 On the Result Type page, select **System Management** as Feature Group, and select **Managed Systems** as Result Types, then click **Next**. The Chart page appears.
- 3 Select **Boolean Pie Chart** from the Display Result As list, then click **Configure Criteria**. The Configure Criteria page appears.
- 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**. The Columns page appears.
NOTE: These properties define what is compliant for systems managed by this ePO server.
- 5 Select the columns to be included in the query, then click **Next**.
- 6 Select any filters to be applied to the query, click **Run**, then click **Save**.

Generating compliance events

Use this task to create a Run Query server task using the information that defines compliance.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder wizard opens.
- 2 On the Description page, type a name for the new task, then click **Next**. The Actions page appears.
- 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 and VirusScan Enterprise (for Windows) Compliance Summary** in the Shared Groups section, or a user-created query, such as one described in *Creating a query to define compliance*.
- 6 From the **Sub-Actions** drop-down menu, select **Generate Compliance Event** and specify the percentage or number of target systems, then click **Next**. The Schedule page appears.
NOTE: 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**. The Summary page appears.
- 8 Review the details, then click **Save**.

The Audit Log

Use the Audit Log to maintain and access a record of all ePO user actions. The Audit Log entries are displayed in a sortable table. For added flexibility, you can also filter the log so that it displays only failed actions, or only entries that are within a certain age.

The Audit Log displays seven columns:

- **Action** — The name of the action the ePO user attempted.
- **Completion Time** — The time the action finished.
- **Details** — More information about the action.
- **Priority** — Importance of the action.
- **Start Time** — The time the action was initiated.
- **Success** — Whether the action was successfully completed.
- **User Name** — User name of the logged-on user account that was used to take the action.

Audit Log entries can be queried against. You can create queries with the Query Builder wizard that target this data, or you can use the default queries that target this data. For example, the Failed Logon Attempts query retrieves a table of all failed logon attempts.

Working with the Audit Log

Use these tasks to view and purge the Audit Log. The Audit Log records actions taken by ePO users.

Tasks

- ▶ [Viewing the Audit Log](#)
- ▶ [Purging the Audit Log](#)
- ▶ [Purging the Audit Log on a schedule](#)

Viewing the Audit Log

Use this task to view a history of administrator actions. Available data depends on how often and by what age the Audit Log is purged.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Audit Log**. The details of administrator actions are displayed in a table.
- 2 Click any of the column titles to sort the table by that column (alphabetically).
- 3 From the **Filter** drop-down list, select an option to narrow the amount of visible data. You can remove all but the failed actions, or show only actions that occurred within a selected amount of time.
- 4 Click any entry to view its details.

Purging the Audit Log

Use this task to purge the Audit Log. You can only purge Audit Log records by age. When you purge the Audit Log, the records are deleted permanently.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Audit Log**.
- 2 Click **Actions | Purge**.
- 3 In the Purge dialog box, next to **Purge records older than**, type a number and select a time unit.
- 4 Click **OK**.

All records older than the specified timeframe are purged.

Purging the Audit Log on a schedule

Use this task to purge the Audit Log with a scheduled server task.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder wizard opens to the Description page.

- 2 Name, describe the task, and click **Enabled** after Schedule Status.
- 3 Click **Next**. The Actions page appears.
- 4 Select **Purge Audit Log** from the drop-down list.
- 5 After **Purge records older than**, type a number and select the time unit to use before purging the Audit Log entries.
- 6 Click **Next**. The Schedule page appears.
- 7 Schedule the task as needed, then click **Next**. The Summary page appears.
- 8 Review the task's details, then click **Save**.

The Server Task log

You can use server tasks and the Server Task Log to help manage and report on system status throughout your network. The default set of server tasks actions is described here.

Improvements to server tasks

Server tasks are now more configurable, allowing you to chain multiple actions and subactions within a single task, and provide more flexible scheduling.

Server task actions

- **Active Directory Synchronization/NT Domain** — Synchronizes selected Windows NT domains and Active Directory containers that are mapped to System Tree groups.
- **Delete Detected Systems** — Deletes any detected systems returned as a result of this task.
- **Event Migration (3.6.x -> 4.x)** — If you upgrade from a previous ePolicy Orchestrator installation, this task migrates events from the old database to the new database, so that you can run queries against your historical data. McAfee recommends scheduling this task to run at off hours as soon as possible after upgrading.
- **Export Agent Handler Assignments** — Downloads SiteList.xml, which contains the list of Agent Handler assignments.
- **Export Policies** — Downloads an xml file that contains the associated policy.
- **Export Queries** — Generates a query output file that can be saved or emailed to a recipient.
- **Host IPS Policy Migration** — Use this task to enable policies created with previous versions of Host IPS to the current version of the software.
- **Host IPS Property Translator** — Translates client rule properties and populates appropriate database tables with this data.
- **Import Agent Handler Assignments** — Imports a previously exported Agent Handler list, for example, SiteList.xml.
- **Load Systems by File** — Imports the systems from a text file that includes system name or IP addresses each on a new line.
- **Product License Usage: Count by Product** — Exports or emails the number of licenses used, based on the products installed on the server.
- **Product License Usage: Entitlement Information** — Generates a report that summarizes installations of your software on managed systems that have communicated to this ePO server in the last 180 days. The report can be exported or emailed.

- **Purge Audit Log** — Deletes entries from the Audit Log based on user-configured age.
- **Purge Client Events** — Deletes client events based on a time unit or using a query.
- **Purge Closed Issues** — Deletes all closed issues from the database based on user-configured criteria.
- **Purge Compliance History** — Deletes entries from the database based on user-configured criteria.
- **Purge Rolled-up Data** — Deletes selected Data Types from other registered ePO servers.
 - **Events** — Deletes event summary data.
 - **Compliance History** — Deletes compliance summary data.
 - **Managed Systems** — Deletes systems summary data.
 - **Policy Assignments** — Deletes policy assignment summary data.
- **Purge Server Task Log** — Deletes entries from the Server Task Log based on user-configured age.
- **Purge Threat Event Log** — Deletes threat event logs based on a time unit or using a query.
- **Repository Pull** — Retrieves packages from a chosen source site, then places them in the master repository.
- **Repository Replication** — Updates distributed repositories from the master repository.
- **Roll Up Data** — Imports selected Data Types from other registered ePO servers.
 - **Compliance History** — Imports compliance summary data.
 - **Managed Systems** — Imports managed systems summary data.
 - **Events** — Imports events summary data.
 - **Policy Assignments** — Imports policy assignment summary data.
- **Run Query** — Runs a selected query and allows you to chain sub-actions related to the query results. For example, you can email the results to someone in your organization, or deploy agents to all systems in the query results. Subactions include:
 - **Add to System Tree** — Adds the selected query to the specified group of systems in the System Tree.
 - **Apply Tag** — Applies a specified tag to all systems (that are not excluded from the tag) in the query results. This option is valid only for queries that result in a table of systems.
 - **Assign Policy** — Allows you to specify a previous created policy to the systems returned in the query results.
 - **Change Sorting Status** — Enables or disables System Tree sorting on all systems in the query results. This option is valid only for queries that result in a table of systems.
 - **Clear Agent GUID Sequence Error Count** — Clears the Sequence Error count generated due to a duplicate GUID.
 - **Clear Tag** — Removes a specified tag from all systems in the query results. This option is valid only for queries that result in a table of systems.
 - **Delete Sensor** — Deletes the Rogue System Sensor data. Make sure the sensor is uninstalled from the managed system before deleting the sensor.
 - **Delete Systems** — Deletes specified systems from the System Tree. You can also remove the agent from the systems at the same time.
 - **Deploy McAfee Agent** — Installs the agent on the Windows systems managed by that ePO server.

- **Detected System Exceptions** — Specifies what to do with the system exceptions detected by the query.
- **Email File** — Sends the results of the query to a specified recipient, in a user-configured format (PDF, XML, CSV, or HTML).
- **Exclude Tag** — Excludes a specified tag from all systems in the query results. This option is valid only for queries that result in a table of systems.
- **Export to File** — Exports the query results to a specified format. The exported file is placed in a location specified in the Printing and Exporting server settings.
- **Generate Compliance Event** — Generates an event based on a percentage or actual number threshold of systems that do not match the criteria in the query. This action is intended for compliance-based Boolean pie chart queries that retrieve data on managed systems (for example, the ePO: Compliance Summary default query). This action is part of the replacement of the Compliance Check server task of previous versions of ePolicy Orchestrator.
- **Move Agent GUID to Duplicate List and Delete Systems** — Moves the GUID of the agent to the Duplicate List and deletes the system from the System Tree.
- **Move Systems to Another Group** — Moves all systems in the query results to the specified group in the System Tree. This option is valid only for queries that result in a table of systems.
- **Repository Replication** — Replicates master repository contents to the distributed repositories in the query results. This is valuable for queries that return a list of out-of-date repositories (for example, the ePO: Distributed Repository Status default query). This option is valid only for queries that result in a table of distributed repositories.
- **Resort Systems** — Sorts the systems based on the IP address and tags assigned to them.
- **Install Rogue Sensor** — Installs a Rogue System Sensor on all managed systems in the query results.
- **Remove Rogue Sensor** — Removes the Rogue System Sensor from all managed systems in the query results.
- **Sensor Blacklist Management** — Adds or removes the Rogue Sensor Blacklist on all systems in the query results.
- **Set System Description** — Specifies any additional information about systems in the query results.
- **Transfer Systems** — Transfers the system in the query results to other registered ePO servers.
- **Update Agents** — Updates the Agents on systems returned by the query results with the latest packages checked into your master repository. For more information, see *Update tasks* in *Deploying Products and Updates*.
- **Wake Up Agents** — Performs an Agent Wake Up call on the systems returned in the query results.
- **Run Tag Criteria** — Evaluates all managed systems against a selected tag's criteria, and applies the tag to all matching systems.
- **Share Policies** — Synchronizes all policies with other registered servers.
- **System Search** — Searches for a system based on the specified tag or group.
- **Update Sensor Deployment Client Tasks** — Disabled by default, this action updates all sensor deployment client tasks.

Working with the Server Task Log

Use these tasks to view and maintain the Server Task Log.

Tasks

- ▶ [Viewing the Server Task Log](#)
- ▶ [Filtering the Server Task Log](#)
- ▶ [Purging the Server Task Log](#)

Viewing the Server Task Log

Use this task to review the status of server tasks and long-running actions.

The status of each server task appears in the **Status** column:

- **Completed** — Task completed successfully.
- **Failed** — Task was started but did not complete successfully.
- **In progress** — Task has started but not finished.
- **Waiting** — Task is waiting for another task to finish.
- **Terminated** — Task was terminated manually before it finished.

Task

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

- 1 Click **Menu | Automation | Server Task Log**. The Server Task Log display appears.
- 2 Click any of the column titles to sort the events.
- 3 Select any of the task logs, click **Actions**, then select one of the following to manipulate the server task log:
 - **Choose Columns** — The Select Columns to Display page appears.
 - **Export Table** — The Export page appears.
 - **Purge** — The Purge dialog box appears. Type a number and a time unit to determine the number of task log entries to delete, then click **OK**.
 - **Terminate Task** — Stop a task that is in progress.

Filtering the Server Task Log

As the Server Task Log grows, you can filter it to show only the most recent activity. You can filter the log to show only entries from the last day, last seven days, last 30 days, or by Failed or In Progress task status.

Task

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

- 1 Click **Menu | Automation | Server Task Log**.
- 2 Select the desired filter from the **Filter** drop-down list.

Purging the Server Task Log

As the Server Task Log grows, you can purge items older than a specified (user-configurable) number of days, weeks, months, or years.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Task Log**, then click **Actions | Purge**.
- 2 In the Purge dialog box, type a number of days, weeks, months, or years. Any item of this age and older are deleted.
- 3 Click **OK**.

Allowed Cron syntax when scheduling a server task

Cron syntax is made up of six or seven fields, separated by a space. Accepted Cron syntax, by field in descending order, is detailed in the following table. Most Cron syntax is acceptable, but a few cases are not supported. For example, you cannot specify both the Day of Week and Day of Month values.

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	, - * /

Notes on allowed special characters

- Commas (,) are allowed to specify additional values. For example, "5,10,30" or "MON,WED,FRI".
- Asterisks (*) are used for "every." For example, "*" in the minutes field is "every minute".
- Question marks (?) are allowed to specify no specific value in the Day of Week or Day of Month fields.

NOTE: 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.

NOTE: If the month does not have a fifth Wednesday, the task does not run.

The Threat Event Log

Use the Threat Event Log to quickly view and sort through events in the database. The log can be purged only by age.

You can choose which columns are displayed in the sortable table. You can choose from a variety of event data to use as columns.

Depending on which products you are managing, you can also take certain actions on the events. Actions are available in the Actions menu at the bottom of the page.

Common event format

Most managed products now use a common event format. The fields of this format can be used as columns in the Threat Event Log. These include:

- **Action Taken** — Action that was taken by the product in response to the threat.
- **Agent GUID** — Unique identifier of the agent that forwarded the event.
- **DAT Version** — DAT version on the system that sent the event.
- **Detecting Product Host Name** — Name of the system hosting the detecting product.
- **Detecting Product ID** — ID of the detecting product.
- **Detecting Product IPv4 Address** — IPv4 address of the system hosting the detecting product (if applicable).
- **Detecting Product IPv6 Address** — IPv6 address of the system hosting the detecting product (if applicable).
- **Detecting Product MAC Address** — MAC address of the system hosting the detecting product.
- **Detecting Product Name** — Name of the detecting managed product.
- **Detecting Product Version** — Version number of the detecting product.
- **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 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.

Working with the Threat Event Log

Use these tasks to view and purge the Threat Event Log

Tasks

- ▶ [Viewing the Threat Event Log](#)
- ▶ [Purging Threat Events](#)
- ▶ [Purging the Threat Event Log on a schedule](#)

Viewing the Threat Event Log

Use this task to view the Threat Event Log.

Before you begin

You must have appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Reporting | Threat Event Log**.
- 2 Click any of the column titles to sort the events. You can also click **Actions | Choose Columns** and the Select Columns to Display page appears.
- 3 From the Available Columns list, select different table columns that meet your needs, then click **Save**.

- 4 Select events in the table, then click **Actions** and select **Show Related Systems** to see the details of the systems that sent the selected events.

Purging Threat Events

Use this task to purge Threat Event records from the database. Purging Threat Event records deletes them permanently.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Threat Event Log**.
- 2 Click **Actions | Purge**.
- 3 In the Purge dialog box, next to **Purge records older than**, type a number and select a time unit.
- 4 Click **OK**.

Records older than the specified age are deleted permanently.

Purging the Threat Event Log on a schedule

Use this task to purge the Threat Event Log with a scheduled server task.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Server Task Builder wizard opens to the Description page.
- 2 Name, describe the task, and click **Enabled** after **Schedule Status**.
- 3 Click **Next**. The Actions page appears.
- 4 Select **Purge Threat Event Log** from the drop-down list.
- 5 Select whether to purge by age or from a queries results. If you purge by query, you must pick a query that results in a table of events.
- 6 Click **Next**. The Schedule page appears.
- 7 Schedule the task as needed, then click **Next**. The Summary page appears.
- 8 Review the task's details, then click **Save**.

Data exports from any table or chart

Data in any chart or table in ePolicy Orchestrator can be exported to four different formats. Exported results are historical data and are not refreshed.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- **CSV** — Use this format to use the data in a spreadsheet application (for example, Microsoft Excel).
- **XML** — Use this format to transform the data for other purposes.
- **HTML** — Use this report format to view the exported results as a web page.
- **PDF** — Use this report format when you need to print the results.

Exported data can be named and saved to any location, or emailed as attachments.

Monitoring with Dashboards

Dashboards allow you to keep constant watch on your environment. Dashboards are collections of monitors. Monitors can be anything from a chart-based query, to a small web application, like the MyAvert Security Threats, that is refreshed at a user-configured interval.

Users must have the appropriate permissions to use and create dashboards.

Are you setting up dashboards for the first time?

When setting up dashboards for the first time:

- 1 Decide which default dashboards and default monitors you want to use.
- 2 Create any needed dashboards and their monitors, and be sure to make active any you want available as tabs from the navigation bar.

Contents

- ▶ [Default dashboards and their monitors](#)
- ▶ [Setting up dashboard access and behavior](#)
- ▶ [Working with Dashboards](#)

Default dashboards and their monitors

Dashboards are collections of user-selected and configured monitors that provide current data about your environment. You can create your own dashboards from query results and use ePolicy Orchestrators default dashboards.

Queries as dashboard monitors

Use any chart-based query as a dashboard that is refreshed at a user-configured frequency, so you can use your most useful queries on a live dashboard.

Default dashboards and their monitors

This release of ePolicy Orchestrator ships with several default dashboards, each of which has its own default monitors.

NOTE: All dashboards, other than the default (typically ePO Summary) are owned by the Global Administrator who installed ePolicy Orchestrator. The Global Administrator who performed the installation must make additional dashboards active and public before other ePO users can view them.

NOTE: By default, when you log into ePolicy Orchestrator, the ePO Summary dashboard is the only dashboard you see until you make other dashboards active. To make a dashboard active,

in the Dashboards page click **Options | Select Active Dashboards**, and select from the Available Dashboards.

Audit dashboard

The Audit dashboard provides an overview of access-related activities occurring on your 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.
- **User Configuration 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.

ePO Summary dashboard

The 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:

- **My Avert Threat Advisory** — Displays the protection available, any new threats reported, latest DAT and engine available and, if they are in My Repository, a link to the MyAvert Security Threats page and the time last checked.
- **Systems per Top-Level Group** — Displays a bar chart of your managed systems, organized by top-level System Tree group.
- **Quick System Search** — You can search for systems by system name, IP address, MAC address, user name, or agent GUID.
- **McAfee Links** — Displays links to McAfee technical support, escalation tools, virus information library, and more.
- **McAfee Agent and VirusScan Enterprise (for Windows) Compliance Summary** — Displays a Boolean pie chart of managed systems in your environment, which are compliant or noncompliant, by version of VirusScan Enterprise (for Windows), McAfee Agent, and DAT files.
- **Malware Detection History** — Displays a line chart of the number of internal virus detections over the past quarter.

Executive dashboard

The Executive dashboard provides a set of monitors providing some high-level reports on security threats and compliance, with links to more specific product- and McAfee-specific information. The monitors included in this dashboard are:

- **My Avert Threat Advisory** — Displays the protection available, any new threats reported, latest DAT and engine available and, if they are in My Repository, a link to the MyAvert Security Threats page and the time last checked.
- **Malware Detection History** — Displays a line chart of the number of internal virus detections over the past quarter.

- **Product Deployment in the Last 24 Hours** — Displays a Boolean pie chart of all product deployments in the last 24 hours. Successful deployments are shown in green.
- **Product Updates in the Last 24 Hours** — Displays a Boolean pie chart off all product updates in the last 24 hours. Successful updates are shown in green.

Product Deployment dashboard

The Product Deployment dashboard provides an overview of product deployment and update activities in your network. The monitors included in this dashboard are:

- **Product Deployment in the Last 24 Hours** — Displays a Boolean pie chart of all product deployments in the last 24 hours. Successful deployments are shown in green.
- **Product Updates in the Last 24 Hours** — Displays a Boolean pie chart of all product updates in the last 24 hours. Successful updates are shown in green.
- **Failed Product Deployment in the Last 24 Hours** — Displays a single group bar chart, grouped by product code, of all the failed product deployments in the last 24 hours.
- **Quick System Search** — You can search for systems by system name, IP address, MAC address, user name, or agent GUID.
- **Failed Product Updates in the Last 24 Hours** — Displays a single group bar chart, grouped by product code, of all failed product updates in the last 24 hours.
- **Agent Uninstalls Attempted in the Last 24 Hours** — Displays a single bar chart, grouped by day, of all agent uninstall client events in the last 24 hours.

RSD Summary dashboard

The RSD (Rogue System Detection) Summary dashboard provides a summary of the state of detected systems on your network. The monitors included in this dashboard are:

- **Rogue Systems, by Domain** — Rogue system interfaces detected by Rogue System Sensors in the last week, grouped by domain.
- **Active Sensor Responses** — Displays a Boolean pie chart of active Rogue System Sensors that have or haven't communicated with the ePO server in the last 24 hours.
- **Subnet Coverage** — Subnets that are or aren't covered by Rogue System Sensors.
- **Rogue Systems, By OS** — Rogue system interfaces detected by Rogue System Sensors over the last week, grouped by operating system.
- **Passive Sensor Response** — Passive Rogue System Sensors that have or haven't communicated with the ePO server in the last 24 hours.
- **Rogue Systems, By OUI** — Rogue system interfaces detected by Rogue System Sensors over the last week, grouped by OUI (Organizationally Unique Identifier) in the last week.

