COPYRIGHT
Copyright © 2019 McAfee, LLC

TRADEMARK ATTRIBUTIONS
McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

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

1  Product overview .......................................................... 13
   Overview of McAfee ePO .............................................. 13
   Key features of McAfee ePO ....................................... 13
   How McAfee ePO works .............................................. 14

2  Monitoring the health of your network ................................ 17
   Log on and log off .................................................... 17
   Provide feedback ....................................................... 17
   Navigating the interface .............................................. 18
      Using the McAfee ePO navigation menu ...................... 18
      Customizing the shortcut bar .................................. 18
      Personal settings categories .................................... 19
      Server settings ...................................................... 19
   Working with lists and tables ....................................... 21
      Filter a list ......................................................... 21
      Create a custom filter .......................................... 21
      Search for specific list items ................................. 22
      Clicking table row checkboxes ................................ 22
      Select the Columns to Display page ......................... 23
      Selecting items in tree lists .................................... 23

3  Dashboards and monitors .................................................. 25
   Using dashboards and monitors .................................... 25
   Manage dashboards ................................................... 26
   Export and import dashboards ..................................... 27
   Specify first-time dashboards ..................................... 28
   Manage dashboard monitors ....................................... 29
      Move and resize dashboard monitors ......................... 30
      Set default monitor refresh intervals ....................... 30

4  Generating queries and reports ......................................... 33
   Query and report permissions ..................................... 34
   Introduction to queries .............................................. 35
   Query Builder .......................................................... 36
   Work with queries ..................................................... 37
      Manage custom queries .......................................... 37
      Run a query on a schedule ..................................... 39
      Create a query group ............................................ 39
   About reports .......................................................... 40
   Structure of a report ................................................. 40
   Create a report ........................................................ 41
   Edit an existing report .............................................. 41
      Add elements to a report ....................................... 42
      Configure image report elements ................................ 42
      Configure text report elements ................................ 43
## 5 Disaster Recovery

- **What is Disaster Recovery?**
- **Disaster Recovery components**
- **How Disaster Recovery works**
  - Disaster Recovery Snapshot and backup overview
  - McAfee ePO server recovery installation overview
- **Create Snapshot**
  - Create a snapshot from the McAfee ePO
  - Create snapshot from Web API
- **Configure Disaster Recovery server settings**
- **Open a remote console connection**
- **Plan your disaster recovery**
  - Disaster Recovery
  - Server clusters for disaster recovery
  - Cold and hot spares on one physical site
  - Cold and hot spares on two physical sites

## 6 Using the System Tree and Tags

- **Organizing systems**
  - Considerations when planning your System Tree
  - Active Directory synchronization
  - Types of Active Directory synchronization
  - NT domain synchronization
  - Criteria-based sorting
  - View system information details
  - Creating and populating System Tree groups
  - Add systems to an existing group manually
  - Create groups manually
  - Export systems from the System Tree
  - Create a text file of groups and systems
  - Import systems and groups from a text file
  - Sort systems into criteria-based groups
  - Import Active Directory containers
  - Import NT domains into an existing group
  - Schedule System Tree synchronization
  - Update a synchronized group with an NT domain manually
  - Move systems within the System Tree
  - How Transfer Systems works
  - How the Automatic Responses feature interacts with the System Tree
- **Tags**
  - Create tags
  - Manage tags
  - Create, delete, and change tag subgroups
  - Exclude systems from automatic tagging
  - Create a query to list systems based on tags
  - Apply tags to selected systems
  - Clear tags from systems
  - Apply criteria-based tags to all matching systems
7 User accounts and permission sets

Apply criteria-based tags on a schedule ........................................ 88

7 User accounts and permission sets ............................................. 89

Users ......................................................................................... 89

Managing McAfee ePO users with Active Directory ..................... 89
Windows authentication and authorization strategies ...................... 91
Enable Windows authentication in the McAfee ePO server .............. 91
Configure Windows authentication ............................................. 92
Configure Windows authorization ............................................. 93
Create a custom logon message ............................................. 93
Restrict a user session to a single IP address ............................ 93
The Audit Log ................................................................. 94

Authenticating with certificates .............................................. 96
Configure McAfee ePO for certificate-based authentication ........ 96
Disable certificate-based authentication .................................... 97
Configure user accounts for certificate-based authentication .......... 98
Update the certificate revocation list ...................................... 98
Troubleshooting certificate-based authentication ...................... 99

Permission sets ......................................................................... 100
How users, groups, and permission sets fit together .................. 100
Manage permission sets ....................................................... 101

8 Software Manager ..................................................................... 103

What’s in the Software Manager ............................................ 103
Check in, update, and remove software using the Software Manager .... 104
Checking product compatibility ............................................ 105
Reconfigure Product Compatibility List download .................. 106

9 Manual package and update management .................................. 109

Bring products under management ........................................ 109
Check in packages manually .................................................. 109
Delete DAT or engine packages from the Master Repository ........ 110
Move DAT and engine packages between branches .................. 110
Check in Engine, DAT, and Extra.DAT update packages manually .... 111
Best practice: Automating DAT file testing ............................... 111
Pull and copy DAT updates from McAfee ............................... 113
Best practice: Create a test group of systems ......................... 115
Best practice: Configure an agent policy for the test group .......... 115
Best practice: Configure an on-demand scan of the test group .... 116
Best practice: Schedule an on-demand scan of the test group ....... 117
Best practice: Configure an Automatic Response for malware detection .... 118

10 Deploying products ............................................................... 121

Product deployment steps ....................................................... 121
Choosing a product deployment method .................................. 122
Benefits of product deployment projects .................................. 123
Viewing Product Deployment audit logs ................................ 124
View product deployment ....................................................... 124
Deploy products using a deployment project ............................ 124
Monitor and edit deployment projects ..................................... 126
Global updating ................................................................. 127
Deploy update packages automatically with global updating ....... 128

11 ePO Support Center ............................................................... 131

ePO Server Health ............................................................... 131
Manual server health checks .................................................. 133
6 Support Notifications .......................................................... 134
   Create Support Notification tags ........................................ 134
   Apply Support Notification tags ......................................... 134
   Remove a support notification tag ...................................... 135
   Delete a support notification tag ....................................... 135
   Edit a support notification tag .......................................... 135
   Filter tagged support notifications .................................... 135

Search Support .................................................................. 135

Product Information .......................................................... 136

12 Enforcing policies ......................................................... 137

About policies .................................................................. 137
   When policies are applied and enforced ............................. 138
   How policies are assigned to systems ............................... 139
   Policy ownership ............................................................ 140

Policy assignment rules .................................................... 140
   Policy assignment rule priority ......................................... 140
   User-based policy assignment ......................................... 141
   System-based policy assignment ..................................... 141

Create and manage policies ................................................. 142
   Create a policy from the Policy Catalog page ...................... 142
   Enforcing product policies .............................................. 143
   Enforce policies for a product in a System Tree group ......... 143
   Enforce policies for a product on a system ....................... 143
   Managing policy history .................................................. 144
   Manage policy history ..................................................... 144
   Edit policy history permission sets ................................... 145
   Compare policies ............................................................ 145
   Change the owners of a policy .......................................... 146

Move and share policies between McAfee ePO servers .......... 146
   Register servers for policy sharing .................................... 146
   Designate policies for sharing ......................................... 146
   Schedule server tasks to share policies ............................. 147