Setting up dashboard access and behavior

Use these tasks to ensure that users have the appropriate access to dashboards, and how often dashboards are refreshed.

Tasks

- ▶ [Giving users permissions to dashboards](#)
- ▶ [Configuring the refresh frequency of dashboards](#)

Giving users permissions to dashboards

Use this task to give users the needed permissions to dashboards. For a user to be able to access or use dashboards, they must have the appropriate permissions.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | User Management | Permission Sets**, then create a new permission set or select an existing permission set.
- 2 Next to **Dashboards**, click **Edit**. The Edit Permission Set: Dashboards page appears.
- 3 Select a permission:
 - **No permissions**
 - **Use public dashboards**
 - **Use public dashboards; create and edit personal dashboards**
 - **Edit public dashboards; create and edit personal dashboards; make personal dashboards public**
- 4 Click **Save**.

Configuring the refresh frequency of dashboards

Use this task to configure how often (in minutes) dashboards are refreshed. This setting is unique to each user account.

When setting this, consider the number of users that you anticipate will be logged on at anytime. Each user logged on with a dashboard displayed creates additional performance usage when the dashboards are refreshed.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Dashboards**, then click **Options | Edit Dashboard Preferences**. The Dashboard Preferences page appears.
- 2 Next to **Dashboard page refresh interval**, type the number of minutes you want between refreshes. Maximum page refresh interval is 60 minutes.
- 3 Click **Save**.

Working with Dashboards

Use these tasks to create and manage dashboards.

Tasks

- ▶ [Creating dashboards](#)
- ▶ [Making a dashboard active](#)
- ▶ [Selecting all active dashboards](#)
- ▶ [Making a dashboard public](#)

Creating dashboards

Use this task to create a dashboard.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Dashboards**, then click **Options | Manage Dashboards**. The Manage Dashboards page appears.
- 2 Click **New Dashboard**.
- 3 Type a name and select a size for the dashboard.
- 4 For each monitor, click **New Monitor**, select the monitor to display in the dashboard, then click **OK**.
- 5 Click **Save**, then select whether to make this dashboard active. Active dashboards are displayed on the tab bar of **Dashboards**.
- 6 Optionally, you can make this dashboard public from the Manage Dashboards page by clicking **Make Public**

NOTE: All new dashboards are saved to the private My Dashboards category.

Making a dashboard active

Use this task to make a dashboard part of your active set.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Dashboards**, then click **Options | Select Active Dashboards**. The Select Active Dashboards page appears.
- 2 Select the dashboards you want to activate from the **Available Dashboards** list, then click **OK**.

Selecting all active dashboards

Use this task to select all dashboards that make up your active set. Active dashboards are accessible on the tab bar under **Dashboards**.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Dashboards**, then click **Options | Select Active Dashboards**. The Select Active Dashboards page appears.

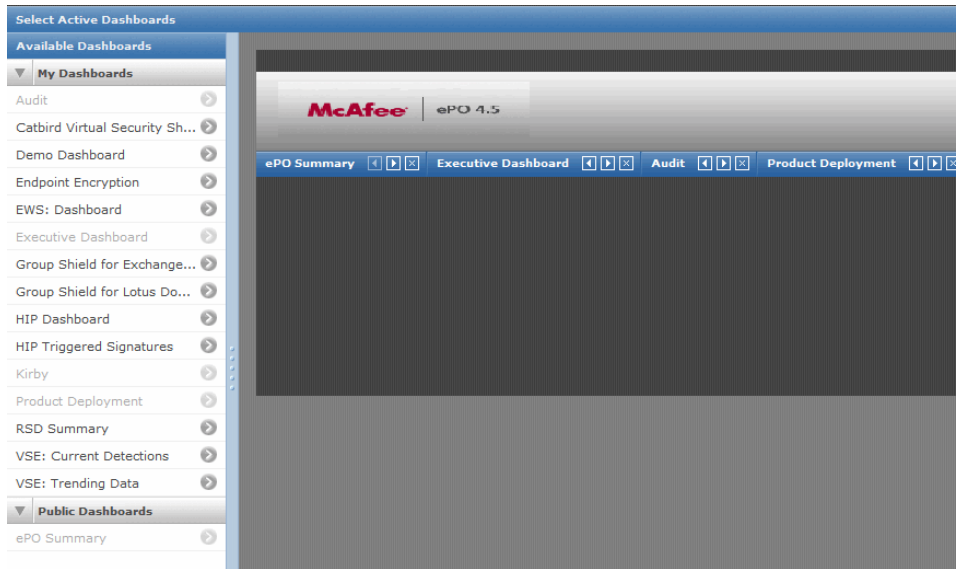


Figure 12: Select Active Dashboards page

- 2 Click the desired dashboards from the **Available Dashboards** list. They are added to the content pane.
- 3 Repeat until all desired dashboards are selected.
- 4 Arrange the selected dashboards in the order you want them to appear on the tab bar.
- 5 Click **OK**.

The selected dashboards appear on the tab bar whenever you open the Dashboards page of the product.

Making a dashboard public

Use this task to make a private dashboard public. Public dashboards can be used by any user with permissions to public dashboards.

Task

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

- 1 Click **Menu | Reporting | Dashboards**, then click **Options | Manage Dashboards**. The Manage Dashboards page appears.
- 2 Select the desired dashboard from the **Available Dashboards** list, then click **Make Public**.
- 3 Click **OK** when prompted.
- 4 Click **Close**.

The dashboard appears in the Public Dashboards list on the Manage Dashboards page.

Detecting Rogue Systems

Unprotected systems are often the weak spot of any security strategy, creating entry points through which viruses and other potentially harmful programs can access your network. Even in a managed network environment, some systems might not have an active McAfee Agent on them. These can be systems that frequently log on and off the network, including test servers, laptops, or wireless devices.

Rogue System Detection provides real-time discovery of rogue systems through the use of a Rogue System Sensor installed throughout your network. The sensor listens to network broadcast messages and DHCP responses to detect systems connected to the network.

When a sensor detects a system on the network, it sends a message to the ePolicy Orchestrator server. The server then checks whether the system has an active agent installed and managed. If the system is unknown to the ePO server, Rogue System Detection provides information to ePolicy Orchestrator to allow you to take remediation steps, which include alerting network and anti-virus administrators or automatically deploying an agent to the system.

In addition to Rogue System Detection, other McAfee products, like McAfee Network Access Control, add detected systems control to ePolicy Orchestrator.

Contents

- ▶ [What are rogue systems](#)
- ▶ [How the Rogue System Sensor works](#)
- ▶ [How detected systems are matched and merged](#)
- ▶ [Rogue System Detection states](#)
- ▶ [Rogue Sensor Blacklist](#)
- ▶ [Rogue System Detection policy settings](#)
- ▶ [Rogue System Detection permission sets](#)
- ▶ [Setting up Rogue System Detection](#)
- ▶ [Configuring Rogue System Detection policy settings](#)
- ▶ [Configuring server settings for Rogue System Detection](#)
- ▶ [Working with detected systems](#)
- ▶ [Working with sensors](#)
- ▶ [Working with subnets](#)
- ▶ [Rogue System Detection command-line options](#)
- ▶ [Default Rogue System Detection queries](#)

What are rogue systems

Rogue systems are systems that access your network, but are not managed by your ePO server. Unprotected systems are often the weak spot of any security strategy, creating entry points through which viruses and other potentially harmful programs can access your network. Even in a managed network environment, some systems might not have an active McAfee Agent on them. These can be systems that frequently log on and off the network, including test servers, laptops, or wireless devices.

A rogue system is any device on your network with a network interface card (NIC). On systems with multiple NICs, each resulting interface is identified as a separate system. When these interfaces are detected, they appear as multiple rogue interfaces.

You can specify how the system interfaces are matched in the same manner you use to specify how detected systems are matched. Identifying these systems and their interfaces, and managing them with Rogue System Detection and ePolicy Orchestrator helps provide the network security your organization needs.

How the Rogue System Sensor works

The Rogue System Sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect systems, routers, printers, and other devices connected to your network. They gather information about the devices they detect, and forward the information to the ePO server.

The sensor is a Win32 native executable application that runs on any NT-based Windows operating system, including:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows 2008
- Windows Vista

It can be installed on systems throughout your network. A sensor reports on all systems in the broadcast segment where it is installed. A sensor installed on a DHCP server reports on all systems or subnets using DHCP. To maintain coverage in networks or broadcast segments that don't use DHCP servers, you must install at least one sensor in each broadcast segment, usually the same as a subnet. DHCP deployment can be used with segment-specific deployment of the Rogue System Sensor for the most comprehensive coverage.

Passive listening to layer-2 traffic

To detect systems on the network, the sensor uses WinPCap, a packet capture library. It captures layer-2 broadcast packets sent by systems that are connected to the same network broadcast segment. It also listens passively to all layer-2 traffic for Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), IP traffic, and DHCP responses.

To obtain additional information, the sensor also performs NetBIOS calls and OS fingerprinting on systems that were already detected. It does this by listening to the broadcast traffic of all devices in its broadcast segment, and by using NetBIOS calls, actively probing the network to

gather additional information about the devices connected to it, such as the operating system of a detected system.

NOTE: The sensor does not determine whether the system is a rogue system. It detects systems connected to the network and reports these detections back to the ePO server, which determines whether the system is rogue based on user-configured settings.

Intelligent filtering of network traffic

The sensor filters network traffic "intelligently" — it ignores unnecessary messages and captures only what it needs, which is Ethernet and IP broadcast traffic. By filtering out unicast traffic, which might contain non-local IP addresses, the sensor focuses only on devices that are part of the local network.

To optimize performance and minimize network traffic, the sensor limits its communication to the server by relaying only new system detections, and by ignoring any re-detected systems for a user-configured time. For example, the sensor detects itself among the list of detected systems. If the sensor sent a message every time it detected a packet from itself, the result would be a network overloaded with sensor detection messages.

The sensor further filters on systems that were already detected:

- The sensor reports any system the first time it is detected on the network.
- For each detected system, the sensor adds the MAC address to the packet filter, so that it is not detected again, until the user-configured time elapses.
- The sensor implements aging on the MAC filter. After a specified time, MAC addresses for systems that have already been detected are removed from the filter, causing those systems to be re-detected and reported to the server. This process ensures that you receive accurate and current information about detected systems.

Data gathering and communications to the server

Once the sensor detects a system on the local network, it gathers information about that system using active scanning and NetBIOS calls. This information includes:

- DNS name
- Operating system version
- NetBIOS information (domain membership, system name, and the list of currently logged-on users)

All NetBIOS-related information that is gathered is subject to standard limitations of authorization, and other limitations documented in the Microsoft management API.

The sensor packages the gathered information into an XML message, then sends the message via secure HTTPS to the ePolicy Orchestrator server for processing. The server then uses the ePolicy Orchestrator data to determine whether the system is a rogue system.

Bandwidth use and sensor configuration

To save bandwidth in large deployments, you can configure how often the sensor sends detection messages to the server. You can configure the sensor to cache detection events for a given time period, such as one hour, then to send a single message containing all the events from that time period. For more information, see *Configuring Rogue System Detection policy settings*.

Systems that host sensors

Install sensors on systems that are likely to remain on and connected to the network at all times, such as servers. If you don't have a server running in a given broadcast segment, install sensors on several workstations to ensure that at least one sensor is connected to the network at all times.

TIP: To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor in each broadcast segment of your network. Installing more than one sensor in a broadcast segment does not create issues around duplicate messages because the server filters any duplicates. However, additional active sensors in each subnet results in traffic sent from each sensor to the server. While maintaining as many as five or ten sensors in a broadcast segment should not cause any bandwidth issues, you should not maintain more sensors in a broadcast segment than is necessary to guarantee coverage.

DHCP servers

If you use DHCP servers in your network, you can install sensors on them. Sensors installed on DHCP servers report on all connected subnets by listening for DHCP responses. Using sensors on DHCP servers reduces the number of sensors you need to install and manage on your network to ensure coverage, but it does not eliminate the need to install sensors to network segments that use static IP address.

TIP: Installing sensors on DHCP servers can improve coverage of your network. However, it is still necessary to install sensors in broadcast segments that use static IP address, or that have a mixed environment. A sensor installed on a DHCP server does not report on systems covered by that server if the system uses a static IP address.

How detected systems are matched and merged

When a system connects to your network, Rogue System Detection automatically checks the ePO database to determine whether the incoming system is new or corresponds to a previously detected system. If the system has been previously detected, Rogue System Detection automatically matches it to the existing record in the ePO database. When a detected system is not matched automatically, you can manually merge the system with an existing detected system.

Matching detected systems

Automatic matching of detected systems is necessary to prevent previously detected systems from being identified as new systems on your network. By default, systems are first matched against an agent's unique ID. If this unique ID does not exist, the ePO database uses attributes specified in the Rogue System Matching server settings. You can specify which attributes the database uses for matching, based on which attributes are unique in your environment.

If a system on your network has multiple NICs, each system interface can result in separate detections. Use the Detected System Matching Server Setting to match multiple interfaces to an existing detected system in order to eliminate duplicate systems.

Merging detected systems

When the ePO server cannot automatically match detected systems, you can merge them manually using Merge systems. For example, the ePO server might not be able to match a

detected system interface that was generated by a system with multiple NICs, based on the matching attributes you have specified.

Rogue System Detection states

Rogue System Detection categorizes systems, sensors, and subnets on your network with different states to make monitoring and managing your network easier. These states determine the following:

- Overall system status
- Rogue System Sensor status
- Subnet status

The Detected Systems page displays information on each of these states via corresponding status monitors. This page also displays the 25 subnets with the most rogue system interfaces in the Top 25 Subnets list and the adjacent Rogue System Interfaces by Subnet table.

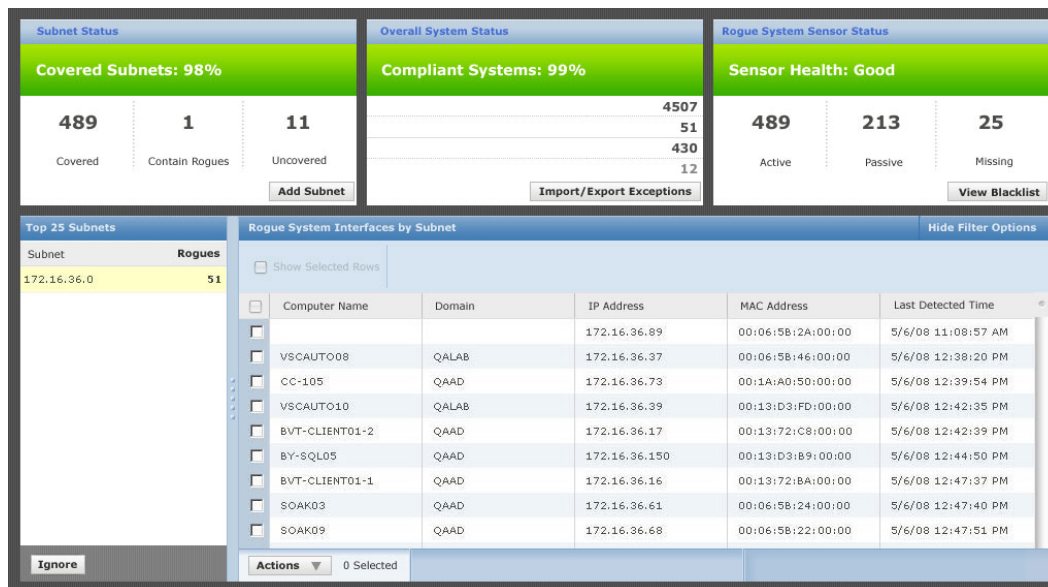


Figure 13: Detected Systems page

Overall system status

Overall system status is presented in the Overall System Status monitor as a percentage of compliant systems. Systems states are separated into these categories:

- Exceptions
- Inactive
- Managed
- Rogue

The percentage of compliant systems is the ratio of systems in the Managed and Exceptions categories to those in the Rogue and Inactive categories.

Exceptions

Exceptions are systems that don't need a McAfee Agent, such as routers, printers, or systems from which you no longer want to receive detection information. Identify these systems and mark them as exceptions to prevent them from being categorized as rogue systems. Mark a system as an exception only when it does not represent a vulnerability in your environment.

Inactive

Inactive systems are listed in the ePO database, but have not been detected by a detection source in a specified time, which exceeds the period specified in the Rogue category. Most likely these are systems that are shut down or disconnected from the network, for example, a laptop or retired system. The default time period for marking systems as inactive is 45 days.

Managed

Managed systems have an active McAfee Agent that has communicated with the ePO server in a specified time. To ensure security, the majority of detected systems on your network should be managed.

NOTE: Systems on your network with an installed active agent are displayed in this list, even before you deploy sensors to the subnets that contain these systems. When the agent reports to the ePO database, the system is automatically listed in the Managed category.

Rogue

Rogue systems are systems that are not managed by your ePO server. There are three rogue states:

- **Alien agent** — These systems have a McAfee Agent that is not in the local ePO database, or any database associated with additional ePO servers you have registered with the local server.
- **Inactive agent** — These systems have a McAfee Agent in the ePO database that has not communicated in a specified time.
- **Rogue** — These systems don't have a McAfee Agent.

Systems in any of these three rogue states are categorized as Rogue systems.

Rogue System Sensor status

Rogue System Sensor status is the measure of how many sensors installed on your network are actively reporting to the ePO server, and is displayed in terms of health. Health is determined by the ratio of active sensors to missing sensors on your network. Sensor states are categorized into these groups:

- Active
- Missing
- Passive

Active

Active sensors report information about their broadcast segment to the ePO server at regular intervals, over a fixed time. Both the reporting period and the active period are user-configured. A sensor becomes passive when the active period lapses, at which time the next passive sensor to report in is made active.

Missing

Missing sensors have not communicated with the ePO server in a user-configured time. These sensors could be on a system that has been turned off or removed from the network.

Passive

Passive sensors check in with the ePO server, but do not report information about detected systems. They wait for instructions from the ePO server to replace other sensors that become passive.

Subnet status

Subnet status is the measure of how many detected subnets on your network are covered. Coverage is determined by the ratio of covered subnets to uncovered subnets on your network. Subnet states are categorized into these groups:

- Contains Rogues
- Covered
- Uncovered

NOTE: Subnets must be known by the ePO server or be seen by a sensor to fall into one of these categories. Once a subnet has been detected, you can mark it **Ignored** to prevent receiving further reporting about its status.

Contains Rogues

Subnets that contain rogue systems are listed in the Contains Rogues category to make it easier to take action on them.

Covered

Covered subnets have sensors installed on them that are actively reporting information about detected systems to the ePO server. The Covered subnets category also includes the systems listed in the Contains Rogues category. For example, the Covered subnets category contains subnets A, B, and C. Subnet B contains rogues, while A and C do not. All three are listed in the Covered category; only subnet B is listed in the Contains Rogues category.

Uncovered

Uncovered subnets don't have any active sensors on them. Subnets that are uncovered are not reporting information about detected systems to the ePO server. However, there might be managed systems on this subnet that are being reported on through other means, such as agent-server communication.

Top 25 Subnets

The Top 25 Subnets list provides the subnet list, by name or IP, for the 25 subnets that contain the most rogue system interfaces on your network. When a top 25 subnet is selected, the rogue system interfaces it contains are displayed in the adjacent Rogue System Interfaces by Subnet table.

Rogue Sensor Blacklist

The Rogue Sensor Blacklist is the list of managed systems where you do not want sensors installed. These can include systems that would be adversely affected if a sensor were installed on them, or systems you have otherwise determined should not host sensors. For example, mission critical servers where peak performance of core services is essential, such as database servers or servers in the DMZ (demilitarized zone). Also, systems that might spend significant time outside your network, such as laptops.

The Rogue Sensor Blacklist is different than the Exceptions list, in that systems on the Exceptions list are those that either can't have an agent on them, or that you don't want categorized as Rogue, such as printers or routers.

Rogue System Detection policy settings

Rogue System Detection policy settings allow you to configure and manage the instances of the Rogue System Sensor installed throughout your network. Settings can be applied to individual systems, groups of systems, and IP ranges.

You can configure policy settings for all sensors deployed by the server. This is similar to managing policies for any deployed product, such as VirusScan Enterprise. The Rogue System Detection policy pages are installed on the ePO server at installation.

Configure the sensor policy settings in the Rogue System Detection policy pages the same way you would for any managed security product. Policy settings that you assign to higher levels of the System Tree are inherited by lower-level groups or individual systems. For more information about policies and how they work, see *Managing your Network with Policies and Client Tasks*.

TIP: McAfee recommends that you configure policy settings before you deploy sensors to your network. Doing so ensures that the sensors work according to your intended use. For example, DHCP monitoring is disabled by default. As a result, if you deploy sensors to DHCP servers without enabling DHCP monitoring during your initial configuration, those sensors report limited information to the ePO server. If you deploy sensors before you configure your policies, you can update them to change sensor functionality.

Considerations for policy settings

Policy settings configure the features and performance of the Rogue System Sensor. These settings are separated into four groups:

- Communication settings
- Detection settings
- General settings
- Interface settings

Communication settings

Communication settings determine:

- Communication time for inactive sensors.
- Reporting time for active sensors.
- Sensor's detected system cache lifetime.

The communication time for inactive sensors determines how often passive sensors check in with the server.

The Reporting time for active sensors determines how often active sensors report to the ePO server. Setting this value too low can have the same effect as setting the value for the sensor's detected system cache lifetime.

The sensor's detected system cache lifetime is the amount of time a detected system remains in the sensor's cache. This value controls how often the sensor reports that a system is newly detected. The lower the value, the more often the sensor reports a system detection to the server. Setting this value too low can overwhelm your server with system detections. Setting this value too high prevents you from having current information on system detections.

TIP: McAfee recommends that you set the sensor's detected system cache lifetime and the reporting time for active sensors settings to the same value.

Detection settings

Detection settings determine whether:

- Device details detection is enabled.
- DHCP monitoring is enabled.
- Reporting on self-configured subnets is enabled.

If you use DHCP servers on your network, you can install sensors on them to monitor your network. This allows you to use a single sensor to report on all subnets and systems that connect to it. DHCP monitoring allows you to cover your network with fewer sensors to deploy and manage, and reduces the potential for missed subnets and systems.

Device details detection allows you to specify the type of information the Rogue System Sensor scans systems for.

- Operating System (OS) details — This option allows the sensor to determine detailed information about a device's operating system. If you enable OS details scanning, you can also choose to scan the systems you have marked as exceptions.
- You can also specify which systems and networks are scanned using OS detection by choosing to scan all networks or only specific networks. You can limit OS detection to specific subnets by included or excluding specific IP addresses.

The Rogue System Sensor uses NetBIOS calls and OS fingerprinting to provide more detailed information about the devices on your network. You can enable active probing on your entire network, or include or exclude specific subnets.

CAUTION: This Device details detection feature provides accurate matching of detected system interfaces and should be disabled only if you have specific reasons to do so.

General settings

General settings determine:

- Sensor-to-server communication port.
- Server IP address or DNS name.
- Whether the Rogue System Sensor is enabled.

The server IP address default value is the address of the ePO server that you are using to install sensors. Rogue System Detection reports system detections to the specified server. When this

server detects a system that has an agent deployed by an ePO server with a different IP address, that system is detected as a rogue because the agent is considered an alien agent.

NOTE: The sensor-to-server communication port server setting can be changed only during installation. Whichever port you have specified during installation must also be specified in the General tab of Rogue System Detection policies.

Interface settings

Interface settings determine whether sensors:

- Do not listen on interfaces whose IP addresses are included in specific networks.
- Only listen on an interface if its IP address is included on a network found during installation.
- Only listen on interfaces whose IP addresses are included in specific networks.

Specifying these settings allows you to choose the networks that the sensor reports on.

Rogue System Detection permission sets

Permission sets for Rogue System Detection determine what information a user group can view, modify, or create for Rogue System Detection. One or more permission sets can be assigned. By default, permission sets for global administrators are automatically assigned to include full access to all products and features.

The permission sets and their available privileges for Rogue System Detection are listed in the following table.

Permission set	Rights
Rogue System Detection	<ul style="list-style-type: none">• Create and edit Rogue System information; manage sensors.• Create and edit Rogue System information; manage sensors; deploy McAfee Agents and add to System Tree.• No permissions.• View Rogue System information.
Rogue System Sensor	<ul style="list-style-type: none">• No permissions.• View and change settings.• View settings.

Setting up Rogue System Detection

Use these tasks to set up Rogue System Detection.

Protecting your network requires accurate information about the systems that connect to it. Rogue System Detection uses sensors to monitor the detected systems on your network to provide this information.

Before you begin

Before you begin setting up Rogue System Detection:

- Make sure you have agents distributed to your systems. For more information, see *Distributing agents*.
- Review the information in the preceding sections to understand the sensor and its policies.

Tasks

- ▶ [Configuring Rogue System Detection policy settings](#)
- ▶ [Configuring server settings for Rogue System Detection](#)

Configuring Rogue System Detection policy settings

Use this task to configure Rogue System Detection policy settings. Policy settings determine how the sensor obtains and reports information about systems detected on your network.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then from the Product drop-down list select **Rogue System Detection x.x.x**, and from the Category drop-down list, select **General**. All created policies for Rogue System Detection appear.
- 2 Edit an existing policy, or create a new policy.
 - To edit an existing policy, locate the desired policy and click **Edit Settings** in its row.
 - To create a new policy, click **Actions | New Policy**, from the **Create a policy based on this existing policy** drop-down menu, then select an existing policy on which to base the new policy. Name the new policy and click **OK**.
- 3 Configure the desired settings, then click **Save**.

Configuring server settings for Rogue System Detection

Use these tasks to configure server settings for Rogue System Detection. These settings determine how information about subnets and detected systems is displayed in the **Detected Systems** page. Server settings allow you to customize Rogue System Detection to meet the specific needs of your organization.

Tasks

- ▶ [Editing Detected System Compliance](#)
- ▶ [Editing Detected Systems Matching](#)
- ▶ [Editing Rogue System Sensor settings](#)
- ▶ [Editing Detected System Exception Categories](#)
- ▶ [Editing Detected System OUIs](#)

Editing Detected System Compliance

Use this task to edit the Detected System Compliance settings. These settings are user-configured and have two important functions:

- They specify the time-frame that determines the state of detected systems (Managed, Rogue, Exception, Inactive).

- They control the visual feedback of the Rogue System Detection status monitors on the Detected Systems page.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, then in the Settings Categories list, click **Detected System Compliance**.
- 2 In the details pane, click **Edit**.
- 3 Edit the number of days to categorize Detected Systems as Managed or Inactive.
NOTE: The number of days in **Rogue | Has Agent in ePO Database, but is older than__ days** is controlled by the number of days set in the Managed field.
- 4 Edit the percentage levels for these options, so that the color codes represent your requirements:
 - **Covered Subnets** — Required coverage.
 - **Compliant Systems** — Required compliance status.
 - **Sensor Health** — Ratio of active to missing sensors.
- 5 **ePO Servers** — Configure additional ePO servers whose detected systems should not be considered rogue systems.
- 6 Click **Save**.

Editing Detected Systems Matching

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

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, then in the Settings Categories list select **Detected System Matching** and click **Edit**.
- 2 Use the **Matching Detected Systems** table to define the properties that determine when to match detected systems.
- 3 Use the **Matching Managed Systems** table to define the properties that determine when a newly detected interface belongs to an existing managed system.
- 4 In **Static IP Ranges for Matching**, type the static IP ranges to use when matching on static IP addresses.
- 5 In **Alternative McAfee Agent Ports**, specify any alternate ports you want to use when querying detected systems to check for a McAfee Agent.
- 6 Click **Save**.

Editing Rogue System Sensor settings

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

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

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, then in the Settings Categories list, select **Rogue System Sensor** and click **Edit**.
- 2 Edit the **Sensor Timeout** field to set the maximum number of time the server waits for a sensor to call in before marking it as missing.
- 3 Edit the **Sensors per Subnet** field to set the maximum number of sensors active in each subnet, or select **All sensors active**.
- 4 Add a list of **Sensor Scanning** MAC addresses and OUIs that the sensors should not actively probe, regardless of the configured policy.
- 5 Edit the **Active Period** time field to set the maximum amount of time that passes before the server tells a sensor to sleep, to allow a new sensor to become active.

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

- 6 Click **Save**.

Editing Detected System Exception Categories

Use this task to configure and edit the categories to use to manage exception systems in your network. Exceptions are system that you know are unmanaged (don't have a McAfee Agent on them).

Task

For option definitions, click ? in the interface.

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

NOTE: Use the **Delete** and **Change** links to modify existing exceptions categories.

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

Editing Detected System OUIs

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

Task

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

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

Working with detected systems

Use these tasks to manage detected systems in Rogue System Detection.

Tasks

- ▶ [Adding systems to the Exceptions list](#)
- ▶ [Adding systems to the Rogue Sensor Blacklist](#)
- ▶ [Adding detected systems to the System Tree](#)
- ▶ [Editing system comments](#)
- ▶ [Exporting the Exceptions list](#)
- ▶ [Importing systems to the Exceptions list](#)
- ▶ [Merging detected systems](#)
- ▶ [Pinging a detected system](#)
- ▶ [Querying detected system Agents](#)
- ▶ [Removing systems from the Detected Systems list](#)
- ▶ [Removing systems from the Exceptions list](#)
- ▶ [Removing systems from the Rogue Sensor Blacklist](#)
- ▶ [Viewing detected systems and their details](#)

Adding systems to the Exceptions list

Use this task to add detected systems to the Exceptions list.

Task

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

From the **Detected Systems** page:

- 1 Click **Menu | Systems | Detected Systems**.
- 2 From **Rogue System Interfaces by Subnet** pane, click any system.
- 3 Click **Actions** and select **Add to Exceptions**. The Add to Exceptions dialog box appears.
- 4 Select one of the following to configure the Detected Systems | Exceptions display, and click **OK**:
 - **No Category** — Displayed without a category entry.
 - **New Category** — Displayed with the new category name you type.
 - **Select Category** — Displayed with the category selected from the list.

NOTE: To configure categories, see *Editing Detected System Exception Categories*.

From the **Detected Systems Details** page:

- 1 Click **Menu | Systems | Detected Systems**,
- 2 From **Overall System Status** monitor pane, click any detected system category
- 3 From the **Detected Systems Details** page, click any system.
- 4 Click **Actions** and select **Detected Systems | Add to Exceptions**. The Add to Exceptions dialog box appears.
- 5 Select one of the following to configure the Detected Systems | Exceptions display, and click **OK**:
 - **No Category** — Displayed without a category entry.
 - **New Category** — Displayed with the new category name you type.
 - **Select Category** — Displayed with the category selected from the list.

NOTE: To configure categories, see *Editing Detected System Exception Categories*.

Adding systems to the Rogue Sensor Blacklist

Use this task to add detected systems to the **Rogue Sensor Blacklist**.

Task

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

- 1 Click **Menu | Systems | System Tree | Systems** and select the detected systems you want to add to the Rogue Sensor Blacklist.
- 2 Click **Actions**, then select **Rogue Sensor | Add to Sensor Blacklist**.
- 3 Click **OK** to confirm the change.
- 4 To confirm that the system is moved to the Rogue Sensor Blacklist, click **Menu | Systems | Detected Systems**, then from the Rogue System Sensor Status monitor, click **View Blacklist**.

Adding detected systems to the System Tree

Use this task to add detected systems to the System Tree from the Detected Systems pages

This task can be performed from:	Getting there
Detected Systems page	Click Menu Systems Detected Systems .
Detected Systems Status page	Click Menu Systems Detected Systems , then click any category in the Overall System Status monitor.

Task

For option definitions, click ? in the interface.

- 1 Select the detected systems you want to add to the System Tree.
- 2 Click **Actions | Detected Systems | Add to System Tree**. The Add to System Tree page opens.
- 3 Click **Browse** to open the Select System Tree Group dialog box, which allows you to navigate to the location where you want to add the selected systems.
- 4 Specify whether to
 - **Tag and Sort Systems** — Applies tags and sorts system immediately after adding the systems to the System Tree.
 - **Duplicate System Names** — Allows duplicate entries to be added to the System Tree.

Editing system comments

Use this task to edit system comments. System comments can be useful for noting important “human readable” information to a detected system entry.

This task can be performed from:	Getting there
Detected Systems Details page.	Click Menu Systems Detected Systems , click any detected system category in the Overall System Status monitor, then click any system.
Detected Systems page.	Click Menu Systems Detected Systems , then click any detected system category in the Overall System Status monitor.

Task

For option definitions, click ? in the interface.

- 1 Select the system whose comment you want to edit, then click **Actions** and select **Edit Comment**.
- 2 Type your comments in the Enter New Comment field of the popup, then click **OK**.

Exporting the Exceptions list

Use this task to export the list of MAC addresses of the detected systems on your network that are marked as Exceptions.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**, click **Import/Export Exceptions** from the Overall System Status monitor, then click the **Export Exceptions** tab.

- 2 Click **Export Exceptions**, then select **download exceptions**.

NOTE: Files are exported in the Comma Separated Value format. The file name for your Exceptions list is predefined as RSDExportedExceptions.csv. You can change the name of the file when you download it to your local system.

Importing systems to the Exceptions list

Use this task to import systems to your network's Exceptions list.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**, click **Import/Export Exceptions** from the Overall System Status monitor, then click the **Import Exceptions** tab.
- 2 Choose the method you want to use to import, specify the systems or file, then click **Import Exceptions**.

NOTE: When importing systems, only MAC addresses are recognized. MAC addresses can be separated by whitespace, commas, or semicolons. The MAC address can include colons, but they are not required.

Merging detected systems

Use this task to merge detected systems.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**, then from Overall System Status monitor, select **Rogue**. The rogue systems appear in the display.
- 2 Select the systems you want to merge.
- 3 Click **Actions**, then select **Detected Systems | Merge Systems**. The Merge Systems page appears.
- 4 Click **Merge**.
- 5 When the merge warning message appears, click **OK**.

Pinging a detected system

Use this task to ping a detected system to confirm that it can be reached over the network.

This task can be performed from:	Getting there
Detected Systems Status page	Click Menu Systems Detected Systems , then click any category in the Overall System Status monitor.
System Tree page.	Click Menu Systems System Tree .

Task

For option definitions, click ? in the interface.

- 1 Select the system you want to ping.

NOTE: You can only ping one system at a time.

- 2 Click **Actions | Detected Systems** or **Directory Management**, then click **Ping**. The result is displayed on the Actions bar in the notification panel at the bottom right corner of the ePO console window.

Querying detected system Agents

Use this task to query Agents installed on detected systems. Not all detected systems have a McAfee Agent installed. The results of this task indicate whether an Agent is installed and provides links to details about the system and the agent, if available.

This task can be performed from:	Getting there
Detected Systems page	Click Menu Systems Detected Systems .
Detected Systems Status page	Click Menu Systems Detected Systems , then click any category in the Overall System Status monitor.

Task

For option definitions, click ? in the interface.

- 1 Select the systems whose Agents you want to query.
- 2 Click **Actions | Detected Systems | Query Agent** or **Actions | Query Agent**. The Query McAfee Agent Results page opens.

Removing systems from the Detected Systems list

Use this task to remove systems from the Detected Systems list. You might want to remove a system from this list when you know it is no longer in service. Once a system has been removed, it does not appear in the Detected Systems list until the next time the system is detected.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**.
- 2 In the Overall System Status monitor, click any detected system category then click the system you want to remove.
- 3 Click **Actions**, select **Detected Systems | Delete**, then click **OK** when prompted.

Removing systems from the Exceptions list

Use this task to remove detected systems from the Exceptions list. You might want to remove systems from this list if you would like to start receiving detection information about it, or you know that the system is no longer connected to your network.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**.

- 2 In the Overall System Status monitor, click the **Exceptions** category, then select the system you want to remove.
- 3 Click **Actions**, select **Detected Systems | Remove from Exceptions**, then click **OK** when prompted.

Removing systems from the Rogue Sensor Blacklist

Use this task to remove detected systems from the **Rogue Sensor Blacklist**. Rogue System Detection prevents sensors from being installed on systems included in the blacklist. If you want to install a sensor on a system that has been blacklisted, you must remove the system from the list.

Task

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

- 1 Click **Menu | Systems | Detected Systems**.
- 2 In the Rogue System Sensor Status monitor, click **View Blacklist**.
- 3 Select the system you want to remove from the Rogue System Blacklist page.
- 4 Click **Actions**, select **Rogue Sensor | Remove from Blacklist**, then click **OK** when prompted.

Viewing detected systems and their details

Use this task to view detected systems and their details. You can view detected system details from any page that displays detected systems.

Task

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

- 1 Click **Menu | Systems | Detected Systems**.
- 2 In the Overall System Status monitor, click any category to view the list of detected systems it contains, such as **Managed**. The Detected Systems page appears.
- 3 Click any detected system to view its details.

NOTE: The System Details page is different than the Detected Systems Details page. The Detected Systems Details page displays some information that is unique to Rogue System Detection.

Working with sensors

Use these tasks when working with sensors, for example, to change install or remove a sensor.

Tasks

- ▶ [Changing the sensor-to-server port number](#)
- ▶ [Installing sensors](#)
- ▶ [Editing sensor descriptions](#)
- ▶ [Removing sensors](#)

Changing the sensor-to-server port number

Use this task to change the sensor-to-server port number. You can change the port that the Rogue System Sensor uses to communicate with the ePO server.

NOTE: The port number specified in the Server Settings page can be changed only during installation of ePolicy Orchestrator. If you changed this port number during installation, you must also change it in the Rogue System Detection policy settings, to allow sensors to communicate with the server.

Task

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

- 1 Click **Menu | Policy | Policy Catalog**, then from the Product drop-down list, select **Rogue System Detection x.x.x**, and from the Category drop-down list, select **General**. All created policies for Rogue System Detection appear in the details pane.
- 2 Locate the desired policy and click **Edit Settings** in its row.
- 3 Under the General tab, change the **Sensor-to-Server Communication Port** to the desired port number, then click **Save**.

Installing sensors

Use any of these tasks to deploy sensors to your network.

Tasks

- ▶ [Installing sensors on specific systems](#)
- ▶ [Using queries and server tasks to install sensors](#)

Installing sensors on specific systems

Use this task to install sensors to specific systems on your network. This task creates a deployment task that installs the sensor to the selected systems, then performs an immediate agent wake-up call on them.

This task can be performed from:	Getting there
Managed Systems for Subnet xxx.xxx.xxx.xxx page	Click Menu Systems Detected Systems , click Covered or Contains Rogues in the Subnet Status monitor, then select any subnet and click View Managed Systems .
Systems Details page	Click Menu Systems System Tree Systems and click any system.
Systems page	Click Menu Systems System Tree .

Task

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

- 1 Select the systems where you want to install sensors, then click **Actions | Rogue Sensor | Install Rogue Sensor**.
 - In the Managed Systems for Subnet xxx.xx.xx.x page, select the systems where you want to install sensors.

- In the Systems Details page, you can install the sensor only from the system you are viewing.
 - In the Systems page, select the desired group in the System Tree, and select the systems where you want to install sensors.
- 2 In the Action pane, click **OK**.

Using queries and server tasks to install sensors

Use this task to create a query that can run as a server task action that installs sensors on managed systems.

Task

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

- 1 Click **Menu | Reporting | Queries**, then click **Actions** and select **New Query**. The Query Builder wizard opens.
- 2 On the Result Type page, select **Managed Systems** and click **Next**.
- 3 From the Display Results As column on the Chart page, expand the **List** display and select **Table**, then click **Next**.
- 4 From the Available Columns pane on the Columns page, click the types of information you want your query to return, then click **Next**.
- 5 On the Filter page, click the properties you want to filter with and specify the values for each, then click **Run**.
- 6 Click **Save** and specify the name of your query and any notes, then click **Save** again.
TIP: McAfee recommends using a product-specific prefix when naming your queries, to keep them organized and make them easier to find. For example, RSD: QueryName.
- 7 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Client Task Builder wizard opens.
- 8 On the Description page, name and describe the task and specify the Schedule status, then click **Next**.
- 9 On the Action page, select **Run Query** from the drop-down list.
- 10 From the Query list, select the query you created. Then from the Language drop-down list, select the language you want for the displayed results.
- 11 Select **Install Rogue Sensor** as the subaction to take on the results of the query, then click **Next**.
- 12 On the Schedule page, specify the schedule for the task, then click **Next**.
- 13 Review the summary of the task, then click **Save**.

Using client tasks to install sensors

Use this task to create a client task that installs sensors to systems on your network.

Task

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

- 1 Click **Menu | Systems | System Tree | Client Tasks**, select a group in the System Tree, then click **Actions | New Task**. The Client Task Builder wizard opens.

- 2 On the Description, type a name for the task you are creating and any notes, then from the Type drop-down list, select **Sensor Deployment** and click **Next**.
- 3 On the Configuration page, select **Install**, then click **Next**.
Select **Run at every policy enforcement** if needed.
- 4 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click **Next**.
- 5 Review the summary, then click **Save**.

Editing sensor descriptions

Use this task to edit sensor descriptions.