Create and manage policy assignment rules ......................... 147
   Create policy assignment rules ......................................... 147
   Manage policy assignment rules ....................................... 148

Policy management users .................................................. 149
   Best practice: Set policy management globally .................... 149
   Create policy management permission sets ....................... 150
   Create policy management users ..................................... 151
   Submit policy changes for acceptance .............................. 152
   Accept policy changes .................................................... 153

Assign policies to managed systems .................................... 153
   Assign a policy to a System Tree group ............................ 153
   Assign a policy to a managed system ............................... 154
   Assign a policy to systems in a System Tree group ............. 154

Copy and paste policy assignments ..................................... 155
   Copy policy assignments from a group ............................. 155
   Copy policy assignments from a system ............................ 155
   Paste policy assignments to a group ................................ 156
   Paste policy assignments to a specific system .................... 156

View policy information .................................................... 156
   View groups and systems where a policy is assigned .......... 157
   View policy settings ...................................................... 157
   View policy ownership .................................................. 158
   View assignments where policy enforcement is disabled ...... 158
13 Server and client tasks

Server tasks
- View server tasks
- Server task status
- Create a server task
- Remove outdated server tasks from the Server Task Log: best practice
- Remove outdated log items automatically
- Accepted Cron syntax when scheduling a server task

Client tasks
- How the Client Task Catalog works
- Deployment tasks
- Use the Product Deployment task to deploy products to managed systems
- Updating tasks
- Manage client tasks

14 Setting up automatic responses

Using Automatic Responses
- Event thresholds
- Default automatic response rules
- Response planning
- Determine how events are forwarded
  - Determine which events are forwarded immediately
  - Determine which events are forwarded to the server
- Configure Automatic Responses
  - Assign permissions to notifications
  - Assign permissions to Automatic Responses
  - Manage SNMP servers
- Choose a notification interval
- Create and edit Automatic Response rules
  - Define a rule
  - Set filters for the rule
  - Set Aggregation and grouping criteria for the rule
  - Configure the actions for an automatic response rule

15 Manage registered executables and external commands

16 Agent-server communication

How agent-server communication works
- Best practices: Estimating and adjusting the ASCI
  - Estimating the best ASCI: best practice
  - Configure the ASCI setting: best practice
- Managing agent-server communication
  - Allow agent deployment credentials to be cached
  - Change agent communication ports

17 Automating and optimizing McAfee ePO workflow

Best practice: Find systems with the same GUID
- Best practices: Purging events automatically
  - Create a purge events server task best practice
  - Purge events by query
### Contents

- Export the repository list for backup or use by other servers ........................................... 252
- Import distributed repositories from the repository list ......................................................... 252
- Import source sites from the SiteMgr.xml file ........................................................................ 252
- Change credentials on multiple distributed repositories ......................................................... 253
- Pulling tasks ......................................................................................................................... 253
- Replication tasks ................................................................................................................ 254
- Repository selection ........................................................................................................... 254

#### 19 Agent Handlers

- How Agent Handlers work ..................................................................................................... 257
- Agent Handler details ............................................................................................................ 259
- Best practice: Agent Handlers eliminate multiple McAfee ePO servers ................................. 261
- Agent Handler functionality ................................................................................................ 261
- Providing scalability ............................................................................................................. 261
- Failover protection with Agent Handlers best practice ......................................................... 262
- Best practices: Network topology and deployment considerations ....................................... 263

Best Practices: Agent Handler installation and configuration ............................................. 266
- Deployment considerations ................................................................................................. 266
- Agent Handler configuration overview ............................................................................... 266
- Configure Agent Handlers list ............................................................................................ 268
- Configure Agent Handlers groups and virtual groups ......................................................... 268
- Configure Agent Handlers priority ..................................................................................... 269
- Configure assignments for Agent Handlers ....................................................................... 269

Best Practices: Adding an Agent Handler in the DMZ ......................................................... 270
- Install software and configure the Agent Handler ............................................................... 271
- Connect an Agent Handler in the DMZ to a McAfee ePO server in a domain ..................... 274
- Handler groups and priority ............................................................................................... 275
- Assign McAfee agents to Agent Handlers ......................................................................... 276
- Manage Agent Handler assignments ................................................................................. 277
- Create Agent Handler groups ............................................................................................ 277
- Manage Agent Handler groups .......................................................................................... 278
- Move agents between handlers .......................................................................................... 278
- Group agents using Agent Handler assignments .............................................................. 278
- Group agents by assignment priority ................................................................................. 279
- Group agents using the System Tree ............................................................................... 280
- Frequently asked questions ............................................................................................... 280

#### 20 Maintaining your McAfee ePO server, SQL databases, and bandwidth

- Maintaining your McAfee ePO server ................................................................................... 283
- Best practices: Monitoring server performance .................................................................. 283
- Maintaining your SQL database .......................................................................................... 286
- Best practices: Recommended tasks .................................................................................... 288
- Managing SQL databases ..................................................................................................... 296
- Best practice: Maintaining SQL databases ........................................................................ 296
- Use a remote command to determine the Microsoft SQL database server and name ...... 297
- Configure a Snapshot and restore the SQL database .......................................................... 297
- Use Microsoft SQL Server Management Studio to find McAfee ePO server information .... 299
- Common event format .......................................................................................................... 299
- Bandwidth usage .................................................................................................................. 301
- Best practice: Agent deployment and bandwidth ............................................................... 302
- Best practices: Bandwidth recommendations for repository distribution ......................... 303

#### 21 Reporting with queries

- Reporting features ............................................................................................................... 307
- Best practices: How to use custom queries ......................................................................... 308
Create custom event queries
How event summary queries work best practice
Create custom table queries: best practice
Multi-server rollup querying
Create a Rollup Data server task
Create a query to define compliance
Generate compliance events
Export query results to other formats
Best practices: Running reports with the web API
Use the web URL API or the McAfee ePO user interface
McAfee ePO command framework: best practice
Using the web URL Help: best practice
Using S-Expressions in web URL queries: best practice
Parsing query export data to create web URL queries best practice
Run query with ID number: best practice
Run query with XML data best practice
Run query using table objects, commands, and arguments: best practice

22 Adding systems connected over a VPN
Determining connected VPN server’s OUI
Use the System Tree to find VPN server MAC address
Create report to find VPN server MAC address best practice
Best practice: Use SQL Server Management Studio to add virtual MAC vendor ID value

22 Adding systems connected over a VPN
Determining connected VPN server’s OUI
Use the System Tree to find VPN server MAC address
Create report to find VPN server MAC address best practice
Best practice: Use SQL Server Management Studio to add virtual MAC vendor ID value

A Registered servers
Register McAfee ePO servers
Using database servers
Register a database server
Modify a database registration
Remove a registered database
Register SNMP servers
Register syslog servers
Register LDAP servers
Mirroring an LDAP server
Sharing objects between servers
Export objects and data from your McAfee ePO server
Importing items into McAfee ePO

B Issues
Issues and how they work
View issues
Remove closed issues from the Issues table
Create issues manually
Configure responses to automatically create issues
Manage issues
Use tickets with McAfee ePO

C SSL certificates
Create a self-signed certificate with OpenSSL
Other useful OpenSSL commands
Convert an existing PVK file to a PEM file
Migrate SHA-1 certificates to SHA-2 or higher
Security keys and how they work
Master Repository key pair
Other repository public keys
Manage repository keys
Product overview

Overview of McAfee ePO

McAfee ePolicy Orchestrator™ (McAfee® ePO™) is an extensible platform that enables centralized policy management and enforcement of your security policies.