This task can be performed from:	Getting there
Rogue System Sensor Details page	Click Menu Systems Detected Systems , click any sensor category in the Rogue System Sensor Status monitor, then click any sensor.
Rogue System Sensor page	Click Menu Systems Detected Systems , then click any sensor category in the Rogue System Sensor Status monitor.

Task

For option definitions, click ? in the interface.

- 1 Select the system whose description you want to edit, click **Actions**, then select **Detected Systems | Edit Description**.
- 2 In the Edit Description pane, type the description, then click **OK**.

Removing sensors

Use this task to remove sensors from specific systems on your network. This task creates a deployment task that removes the sensor from the selected systems, then performs an immediate agent wake-up call on them.

This task can be performed from:	Getting there
Managed Systems for Subnet xxx.xxx.xxx.xxx page	Click Menu Systems Detected Systems , click any Covered or Contains Rogues Systems .
Systems Details page	Click Menu Systems System Tree Systems , then click any system.
Systems page	Click Menu Systems System Tree .

Task

For option definitions, click ? in the interface.

- 1 From the Systems page or Systems Details page, select the systems where you want to remove sensors, then click **Actions | Rogue Sensor | Remove Rogue Sensor**.
 - In the Managed Systems for Subnet xxx.xx.xx.x page, select the systems where you want to remove sensors.
 - In the Systems Details page, you can remove the sensor from only the system you are viewing.

- In the Systems page, select the desired group in the System Tree, then select the systems where you want to remove sensors.
- 2 In the **Action** pane, click **OK**.

Working with subnets

Use these tasks when working with subnets in Rogue System Detection, for example, adding, including, and deleting subnets.

Tasks

- ▶ [Adding subnets](#)
- ▶ [Deleting subnets](#)
- ▶ [Ignoring subnets](#)
- ▶ [Including subnets](#)
- ▶ [Renaming subnets](#)
- ▶ [Viewing detected subnets and their details](#)

Adding subnets

Use this task to add subnets to Rogue System Detection.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**, then in the Subnet Status monitor, click **Add Subnet**. The Add Subnets page appears.
- 2 Choose the method you want to use to add subnets, specify the subnets you want to add, then click **Import**.

Deleting subnets

Use this task to delete subnets from Rogue System Detection.

This task can be performed from:	Getting there
Detected Subnets Details page	Click Menu Systems Detected Systems , click any category in the Subnet Status monitor, then click any subnet.
Detected Subnets page	Click Menu Systems Detected Systems , then click any category in the Subnet Status monitor.

Task

For option definitions, click ? in the interface.

- 1 Select the subnets you want to delete, click **Actions**, then select **Detected Systems | Delete**.
- 2 In the **Delete** confirmation pane, click **Yes**.

Ignoring subnets

Use this task to ignore subnets that you do not want to receive information about.

This task can be performed from:	Getting there
Detected Subnets Details page	Click Menu Systems Detected Systems , click any category in the Subnet Status monitor, then click any subnet.
Detected Subnets page	Click Menu Systems Detected Systems , then click any category in the Subnet Status monitor.
Detected Systems page	Click Menu Systems Detected Systems .

CAUTION: Ignoring a subnet deletes all detected interfaces associated with that subnet. All further detections on that subnet are also ignored. To view the list of ignored subnets click the **Ignored** link in the **Subnet Status** monitor. This link only appears when there are subnets being ignored.

Task

For option definitions, click ? in the interface.

- 1 Select the subnets you want to ignore, click **Actions**, then select **Detected Systems | Ignore**.
- 2 In the Ignore dialog box, click **OK**.
When ignoring a subnet on the Detected Systems page in the Top 25 Subnets list, a dialog box opens. Click **OK**.

Including subnets

Use this task to include subnets that have previously been ignored by Rogue System Detection. This task can be performed by querying ignored subnets using the steps below, or you can include subnets from the Ignored Subnets page. Click the **Ignored** link in the **Subnet Status** monitor on the Detected Systems page to see the list of ignored subnets, where you can optionally choose to include one or more ignored subnets.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Queries**, and query for any ignored subnets. For more information on working with queries, see *Reporting on System Status*.
- 2 On the Unsaved Queries page, click **Include**.
- 3 In the Include dialog box, click **OK**.

Renaming subnets

Use this task to rename subnets.

This task can be performed from:	Getting there
Detected Subnets Details page	Click Menu Systems Detected Systems , click any subnet category in the Subnet Status monitor, then click any subnet.

This task can be performed from:	Getting there
Detected Subnets page	Click Menu Systems Detected Systems , then click any subnet category in the Subnet Status monitor.

Task

For option definitions, click ? in the interface.

- 1 Select the subnet you want to rename, then click **Actions** and select **Detected Systems | Rename**.
- 2 In the Rename dialog box, type the new name for the subnet, then click **OK**.

Viewing detected subnets and their details

Use this task to view detected subnets and their details. You can view detected subnets details from any page that displays detected subnets.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | Detected Systems**.
- 2 In the Subnet Status monitor, click any category to view the list of detected subnets it contains, such as **Covered**. The Detected Subnets page appears and displays the subnets in that category.
- 3 Click any detected subnet to view its details. The Detected Subnet Details page appears.

Rogue System Detection command-line options

You can run command-line options from the client system. You can start the sensor manually from the command-line instead of starting it as a Windows service. You might want to do this if you are testing functionality, or to check the sensor version. The following table lists the run-time command-line options for the sensor.

Switch	Description
--console	Forces the sensor to run as a normal command-line executable; otherwise it must be run as an NT service.
--help	Prints the Help screen and lists available command-line options.
--install	Registers the sensor with the Windows Service Control Manager.
--port	Overrides the Server Port configuration setting in the registry that you specified during installation. NOTE: This parameter takes effect only when running in command-line mode, which also requires the --console command-line switch. Sample syntax: sensor.exe --port "8081" --console

Switch	Description
--server "[server name]" or "[IP address]"	<p>Overrides the Server Name configuration setting in the registry that you specified during installation.</p> <p>NOTE: This parameter takes effect only when running in command-line mode, which also requires the --console command-line switch.</p> <p>Sample syntax:</p> <pre>sensor.exe --server "MyServerName" --console</pre>
--uninstall	Unregisters the sensor with the Windows Service Control Manager.
--version	Prints the version of the sensor and exits.

Default Rogue System Detection queries

Rogue System Detection provides default queries that you can use to retrieve specific information from your network. These queries can be modified or duplicated in the same manner as other queries in ePolicy Orchestrator. You can also create custom queries, display query results in dashboard monitors, and add those dashboard monitors to the Dashboards section in ePolicy Orchestrator. For more information on using dashboards, see *Assessing Your Environment With Dashboards*.

Rogue System Detection query definitions

Query	Definition
Active Sensor Response (Last 24 Hours)	Returns the details of active sensors installed on your network in the last 24 hours, in pie chart format.
Passive Sensor Response (Last 24 Hours)	Returns the details of passive sensors installed on your network in the last 24 hours, in pie chart format.
Rogue Systems, By Domain (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by domain, in table format.
Rogue Systems, By OS (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by operating system, in pie chart format.
Rogue Systems, By OUI (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by organizationally unique identifier, in pie chart format.
Subnet Coverage	Returns the details of detected subnets on your network, in pie chart format.

Setting Up Automatic Responses

The ePolicy Orchestrator Automatic Responses feature alerts you to events that occur on your managed systems or on the ePO server, then takes designated actions on those events. You can configure responses to specific events that are received and processed by the ePolicy Orchestrator server. When a response is triggered, a user-configured action is carried out. These actions include:

- Send email messages
- Send SNMP traps
- Run external commands
- Schedule server task
- Create issues

The ability to specify the event categories that generate a notification message and the frequencies with which such messages are sent are highly configurable.

This feature is designed to create user-configured notifications and actions when the conditions of a rule are met. These include, but are not limited to:

- Detection of threats by your anti-virus software product. Although many anti-virus software products are supported, events from VirusScan Enterprise include the IP address of the source attacker so that you can isolate the system infecting the rest of your environment.
- Outbreak situations. For example, 1000 virus-detected events are received within five minutes.
- High-level compliance of ePolicy Orchestrator server events. For example, a repository update or a replication task failed.
- Detection of new rogue systems.

Are you creating an Automatic Response rule for the first time?

When creating a new automatic response rule for the first time:

- 1** Understand Automatic Responses and how it works with the System Tree and your network.
- 2** Plan your implementation. Which users need to know about which events?
- 3** Prepare the components and permissions used with Automatic Responses, including:
 - Automatic Responses permissions — Create or edit permission sets and ensure that they are assigned to the appropriate ePO users.
 - Email server — Configure the email (SMTP) server at **Server Settings**.
 - Email contacts list — Specify the list from which you select recipients of notification messages at **Contacts**.
 - Registered executables — Specify a list of registered executables to run when the conditions of a rule are met.
 - Rogue System Detection permission — Create or edit permission sets and ensure that they are assigned to the appropriate ePO users.

- Server tasks — Create server tasks for use as actions to be carried out as a result of a response rule.
- SNMP servers — Specify a list of SNMP servers to use while creating rules. You can configure rules to send SNMP traps to SNMP servers when the conditions are met to initiate a notification message.

Contents

- ▶ [Automatic Responses and how it works](#)
- ▶ [Planning](#)
- ▶ [Determining how events are forwarded](#)
- ▶ [Configuring Automatic Responses](#)
- ▶ [Creating and editing Automatic Response rules](#)

Automatic Responses and how it works

Before you plan the implementation of Automatic Responses, you should understand how this feature works with ePolicy Orchestrator and the System Tree.

NOTE: This feature does not follow the inheritance model used when enforcing policies.

Automatic Responses use events that occur on systems in your environment that are delivered to the server and configured response rules associated with the group that contains the affected systems and each parent above it. If the conditions of any such rule are met, designated actions are taken, per the rule's configurations.

This design allows you to configure independent rules at different levels of the System Tree. These rules can have different:

- **Thresholds for sending a notification message.** For example, an administrator of a particular group wants to be notified if viruses are detected on 100 systems within 10 minutes on the group, but a global administrator does not want to be notified unless viruses are detected on 1,000 systems within the entire environment in the same amount of time.
- **Recipients for the notification message.** For example, an administrator for a particular group wants to be notified only if a specified number of virus detection events occur within the group. Or, a global administrator wants each group administrator to be notified if a specified number of virus detection events occur within the entire System Tree.

NOTE: 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
- Grouping

Aggregation

Use aggregation to determine the thresholds of events when the rule sends a notification message. For example, configure the same rule to send a notification message when the server

receives 1,000 virus detection events from different systems within an hour *or* whenever it has received 100 virus detection events from any system.

Throttling

Once you have configured the rule to notify you of a possible outbreak, use throttling to ensure that you do not receive too many notification messages. If you are administering a large network, you might be receiving tens of thousands of events during an hour, creating thousands of notification messages based on such a rule. Responses allows you to throttle the number of notification messages you receive based on a single rule. For example, you can specify in this same rule that you don't want to receive more than one notification message in an hour.

Grouping

Use grouping to combine multiple aggregated events. For example, events with the same severity can be combined into a single group. Grouping allows an administrator to take actions on all the events with the same and higher severity at once. It also allows you to prioritize the events generated at managed systems or at servers.

Default rules

ePolicy Orchestrator provides four default rules that you can enable for immediate use while you learn more about the feature.

Before enabling any of the default rules:

- Specify the email server (click **Menu | Configuration | Server Settings**) from which the notification messages are sent.
- Ensure the recipient email address is the one you want to receive email messages. This address is configured on the Actions page of the wizard.

Default notification rules

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.
RSD: Query New Rogue Detection	New rogue system detected	Queries the newly detected system for a McAfee Agent.

Planning

Before creating rules that send notifications, save time by planning:

- The event type and group (product and server) that trigger notification messages in your environment.
- Who should receive which notification messages. For example, it might not be necessary to notify the administrator of group B about a failed replication in group A, but you might want all administrators to know that an infected file was discovered in group A.
- Which types and levels of thresholds you want to set for each rule. For example, you might not want to receive an email message every time an infected file is detected during an outbreak. Instead, you can choose to have such a message sent at most once every five minutes, regardless of how often that server is receiving the event.
- Which commands or registered executables you want to run when the conditions of a rule are met.
- Which server task you want to run when the conditions of a rule are met.

Determining how events are forwarded

Use these tasks to determine when events are forwarded and which events are forwarded immediately.

The server receives event notifications from McAfee Agents. You can configure agent policies to forward events either immediately to the server or only at agent-to-server communication intervals.

If you choose to send events immediately (as set by default), the agent forwards all events as soon as they are received.

NOTE: 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 Settings**).

If you choose not to have all events sent immediately, the agent forwards immediately only events that are designated by the issuing product as high priority. Other events are sent only at the agent-server communication.

Tasks

- ▶ [Determining which events are forwarded immediately](#)
- ▶ [Determining which events are forwarded](#)

Determining which events are forwarded immediately

Use this task to determine whether events are forwarded immediately or only at the agent-to-server communication interval.

If the currently applied policy is not set for immediate uploading of events, either edit the currently applied policy or create a new McAfee Agent policy. This setting is configured on the Threat Event Log page.

Task

For option definitions click ? in the interface.

- 1 Click **Menu | Policy | Policy Catalog**, then click **Product | McAfee Agent**.
- 2 Click **Edit Settings** of an existing agent policy.
- 3 On the Events tab, select **Enable priority event forwarding**.
- 4 Select the event severity. Events of the selected severity (and greater) are forwarded immediately to the server.
- 5 To regulate traffic, type an **Interval between uploads** (in minutes).
- 6 To regulate traffic size, type the **Maximum number of events per upload**.
- 7 Click **Save**.

Determining which events are forwarded

Use this task to determine which events are forwarded to the server.

Task

For option definitions click ? in the interface.

- 1 Click **Menu | Configuration | Server Settings**, select **Event Filtering**, then click **Edit**.
- 2 Select the desired events, then click **Save**.

These settings take effect once all agents have called in.

Configuring Automatic Responses

Use these tasks to configure the necessary resources to fully leverage Automatic Responses.

Tasks

- ▶ [Assigning permission sets to access Automatic Responses](#)
- ▶ [Working with SNMP servers](#)
- ▶ [Working with registered executables and external commands](#)

Assigning permission sets to access Automatic Responses

Use these tasks to assign the appropriate permission sets to access the Automatic Responses feature. There are two permission sets specific to the Automatic Responses feature:

- Automatic Responses
- Event Notifications

Users accessing this feature require additional permissions, depending on the specific component used. For example, to create an automatic response that triggers a predefined server task, users need full rights to the **Server tasks** permission sets. Additional permission sets that might be required include:

- Client Events
- Contacts
- Event Notifications

- Issue Management
- Queries
- Registered servers
- Rogue System Detection
- System Tree access
- Threat Event log

Tasks

- ▶ [Assigning permissions to Notifications](#)
- ▶ [Assigning permissions to Automatic Responses](#)

Assigning permissions to Notifications

Use this task to ensure that all desired administrators and users have the appropriate permissions to Notifications. The permissions to Notification enables ePO users to add registered executables.

Task

For option definitions click ? in the interface.

- 1 Click **Menu | User Management | Permission Sets**, then select either **New Permission Set** or an existing one.
- 2 Next to **Event Notifications**, click **Edit**.
- 3 Select the desired Notifications permission:
 - **No permissions**
 - **View registered executables**
 - **Create and edit registered executables**
 - **View rules and notifications for entire System Tree (overrides System Tree group access permissions)**
- 4 Click **Save**.
- 5 If you created a new permission set, click **Menu | User Management | Users**.
- 6 Select a user to assign the new permission set to, then click **Edit**.
- 7 Next to **Permission sets**, select the checkbox for the permission set with the desired Notifications permissions, then click **Save**.

Assigning permissions to Automatic Responses

Use this task to ensure that all desired administrators and users have the appropriate permissions to Responses. The permissions to Responses enables ePO users to create response rules for different event types and groups.

NOTE: Users need permissions to Threat Event Log, Server Tasks, Detected Systems, and Systems Tree to create a response rule.

Task

For option definitions click ? in the interface.

- 1 Click **Menu | User Management | Permission Sets**, then select either **New Permission Set** or an existing one.

- 2 Next to **Automatic Response**, click **Edit**.
- 3 Select the desired Automatic Response permission:
 - **No permissions**
 - **View Responses; view Response results in the Server Task Log**
 - **Create, edit, view, and cancel Responses; view Response results in the Server Task Log**
- 4 Click **Save**.
- 5 If you created a new permission set, click **Menu | User Management | Users**.
- 6 Select a user to assign the new permission set to, then click **Edit**.
- 7 Next to **Permission sets**, select the checkbox for the permission set with the desired Automatic Response permissions, then click **Save**.

Working with SNMP servers

Use these tasks to configure Responses to use your SNMP server. You can configure Responses to send SNMP (Simple Network Management Protocol) traps to your SNMP server, which allows you to receive SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment.

NOTE: You do not need to make other configurations or start any services to configure this feature.

Tasks

- ▶ [Editing SNMP servers](#)
- ▶ [Deleting an SNMP server](#)
- ▶ [Importing .MIB files](#)

Editing SNMP servers

Use this task to edit existing SNMP server entries.

Task

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

- 1 Click **Menu | Configuration | Registered Servers**.
- 2 From the list of registered server, select the desired SNMP server, then click **Actions | Edit**.
- 3 Edit the following server information as needed, then click **Save**.

Option	Definition
Address	Type the address of the SNMP server. Valid formats include: <ul style="list-style-type: none">• DNS Name — Specifies the DNS Name of the server. For example, myhost.mycompany.com.• IPv4 — Specifies the IPv4 address of the server (xxx.xxx.xxx.xxx/yy).• IPv6 — Specifies the IPv6 address of the server (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/yyy).
Security	Specifies the security details of the SNMP server. <ul style="list-style-type: none">• Community — Specifies the community name of the SNMP protocol.

Option	Definition
	<ul style="list-style-type: none"> • SNMPv3 Security — Specifies the SNMPv3 security details. This field is enabled only if the version of the server is v3. <ul style="list-style-type: none"> • Security Name — Specifies the name of the security settings for the SNMP server. • Authentication Protocol — Specifies the protocol used by the SNMP server for verification of the source. • Authentication Passphrase — Specifies the password for protocol verification. • Confirm Authentication Passphrase — Retype the password for protocol verification. • Privacy Protocol — Specifies the protocol used by the SNMP server to customize the privacy defined by the user. <p>NOTE: If you select AES 192 or AES 245, you must replace the default policy files with the "unlimited strength" version from Sun's Java SE Downloads site. Find the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 download. To apply the unlimited strength policies to the ePO server, replace the policy jar files in directory EPO_DIR/jre/lib/security with those downloaded in the jce_pocliy-6.zip, and restart the ePO server.</p> • Privacy Passphrase — Specifies the password for privacy protocol settings. • Confirm Privacy Passphrase — Retype the password for privacy protocol settings.
SNMP Version	Specifies the SNMP version your server uses.
Send Test Trap	Tests your configuration.

Deleting an SNMP server

Use this task to delete an SNMP server from Notifications.

Task

For option definitions click ? in the interface.

- 1 Click **Menu | Configuration | Registered Servers**.
- 2 From the list of registered servers, select the desired SNMP server, then click **Actions | Delete**.
- 3 When prompted, click **Yes**.

The SNMP server is removed from the Registered Servers list.

Importing .MIB files

Use this task when setting up rules to send notification messages to an SNMP server via an SNMP trap. You must import three .mib files from \Program Files\McAfee\ePolicy Orchestrator\MIB. The files must be imported in the following order:

- 1 NAI-MIB.mib
- 2 TVD-MIB.mib
- 3 EPO-MIB.mib

These files allow your network management program to decode the data in the SNMP traps into meaningful text. The EPO-MIB.mib file depends on the other two files to define the following traps:

- **epoThreatEvent** — This trap is sent when an Automatic Response for an 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 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 ePO Client Status Event is triggered. It contains variables that match the properties of the Client Status event.
- **rsdAddDetectedSystemEvent** — This trap is sent when an Automatic Response for a Rogue System Detected event is triggered. It contains variables that match the properties of the Rogue System Detected event.
- **epoTestEvent** — This is a test trap that is sent when you click **Send Test Trap** in the New SNMP Server or Edit SNMP Server pages.

For instructions on importing and implementing .mib files, see the product documentation for your network management program.

Working with registered executables and external commands

Use these tasks when working with registered executables and external commands. You can configure automatic response rules to run an external command when the rule is initiated.

Before you begin

- Before creating a response rule to run an external command, place the registered executables at a location on the server where the rules can point.
- You must have appropriate permissions to perform these tasks.
- You must use a browser session from the ePO server system.

NOTE: For security purposes, registered executables cannot be added or edited unless you have permission to modify the server system.

Tasks

- ▶ [Adding registered executables](#)
- ▶ [Editing registered executables](#)
- ▶ [Deleting registered executables](#)

Adding registered executables

Use this task to add registered executables to your available resources. You can run external command action by providing the registered executables and their arguments.

Before you begin

You must have appropriate permissions to perform this task.

You must use a browser session from the ePO server system.

Task

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

- 1 Click **Menu | Configuration | Registered Executables**, then click **Actions | New Registered Executable**. The New Registered Executable page appears.
- 2 Type a name for the registered executable.
- 3 Type the path or browse to and select the registered executable that you want a rule to execute when triggered, then click **Save**.

The new registered executable appears in the Registered Executables list.

Editing registered executables

Use this task to edit an existing registered executable entry.

Before you begin

You must have appropriate permissions to perform this task.

You must use a browser session from the ePO server system.

Task

- 1 Click **Menu | Configuration | Registered Executables**, then select **edit** next to the desired executable in the list. The Edit Registered Executable page appears.
- 2 Edit the name or select a different executable on the system, then click **Save**.

Deleting registered executables

Use this task to delete a registered executable entry.

Before you begin

- You must have appropriate permissions to perform this task.
- You must use a browser session from the ePO server system.

Task

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

- 1 Click **Menu | Configuration | Registered Executables**, then select **Delete** next to the desired executable in the list.
- 2 When prompted, click **OK**.

Duplicating registered executables

Use this task to duplicate a registered executables to your available resources.

Before you begin

You must have appropriate permissions to perform this task.

You must use a browser session from the ePO server system.

Task

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

- 1 Click **Menu | Configuration | Registered Executables**, then click **Duplicate** next to the desired registered executable. The Duplicate Registered Executable dialog box appears.
- 2 Type a name for the registered executable, then click **OK**.

The duplicated registered executable appears in the Registered Executables list.

Creating and editing Automatic Response rules

Use these tasks to create and edit Automatic Response rules. These tasks allow you to define when and how a response can be taken on the event occurring either at the server or at a managed system.

NOTE: Automatic Response rules do not have a dependency order.

Tasks

- ▶ [Describing the rule](#)
- ▶ [Setting filters for the rule](#)
- ▶ [Setting thresholds of the rule](#)
- ▶ [Configuring the action for Automatic Response rules](#)

Describing the rule

Use this task to begin creating a rule. The Description page of the Response Builder wizard allows you to:

- Name and describe the rule.
- Specify the language used by the response.
- Specify the event type and group that triggers this response.
- Enable or disable the rule.

Task

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

- 1 Click **Menu | Automation | Automatic Responses**, then click **Actions | New Response**, or **Edit** next to an existing rule. The Response Builder wizard opens.

The screenshot shows the 'Response Builder' wizard at the '1 Description' step. The interface includes a progress bar at the top with steps: 1 Description, 2 Filter, 3 Aggregation, and 4 Action. Below the progress bar is a question: 'What is this response's name, target language, and event type? Is the response enabled?'. The form contains the following fields:

- Name:** A text input field containing 'Distributed Repository Replication failed'.
- Description:** A text area containing 'Sends an e-mail notification when "Distributed Repository Replication failed" events are received.' with up and down arrow icons on the right.
- Language:** A dropdown menu set to 'English'.
- Event:** Two dropdown menus. The first is labeled 'Event group:' and is set to 'ePO Notification Events'. The second is labeled 'Event type:' and is set to 'Server'.
- Status:** Two radio buttons. 'Enabled' is unselected, and 'Disabled' is selected.

Figure 14: Notifications Rules page

- 2 On the Description page, type a unique name and any notes for the rule.
NOTE: Rule names on each server must be unique. For example, if one user creates a rule named Emergency Alert, no other user (including global administrators) can create a rule with that name.
- 3 From the Language menu, select the language the rule uses.
- 4 Select the **Event group** and **Event type** that trigger this response.
- 5 Select whether the rule is **Enabled** or **Disabled** next to Status.
- 6 Click **Next**.

Setting filters for the rule

Use this task to set the filters for the response rule on the Filters page of the Response Builder wizard.

Task

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

- 1 From the Available Properties list, select the desired property and specify the value to filter the response result.

NOTE: Available Properties depend on the event type and event group selected on the Description page of the wizard.

- 2 Click **Next**.

Setting thresholds of the rule

Use this task to define when the event triggers the rule on the Aggregation page of the Response Builder wizard.

A rule's thresholds are a combination of aggregation, throttling, and grouping.

Task

For option definitions click ? in the interface.

- 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.

NOTE: You can select one or both options. For example, you can set the rule to trigger this response if the distinct value of occurrence of event property selected exceeds 300, or when the number of events exceeds 3,000, whichever threshold is crossed first.
- 3 Next to Grouping, select whether to group the aggregated events. If you select to group the aggregated events, specify the property of event on which they are grouped.
- 4 As needed, next to Throttling, select **At most, trigger this response once every** and define an amount of time that must be passed before this rule can send notification messages again. The amount of time can be defined in minutes, hours, or days.
- 5 Click **Next**.

Configuring the action for Automatic Response rules

Use this task to configure the responses that are triggered by the rule on the Responses page of the Response Builder wizard.

You can configure the rule to trigger multiple actions by using the + and - buttons, located next to the drop-down list for the type of notification.

Task

For option definition click ? in the interface.

- 1 If you want the notification message to be sent as an email or text pager message, select **Send Email** from the drop-down list.
 - a Next to Recipients, click ... and select the recipients for the message. This list of available recipients is taken from Contacts (**Menu | User Management | Contacts**). Alternatively, you can manually type email addresses, separated by a comma.
 - b Select the importance of the notification email.
 - c Type the **Subject** of the message. Optionally, you can insert any of the available variables directly into the subject.
 - d Type any text that you want to appear in the **Body** of the message. Optionally, you can insert any of the available variables directly into the body.
 - e Click **Next** if finished, or click + to add another notification.
- 2 If you want the notification message to be sent as an SNMP trap, select **Send SNMP Trap** from the drop-down list.
 - a Select the desired SNMP server from the drop-down list.

- b** Select the type of value that you want to send in the SNMP trap.
 - **Value**
 - **Number of Distinct Values**
 - **List of Distinct Values**
 - **List of All Values**
 - NOTE:** Some events do not include this information. If a selection you made is not represented, the information was not available in the event file.
 - c** Click **Next** if finished, or click **+** to add another notification.
 - 3** If you want the notification to run an external command, select **Run External Command** from the drop-down list.
 - a** Select the desired **Registered Executables** and type any **Arguments** for the command.
 - b** Click **Next** if finished, or click **+** to add another notification.
 - 4** If you want the notification to create an issue, select **Create issue** from the drop-down list.
 - a** Select the type of issue that you want to create.
 - b** Type a unique name and any notes for the issue. Optionally, you can insert any of the available variables directly into the name and description.
 - c** Select the **State, Priority, Severity, and Resolution** for the issue from the respective drop-down list.
 - d** Type the name of the assignee in the text box.
 - e** Click **Next** if finished, or click **+** to add another notification.
 - 5** If you want the notification to run a scheduled task, select **Execute Scheduled Task** from the drop-down list.
 - a** Select the task that you want to run from the **Task to execute** drop-down list.
 - b** Click **Next** if finished, or click **+** to add another notification.
 - 6** On the Summary page, verify the information, then click **Save**.

The new response rule appears in the Responses list.

Frequently asked questions

If I set up a response rule for virus detections, do I have to receive a notification message for each event received during an outbreak.

No. You can configure rules so that a notification can be sent only once per specified quantity of events within a specified amount of time, or sent at a maximum of once in a specified amount of time.

Can I create a rule that generates notifications to multiple recipients?

Yes. You can enter multiple email addresses for recipients in the Response Builder wizard.

Can I create a rule that generates multiple types of notifications?

Yes. Notifications for ePolicy Orchestrator supports any combination of the following notification targets for each rule:

- Email (including standard SMTP, SMS, and text pager)
- SNMP servers (via SNMP traps)
- Any external tool installed on the ePolicy Orchestrator server
- Issues
- Scheduled server tasks

Managing Issues and Tickets

The Issues feature of ePolicy Orchestrator allows you to create, modify, assign, and track issues. Issues are action items that can be prioritized, assigned, and tracked.

Issues

Users can create basic issues manually or the ePO server can automatically create issues in response to product events. For example, users with the proper permissions can configure McAfee Policy Auditor to automatically create a Benchmark Rule Compliance issue if a noncompliant system is discovered during an audit.

Tickets

A ticket is the external equivalent of an issue that exists in a ticketing server. Once a ticket is added to an issue, the issue is referred to as a "ticketed issue." A ticketed issue can have only one associated ticket.

Integrating issues with third-party ticketing servers

Integration of a ticketing server forces the creation of tickets associated with issues that were created in products. ePolicy Orchestrator supports these ticketing servers:

- **Hewlett-Packard Openview Service Desk versions 4.5 and 5.1** — an integrated help desk and trouble ticketing solution.
- **BMC Remedy Action Request System versions 6.3 and 7.0** — a consolidated platform for automating and managing trouble tickets.

Contents

- ▶ [Creating, configuring, and managing issues](#)
- ▶ [Purging closed issues](#)
- ▶ [Tickets and how they work](#)
- ▶ [Integration with ticketing servers](#)
- ▶ [Working with tickets](#)
- ▶ [Working with ticketing servers](#)
- ▶ [Upgrading a registered ticketing server](#)

Ways to manage issues

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, due date, and assignee are all user-defined, and can be changed any time. You can also specify default issue responses from the Responses page. The 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 Product Feature Name 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 manually and automatically purged through a user-configured server task.

Creating, configuring, and managing issues

Use these tasks to create, assign, view details of, edit, delete, and purge issues.

Tasks

- ▶ [Creating basic issues manually](#)
- ▶ [Configuring responses to automatically create issues](#)
- ▶ [Managing issues](#)
- ▶ [Purging closed issues manually](#)
- ▶ [Purging closed issues on a schedule](#)

Creating basic issues manually

Use this task to manually create a basic issue. Issues that are non-basic 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. an issue type. Click **OK**. The New Issue page appears.

Use this...	To do this...
Assignee	Type the user name of the person assigned to the issue.
Description	Type a meaningful description of the issue.
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.
Name	Type a meaningful name for the issue.
Priority	Assign a priority to the issue: <ul style="list-style-type: none">• Unknown• Lowest• Low• Medium• High• Highest
State	Assign a state to the issue: <ul style="list-style-type: none">• Unknown• New• Assign• Resolved

Use this...	To do this...
	<ul style="list-style-type: none"> • Closed
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

3 Click **Save**. The Issues page appears.

Configuring responses to automatically create issues

Use this task to configure responses to automatically create issues.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

1 Click **Menu | Automation | Automatic Responses**, then click **Actions** and select **New Response**. The Description page of the Response Builder appears.

Use this...	To do this...
Name	Type a meaningful name for the response.
Description	Type a description of the response.
Event	<ul style="list-style-type: none"> • Event group — Select an event group, such as Benchmark Compliance Event. • Event type — Select an event type that is part of the event group, such as Benchmark Rule Compliance Event.
Status	Enable or disable the response.

2 Click **Next**. The Filter page appears.

3 Select properties to narrow the events that trigger the response.

4 Click **Next**. The Aggregation page appears.

5 Next to Aggregation, select one:

- **Trigger this response for every event** — generates a response for every event.

- **Trigger this response if multiple events occur within** — generates a response for multiple events that occur during a specified time period and, if needed, after a certain number of events have occurred.
- 6 Next to Grouping, select one:
- **Do not group aggregated events** — events of the same type are not aggregated.
 - **Group aggregated events by** — a property of the event. For example, if you narrow your events by audit, you can aggregate events that are noncompliant with the audit.
- 7 Next to Throttling select the maximum time period that you want this response to occur.

Response Builder 1 Description 2 Filter 3 Aggregation 4 Actions

What kind of aggregation, grouping, and throttling behavior should this response have?

Aggregation:

Trigger this response for every event.

Trigger this response if multiple events occur within: 30 minutes

When the number of distinct values for an event property is at least a certain value.

Property: Agent GUID Number of distinct values: 100

or

When the number of events is at least: 50

Grouping:

Do not group aggregated events.

Group aggregated events by: Agent GUID

Throttling:

At most, trigger this response once every: 1 seconds

- 8 Click **Next**. The Actions page appears. Use this page to select the actions to perform when the response is triggered.
- 9 Select **Create issue** from the drop-down list. Select the type of issue to create. This choice determines the options that appear on this page.
- 10 Type a name and description for the issue. Optionally, select one or more variables for the name and description. This feature provides an number of variables providing information to help fix the issue.

Response Builder 1 Description 2 Filter 3 Aggregation 4 Actions

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

Create issue

Create issue of type: Basic

Name:

Insert variable: Value Response Name Insert

Description:

Insert variable: Value Response Name Insert

State: Unknown

Priority: Unknown

Severity: Unknown

Resolution: None

Assignee:

11 If applicable, type or select the appropriate

Use this...	To do this...
State	Assign a state to the issue: <ul style="list-style-type: none"> • Unknown • New • Assigned • Resolved • Closed
Priority	Assign a priority to the issue: <ul style="list-style-type: none"> • Unknown • Lowest • Low • Medium • High • Highest
State	Assign a state to the issue: <ul style="list-style-type: none"> • Unknown • New • Assign • Resolved • Closed
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.

12 Type the user to whom you want the issue assigned. The assignee must have select one or more variables for the name and description. This feature provides an number of variables providing information to help fix the issue.

Response Builder 1. Description 2. Filter 3. Aggregation 4. Actions

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

▼ Create issue ▼

Create issue of type: Basic ▼

Name: *
 Insert variable: Value ▼ Response Name ▼ Insert

Description: *
 Insert variable: Value ▼ Response Name ▼ Insert

State: Unknown ▼

Priority: Unknown ▼

Severity: Unknown ▼

Resolution: None ▼

Assignee:

13 If applicable, type or select the appropriate

Use this...	To do this...
State	Assign a state to the issue: <ul style="list-style-type: none"> • Unknown • New • Assigned • Resolved • Closed
Priority	Assign a priority to the issue: <ul style="list-style-type: none"> • Unknown • Lowest • Low • Medium • High • Highest
State	Assign a state to the issue: <ul style="list-style-type: none"> • Unknown • New • Assign • Resolved • Closed
Severity	Assign a severity to the issue: <ul style="list-style-type: none"> • Unknown • Lowest • Low • Medium • High

Use this...	To do this...
	<ul style="list-style-type: none"> • 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.

- 14** Type the user to whom you want the issue assigned. The assignee must have a user account in the system.
- 15** Click **Next**. The Summary page appears.
- 16** Review the details for the response, then click **Save**.

Managing issues

Use this task to add comments, assign, delete, edit, and view details of issues.

Before you begin

You must have appropriate permissions to perform these tasks.

Task

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

- 1** Click **Menu | Automation | Issues**,
- 2** Perform the tasks that you want.

Task	Do this...
Adding comments to issues	<ol style="list-style-type: none"> 1 Select the checkbox next to each issue you want to comment, then click Add comment. 2 In the Action 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 .
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.
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.

Task	Do this...
	3 Click Save . NOTE: Editing an issue breaks the issue-ticket connection.
Viewing issue details	Click an issue. The Issue Details page appears. This page shows all of the settings for the issue as well as the Issues Activity Log.

Purging closed issues

Use these tasks to purge closed issues from the database. Purging closed issues deletes them permanently. Purging a closed ticketing issue deletes the issue, but the associated ticket remains in the ticketing server database.

Tasks

- ▶ [Purging closed issues manually](#)
- ▶ [Purging closed issues on a schedule](#)

Purging closed issues manually

Use this task to manually purge all closed issues from the database.

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.

NOTE: This function affects all closed issues; not just those in the current view.

Purging closed issues on a schedule

Use this task to purge closed issues with a scheduled server task.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**. The Description page of the Server Task Builder appears.
- 2 Type a name and description for the server task.
- 3 Enable or disable the schedule for the server task. The server task does not run until it is enabled.

- 4 Click **Next**. The Actions page appears.
- 5 From the drop-down list, select **Purge Closed Issues**.
- 6 Type a number, then select a time unit.
- 7 Click **Next**. The Schedule page appears.
- 8 Schedule the server task, then click **Next**. The Summary page appears.
- 9 Review the details of the server task, then click **Save**. The closed issues are purged at the time of the scheduled task.

Tickets and how they work

A ticket is the external equivalent of an issue that exists in a ticketing server. Once a ticket is added to an issue, the issue is referred to as a "ticketed issue."

Ways to add tickets to issues

A ticket can be added to an issue manually or automatically. A ticketed issue can have only one associated ticket.

When a ticket is added to an issue, the state of the resulting ticketed issue is changed to Ticketed, regardless of the issue's status prior to being ticketed. When the ticket is created in the ticketing server, that ticket's ID is added to the ticketed issue. The ticket ID creates the ticket-to-issue association.

After the steps for integrating a ticketing server are completed, all subsequent issues are ticketed automatically. McAfee recommends always adding an assignee to an issue before the ticket is created. If an assignee is added manually to a ticketed issue, you must add tickets manually to any issues that existed prior to the integration.

Assignment of ticketed issues to users

Adding an assignee manually to a ticketed issue is considered editing an issue, which breaks the issue-to-ticket association. Do this by specifying an assignee in the response, which creates issues. In this way, an assignee is added to the issue automatically when it is created. For details, see *How tickets and ticketed issues are closed*.

How tickets and ticketed issues are closed

Ticketed issues are closed automatically by the system when the server task, which synchronizes ticketed issues, runs. This server task identifies tickets that changed to the Closed state since the last time the task ran. The status of a ticketed issue associated with a closed ticket is then changed to Closed. Also, that ticket's comments replace the comments in the ticketed issue if the integration of the ticketing server was configured to overwrite ticketed issue comments. For details, see *Benefits of adding comments to ticketed issues*.

Benefits of adding comments to ticketed issues

When a comment is added to a ticketed issue, it is added to the associated ticket immediately or the next time the Issue Synchronization server task runs. Ticketed issue comments are added only to tickets that are not in the Closed state.

If the ticketing server allows issue comments to be overwritten by ticket comments, when a ticket's state becomes Closed, comments for that ticket replace all comments in the associated ticketed issue. This process is performed when the server task, which synchronizes ticketed issues, identifies a ticket whose state changed to Closed since the last time the task was run. This task is performed only once for each closed ticket. Allowing issue comments to be overwritten by ticket comments can allow users with access to the system (but not to the ticketing server) the ability to see what happened to the ticket.

How tickets are reopened

A ticket is reopened when it is added to a previously added ticketed issue, whose ID can be matched to a ticket in the ticketing server. If the ID cannot be matched, a new ticket is created. Reopening a ticket does not reopen the associated ticket issue. The configuration mapping for the ticketing server must also be configured to allow tickets to be reopened. See *Required fields for mapping*.

Synchronization of ticketed issues

The Issues feature includes the Issue Synchronization server task, which synchronizes ticketed issues with their associated tickets in the ticketing server. This server task is disabled by default; it will not run until enabled.

When this server task runs, the system attempts to:

- Change the status of ticketed issues from Ticketed to Closed if the state of their associated tickets is closed.
- Create tickets for issues or add comments to tickets that the system was unable to create or add previously. For example, if a communication error occurred when the tickets or the comments were first added.
- Replace the comments of a ticketed issue with the comments of its associated ticket if the ticket's state is Closed, and the integration of the ticketing server was configured to overwrite ticketed issue comments.
- Change the state of each ticketed issue to Assigned if the ticketed issue does not have an assignee specified, or New if the registered server for the ticketing server is deleted.

Integration with ticketing servers

Integration of a ticketing server forces the creation of tickets associated with issues that were created in products. ePolicy Orchestrator supports these ticketing servers:

- **Hewlett-Packard Openview Service Desk versions 4.5 and 5.1** — an integrated help desk and trouble ticketing solution.
- **BMC Remedy Action Request System versions 6.3 and 7.0** — a consolidated platform for automating and managing trouble tickets.

The person who performs this integration should be familiar with the ticketing server and its fields and forms. Integrating a ticketing server consists of these basic steps:

- 1 Configure ePolicy Orchestrator to integrate with the ticketing server.

NOTE: The system running the ticketing extension must be able to resolve the address of the Hewlett-Packard Openview Service Desk system. This might involve adding the IP address of the Service Desk system to the hosts file on the system running the ticketing

extension, or setting up a domain trust between the two systems. See *Configuring the DNS for Service Desk 4.5*.

- 2 Integrate a ticketing server with ePolicy Orchestrator. Only one registered ticketing server can be integrated with ePolicy Orchestrator.
- 3 Configure the field mappings between issues and tickets.