McAfee ePO performs complete network management, detecting threats and protecting endpoints against these threats.

By using McAfee ePO, you can perform many network and client tasks, including:

- Managing and enforcing network and endpoint security using policy assignments and client tasks.
- Monitoring the health of your network.
- Collecting data on events and alerts.
- Creating reports using the query system builder, which displays configurable charts and tables of your network security data.
- Automating product deployments, patch installations, and security updates.

Contents

- Key features of McAfee ePO
- How McAfee ePO works

Key features of McAfee ePO

McAfee ePO software provides flexible, automated management to identify and respond quickly to security issues and threats.

From the single view of McAfee ePO, you can access managed clients, networks, data, and compliance solutions to protect your network.

Flexible security management

- Organize managed systems in groups to monitor, assign policies, schedule tasks, and take actions.
- Allow users access to specific groups of systems or give administrators full control.
- Open framework unifies security management for systems, applications, networks, data, and compliance solutions.
- Unify security management across endpoints, networks, data, and compliance solutions from McAfee and third-party solutions.
- Define how McAfee ePO software directs alerts and security responses based on the type and criticality of security events in your environment.
Streamlined processes

- Guided Configuration, automated workflows, and predefined dashboards protect your network clients.
- Tag-based policies allow you to precisely assign predefined security profiles to systems based on their business role or at-risk status.
- Server Task Catalog and automated management capabilities streamline administrative processes and reduce overhead.
- Automated workflows between your security and IT operations systems quickly remediate outstanding issues.

Support for large-scale enterprise deployments

- Enterprise-class architecture supports hundreds of thousands of devices on a single server, and complex and diverse IT environments.
- McAfee ePO supports enterprise reporting across on-premises and cloud security information.

Unified view of your environment

- A single web interface aligns security processes for maximum visibility, while a single agent reduces the risk of endpoint conflicts.
- Drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks.
- Shorten response time through actionable dashboards with advanced queries and reports.
- Rogue System Detection identifies unknown assets on your network, and brings them under control.

How McAfee ePO works

McAfee security software and McAfee ePO work together to stop malware attacks on your systems and notify you when an attack occurs.

How McAfee software responds to an attack

This diagram shows the components and processes that stop an attack, notify you when the attack occurs, and record the incident.

1. Malware attacks a computer in your McAfee ePO managed network.
2. McAfee product software, for example McAfee® Endpoint Security, cleans or deletes the malware file.
3. McAfee Agent notifies McAfee ePO of the attack.
4. McAfee ePO stores the attack information.
5. McAfee ePO displays the notification of the attack on the Number of Threat Events dashboard and saves the history of the attack in the Threat Event Log.
McAfee ePO components

The architecture of the McAfee ePO software and its components is designed to help you successfully manage and protect your environment, no matter how large or small.

1 McAfee ePO server — Provides these features:
   • Manages and deploys products, upgrades, and patches
   • Connects to the McAfee ePO update server to download the latest security content
   • Enforces policies on your endpoints
   • Collects events, product properties, and system properties from the managed endpoints and sends them back to McAfee ePO
   • Reports on your endpoint security

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

3 McAfee Agent installed on clients — Provides these features:
   • Policy enforcement
   • Product deployments and updates
   • Connections to send events, product, and system properties to the McAfee ePO server

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

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

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

7 Distributed repositories — Host your security content locally throughout your network so that agents can receive updates more quickly.

8 Agent Handlers — Reduces the workload of the server by off-loading event processing and McAfee Agent connectivity duties.
9 **LDAP or Ticketing system** — Connects your McAfee ePO server to your LDAP server or SNMP ticketing server.

10 **Automatic Responses** — Notifies administrators and task automation when an event occurs.

11 **Web Console connection** — Provides HTTPS connection between the McAfee ePO server and the web browser using default port 8443.

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

13 **Agent Handler in DMZ** — Agent Handlers installed in the DMZ require specific port connections.

Figure 1-1 Major McAfee ePO components
Monitoring the health of your network

Log on to the console to configure McAfee ePO to manage and monitor your network security.

Contents
- Log on and log off
- Provide feedback
- Navigating the interface
- Working with lists and tables

Log on and log off
To access the McAfee ePO software, enter your user name and password on the logon screen.

Before you begin
You must have an assigned user name and password before you can log on to McAfee ePO.

When you connect to McAfee ePO, the first screen you see is the McAfee ePO logon screen.

Task
1. Type your user name, password, and click Log On.
   
   Your McAfee ePO software displays the default dashboard.

2. To end your McAfee ePO session, click Log Off.

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

Provide feedback
Submit information about your McAfee ePO experience including product concept submissions, feature requests, and comments.

Task
1. From the McAfee ePO console, in the upper-right corner, click Feedback.

2. In the Provide Feedback window, enter your information.

3. Click Send.

Thank you for taking the time to send your feedback. Although we can’t guarantee a response, we appreciate your suggestions.
Navigating the interface

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

Menu sections represent top-level features like Reporting, Systems, and Policy. As you add managed products to McAfee ePO, the main menu options like Dashboards, System Tree, and Policy Catalog include new options to select.

Using the McAfee ePO navigation menu

Open the McAfee ePO menu to navigate the McAfee ePO interface.

The menu uses categories that include features and functionality of McAfee ePO. Each category contains a list of primary feature pages associated with a unique icon. Select a category in Menu to view and navigate to the primary pages that make up that feature.

Customizing the shortcut bar

Customize the shortcut bar for quick access to the features and functionality you use most often.

You can decide which icons are displayed on the shortcut bar by dragging any menu item on or off the shortcut bar.

When you place more icons on the shortcut bar than can be viewed, an overflow menu is created on the right side of the bar. Click the down-arrow to access the hidden menu items not displayed in the shortcut bar.

The icons displayed in the shortcut bar are stored as user preferences. Each user’s customized shortcut bar is displayed regardless of which console they use to log on to the server.
Personal settings categories
Adjust personal settings to tailor your McAfee ePO experience. Your customizations affect only your user sessions.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Changes your McAfee ePO logon password.</td>
</tr>
<tr>
<td>Queries and Reports Warning</td>
<td>Determines whether a warning message appears when you try to drag a query from one query group to another.</td>
</tr>
<tr>
<td>System Tree Warning</td>
<td>Determines whether a warning message appears when you try to drag systems or groups from one System Tree group to another.</td>
</tr>
<tr>
<td>Tables</td>
<td>Specifies how often auto-refreshed tables are refreshed during your session.</td>
</tr>
<tr>
<td>User Session</td>
<td>Controls the length of time that your user session remains open after you stop interacting with the user interface.</td>
</tr>
</tbody>
</table>

Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Categories</td>
<td>Lists the available settings that you can view and change. Selecting a category displays its current settings.</td>
</tr>
<tr>
<td>Search box</td>
<td>Highlights the category that matches the search text. Enter the first few characters of the category you want to find.</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to change the current settings.</td>
</tr>
</tbody>
</table>

Server settings
Adjust server settings to fine-tune McAfee ePO for the needs of your organization. Your customizations affect all your McAfee ePO users.