Considerations when deleting a registered ticketing server

There might be times when you want to delete the registered server for your ticketing server. For example, if you upgrade your ticketing server. When the registered server is deleted, the system changes the state of each ticketed issue to Assigned, or to New if the ticketed issue does not have a specified assignee. The system only performs this action when the server task, which synchronizes ticketed issues, runs. This is why it is important to disable that server task if you are upgrading the ticketing server. For more details, see the section in this guide about upgrading registered ticketing servers.

When the registered ticketing server is deleted, the ticket ID that associated the ticket to the ticketed issue remains with that ticketed issue. This allows the ticket to be reopened if the issue-to-ticket association is broken. For example, if the server task runs before the upgraded server is registered. See the *How tickets are reopened* and *Upgrading a registered ticketing server*.

Required fields for mapping

Mapping is the process by which information in issues is mapped to information in tickets. Each piece of information is called a field, and the fields in issues need to be mapped to corresponding fields in tickets.

To determine which ticket fields must be mapped, on the ticketing form review the fields required to create a ticket in the ticketing server. For information about which fields are required, see the documentation for your ticketing server.

For the system to know when to close ticketed issues, the field with the ticket's state must be mapped.

Sample mappings

When you register your ticketing server, you must also configure the field mappings for issues and tickets. The field mappings in the following examples are provided for reference only. Your mappings will vary based on the fields required in your ticketing server and the values those fields accept.

Mapping is a two-way process. These examples demonstrate how to map an issue to a ticket and to map the ticket's status back to the issue's status. For example, if the ticket is marked as closed, the issue status will be updated to show that it is closed.

Sample mapping for Hewlett-Packard Openview Service Desk

This is a reference-only sample mapping for Hewlett-Packard Openview Service Desk versions 4.5 and 5.1.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

Map Issue to Ticket

- **Ticket form:** Default_Problem
- **Ticket field:** Description
 - **Operation:** Identity
 - **Source field:** Name
- **Ticket field:** Status
 - **Operation:** Substitution
 - **Source field:** State
 - **Values: Default Value:** 10

Source Value	Mapped Value
NEW	10
RESOLVED	20
UNKNOWN	20
ASSIGNED	20

- **Ticket field:** Information
 - **Operation:** Identity
 - **Source field:** Description
- **Ticket field:** HistoryLines
 - **Operation:** Identity
 - **Source field:** Activity Log
- **Ticket field:** Type the name or ID for any open text field.
 - **Operation:** Identity
 - **Source field:** URL

Map Ticket back to Issue Status field

NOTE: Because this section only maps the ticket's status, you are not prompted to add the ID of the issue's status field. This field is implied.

- **Operation:** Substitution
- **Source field:** Status
- **Values: Default Value:** TICKETED

Source Value	Mapped Value
40	CLOSED

- **Overwrite issue comments with ticket comments:** selected
- **Ticket Comment field:** HistoryLines
- **Tickets can be re-opened:** selected

Sample mapping for BMC Remedy Action Request System

This is a reference-only sample mapping for BMC Remedy Action Request System versions 6.3 and 7.0.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

Map Issue to Ticket

- **Ticket form:** Help Desk
- **Ticket field:** 8
 - **Operation:** Identity
 - **Source field:** Name
- **Ticket field:** 7
 - **Operation:** Substitution
 - **Source field:** State
 - **Values:** **Default Value:** 0

Source Value	Mapped Value
NEW	0
RESOLVED	2
ASSIGNED	1

- **Ticket field:** 2
 - **Operation:** Custom Mapping
 - **Source field:** Type the user name for the ticketing server. This is the same user name provided for Authentication on the Description page of the Registered Server Builder.
- **Ticket field:** 200000004
 - **Operation:** Custom Mapping
 - **Source field:** External

TIP: In this example, "External" specifies that the ticket was created by a product external to the ticketing server. You can type the name of the product instead, to indicate which product created the ticket.
- **Ticket field:** 240000008

NOTE: Ticketing systems can have multiple comment or diary fields. Make sure to choose the one you want used for this integration. If a comment field is not mapped, ticketed issue comments cannot be added to tickets.

 - **Operation:** Identity
 - **Source field:** Activity Log
- **Ticket field:** Type the name or ID for any open text field.
 - **Operation:** Identity
 - **Source field:** URL

Map Ticket back to Issue Status field

NOTE: Because this section only maps the ticket's status, you are not prompted to add the ID of the issue's status field. This field is implied.

- **Operation:** Substitution
- **Source field:** 7
- **Values: Default Value:** 0

Source Value	Mapped Value
4	CLOSED

- **Overwrite issue comments with ticket comments:** selected
- **Ticket Comment field:** 240000008
- **Tickets can be re-opened:** selected

Working with tickets

Use these tasks to add tickets to issues and to synchronize ticketed issues with the Issue Synchronization server task.

Tasks

- ▶ [Adding tickets to issues](#)
- ▶ [Synchronizing ticketed issues](#)
- ▶ [Synchronizing ticketed issues on a schedule](#)

Adding tickets to issues

Use this task to add a ticket to a single issue, or to add tickets to multiple issues at once. A ticket can be added in a similar way when viewing the details of an issue. When a ticket is added, a new ticket is created automatically in the ticketing server. Issues with existing tickets are ignored.

Before you begin

Make sure you have integrated a ticketing server.

Task

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

- 1 Click **Menu | Automation | Issues**, select the checkbox next to each issue, then click **Actions | Add ticket**.
- 2 In the **Action** panel, click **OK** to add a ticket to each selected issue.

Synchronizing ticketed issues

Use this task to run the Issue Synchronization server task, which updates ticketed issues and their associated tickets in the ticketing server.

Before you begin

Make sure you have integrated a ticketing server.

Task

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

- 1 Click **Menu | Automation | Server Tasks**.
- 2 Click **Run** next to the **Issue synchronization** task. The Server Task Log page appears.
- 3 Review the results of the server task. For more details, see the section in this guide about the server task log.

Synchronizing ticketed issues on a schedule

The Issue Synchronization server task updates ticketed issues and their associated tickets in the ticketing server. Use this task to configure the Issue Synchronization server task to run on a schedule.

NOTE: The schedule for the Issue Synchronization server task is disabled by default.

Before you begin

- You must have permissions to run server tasks and to purge issues to perform this task.
- Make sure you have integrated a ticketing server.

Task

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

- 1 Click **Menu | Automation | Server Tasks**, then click **Edit** in the Actions column for the **Issue synchronization** task. The Description page of the Server Task Builder appears.
- 2 Select **Enable** next to **Schedule status**. If you disable the schedule, the server task will not run on a schedule, but you can still run it manually.
- 3 Click **Next**. The Actions page appears.
- 4 Click **Next**. The Schedule page appears.
- 5 Schedule the server task as needed, then click **Next**. The Summary page appears.
- 6 Review the details of the server task, then click **Save**.

Working with ticketing servers

Use these tasks to integrate your ticketing server.

Tasks

- ▶ [Installing the ticketing server extensions](#)
- ▶ [Registering and mapping a ticketing server](#)
- ▶ [Configuring the field mappings](#)

Installing extensions for ticketing server

Use this task to integrate your ticketing system with ePolicy Orchestrator. The files that you copy to ePolicy Orchestrator depend on your ticketing system.

Task

- 1 Go to **Start | Control Panel | Administrative Tools**, then double-click **Services**.
- 2 In the **Name** column, double-click **McAfee Policy Auditor Application Server**.
- 3 Select the **General** tab.
- 4 Under **Service status**, click **Stop**. The server is now stopped.
- 5 Copy the required files for your ticketing server, then repeat steps 1-3.
- 6 Under **Service status**, click **Start**. The server is now running.

Stopping and starting the server

Use this task to stop the McAfee ePolicy Orchestrator Application server running on a Microsoft Windows system. The server must be stopped before the required files for the ticketing server can be copied. After the files are copied, start the server.

Task

- 1 Go to **Start | Control Panel | Administrative Tools**, then double-click **Services**.
- 2 In the **Name** column, locate then double-click **McAfee Policy Auditor Application Server**.
- 3 Select the **General** tab.
- 4 Under **Service status**, click **Stop**. The server is now stopped.
- 5 Copy the required files for your ticketing server, then repeat steps 1-3.
- 6 Under **Service status**, click **Start**. The server is now running.

Copying the Hewlett-Packard Openview Service Desk files

Use this task to copy the files required for the Hewlett-Packard Openview Service Desk (Service Desk) 5.1 or 4.5 extension. For information about these files, see your Service Desk documentation.

Before you begin

- Stop the server.
- If using Service Desk 5.1, locate these required files to copy:
 - OvObsCommon-05.10.090.jar
 - OvObsSDK-05.10.090.jar
 - OvObsWebApi-Client-05.10.090.jar
 - OvObsWebApi-Common-05.10.090.jar
 - sd-webapi-05.10.090.jar
 - xpl-05.10.090.jar
- If using Service Desk 4.5, locate this required file to copy:

- sd-webapi-4.5.0588.2205.jar

Task

- Copy the required files to the Server\common\lib folder of your ePolicy Orchestrator installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\common\lib.

Copying the BMC Remedy Action Request System files

Use this task to copy the files required for the BMC Remedy Action Request System (Remedy) extension. For information about these files, see your Remedy documentation. The Remedy extension includes support for the Remedy 6.3 and 7.0 servers.

NOTE: You can use the Remedy 5.1 or 7.0 API files for the Remedy extension. McAfee does not support an integration with the Remedy 5.1 server, but the 5.1 API files will work for integrations with the Remedy 6.3 or 7.0 servers. However, the Remedy 6.3 API files are not supported.

Before you begin

- Stop the server.
- If using the Remedy 5.1 API files, locate these required files to copy:
 - arapi51.dll
 - arjni51.dll
 - arrpc51.dll
 - arutl51.dll
 - arapi51.jar
 - arutil51.jar
- If using the Remedy 7.0 API files, locate these required files to copy:
 - arapi70.dll
 - arjni70.dll
 - arrpc70.dll
 - arutiljni70.dll
 - arutl70.dll
 - arxmlutil70.dll
 - icudt32.dll
 - icuin32.dll
 - icuuc32.dll
 - arapi70.jar
 - arutil70.jar

Task

- 1 Copy these required files to the \Server\bin folder of your ePolicy Orchestrator installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin.
 - If using the Remedy 5.1 API files:
 - arapi51.dll

- arjni51.dll
- arrpc51.dll
- arutil51.dll
- If using the Remedy 7.0 API files:
 - arapi70.dll
 - arjni70.dll
 - arrpc70.dll
 - arutiljni70.dll
 - arutil70.dll
 - arxmlutil70.dll
 - icudt32.dll
 - icuin32.dll
 - icuuc32.dll
- 2** Copy these required files to the Server\common\lib folder of your ePolicy Orchestrator installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\common\lib.
 - If using the Remedy 5.1 API files:
 - arapi51.jar
 - arutil51.jar
 - If using the Remedy 7.0 API files:
 - arapi70.jar
 - arutil70.jar

Installing the ticketing server extensions

Use this task to install ticketing server extensions.

Before you begin

- Copy the files required for the ticketing server.
- Restart the server.

Task

For option definitions, click ? in the interface.

- 1** Click **Menu | Software | Extensions**, then click **Install Extension**.
- 2** Browse to and select the extension (zip) file.
 - For Remedy, select **Remedy.zip**. This file includes support for Remedy 6.3 and 7.0.
 - For Service Desk 4.5, select **ServiceDesk_4_5.zip**.
 - For Service Desk 5.1, select **ServiceDesk_5_1.zip**.
- 3** Click **OK**.

Registering and mapping a ticketing server

Use these tasks to register and map a ticketing server. You must complete these tasks before tickets can be added to issues. Only one registered ticketing server can exist at a time.

Tasks

- ▶ [Configuring the DNS for Hewlett-Packard Openview Service Desk 4.5](#)
- ▶ [Registering a ticketing server](#)
- ▶ [Configuring the field mappings](#)

Configuring the DNS for Hewlett-Packard Openview Service Desk 4.5

Use this task to configure DNS for a Service Desk 4.5 integration. The system running the ticketing extension must be able to resolve the address of the Service Desk system.

Task

- 1 On the Product Feature Name server that is integrated with the ticketing system, use a text editor to open the hosts file. The host file should be located in the `c:\windows\system32\drivers\etc\` folder.
- 2 Edit the hosts file to include the IP address of the system running Service Desk 4.5, followed by a space, followed by the DNS suffix (the name of the system on which Service Desk 4.5 is running). For example, `168.212.226.204 SRVDSK45.qaad.com`
- 3 Save and close the hosts file.
- 4 Restart the Product Feature Name server.

Registering a ticketing server

Use this task to register a ticketing server. This task must be completed before tickets can be associated with issues.

Before you begin

- Make sure you have installed the extension for your ticketing server.
- You must have appropriate permissions to perform this task.

Task

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

- 1 Click **Menu | Configuration | Registered Servers**, then click **New Server**. The Description page of the Registered Server Builder appears.
- 2 Select the server type for your ticketing server. This choice determines the options available on subsequent pages of the builder.
- 3 Type a name and description, then click **Next**. The Details page appears.
- 4 Type the host for the server.
- 5 Type the port, user name, and password for the server.
- 6 If Service Desk 4.5 or 5.1 was selected, select a **Workflow**.

Configuring the field mappings

Use these tasks to configure the field mappings for a ticketing server. You must complete these tasks before tickets can be associated to issues.

Before you begin

- The ticketing server you want to configure must be running.
- Know which fields from the ticketing server need to be mapped.

Tasks

- ▶ [Mapping issues to tickets](#)
- ▶ [Mapping tickets back to issue status](#)

Mapping issues to tickets

Use this task to configure the field mapping from the issue to the ticket.

Task

For option definitions, click ? in the interface.

NOTE: Source values, mapped values, and field IDs are case-sensitive.

- 1 Next to **Configure mapping**, click **Configure**. The Mapping page appears.
- 2 Select the options from the **Mapping Options** pane as needed. Selected options appear in the Mapping Definitions pane with operators to specify how an issue should be mapped to a ticket, and how a ticket should be mapped back to an issue. Both mappings must be completed.
- 3 Under **Map Issue to Ticket**, type the name of a **Ticket form**.
- 4 Type a **Ticket field ID**.
- 5 Select an **Operation**.
- 6 Do one of the following:
 - If **Substitution** is selected, select an issue field in the **Source field** drop-down list, then click **Edit** next to **Values**. The Edit Substitution Mapping dialog box appears.
 - 1 Type a **Default Value** that should be substituted if a source value, which is not mapped, is returned.
 - 2 Type a **Source Value** for the issue, then type the **Mapped Value** that should be substituted for this value in the ticket.
 - 3 Click **+** to map another value.
 - 4 When finished, click **OK**.
 - If **Numeric Range** is selected, select an issue field to map in the **Source field** drop-down list, then click **Edit** next to **Values**. The Edit Numeric Range Mapping dialog box appears.
 - 1 Type a **Default Value** that should be substituted if a source range, that is not mapped, is returned.
 - 2 Type the **Source Range** for the issue, then type the **Mapped Value** that should be substituted for this range in the ticket.
 - 3 Click **+** to map another value.

- 4 When finished, click **OK**.
- If **Custom Mapping** is selected, type the **Value** that should be added to the ticket.
- 7 Click **+** to map another ticket field.

Mapping tickets back to issue status

Use this task to configure the field mapping from the ticket back to the issue's status (state) field.

NOTE: Because this section only maps the ticket's state/status, you are not prompted to add the ID of the issue's status (state) field. This field is implied.

Task

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

NOTE: Source values, mapped values, and field IDs are case-sensitive.

- 1 Under **Map Ticket back to Issue Status field**, select an **Operation**.
- 2 In the **Source field**, type the ID of the ticket field that contains the state/status of the ticket.
- 3 If **Numeric Range** or **Substitution** is selected for the **Operation**, click **Edit** next to **Values**. A dialog box appears.
 - If **Numeric Range** is selected, type a range of **Ticket Values** for the ticket, then type the **Label** that is substituted for this range in the issue.
 - If **Substitution** is selected, type a **Source Value** for the ticket, then type the **Mapped Value** that is substituted for this value in the issue.
- 4 Select the checkbox if you want to **Overwrite issue comments with ticket comments**, then type the ID of the **Ticket comment field** that overwrites the data in the issue's comment field.
- 5 Select the checkbox if **Tickets can be re-opened**.
- 6 When finished, click **Test Mapping**.
- 7 If the test is successful, a ticket ID appears in a dialog box. This is the ID for a test ticket, which was created in your ticketing server. Locate this ticket in your ticketing server, and verify that all the values for the basic issue type are mapped correctly, including the test's comments.

NOTE: The test mapping function verifies the mapping for the basic issue type, regardless of the issue type configured. Therefore, testing the mapping for issue types from other product extensions (extended issue types) can be successful per the basic mapping test, but you might see unexpected results in the tickets. For these issue types, verify that tickets added to issues after your ticketing server is fully integrated are created correctly.

- 8 Click **OK**.
- 9 If the test was unsuccessful, review your mappings and the status of the ticketing server.
- 10 When finished testing the mapping, click **Save**. The Details page of the Registered Server Builder appears.

NOTE: You can save the configuration and register the server even if the mapping test fails.

- 11 When finished, click **Save**.

Upgrading a registered ticketing server

Use this task to modify the integration of the existing ticketing server if your ticketing server is upgraded.

Before you begin

- Make sure the upgraded version of the ticketing server is running.

Task

CAUTION: If the server task, which synchronizes ticketed issues, runs after the existing registered ticketing server is modified or deleted, but before the upgraded ticketing server is integrated, the issue-to-ticket association is broken. If this occurs, complete this task, then manually add tickets to all previously ticketed issues. This causes the reopen function to run. For more details, see the section in this guide about how tickets are reopened.

- 1 Do the following to disable the server task, which synchronizes ticketed issues.
 - a Click **Menu | Automation | Server Tasks**, then click the issue synchronization server task. The Description page of the Server Task Builder appears.
 - b Select **Disable** next to **Schedule status**.
 - c Click **Save**.
- 2 Ensure that no instances of the server task are running. If an instance is running, wait for it to complete or cancel it before continuing.
- 3 Do one of the following:
 - Edit the existing registered ticketing server based on the configuration requirements for the upgraded ticketing server.
 - Delete the existing registered ticketing server, then create a new one based on the configuration requirements for the upgraded ticketing server.For more details, see the sections in this guide about integrating ticketing servers, installing ticketing server extensions, and registering and configuring a ticketing server.
- 4 After you have configured the integration with the upgraded ticketing server, enable the server task, which synchronizes ticketed issues.

Appendix: Maintaining ePolicy Orchestrator Databases

Your databases require regular maintenance to promote optimal performance and to protect your data. Use the Microsoft management tool appropriate for your version of SQL:

SQL Version	Management Tool
SQL 2005	SQL Server Enterprise Manager
SQL 2008	SQL Server Management Studio
SQL Express	SQL Server Management Studio Express

Depending on your deployment of ePolicy Orchestrator, plan on spending a few hours each week on regular database backups and maintenance. The tasks discussed in this section should be performed on a regular basis, either weekly or daily. However, these are not the only maintenance tasks available. See your SQL documentation for details on what else you can do to maintain your database.

Contents

- ▶ [Perform regular maintenance of SQL Server databases](#)
- ▶ [Backup and restore ePolicy Orchestrator databases](#)
- ▶ [Changing SQL Server information](#)

Perform regular maintenance of SQL Server databases

Simple recovery mode is recommended because the transaction log is not essential in simple recovery mode and does not swell during backup. If you have multiple databases with different recovery models, you can create separate database maintenance plans for each recovery model. In this way you can include a step to back up your transaction logs only on the databases that do not use the simple recovery mode.

In simple recovery, once a checkpoint is complete, the transaction logs for the time before the checkpoint are dropped from the active database. A checkpoint automatically occurs when the backup is made. We recommend having a database maintenance plan that performs a backup of the ePO database, together with "Simple Recovery." In this way, once a backup is successfully created, the portion of the transaction log in the active database is dropped; it is no longer needed because a backup file exists.

Ensure that the recovery model is set to **simple**. See the SQL documentation for information on simple recovery. If you choose not to use simple recovery, you need to regularly back up the transaction log.

Backup and restore ePolicy Orchestrator databases

McAfee recommends that you back up ePolicy Orchestrator databases regularly to protect your data and guard against hardware and software failure. If you ever need to reinstall the server, you might need to restore from a backup.

How often you back up depends on how much of your data you are willing to risk. Some possible approaches include:

- Back up your database at least once a week.
- If you have made many changes to your deployment, you might want to back up daily.
- To mitigate bandwidth demands during regular business hours, you might schedule automated nightly backups.
- To further balance the load, you might perform incremental daily or nightly backups, and a full weekly backup each week.