Here are descriptions of the default categories.

For descriptions of the categories provided by managed products, see your managed product documentation.

Table 2-1 Default server settings

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Groups</td>
<td>Specifies the LDAP server to use for each domain.</td>
</tr>
<tr>
<td>Active Directory User Login</td>
<td>Specifies whether members of your mapped Active Directory (AD) groups can log on to your server using their AD credentials once the Active Directory User Login feature is fully configured.</td>
</tr>
<tr>
<td>Agent Contact Method</td>
<td>Specifies the priority of methods that McAfee ePO uses when it attempts to contact a McAfee Agent.</td>
</tr>
<tr>
<td></td>
<td>To change the priority, select Agent Contact Method under Setting Categories, click Edit, then select the priority. Each contact method must have a different priority level. The methods to contact a McAfee Agent are:</td>
</tr>
<tr>
<td></td>
<td>• Fully Qualified Domain Name</td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td>Agent Deployment Credentials</td>
<td>Specifies whether users are allowed to cache agent deployment credentials.</td>
</tr>
<tr>
<td>Certificate Based Authentication</td>
<td>Specifies whether Certificate Based Authentication is enabled, and the settings and configurations required for the Certificate Authority (CA) certificate being used.</td>
</tr>
</tbody>
</table>
Table 2-1  Default server settings (continued)

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>Specifies the default active dashboard that is assigned to new users’ accounts at the time of account creation, and the default refresh rate (5 minutes) for dashboard monitors.</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Enables and sets the keystore encryption passphrase for Disaster Recovery.</td>
</tr>
<tr>
<td>Email Server</td>
<td>Specifies the email server that McAfee ePO uses to send email messages.</td>
</tr>
<tr>
<td>Event Filtering</td>
<td>Specifies which events the agent forwards.</td>
</tr>
<tr>
<td>Event Notifications</td>
<td>Specifies how often McAfee ePO checks your notifications to see if any trigger Automatic Responses.</td>
</tr>
<tr>
<td>Global Updating</td>
<td>Specifies whether and how global updating is enabled.</td>
</tr>
<tr>
<td>License Key</td>
<td>Specifies the license key used to register this McAfee ePO software.</td>
</tr>
<tr>
<td>Logon Message</td>
<td>Specifies whether a custom message is displayed when users log on to the McAfee ePO console, and the message content.</td>
</tr>
<tr>
<td>Policy and Task Retention</td>
<td>Specifies whether the policies and client task data is removed when you delete the product extension.</td>
</tr>
<tr>
<td>Ports</td>
<td>Specifies the ports used by the server when it communicates with agents and the database.</td>
</tr>
<tr>
<td>Printing and Exporting</td>
<td>Specifies how information is exported to other formats, and the template for PDF exports. It also specifies the default location where the exported files are stored.</td>
</tr>
<tr>
<td>Product Compatibility List</td>
<td>Specifies whether the Product Compatibility List is automatically downloaded and whether it displays any incompatible product extensions.</td>
</tr>
<tr>
<td>Product Improvement Program</td>
<td>Specifies whether McAfee ePO can collect data proactively and periodically from the managed client systems.</td>
</tr>
<tr>
<td>Proxy Settings</td>
<td>Specifies the type of proxy settings configured for your McAfee ePO server.</td>
</tr>
<tr>
<td>Scheduler Tasks</td>
<td>Specifies the number of server tasks that run at the same time.</td>
</tr>
<tr>
<td>Security Keys</td>
<td>Specifies and manages the agent-server secure communication keys and repository keys.</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>Specifies the server certificate that your McAfee ePO server uses for HTTPS communication with browsers.</td>
</tr>
<tr>
<td>Server Information</td>
<td>Specifies Java, OpenSSL, and Apache server information, such as name, IP address, and version information.</td>
</tr>
<tr>
<td>Software Evaluation</td>
<td>Specifies the information required to enable check-in and deployment of evaluation software from the Software Manager.</td>
</tr>
<tr>
<td>Source Sites</td>
<td>Specifies which source sites your server connects to for updates, and which sites are fallback sites.</td>
</tr>
<tr>
<td>System Details</td>
<td>Specifies which queries and systems properties are displayed in the System Details page for your managed systems.</td>
</tr>
<tr>
<td>System Tree Sorting</td>
<td>Specifies whether and how System Tree sorting is enabled in your environment.</td>
</tr>
<tr>
<td>User Policies</td>
<td>Enables or disables database mirroring to improve performance for policy assignment rules.</td>
</tr>
<tr>
<td>User Session</td>
<td>Specifies the amount of time a user can be inactive before the system logs them out.</td>
</tr>
</tbody>
</table>
Configure server settings
To familiarize yourself with configuring server settings, change the user session timeout interval from the default 30 minutes to 60 minutes.

By default when you are logged on to McAfee ePO, if you don’t use the interface for 30 minutes, the user session closes and you must log back on. Change the default setting to 60 minutes.

Task

1. Select Menu | Configuration | Server Settings, select User Session from the Setting Categories, then click Edit.

2. Configure these settings, then click Save.
   - Default session timeout interval (minutes) — Type 60 to replace the default.
   - Maximum session timeout interval (minutes) — Type 60 to replace the default.

Now you aren't prompted to log on after only 30 minutes of inactivity.

Working with lists and tables
Use McAfee ePO search and filter functions to sort lists of data.
Lists of data in McAfee ePO can have hundreds or thousands of entries. Manually searching for specific entries in these lists can be hard without the Quick Find search filter.

This screenshot shows the Quick Find search filter for queries.

Filter a list
Use filters to select specific rows in the lists of data in the McAfee ePO interface.

Task

1. From the bar at the top of a list, select the filter that you want to use to filter the list.
   Only items that meet the filter criteria are displayed.

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

Only the selected rows are displayed.
Create a custom filter
Custom filters help you quickly sort through long lists of table entries, such as log items or server tasks, so you can focus on relevant information. The custom filters you create are added to the Custom filter drop-down at the top of your table, so you can reuse them later.

Task

1. From the top of the table, select Custom | Add.
2. From the Available Properties list, click the properties you want to include in your filter.
   The selected properties move the Property pane.
3. For each property, select a comparison and a value.
   The options you can select depend on the property you selected. Use the + or - signs to add or remove comparison and value pairs.
4. Once all the properties that you selected are populated with valid and complete values, click Update Filter.

The new custom filter appears in the Custom drop-down list.

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

Task

1. Enter your search terms in the Quick Find field.
2. Click Apply.

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

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

Example: Find detection queries
Here is an example of a valid search for a specific list of queries.

1. Select Menu | Reporting | Queries & Reports, then click Query.
   All queries that are available in McAfee ePO appear in the list.

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

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

Clicking table row checkboxes
The McAfee ePO interface has special table row selection actions and shortcuts that allow you to select table row checkboxes using click or Shift+click.

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

This table row selection action does not work in the Audit Log table.
This table lists the actions used to select table row checkboxes.

<table>
<thead>
<tr>
<th>To select...</th>
<th>Action</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual rows</td>
<td>Click checkbox for individual rows.</td>
<td>Selects each individual row independently.</td>
</tr>
<tr>
<td>Group of rows</td>
<td>Click one checkbox, then hold <strong>Shift</strong> while you click the last checkbox in the group.</td>
<td>Selects all rows between and including the first and last rows that you clicked.</td>
</tr>
<tr>
<td>All rows</td>
<td>Click the top checkbox in table headings.</td>
<td>Selects every row in the table.</td>
</tr>
</tbody>
</table>

**Select the Columns to Display page**

Use this page to choose the columns to display for the table on the selected page. Available columns of data depend on the table you are configuring.