Save the backup copy to a different server than the one hosting your live database. If your database server crashes, you don't want to lose your backup too.

Performing regular backups provides the ability to restore your database if that should ever become necessary because of software or hardware failure, or because of an upgrade to server or database server hardware.

For information on backing up and restoring your SQL database, see:

- Microsoft documentation for the management tool appropriate for the database you are using.
- McAfee KnowledgeBase article KB52126.

Changing SQL Server information

Use this task to edit the SQL Server connection configuration details. This is useful to make changes to the user account information in ePolicy Orchestrator when you make changes to the SQL Server authentication modes in SQL Server Enterprise Manager or SQL Server Management Studio. Do this if you need to use a privileged SQL user account for added network security.

CAUTION: Changing the database settings to point this ePO server to an ePO database that is not an *exact* match can cause the removal of product extensions and the loss of all associated data. McAfee recommends performing this task only to change the configuration of your existing database.

You can use the web page at <https://servername:port/core/config> to adjust any database configuration file information that used to be done with the Cfgnaims.exe file.

Things to know about this page:

- Authentication — If the database is up, this page uses normal ePO user authentication and only a global administrator can access it. If the database is down, a connection is required from the system running the SQL server.
- The ePO server must be restarted for any configuration changes to take effect.
- As a last resort, you might edit the configuration file by hand (<ePO installation directory>server\conf\orion\db.properties), putting in the plaintext password, starting the server, then using the config page to re-edit the db config, which stores the encrypted version of the passphrase.

Task

- 1 Log on to ePolicy Orchestrator with global administrator credentials.
- 2 Type the following URL in the browser's address field.
`https://servername:port/core/config`
- 3 On the Configure Database Settings page, change the credentials or SQL Server information, as needed.
- 4 Click **OK** when done.
- 5 Restart the system or ePolicy Orchestrator services to apply the changes.

Index

A

access requirements for System Tree 105

accounts, See user accounts

actions, Rogue System Detection

events and 234

queries and installing sensors 242

Active Directory

adding systems to the System Tree 20

configuring Windows authorization 38

containers, mapping to System Tree groups 123

enabling user autcreation 32

systems only synchronization 109

Active Directory synchronization

borders and 106

deleting systems 108, 109

duplicate entry handling 108

integration with System Tree 108

Synchronize Now action 108

systems and structure 109

tasks 108

to System Tree structure 123

types 109

adding comments to issues 269

administrator accounts, See user accounts

administrators, global, See global administrators

advanced features, ePolicy Orchestrator 22

agent

alien, on rogue systems 226

command-line options 97

configuring client tasks 87, 88

configuring policies to use repositories 187

configuring proxy settings for 135

distributing to systems 21

enabling on unmanaged McAfee products 76

first call to server 112

grouping 56

grouping by assignment rules 56

GUID and System Tree location 112

inactive, on rogue systems 226

installation, See agent installation

introduction to 60

maintenance 89

manage systems using 21

McAfee Agent, ePO components 14

modes, converting 76

properties, viewing 89

removal methods 98, 99, 100

removing from systems in query results 100

responses and event forwarding 251

restoring a previous UNIX version 83

restoring a previous Windows version 83

Rogue System Detection configuration 231

settings, viewing 96

status 101

agent (*continued*)

system requirements 63

tasks, running from managed systems 93

uninstalling 99

UNIX installation folder 78

upgrading with phased approach 82

user interface 93

viewing system information 90

wake-up calls 92

Windows installation folder 78

agent activity logs 101, 102

agent distribution

FrmInst.exe command-line 99

Agent Handlers

about 52

assigning agents 53

assignment priority 57

configuring and managing 53

how they work 52

introduction to 60

moving agents between 56

multiple 52

priority

in sitelist file 52

agent installation

CmdAgent.exe 97

command-line options 80

creating custom packages 70

deployment methods 65

force 66

from an image 72

manually on Windows 68

on UNIX 69

on Windows from ePolicy Orchestrator 66

on Windows via push technology 74

package, location of 71, 79

uninstalling 99

update packages 82

using login scripts 71

Agent Monitor 95

agent upgrade 81, 82, 83

agent-server communication

about 61

after agent setup 62

interval, (ASCI) 72

secure communication keys (ASSC) 46

System Tree sorting 111

agent-server secure communication (ASSC)

about 41

using different key pairs for servers 49

using one key pair 48

viewing systems that use a key pair 49

working with keys 46, 47

aggregation, See notifications

Applied Policies

creating queries 151

- Apply Tag action [113](#)
 - ASCI (See agent-to-server communication interval) [62](#)
 - assigning issues [269](#)
 - assignment of ticketed issues to users [271](#)
 - assignment rules
 - agents and handlers [56](#)
 - Audit Log [195](#), [205](#), [206](#)
 - about [205](#)
 - purging [206](#)
 - viewing action history [206](#)
 - working with [205](#)
 - authentication
 - configuring for Windows [37](#)
 - authentication, configuring for Windows [36](#)
 - autocreation, enabling for Active Directory users [32](#)
- B**
- bandwidth
 - considerations for event forwarding [32](#)
 - considerations for pull tasks [175](#)
 - distributed repositories and [130](#)
 - replication tasks and [176](#)
 - Rogue System Sensor and [224](#)
 - sensor-to-server traffic [225](#)
 - best practices
 - agent-to-server communication interval [61](#)
 - duplicating policies before assigning [150](#)
 - importing Active Directory containers [123](#)
 - policy assignment locking [150](#)
 - product deployment [173](#)
 - System Tree creation [116](#)
 - BMC Remedy Action Request System [263](#)
 - BMC Remedy Action Request System versions 6.3 and 7.0 [272](#)
 - borders (See System Tree organization) [106](#)
 - branches
 - Change Branch action [191](#)
 - Current [184](#), [189](#)
 - deleting DAT and engine packages [192](#)
 - Evaluation [191](#)
 - manually moving packages between [192](#)
 - Previous [178](#)
 - types of, and repositories [133](#)
 - broadcast segments and Rogue System Sensor [223](#)
 - Broken Inheritance
 - creating queries [151](#)
- C**
- catch-all groups [112](#)
 - Change Branch action [191](#)
 - charts (See queries) [195](#)
 - Check IP Integrity action [111](#)
 - client tasks
 - about [22](#), [152](#)
 - configuring, agent scheduler policy [87](#), [88](#)
 - creating and scheduling [164](#)
 - deleting [165](#)
 - editing settings for [164](#)
 - installing RSD sensors [242](#)
 - mirror [88](#)
 - schedule [22](#)
 - update [88](#)
 - wake-up [88](#)
 - working with [164](#)
 - cmdagent.exe [96](#)
 - Command Agent tool (CmdAgent.exe) [62](#), [97](#)
 - command-line options [62](#)
 - command-line options
 - agent [97](#)
 - agent installation [80](#)
 - CmdAgent.exe [62](#), [97](#)
 - FrmInst.exe [99](#)
 - notifications and registered executables [256](#), [257](#)
 - rogue system detection [246](#)
 - communication port, Rogue System Detection [229](#)
 - communication ports, ePolicy Orchestrator [33](#)
 - communication to the server [224](#)
 - compliance
 - compliant systems [226](#)
 - configuring RSD settings [232](#)
 - components
 - ePO server, about [14](#)
 - ePolicy Orchestrator, about [14](#)
 - repositories, about [130](#)
 - contacts
 - notifications and [28](#)
 - responses and [260](#)
 - working with [28](#), [29](#)
 - creating issues [264](#)
 - creating tickets [271](#)
 - credentials
 - changing, on distributed repositories [147](#)
 - required for agent installation [70](#)
 - criteria-based tags
 - applying [115](#), [116](#)
 - sorting [121](#)
 - Current branch
 - checking in update packages [189](#)
 - defined [133](#)
 - for updates [184](#)
- D**
- dashboards
 - active set [220](#)
 - chart-based queries and [216](#)
 - configuring access and behavior [218](#)
 - configuring for exported reports [31](#)
 - configuring refresh frequency [219](#)
 - creating [220](#)
 - default monitors [216](#)
 - granting permissions to [219](#)
 - how they work [216](#)
 - making active [220](#)
 - making public [221](#)
 - Rogue System Detection [226](#)
 - selecting all in a set [220](#)
 - DAT file updating
 - checking in manually [189](#)
 - checking versions [190](#)
 - considerations for creating tasks [174](#)
 - daily task [190](#)
 - deployment [173](#)
 - from source sites [137](#)
 - in master repository [133](#)
 - scheduling a task [190](#)
 - DAT files
 - deleting from repository [192](#)
 - evaluating [191](#)
 - repository branches [192](#)
 - Data Execution Prevention [63](#)

- Data Rollup server task [203](#)
 - databases
 - ePO, systems listed in [226](#)
 - multi-server querying [202](#)
 - ports and communication [29](#)
 - public and personal queries [194](#)
 - queries and retrieving data [193](#)
 - registering servers for rollout queries [203](#)
 - deleting issues [269](#)
 - DEP, See Data Execution Prevention
 - deployment
 - checking in packages manually [178](#)
 - global updating [181](#)
 - installation, definition and methods [65](#)
 - installing products [179](#), [180](#)
 - methods [65](#)
 - package security [171](#)
 - products and updates [173](#)
 - push technology via [74](#)
 - supported packages [171](#)
 - tasks [173](#)
 - tasks, for managed systems [179](#)
 - upgrading agents [82](#)
 - detected systems
 - configuring policy settings [232](#)
 - Exceptions list, adding to [235](#)
 - Exceptions list, importing to [238](#)
 - homepage [226](#)
 - how Rogue System Sensor work [223](#)
 - merging [238](#)
 - merging and matching [225](#)
 - removing from lists [239](#), [240](#)
 - Rogue Sensor Blacklist, adding to [236](#)
 - status monitors [226](#)
 - viewing [240](#)
 - working with [235](#)
 - Detected Systems list, removing systems from [239](#)
 - detections
 - configuring RSD policies [232](#)
 - settings for rogue systems [229](#)
 - subnet status and rogue systems [228](#)
 - devices, detected by Rogue System Sensor [223](#)
 - DHCP servers
 - Rogue System Sensor and [225](#), [229](#)
 - system and subnet reporting [223](#)
 - Directory (See System Tree) [123](#)
 - distributed repositories
 - about [21](#), [130](#), [132](#)
 - adding to ePO [142](#)
 - changing credentials on [147](#)
 - creating and configuring [141](#)
 - deleting [145](#)
 - deleting SuperAgent repositories [141](#)
 - editing existing [144](#)
 - enabling folder sharing [144](#)
 - ePO components [14](#)
 - folder, creating [141](#)
 - how agents select [177](#)
 - limited bandwidth and [130](#)
 - replicating packages to SuperAgent repositories [140](#)
 - replicating to [185](#), [186](#)
 - SuperAgent, tasks [139](#)
 - types [132](#)
 - unmanaged [132](#)
 - unmanaged, copying content to [188](#)
 - domain synchronization [106](#)
 - duplicate entries in the System Tree [125](#)
- ## E
- editing issues [269](#)
 - email addresses [28](#)
 - email servers
 - configuring responses [252](#)
 - defining [30](#)
 - enforcement (See policy enforcement) [161](#)
 - engine updating
 - checking in manually [189](#)
 - deployment packages [173](#)
 - from source sites [137](#)
 - in master repository [133](#)
 - scheduling a task [190](#)
 - engines
 - deleting from repository [192](#)
 - repository branches [192](#)
 - ePO interface
 - comparing version 4.0 and 4.5 [18](#)
 - Menu [18](#)
 - using [18](#)
 - ePO servers
 - configuring [20](#)
 - transferring systems [129](#)
 - Evaluation branch
 - defined [133](#)
 - using for new DATs and engine [191](#)
 - events
 - contacts for notifications [28](#)
 - determining which are forwarded [32](#)
 - filtering, server settings [29](#)
 - forwarding and notifications [251](#)
 - forwarding, agent configuration and [85](#)
 - events, Rogue System Detection
 - actions and [242](#)
 - sensor settings [234](#)
 - exceptions
 - Rogue System Blacklist [229](#)
 - rogue system status [226](#)
 - Exceptions list
 - adding systems [235](#)
 - compared to Rogue Sensor Blacklist [229](#)
 - exporting [237](#)
 - importing systems to [238](#)
 - removing systems from [239](#)
 - executables
 - configuring [256](#)
 - deleting [257](#)
 - editing, notifications and [257](#)
 - registered, adding [256](#)
 - registered, duplicating [257](#)
 - working with, for responses [256](#)
 - extension files
 - about [148](#)
 - functionality added to managed products [148](#)
 - installing [153](#)
 - permission sets and installation [25](#)
 - Rogue System Detection [223](#)
 - UNIX, agent package file name [69](#)
 - viewing version [18](#)
- ## F
- fallback sites
 - about [130](#)

- fallback sites (*continued*)
 - configuring [137](#)
 - deleting [139](#)
 - edit existing [138](#)
 - switching to source [137](#)
 - features, ePolicy Orchestrator components [14](#)
 - filters
 - Event Filtering settings [29](#)
 - for server task log [210](#)
 - query results [195](#)
 - setting for response rules [259](#)
 - force
 - agent call to server [96](#)
 - installation of agent [66](#)
 - FRAMEPKG.EXE [79](#)
 - FTP repositories
 - about [132](#)
 - creating and configuring [141](#)
 - editing [144](#)
 - enabling folder sharing [144](#)
- G**
- geographic borders, advantages of [106](#)
 - global administrator
 - server settings, working with [30](#)
 - global administrators
 - about [24](#)
 - assigning permission sets [25](#)
 - changing passwords on user accounts [25](#)
 - creating groups [104](#)
 - creating permission sets for user accounts [26](#)
 - creating user accounts [24](#)
 - deleting permission sets [28](#)
 - deleting user accounts [25](#)
 - duplicating permission sets [27](#)
 - editing permission sets [27](#)
 - permissions [24](#)
 - source sites, configuring [137](#)
 - global unique identifier (GUID) [72](#), [73](#), [112](#)
 - correcting duplicates [72](#)
 - duplicate [72](#)
 - scheduling corrective action for duplicates [73](#)
 - global updating
 - enabling [181](#)
 - event forwarding and agent settings [85](#)
 - process description [174](#)
 - requirements [174](#)
 - grouping, See notifications
 - groups
 - catch-all [112](#)
 - configuring criteria for sorting [121](#)
 - creating manually [118](#)
 - criteria-based [112](#)
 - defined [104](#)
 - deleting from System Tree [99](#)
 - importing NT domains [125](#)
 - moving systems manually [128](#)
 - operating systems and [107](#)
 - pasting policy assignments to [163](#)
 - policies, inheritance of [104](#)
 - policy enforcement for a product [161](#)
 - sorting criteria [121](#)
 - sorting, automated [107](#)
 - updating manually with NT domains [128](#)
 - groups (*continued*)
 - using IP address to define [106](#)
 - viewing policy assignment [155](#)
 - GUID, See global unique identifier
- H**
- handler assignment
 - editing priority [54](#), [57](#)
 - managing [54](#)
 - viewing summary [54](#)
 - handler groups
 - about [52](#)
 - creating [55](#)
 - deleting [55](#)
 - editing settings [55](#)
 - handlers
 - creating groups [55](#)
 - grouping agents [58](#)
 - moving agents between [56](#)
 - priority [52](#)
 - Hewlett-Packard Openview Service Desk [263](#)
 - Hewlett-Packard Openview Service Desk versions 4.5 and 5.1 [272](#)
 - HTTP repositories
 - about [132](#)
 - creating and configuring [141](#)
 - editing [144](#)
 - enabling folder sharing [144](#)
- I**
- icon, system tray, See system tray icon
 - inactive agents [93](#)
 - inactive systems, rogue system status [226](#)
 - inheritance
 - and policy settings [150](#)
 - broken, resetting [155](#)
 - defined [104](#)
 - viewing for policies [155](#)
 - installation
 - agent, See agent installation
 - Rogue System Sensor [241](#)
 - installation folder
 - UNIX [78](#)
 - Windows [78](#)
 - intelligent filtering and Rogue System Sensor [224](#)
 - Internet Explorer
 - configuring proxy settings [135](#)
 - proxy settings and ePO [136](#)
 - IP address
 - as grouping criteria [106](#)
 - checking IP overlap [111](#)
 - IPv6 [58](#)
 - range, as sorting criteria [121](#)
 - sorting [111](#)
 - sorting criteria [116](#), [121](#)
 - subnet mask, as sorting criteria [121](#)
 - issue management [263](#)
 - issue synchronization server taskl [272](#)
 - issues
 - adding comments [269](#)
 - about [263](#)
 - adding comments [269](#)
 - adding tickets to [276](#)
 - assigning [269](#)
 - associations with tickets (See ticketed issues) [271](#)
 - creating [264](#)

- issues (*continued*)
 - creating automatically from responses 265
 - deleting 269
 - editing 269
 - managing 263
 - viewing details 269
- issues, purging
 - closed issues 270
 - closed issues on a schedule 270
- K**
- keys, See security keys
- L**
- LAN connections and geographical borders 106
- language packages (See agent) 106
- LDAP servers, registering 40
- local distributed repositories 188
- Locale IDs, settings for installation 80
- login scripts
 - install the agent via 71
- M**
- Make public queries 200
- managed mode
 - convert from unmanaged mode in Windows 76
 - convert from unmanaged mode on UNIX 77
 - convert from updater mode 76
- managed systems
 - agent-server communication 61
 - deployment tasks for 179
 - Detected Systems list 239
 - Exceptions list 235
 - global updating and 130
 - installing products on 180
 - policy assignment 155
 - policy management on 149
 - Rogue Sensor Blacklist 229, 236
 - rogue system status 226
 - rollup querying 202
 - running an update task manually 94, 95
 - sorting, criteria-based 110
 - tasks for 179
 - viewing agent activity log 101
 - viewing information on 90
- master repositories
 - about 130
 - accessing 21
 - checking in packages manually 189
 - communicating with source sites 135
 - configuring proxy settings 135
 - ePO components 14
 - key pair for unsigned content 44
 - pulling from source site 183, 184
 - replicating to distributed repositories 185, 186
 - security keys in multi-server environments 45
 - updating with pull tasks 175
 - using replication tasks 176
- McAfee Agent (see agent) 14
- McAfee Default policy
 - frequently asked questions 165
- McAfee Links, default monitor 216
- McAfee recommendations
 - configure RSD sensor policies before deploying sensors 229
- McAfee recommendations (*continued*)
 - create a Rollup Data server task 203
 - deploy agents when importing large domains 125
 - duplicate policies before assignment 150
 - evaluate borders for organization 106
 - install multiple Rogue System Sensors per broadcast segment 225
 - phased rollout for product deployment 173
 - schedule replication tasks 176
 - System Tree planning 105
 - use global updating 174
 - use IP addresses for sorting 106
 - use tag-based sorting criteria 107
- Menu
 - navigating in the interface 19
- menu-based navigation 18
- Microsoft Internet Information Services (IIS) 132
- Microsoft Windows Resource Kit 120
- monitors (See dashboards) 216
- monitors, Rogue System Detection
 - overall system status 226
 - status monitors 226
- multiple ePO servers
 - policy sharing 167
- My Default policy
 - frequently asked questions 165
- MyAvert
 - Security Threats page 50
 - Security Threats, working with 50
 - Theat Service, default monitor 216
- N**
- NAP files (See extension files) 148
- navigation
 - menu-based 18
- navigation, in ePO
 - Menu 18
 - menu-based 18
 - navigation bar 19
- NETDOM.EXE utility, creating a text file 120
- network bandwidth (See System Tree organization) 106
- network traffic
 - bandwidth 225
 - Rogue System Sensor and 224
- New Group wizard
 - creating new groups 199
- notification rules
 - defaults 250
 - importing .MIB files 255
- notifications
 - assigning permissions 253
 - contacts for 28
 - event forwarding 251, 252
 - event forwarding and agent settings 85
 - how they work 249
 - recipients 249
 - registered executables, working with 257
 - SNMP servers 41, 254
 - throttling, aggregation, and grouping 249
 - viewing threats 51
- NT domains
 - importing to manually created groups 125
 - integration with System Tree 108
 - synchronization 110, 125
 - updating synchronized groups 128

O

- operating systems
 - filters for response rule [259](#)
 - grouping [107](#)
 - legacy systems (Windows 95, Windows 98) [107](#)
 - McAfee Agent and [63](#)
 - Rogue System Detection and [223](#)
 - Rogue System Sensor and [223](#)
- overall system status, Rogue System Detection [226](#)