**Table 2-2 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Columns</strong></td>
<td>Available columns of data depend on the table you are configuring. Click the column titles or the icons next to them to move them to the <strong>Selected Columns</strong> list.</td>
</tr>
<tr>
<td><strong>Selected Columns</strong></td>
<td>Shows the columns currently selected for display in the associated table. You can change or reorder the columns using the:</td>
</tr>
<tr>
<td></td>
<td>• Delete icon (x) — Removes column from the selections.</td>
</tr>
<tr>
<td></td>
<td>• Left arrow icon (&lt;) — Moves column to the left.</td>
</tr>
<tr>
<td></td>
<td>• Right arrow icon (&gt;) — Moves column to the right.</td>
</tr>
</tbody>
</table>

**Selecting items in tree lists**

You can press **Ctrl+click** to select consecutive or non-consecutive items in tree lists.

Hierarchical tree lists, for example System Tree (Subgroups) and Tag Group Tree lists, let you select list items:

- Individually — Click an item.
- As a consecutive group — Press **Ctrl+click** and select the items sequentially.
- As a non-consecutive group — Press **Ctrl+click** and select each item individually.
Dashboards and monitors

Dashboards help you keep constant watch on your environment. Dashboards are collections of monitors. Monitors condense information about your environment into easily understood graphs and charts.

Usually, related monitors are grouped on a specific dashboard. For example, the Threat Events dashboard contains four monitors that display information about threats to your network.

You must have the right permissions to view or modify dashboards and monitors.

Contents

- Using dashboards and monitors
- Manage dashboards
- Export and import dashboards
- Specify first-time dashboards
- Manage dashboard monitors
- Move and resize dashboard monitors
- Set default monitor refresh intervals

Using dashboards and monitors

Customize your dashboards and monitors to get the information you need for your role and environment. Dashboards are collections of monitors. Monitors condense information about your environment into easily understood graphs and charts. Usually, related monitors are grouped on a specific dashboard. For example, the Threat Events dashboard contains four monitors that display information about threats to your network.

The McAfee ePO console has a default dashboard that appears the first time you log on. The next time you log on, the Dashboards page displays the last dashboard you used.

If you have deleted all default dashboards, when you start McAfee ePO, this text appears in the middle of the dashboards page: No dashboards are configured. Create a new dashboard or import an existing dashboard.

You can switch dashboards by selecting a different dashboard from the drop-down list. There are three different kinds of dashboards you can choose from.

- **McAfee Dashboards** — McAfee dashboards are not editable, and can be viewed by all users. You can duplicate a McAfee Dashboard as a starting point for your own customized dashboards.

- **Public Dashboards** — Public dashboards are user-created dashboards that are shared across users.

- **Private Dashboards** — These are the dashboards you have created for your own use. Private dashboards are not shared across users.

When you create a private or public dashboard, you can drag and drop the monitors you want from the Monitor Gallery to the new dashboard.
Manage dashboards

Create, edit, duplicate, delete, and assign permissions to dashboards.

**Before you begin**
You must have the correct permissions to modify a dashboard.

The default dashboards and predefined queries, shipped with ePolicy Orchestrator Cloud, cannot be modified or deleted. To change them, duplicate, rename, and modify the renamed dashboard or query.

**Task**

1. Select **Menu | Reporting | Dashboards**, to navigate to the Dashboards page.
2. Select one of these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a dashboard</td>
<td>To create a different view on your environment, create a new dashboard.</td>
</tr>
<tr>
<td></td>
<td>1 Click Dashboard Actions</td>
</tr>
<tr>
<td></td>
<td>2 Type a name, select a dashboard visibility option, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>A new blank dashboard is displayed. You can add monitors to the new dashboard as needed.</td>
</tr>
<tr>
<td>Edit and assign permissions to a dashboard</td>
<td>Dashboards are only visible to users with proper permission. Dashboards are assigned permissions identically to queries or reports. They can either be entirely private, entirely public, or shared with one or more permission sets.</td>
</tr>
<tr>
<td></td>
<td>1 Click Dashboard Actions</td>
</tr>
<tr>
<td></td>
<td>2 Select a permission:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private</strong> — Do not share this dashboard</td>
</tr>
<tr>
<td></td>
<td>• <strong>Public</strong> — Share this dashboard with everyone</td>
</tr>
<tr>
<td></td>
<td>• <strong>Shared</strong> — Share this dashboard with the following permission sets</td>
</tr>
<tr>
<td></td>
<td>With this option, you must also choose one or more permission sets.</td>
</tr>
<tr>
<td></td>
<td>3 Click <strong>OK</strong> to change the dashboard.</td>
</tr>
<tr>
<td></td>
<td>It is possible to create a dashboard with more expansive permissions than one or more queries contained on the dashboard. If you do this, users that have access to the underlying data will see the query when opening the dashboard. Users that do not have access to the underlying data will receive a message telling them they do not have permission for that query. If the query is private to the dashboard creator, only the dashboard creator can modify the query or remove it from the dashboard.</td>
</tr>
</tbody>
</table>
### Action Steps

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Duplicate a dashboard   | Sometimes the easiest way to create a new dashboard is to copy an existing one that's close to what you want.  
1. Click **Dashboard Actions | Duplicate**.  
2. ePolicy Orchestrator Cloud names the duplicate by appending " (copy)" to the existing name. If you want to modify this name, do so now and click **OK**.  
The duplicated dashboard now opens. The duplicate is an exact copy of the original dashboard including all permissions. Only the name is changed. |
| Delete a dashboard      | 1. Click **Dashboard Actions | Delete**.  
2. Click **OK** to delete the dashboard.  
The dashboard is deleted and you see the system default dashboard. Users who had this dashboard as their last viewed dashboard see the system default dashboard when they next log on. |

---

## Export and import dashboards

Once you have fully defined your dashboard and monitors, the fastest way to migrate them to other McAfee ePO servers is to export them and import them onto the other servers.

### Before you begin

To import a dashboard, you must have access to a previously exported dashboard contained in an XML file.

A dashboard exported as an XML file can be imported to the same or a different system.

### Task

1. Select **Menu | Reporting | Dashboards**.
2. Select one of these actions.
### Export dashboard

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Export dashboard</td>
<td>1. Click **Dashboard Actions</td>
<td>Export**. Your browser attempts to download an XML file according to your browser settings.</td>
</tr>
<tr>
<td></td>
<td>2. Save the exported XML file to an appropriate location.</td>
<td></td>
</tr>
</tbody>
</table>

### Import dashboard

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Import dashboard</td>
<td>1. Click **Dashboard Actions</td>
<td>Import**. The Import Dashboard dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Browse</strong> and select the XML file containing an exported dashboard. Click <strong>Open</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Save</strong>. The Import Dashboard confirmation dialog box appears. The name of the dashboard in the file is displayed, as well as how it will be named in the system. By default, this is the name of the dashboard as exported with <em>(imported)</em> appended.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>. If you do not want to import the dashboard, click <strong>Close</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

The imported dashboard is displayed. Regardless of their permissions at the time they were exported, imported dashboards are given private permissions. If you want them to have different permissions, change them after you import the dashboard.

### Specify first-time dashboards

Use the Dashboards server setting to determine which dashboard appears when a user logs on for the first time.

You can specify which dashboard a user sees when they first log on by mapping the dashboard to the user's permission set. Mapping dashboards to permission sets ensures that users assigned a particular role are automatically presented with the information they need.

**Task**

1. Open the Edit Dashboards page.
   - Select **Menu | Configuration | Server Settings**.
   - From the **Setting Categories** list, select **Dashboards**.
   - Click **Edit**.
2. Next to **Default dashboard for specific permission sets**, specify the default dashboard that appears for each permission set. Select a permission set and default dashboard from the menus.
   - Use + and - to add or remove permission set and dashboard pairs. You don't have to specify a default dashboard for every permission set.
   - The order of the pairs determines which default dashboard appears to users with more than one assigned permission set.
3. Click **Save**.

The first time a user logs on, the dashboard you specified for their permission set appears. Subsequent logons return the user to the page they were on when they logged off.
# Manage dashboard monitors

You can create, add, and remove monitors from dashboards.

**Before you begin**

You must have write permissions for the dashboard you are modifying.

If you do not have the necessary rights or product licenses to view a monitor, or if the underlying query for the monitor is no longer available, a message displays in place of the monitor.

## Task

1. Select **Menu | Reporting | Dashboards**. Select a dashboard from the Dashboard drop-down list.
2. Select one of these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Add a monitor   | 1. Click **Add Monitor**. The Monitor Gallery appears at the top of the screen.  
                        2. Select a monitor category from the **View** drop-down list. The available monitors in that category appear in the gallery.  
                        3. Drag a monitor onto the dashboard. As you move the cursor around the dashboard, the nearest available drop location is highlighted. Drop the monitor into your wanted location. The New Monitor dialog appears.  
                        4. Configure the monitor as needed (each monitor has its own set of configuration options), then click **OK**.  
                        5. After you have added monitors to this dashboard, click **Save Changes** to save the newly configured dashboard.  
                        6. When you have completed your changes, click **Close**.  
                        If you add a Custom URL Viewer monitor that contains Adobe Flash content or ActiveX controls to a dashboard, it is possible the content might obscure McAfee ePO menus, making portions of the menu inaccessible. |
| Edit a monitor  | Every monitor type supports different configuration options. For example, a query monitor allows the query, database, and refresh interval to be changed.  
                        1. Choose a monitor to manage, click the arrow in its top-left corner, and select **Edit Monitor**. The monitor’s configuration dialog appears.  
                        2. When you have completed modifying the monitor’s settings, click **OK**. If you decide to not make changes, click **Cancel**.  
                        3. If you decide to save the resulting changes to the dashboard, click **Save**, otherwise click **Discard**. |
| Remove a monitor| 1. Choose a monitor to remove, select the arrow in its top-left corner, and select **Remove Monitor**. The monitor’s configuration dialog appears.  
                        2. When you are finished modifying the dashboard, click **Save Changes**. To revert the dashboard to its prior state, click **Discard Changes**. |
Move and resize dashboard monitors

You can move and resize monitors to efficiently use screen space.

**Before you begin**
You must have write permissions for the dashboard you are modifying.

You can change the size of many dashboard monitors. If the monitor has small diagonal lines in its bottom-right corner, you can resize it. Monitors are moved and resized through drag and drop within the current dashboard.

**Task**

1. **Move or resize a monitor:**
   - **To move a dashboard monitor:**
     1. Drag the monitor by its title bar to where you want it to appear.
        As you move the cursor, the background outline of the monitor shifts to the closest available location for the monitor.
     2. When the background outline has shifted to the location you want, drop the monitor.
        If you attempt to drop the monitor in an invalid location, it returns to its prior location.
   - **To resize a dashboard monitor:**
     1. Drag the resize icon in the bottom-right corner of the monitor toward an appropriate location.
        As you move the cursor, the background outline of the monitor changes shape to reflect the supported size closest to the current cursor location. Monitors might enforce a minimum or maximum size.
     2. When the background outline has changed shape to a size you want, drop the monitor.
        If you attempt to resize the monitor to a shape not supported in the monitor's current location, it returns to its prior size.

2. **Click Save Changes.** To revert to the prior configuration, click Discard Changes.

Set default monitor refresh intervals

Use the Dashboards server setting to specify the default rate at which new monitors are refreshed. Monitors are refreshed automatically. Each time a refresh occurs, the underlying query runs, and the results are displayed on the dashboard. Choose a default refresh interval for new monitors that is frequent enough to ensure accurate and timely information is displayed without consuming undue network resources. The default interval is five minutes.

**Task**

1. **Open the Edit Dashboards page.**
   - **a** Select Menu | Configuration | Server Settings.
   - **b** From the Setting Categories list, select Dashboards.
   - **c** Click Edit.
2 Next to **Default refresh interval for new monitors**, enter a value between one minute and 60 hours.

3 Click **Save**.

New monitors are refreshed according to the interval you specified. Existing monitors retain their original refresh interval.

*Users can always change the refresh interval of an individual monitor in the Edit Monitor window.*
Dashboards and monitors
Set default monitor refresh intervals
McAfee ePO comes with its own querying and reporting capabilities. Included are the Query Builder and Report Builder, which create and run queries and reports that result in user-configured data in user-configured charts and tables. The data for these queries and reports can be obtained from any registered internal or external database in your ePolicy Orchestrator Cloud system.

In addition to the querying and reporting systems, you can use these logs to gather information about activities on your McAfee ePO server and your network:

- Audit Log
- Server Task Log
- Threat Event Log

**Queries**

Queries enable you to poll McAfee ePO data. Information gathered by queries is returned in the form of charts and tables.

A query can be used to get an answer right now. Query results can be exported to several formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can also be used as dashboard monitors, enabling near real-time system monitoring. Queries can also be combined into reports, giving a more broad and systematic look at your McAfee ePO software system.

The default dashboards and predefined queries shipped with McAfee ePO cannot be changed or deleted. But you can duplicate them, then rename and change them as needed.

- Query results are actionable — Query results displayed in tables have actions available for selected items. 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 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, you cannot select an action when viewing exported data. You can export to these file formats: .csv, .xml, .html, and .pdf.
- Combining queries in reports — Reports can contain any number of queries, images, static text, and other items. They can be run on demand or on a regular schedule, and produce PDF output for viewing outside McAfee ePO.
- Sharing queries between servers — Any query can be imported and exported, allowing you to share queries between servers. In a multi-server environment, you only have to create a query once.
- Retrieving data from different sources — Queries can retrieve data from any registered server, including databases external to McAfee ePO.
Reports

Reports package query results into a PDF document, enabling offline analysis.

Generate reports to share information about your network environment, such as threat events and malware activity, with security administrators and other stakeholders.

Reports are configurable documents that display data from one or more queries, drawing data from one or more databases. The most recently run result for every report is stored within the system and is readily available for viewing.

You can restrict access to reports by using groups and permission sets in the same manner you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this allows for consistent access control.

Contents

- Query and report permissions
- Introduction to queries
- Query Builder
- Work with queries
- About reports
- Structure of a report
- Create a report
- Edit an existing report
- Run a report on a schedule
- View report output
- Configure the template and location for exported reports
- Group reports together

Query and report permissions

Restrict access to queries and reports in a number of ways.