P

- packages
 - agent file name, for UNIX [69](#)
 - checking in manually [178](#)
 - configuring deployment task [180](#)
 - creating custom for agent installation [70](#)
 - deploying updates with tasks [183](#)
 - moving between branches in repository [192](#)
 - security for [171](#)
- passwords
 - changing on user accounts [25](#)
 - installing agents, command-line options [97](#)
 - logging on to ePO servers [17](#)
- permission sets
 - assigning [20](#)
 - at product installation [25](#)
 - creating for user accounts [26](#)
 - extensions and [25](#)
 - how they work [25](#)
 - mapping to Active Directory groups [36](#)
 - rogue system detection [231](#)
 - System Tree [105](#)
 - working with [26, 27, 28](#)
- permissions
 - assigning for notifications [253](#)
 - assigning for responses [253](#)
 - for queries [194](#)
 - global administrator [24](#)
 - to dashboards [219](#)
- policies
 - about [149](#)
 - assigning and managing [158](#)
 - broken inheritance, resetting [155](#)
 - categories [149](#)
 - changing the owner [159](#)
 - controlling on Policy Catalog page [156, 157, 158](#)
 - controlling, on Policy Catalog page [157](#)
 - enforcing [94](#)
 - frequently asked questions [165](#)
 - group inheritance, viewing [155](#)
 - how they are applied to systems [150](#)
 - importing and exporting [149, 159, 160](#)
 - inheritance [150](#)
 - ownership [150, 154](#)
 - settings, viewing [154](#)
 - sharing between ePO servers [159](#)
 - update settings [95](#)
 - verifying changes [89](#)
 - viewing [149, 153](#)
 - working with Policy Catalog [156](#)
- policies, ePolicy Orchestrator
 - about [22](#)
 - enforcing [22](#)
- policies, McAfee Agent
 - options for policy pages [84](#)
 - policies, McAfee Agent (*continued*)
 - settings, about [84](#)
 - policies, Rogue System Detection
 - about [229](#)
 - compliance settings [232](#)
 - configuring [232](#)
 - considerations [229](#)
 - matching settings [233](#)
 - sensor-to-server port [241](#)
 - policy assignment
 - copying and pasting [162, 163](#)
 - disabled enforcement, viewing [154](#)
 - group, assigning to [160](#)
 - locking [150](#)
 - Policy Catalog [150](#)
 - systems, assigning to [160, 161](#)
 - viewing [153, 155](#)
 - policy assignment rules
 - about [168](#)
 - creating [168](#)
 - deleting and editing [169](#)
 - editing priority [169](#)
 - importing and exporting [169](#)
 - priority [168](#)
 - viewing summary [169](#)
 - Policy Catalog
 - page, viewing [149](#)
 - working with [156](#)
 - policy enforcement
 - enabling and disabling [161](#)
 - for a product [161, 162](#)
 - viewing assignments where disabled [154](#)
 - when policies are enforced [149](#)
 - policy management
 - using groups [104](#)
 - working with client tasks [164](#)
 - Policy Management
 - creating queries [151](#)
 - policy sharing
 - assign [166](#)
 - designating [166](#)
 - multiple ePO servers [166](#)
 - registering server [166](#)
 - using registered server [166](#)
 - using server tasks [166, 167](#)
- ports
 - communication, working with [33](#)
 - RSD sensor-to-server port [229, 241](#)
 - server settings [29](#)
 - server settings and communication [29](#)
- Previous branch
 - defined [133](#)
 - moving DAT and engine packages to [192](#)
 - saving package versions [178](#)
- product deployment packages
 - checking in [178](#)
 - checking in manually [189](#)
 - security and package signing [171](#)
 - supported packages [171](#)
 - updates [171](#)
- product installation
 - configuring deployment tasks [179, 180](#)
 - extensions and permission sets [25](#)
 - installing extension files [153](#)
- product properties [91](#)

- product updates
 - checking in packages manually 178
 - deploying 173
 - package signing and security 171
 - process description 173
 - source sites and 130
 - supported package types 171
 - properties
 - agent, viewing from the console 89
 - custom, for the agent 81
 - minimal vs. full 87
 - product 91
 - retrieving from managed systems 87
 - sending to ePO server 95
 - settings for retrieving 90
 - system 91
 - verifying policy changes 89
 - proxy settings
 - agent policies 86
 - configuring ePO for Internet Explorer 136
 - configuring for master repository 135
 - configuring for the agent 86
 - McAfee Agent 135
 - MyAvert
 - configuring 50
 - pull tasks
 - considerations for scheduling 175
 - deploying updates 183
 - Pull Now task, initiating 184
 - server task log 177
 - updating master repository 175, 183
 - purging closed issues 270
 - push technology
 - initial agent deployment via 74
- Q**
- queries
 - about 193
 - actions on results 193
 - chart types 195
 - contacts 28
 - custom, creating 196
 - duplicating 200
 - exported as reports 193
 - exporting to other formats 201
 - exporting to XML file 201
 - filters 195
 - importing from a server 201
 - making personal queries public 200
 - My Queries list 194
 - permissions 194
 - personal query group 199
 - preparing for rollup queries 202
 - public and personal 194
 - Public Queries list 194
 - registering ePO servers 203
 - removing agents in results of 100
 - report formats 193
 - result type 202
 - results as dashboard monitors 193
 - results as tables 195
 - rollup, from multiple servers 202
 - running existing 197
 - scheduled 197
 - using results to exclude tags on systems 114
 - queries, Rogue System Detection
 - installing sensors 242
 - Query Builder wizard
 - about 195
 - creating custom queries 196
 - result types 195
 - Quick System Search, default monitor 216
- R**
- registered executables, See executables
 - registered executables (See executables) 257
 - registered servers
 - about 39
 - adding SNMP servers 41
 - enabling policy sharing 166
 - LDAP servers, adding 40
 - registering 39
 - Remedy
 - sample mapping for (See ticketing servers) 275
 - removal
 - agent, from UNIX systems 100
 - Replicate Now task 186
 - replication
 - avoiding for selected packages 143, 187
 - disabling of selected packages 144
 - replication tasks
 - copying contents of master repository 185
 - deploying updates 183
 - full vs. incremental 176
 - Replicate Now task from master repository 186
 - scheduling repository replication 185
 - server task log 177
 - updating master repository 176
 - reports
 - configuring template and location for 31
 - exported data 214
 - exported query results 193
 - formats 193, 214
 - repositories
 - branches 133, 191, 192
 - creating SuperAgent repository 139
 - distributed, about 21
 - how they work together 134
 - importing from repository list files 146
 - master, configuring proxy settings for 135
 - replication and selection of 177
 - replication tasks 186
 - scheduling a pull task 183
 - scheduling a replication task 185
 - security keys 41, 45
 - selecting a source for updates 85
 - source site 130, 184
 - types of 21, 130
 - unmanaged, copying content to 188
 - repository list files
 - about 134
 - adding distributed repository to 142
 - exporting to 145, 146
 - importing from 146, 147
 - priority of Agent Handlers 52
 - SiteList.xml, uses for 134
 - working with 145
 - requirements
 - operating systems 63
 - processors 63

- Response Builder wizard [260](#)
 - response rules
 - creating and editing [258](#)
 - Description page [258](#)
 - setting filters for [259](#)
 - setting thresholds [259](#)
 - responses
 - assigning permissions [253](#)
 - configuring [252](#), [256](#), [260](#)
 - configuring to automatically create issues [265](#)
 - contacts for [260](#)
 - event forwarding [251](#)
 - frequently asked questions [261](#)
 - planning [251](#)
 - registered executables, working with [256](#)
 - rules that trigger [260](#)
 - SNMP servers [254](#), [255](#)
 - Rogue Sensor Blacklist
 - about [229](#)
 - adding systems [236](#)
 - removing systems from [240](#)
 - Rogue System Detection
 - about [223](#)
 - agents and [231](#)
 - compliance settings [232](#)
 - configuring server settings [232](#)
 - deploying sensors [241](#)
 - operating system support [223](#)
 - policy configuration [232](#)
 - policy settings [229](#)
 - sensor blacklist [229](#)
 - sensor settings [234](#)
 - sensor-to-server communication port [229](#)
 - setting up [231](#)
 - status and states [226](#)
 - working with subnets [244](#), [245](#), [246](#)
 - Rogue System Sensor
 - about [223](#)
 - active, configuring [234](#)
 - blacklist [229](#)
 - data gathering [224](#)
 - installation [241](#)
 - installing [242](#)
 - operating systems and [223](#)
 - removing [243](#)
 - RSD settings, configuring [234](#)
 - sensor-to-server port, changing [241](#)
 - status and sensor states [227](#)
 - traffic and intelligent filtering [224](#)
 - working with [240](#)
 - rogue systems
 - about [223](#)
 - system status [226](#)
 - Top 25 Subnets list [228](#)
 - rules
 - configuring contacts for responses [260](#)
 - defaults for notifications [250](#)
 - setting up for notifications, SNMP servers [255](#)
 - Run Tag Criteria action [113](#)
- S**
- schedule server task
 - for policy sharing [167](#)
 - scheduling
 - applying criteria-based tags [116](#)
 - scheduling (*continued*)
 - client tasks [164](#)
 - Repository Pull task [183](#)
 - Repository Replication task [185](#)
 - server tasks with Cron syntax [211](#)
 - scripts, login for agent installation [71](#)
 - security certificate
 - certificate authority (CA) [33](#)
 - installing [34](#)
 - security keys
 - agent-server secure communication (ASSC) [41](#), [46](#)
 - ASSC, working with [46](#), [47](#)
 - backing up [43](#)
 - for content from other repositories [44](#)
 - general [41](#)
 - managing [44](#)
 - master keys in multi-server environments [45](#)
 - private and public [44](#)
 - restoring [43](#)
 - server settings [29](#)
 - using one master key [44](#)
 - selected packages
 - avoid replication of [143](#), [187](#)
 - disabling replication of [144](#)
 - sensor-to-server port [229](#), [241](#)
 - sequencing errors, duplicate GUIDs [72](#)
 - server certificate
 - replacing [31](#)
 - server settings
 - configuring [20](#)
 - configuring Rogue System Detection [232](#)
 - global updating [181](#)
 - Internet Explorer [135](#)
 - notifications [250](#)
 - ports and communication [29](#)
 - proxy, and master repositories [130](#)
 - SSL certificates [33](#)
 - types of [29](#)
 - working with [30](#)
 - Server Task Builder wizard [116](#)
 - server task log
 - about [177](#)
 - filtering for recent activity [210](#)
 - Pull Now task [184](#)
 - purging [211](#)
 - Replicate Now task [186](#)
 - reviewing status of tasks [210](#)
 - working with [210](#)
 - Server Task Log
 - server task [207](#)
 - server tasks
 - allowing Cron syntax [211](#)
 - Data Rollup [203](#)
 - defining email servers [30](#)
 - for policy sharing [166](#)
 - installing Rogue System Sensor [242](#)
 - log file, purging [211](#)
 - replacing server certificate [31](#)
 - Repository Pull, scheduled [183](#)
 - Repository Replication [185](#)
 - scheduling a query [197](#)
 - scheduling with Cron syntax [211](#)
 - Synchronize Domain/AD [108](#)
 - types and definitions [207](#)
 - servers
 - configuring ePO servers [20](#)

- servers (*continued*)
 - ePO server, components 14
 - importing and exporting policies 149
 - importing and exporting queries 200
 - importing policies from 160
 - LDAP servers, registering 40
 - logging on and off 17
 - master repository key pair 44
 - registering additional ePO servers 39
 - registering, for queries 203
 - rollup queries 203
 - server task log, about 177
 - settings and controlling behavior 29
 - sharing policies 159
 - SNMP, and notifications 254
 - SNMP, and responses 254
 - tasks, scheduling repository replication 185
 - viewing license information 18
 - viewing version number 18
- Service Desk
 - sample mappings for (See ticketing servers) 273
- sitelist files 52
- sites
 - deleting source or fallback 139
 - editing existing 138
 - fallback 130, 137
 - switching source and fallback 137
- SNMP servers 41
 - See also responses
 - registering 41
 - See also responses
- Sort Now action 110
- sorting criteria
 - configuring 121
 - for groups 121
 - groups, automated 107
 - IP address 111
 - IP address-based 121
 - sorting systems into groups 110
 - tag-based 107, 111, 121
- source sites
 - about 130
 - configuring 137
 - creating 137
 - deleting 139
 - editing existing 138
 - fallback 130
 - importing from SiteMgr.xml 147
 - product updates and 130
 - pulling from 183, 184
 - switching to fallback 137
 - update packages and 173
- SPIPE 61
- SQL server
 - editing information 286
- SQL servers (See databases) 106
- SSL certificates
 - about 33
- status
 - agent 101
 - security 97
- status monitors
 - detected systems 226
- subgroups
 - and policy management 125
 - criteria-based 112
- subnets
 - active RSD sensors, configuring duration 234
 - in Rogue System Detection 244, 245, 246
 - status, Rogue System Detection 228
 - Top 25 Subnets list 228
- subnets, as grouping criteria 106
- SuperAgent repositories
 - about 132
 - creating 139
 - deleting 141
 - global updating requirements 174
 - replicating packages to 140
 - tasks 139
- SuperAgents
 - distributed repositories 132
 - introduction to 60
 - wake-up calls 63, 92
 - wake-up calls to System Tree groups 92
- synchronization
 - Active Directory and 109
 - defaults 112
 - deploying agents automatically 109
 - excluding Active Directory containers 109
 - NT domains 110
 - preventing duplicate entries 109, 110
 - scheduling 127
 - Synchronize Now action 108
 - systems and structures 109
 - systems only, with Active Directory 109
- synchronization of ticketed issues 272
- system requirements 63
- system status
 - monitors 226
 - Rogue System Detection 226
- system tray icon
 - allow users to update from 98
 - options 97
 - security status 97
 - using 97
 - visibility 93, 98
- System Tree
 - access requirements 105
 - adding systems to 20
 - assigning policies to a group 160
 - child groups and inheritance 104
 - creation, automated 106
 - criteria-based sorting 110
 - defined 104
 - deleting systems from 99, 104
 - grouping agents 58
 - groups and manual wake-up calls 92
 - methods to add systems 20
 - My Organization level 104
 - parent groups and inheritance 104
 - permission sets 105
 - populating groups 116
 - removing agents 99
 - removing agents from systems 99
- System Tree organization
 - borders in your network 106
 - creating groups 116
 - duplicate entries 125
 - importing Active Directory containers 123
 - importing systems and groups 118, 120
 - mapping groups to Active Directory containers 123
 - moving systems to groups manually 128

- System Tree organization (*continued*)
 - network bandwidth [106](#)
 - operating systems [107](#)
 - planning considerations [105](#)
 - text files, importing systems and groups [119](#)
 - using subgroups [125](#)
 - System Tree sorting
 - default settings [112](#)
 - enabling [121](#), [122](#)
 - IP address [111](#)
 - on agent-server communication [111](#)
 - ordering subgroups [112](#)
 - server and system settings [29](#), [111](#)
 - sort systems once [111](#)
 - tag-based criteria [111](#)
 - System Tree synchronization
 - Active Directory integration [108](#)
 - NT domain integration [108](#)
 - scheduling [127](#)
 - to Active Directory structure [123](#)
 - systems
 - adding to System Tree [20](#)
 - assigning policies to [160](#), [161](#)
 - pasting policy assignments to [163](#)
 - policy enforcement for a product [162](#)
 - properties [91](#)
 - sorting into groups [122](#)
 - viewing policy assignment [155](#)
- T**
- tables and charts
 - exported as reports [214](#)
 - report formats [214](#)
 - Tag Builder wizard [113](#)
 - Tag Catalog [113](#)
 - tag-based sorting criteria [107](#), [111](#)
 - tags
 - applying [115](#), [116](#)
 - creating with Tag Builder wizard [113](#)
 - criteria-based [107](#), [110](#)
 - criteria-based sorting [121](#)
 - defined [107](#)
 - excluding systems from automatic tagging [114](#)
 - group sorting criteria [107](#)
 - manual application of [115](#)
 - permissions for [107](#)
 - types [107](#)
 - without criteria [107](#)
 - working with [113](#)
 - Test Sort action [110](#)
 - Threat Event Log
 - about [212](#)
 - working with [213](#)
 - throttling, See notifications
 - ticketed issues
 - about [271](#)
 - assignment to users [271](#)
 - creating [263](#)
 - how comments are handled [271](#)
 - how they are closed [271](#)
 - how they are reopened [272](#)
 - how they are synchronized [272](#)
 - synchronizing [276](#)
 - synchronizing on a schedule [277](#)
 - ticketing servers
 - about sample mappings [273](#)
 - BMC Remedy Action Request System versions 6.3 and 7.0 [272](#)
 - configuring DNS for Service Desk 4.5 [281](#)
 - considerations when deleting [273](#)
 - Hewlett-Packard Openview Service Desk versions 4.5 and 5.1 [272](#)
 - installing extensions for [278](#), [280](#)
 - installing extensions for Remedy [279](#)
 - installing extensions for Service Desk [278](#)
 - integration with [272](#)
 - mapping [281](#), [282](#)
 - mapping issues to tickets [282](#)
 - mapping tickets back to issue status [283](#)
 - registering [281](#)
 - required fields for mapping [273](#)
 - sample mapping for Remedy [275](#)
 - sample mappings for Service Desk [273](#)
 - upgrading [284](#)
 - ticketing systems
 - BMC Remedy Action Request System [263](#)
 - Hewlett-Packard Openview Service Desk [263](#)
 - tickets
 - about [263](#), [271](#)
 - adding to issues [276](#)
 - associations with issues (See ticketed issues) [271](#)
 - creating [263](#), [271](#)
 - how comments are handled [271](#)
 - how they are closed [271](#)
 - how they are reopened [272](#)
 - how they are synchronized [272](#)
 - server integrations for [272](#)
 - synchronizing [276](#)
 - synchronizing on a schedule [277](#)
 - troubleshooting
 - agent activity logs [101](#)
 - product deployment [173](#)
 - upgrading agents by group [82](#)
 - verifying properties of agent and products [89](#)
- U**
- UNC share repositories
 - about [132](#)
 - creating and configuring [141](#)
 - editing [144](#)
 - enabling folder sharing [144](#)
 - uninstallation
 - agent, from UNIX systems [100](#)
 - UNIX
 - agent installation folder [78](#)
 - agent package file name [69](#)
 - converting from managed to unmanaged mode [77](#)
 - converting from unmanaged to managed mode [77](#)
 - installing the agent on [69](#)
 - uninstalling the agent from [100](#)
 - unmanaged mode
 - convert to managed mode in Windows [76](#)
 - convert to managed mode on UNIX [77](#)
 - unmanaged products
 - enabling agent on [76](#)
 - unmanaged repositories [132](#)
 - updater mode
 - convert to managed mode in Windows [76](#)
 - convert to managed mode on UNIX [77](#)
 - updates
 - agent installation packages [82](#)

- updates (*continued*)
 - allow users via system tray icon [98](#)
 - checking in manually [178](#)
 - client tasks [174](#)
 - considerations for creating tasks [174](#)
 - deploying packages with tasks [183](#)
 - deployment packages [173](#)
 - for selected systems [89](#)
 - package signing and security [171](#)
 - packages and dependencies [171](#)
 - running tasks manually [94](#), [95](#)
 - scheduling an update task [190](#)
 - security [97](#)
 - source sites and [130](#)
 - upgrading agents [82](#)
 - updating
 - agents, with login scripts or manually [83](#)
 - automatically, with global updating [181](#)
 - DATs and engine [173](#)
 - deployment tasks [173](#)
 - global, event forwarding and agent settings [85](#)
 - global, process [174](#)
 - manually [94](#), [95](#)
 - master repository with pull tasks [183](#)
 - process description [173](#)
 - Pull Now task to update master repository [184](#)
 - scheduling an update task [190](#)
 - user accounts
 - about [24](#)
 - changing passwords [25](#)
 - creating [24](#)
 - creating permission sets for [26](#)
 - user accounts (*continued*)
 - credentials for agent installation [70](#)
 - deleting [25](#)
 - editing [25](#)
 - enabling user autcreation [32](#)
 - permission sets and [25](#)
 - setting up [20](#)
 - working with [24](#)
 - user interface, agent [93](#)
 - utilities
 - NETDOM.EXE, creating a text file [120](#)
- V**
- viewing issue details [269](#)
 - VPN connections and geographical borders [106](#)
- W**
- wake-up calls
 - about [62](#)
 - manual [92](#)
 - SuperAgents and [63](#), [92](#)
 - tasks [62](#)
 - to System Tree groups [92](#)
 - WAN connections and geographical borders [106](#)
 - Windows
 - agent installation folder [78](#)
 - authentication, configuring [36](#), [37](#)
 - Authorization, configuring [38](#)
 - converting agent mode [76](#)
 - enabling user autcreation [32](#)
 - running a manual update [94](#)