To run a query or report, you need permissions to not only that query or report, but the feature sets associated with their result types. A query's results pages only provide access to permitted actions given your permission sets.

Groups and permission sets control access to queries and reports. All queries and reports must belong to a group, and access to that query or report is controlled by the permission level of the group. Query and report groups have one of the following permission levels:

- **Private** — The group is only available to the user that created it.
- **Public** — The group is shared globally.
- **By permission set** — The group is only available to users assigned the selected permission sets.

Permission sets have four levels of access to queries or reports. These permissions include:

- **No permissions** — The Query or Report tab is not available to users with no permissions.
- **Use public queries** — Grants permission to use any queries or reports that have been placed in a Public group.
• **Use public queries; create and edit personal queries** — Grants permission to use any queries or reports that have been placed in a Public group, as well as the ability to use the Query Builder to create and edit queries or reports in Private groups.

• **Edit public queries; create and edit personal queries; make personal queries public** — Grants permission to use and edit any queries or reports placed in Public groups, create and edit queries or reports in Private groups, as well as the ability to move queries or reports from Private groups to Public or Shared groups.

---

### Introduction to queries

Queries enable you to poll McAfee ePO data. Information gathered by queries is returned in the form of charts and tables.

A query can be used to get an answer right now. Query results can be exported to several formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can also be used as dashboard monitors, enabling near real-time system monitoring. Queries can also be combined into reports, giving a more broad and systematic look at your McAfee ePO software system.

The default dashboards and predefined queries shipped with McAfee ePO cannot be changed or deleted. But you can duplicate them, then rename and change them as needed.

#### Query results are actionable

Query results displayed in tables have actions available for selected items. 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 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, you cannot select an action when viewing exported data.

You can export to these file formats:

- **CSV** — Use the data in a spreadsheet.
- **XML** — Use the data for scripts or applications.
- **HTML** — View the exported results in a browser.
- **PDF** — Save the exported results to read or print later.

#### Combining queries in reports

Reports can contain any number of queries, images, static text, and other items. They can be run on demand or on a regular schedule, and produce PDF output for viewing outside McAfee ePO.

#### Sharing queries between servers

Any query can be imported and exported, allowing you to share queries between servers. In a multi-server environment, you only have to create a query once.
Retrieving data from different sources

Queries can retrieve data from any registered server, including databases external to McAfee ePO.

Query Builder

McAfee ePO provides an easy, four-step wizard that is used to create and edit custom queries. With the wizard, you can configure which data is retrieved and displayed, and how it is displayed.

Result types

The first selections you make in the Query Builder are the Schema and result type from a feature group. This selection identifies from where and what type of data the query retrieves, and determines the available selections in the rest of the wizard.

Chart types

McAfee ePO provides a number of charts and tables to display the data it retrieves. These charts and their drill-down tables are highly configurable.

Table do not include drill-down tables.

Table 4-1  Chart type groups

<table>
<thead>
<tr>
<th>Type</th>
<th>Chart or Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar</td>
<td>• Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Grouped Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Stacked Bar Chart</td>
</tr>
<tr>
<td>Pie</td>
<td>• Boolean Pie Chart</td>
</tr>
<tr>
<td></td>
<td>• Pie Chart</td>
</tr>
<tr>
<td>Bubble</td>
<td>• Bubble Chart</td>
</tr>
<tr>
<td>Summary</td>
<td>• Multi-group Summary Table</td>
</tr>
<tr>
<td></td>
<td>• Single Group Summary Table</td>
</tr>
<tr>
<td>Line</td>
<td>• Multi-line Chart</td>
</tr>
<tr>
<td></td>
<td>• Single-Line Chart</td>
</tr>
<tr>
<td>List</td>
<td>• Table</td>
</tr>
</tbody>
</table>

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, it 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.
Work with queries

Queries can be run, exported, and more depending on your needs.

Tasks

- **Manage custom queries on page 37**
  You can create, duplicate, edit, and delete queries as needed.

- **Run a query on a schedule on page 39**
  A server task is used to run a query regularly. Queries can have sub-actions that allow you to perform various tasks, such as emailing the query results or working with tags.

- **Create a query group on page 39**
  Query groups allow you to save queries or reports without allowing other users access to them.

Manage custom queries

You can create, duplicate, edit, and delete queries as needed.

Task

1. Open the Queries & Reports page: select Menu | Reporting | Queries & Reports.
2. Select one of these actions.
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Create custom query | 1 Click **New Query**, and the Query Builder appears.  
2 On the Result Type page, select the **Feature Group** and **Result Type** for this query, then click **Next**.  
3 Select the type of chart or table to display the primary results of the query, then click **Next**. If you select **Boolean Pie Chart**, configure the criteria to include in the query before proceeding.  
4 Select the columns to be included in the query, then click **Next**. If you selected **Table** on the Chart page, the columns you select here are the columns of that table. Otherwise, these columns 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. You can take any available action on items in any table or drill-down table. 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 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 want to save the query, click **Close**.  
• If you want to use this query again, click **Save** and continue to the next step.  
6 The Save Query page appears. Type a name for the query, add any notes, and select one of the following:  
• **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**. The new query appears in the Queries list. |
| Duplicate query     | 1 From the list, select a query to copy, then click **Actions** | **Duplicate**.  
2 In the **Duplicate** dialog box, type a name for the duplicate and select a group to receive a copy of the query, then click **OK**. The duplicated query appears in the Queries list. |
| Edit query          | 1 From the list, select a query to edit, then click **Actions** | **Edit**.  
2 Edit the query settings and click **Save** when done. The changed query appears in the Queries list. |
| Delete query        | 1 From the list, select a query to delete, then click **Actions** | **Delete**.  
2 When the confirmation dialog box appears, click **Yes**. The query no longer appears in the Queries list. If any reports or server tasks used the query, they now appear as invalid until you remove the reference to the deleted query. |
Run a query on a schedule
A server task is used to run a query regularly. Queries can have sub-actions that allow you to perform various tasks, such as emailing the query results or working with tags.

Task

1. Open the Server Task Builder.
   a. From the Queries and Reports page, select a query.
   b. Select Actions | Schedule.
2. On the Description page, name and describe the task, then click Next.
3. From the Actions drop-down menu, select Run Query.
4. In the Query field, browse to the query that you want to run.
5. Select the language for displaying the results.
6. From the Sub-Actions list, select an action to take based on the results. Available sub-actions depend on the permissions of the user, and the products managed by your McAfee ePO server.
   You are not limited to selecting one action for the query results. Click the + button to add actions to take on the query results. Be careful to place the actions in the order you want them to be taken on the query results.
7. Click Next.
8. Schedule the task, then click Next.
9. Verify the configuration of the task, then click Save.

The task is added to the list on the Server Tasks page. If the task is enabled (which it is by default), it runs at the next scheduled time. If the task is disabled, it only runs when you click Run next to the task on the Server Tasks page.

Create a query group
Query groups allow you to save queries or reports without allowing other users access to them.
Creating a group allows you to categorize queries and reports by functionality as well as controlling access. The list of groups you see within the ePolicy Orchestrator Cloud software is the combination of groups you have created and groups you have permission to see.
You can also create private query groups while saving a custom query.

Task

1. Select Menu | Reporting | Queries & Reports, then click Group Actions | New Group.
2. In the New Group page, enter 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. Any user with access to public queries and reports can view queries and reports in the group.
   • Shared by permission set — Adds the new group under Shared Groups. Only users assigned the selected permission sets can access reports or queries in this group.

   Administrators have full access to all Shared by permission set and Public group queries.

4 Click Save.

About reports

Reports package query results into a PDF document, enabling offline analysis.
Generate reports to share information about your network environment with security administrators and other stakeholders.

Reports are configurable documents that display data from one or more queries, drawing data from one or more databases. The most recently run result for every report is stored in the system and is readily available for viewing.

You can restrict access to reports by using groups and permission sets in the same way you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this configuration allows for consistent access control.

Structure of a report

Reports contain a number of elements held within a basic format.
While reports are highly customizable, they have a basic structure that contains all varying elements.

Page size and orientation

McAfee ePO currently supports six combinations of page size and orientation. These combinations include:

Page sizes:
   • US Letter (8.5" x 11")
   • US Legal (8.5" x 14")
   • A4 (210 mm x 297 mm)

Orientation:
   • Landscape
   • Portrait
Headers and footers
Headers and footers also have the option of using a system default, or can be customized in a number of ways, including logos. Elements currently supported for headers and footers are:

- Logo
- Date/Time
- Page Number

- User Name
- Custom text

Page elements
Page elements provide the content of the report. They can be combined in any order, and can be duplicated as needed. Page elements provided with McAfee ePO are:

- Images
- Static text
- Page breaks

- Query Tables
- Query Charts

Create a report
You can create reports and store them in McAfee ePO.

Task

1. Select Menu | Reporting | Queries & Reports, then select the Report tab.
2. Click New Report.
3. Click Name, Description and Group. Name the report, describe it, and select an appropriate group. Click OK.
4. You can now add, remove, rearrange elements, customize the header and footer, and change the page layout. At any point, click Run to check your progress.
5. When you are finished, click Save.

Edit an existing report
You can modify an existing report's contents or the order of presentation.

If you are creating a report, you will arrive at this screen after clicking New Report.

Task

1. Select Menu | Reporting | Queries & Reports, then select the Report tab.
2. Select a report from the list by selecting the checkbox next to its name.
3. Click Edit.

   The Report Layout page appears.
Generating queries and reports
Edit an existing report

Any of the following tasks can now be performed on the report.

**Tasks**

- *Add elements to a report on page 42*
  You can add new elements to an existing report.

- *Configure image report elements on page 42*
  Upload new images and modify the images used within a report.

- *Configure text report elements on page 43*
  You can insert static text within a report to explain its contents.

- *Configure query table report elements on page 43*
  Some queries are better displayed as a table when inside a report.

- *Configure query chart report elements on page 44*
  Some queries are better displayed as a chart when inside a report.

- *Customize a report on page 44*
  Customize a report layout to add, remove, or move the objects that you need.

**Add elements to a report**

You can add new elements to an existing report.

**Before you begin**

You must have a report open on the Report Layout page.

**Task**

1. Select an element from the Toolbox and drag and drop it over the Report Layout.

   Report elements other than Page Break require configuration. The configuration page for the element appears.

2. After configuring the element, click **OK**

**Configure image report elements**

Upload new images and modify the images used within a report.

**Before you begin**

You must have a report open on the Report Layout page.

**Task**

1. To configure an image already in a report, select the arrow at the top left corner of the image, then click **Configure**.

   This displays the Configure Image page. If you are adding an image to the report, the Configure Image page appears immediately after you drag and drop the Image element onto the report.

2. To use an existing image, select it from the gallery.

3. To use a new image, click **Browse** and select the image from your computer, then click **OK**.
To specify a specific image width, enter the width in the Image Width field.

By default, the image is displayed in its existing width without resizing unless that width is wider than the available width on the page. In that case, it is resized to the available width keeping aspect ratio intact.

Select if you want the image aligned left, center, or right, then click OK.

**Configure text report elements**
You can insert static text within a report to explain its contents.

**Before you begin**
You must have a report open on the Report Layout page.

**Task**

1. To configure text already in a report, click the arrow at the top left corner of the text element. Click **Configure**. This displays the Configure Text page. If you are adding new text to the report, the Configure Text page appears immediately after you drop the **Text** element onto the report.

2. Edit the existing text in the **Text** edit box, or add new text.

3. Change the font size as appropriate. The default is 12-pt type.

4. Select the text alignment: left, center, or right.

5. Click **OK**.

The text you entered appears in the text element within the report layout.

**Configure query table report elements**
Some queries are better displayed as a table when inside a report.

**Before you begin**
You must have a report open on the Report Layout page.

**Task**

1. To configure a table already in a report, click the arrow at the top left corner of the table. Click **Configure**. This displays the Configure Query Table page. If you are adding query table to the report, the Configure Query Table page appears immediately after you drop the **Query Table** element onto the report.

2. Select a query from the **Query** drop-down list.

3. Select the database from the **Database** drop-down list to run the query against.

4. Choose the font size used to display the table data. The default is 8-pt type.

5. Click **OK**.
Configure query chart report elements
Some queries are better displayed as a chart when inside a report.

Before you begin
You must have a report open on the Report Layout page.

Task

1. To configure a chart already in a report, click the arrow at the top left corner of the chart. Click Configure.
   This displays the Configure Query Chart page. If you are adding a query chart to the report, the Configure Query Chart page appears immediately after you drop the Query Table element onto the report.

2. Select a query from the Query drop-down list.

3. Select whether to display only the chart, only the legend, or a combination of the two.

4. If you have chosen to display both the chart and legend, select how the chart and legend are placed relative to each other.

5. Select the font size used to display the legend.
   The default is 8-pt type.

6. Select the chart image height in pixels.
   The default is one-third the page height.

7. Click OK.

Customize a report
Customize a report layout to add, remove, or move the objects that you need.

Task


2. Select a report and click Actions | Edit, then perform the required actions.
### Action | Steps
---|---
Customize report headers and footers | Headers and footers provide information about the report.
The 6 fixed locations in the header and footer contain different data fields:
- **Header fields:** The header contains 3 fields. One left-aligned logo and 2 right-aligned fields, one above the other. These fields can contain one of the 4 values:
  - Nothing
  - Date/Time
  - Page Number
  - User name of the user running the report
- **Footer fields:** The footer contains 3 fields. One left-aligned, one centered, and one right-aligned. These 3 fields can also contain the listed values and custom text.
To customize the headers and footers, perform these steps:
1. Click **Header and Footer**.
2. By default, reports use the system setting for headers and footers. If you do not want this, deselect **Use Default Server Setting**.
   To change the system settings for headers and footers, select **Menu | Configuration | Server Settings**, then select **Printing and Exporting** and click **Edit**.
3. To change the logo, click **Edit Logo**.
   a. If you want the logo to be text, select **Text** and enter the text in the edit box.
   b. To upload a new logo, select **Image** then browse to and select the image on your computer and click **OK**.
   c. To use a previously uploaded logo, select it.
   d. Click **Save**.
4. Change the header and footer fields to match the wanted data, then click **OK**.

Remove elements from a report | You can remove elements from a report if no longer needed.
1. Click the arrow in the top left corner of the element you want to delete, then click **Remove**.
   The element is removed from the report.

Reorder elements in a report | You can change the order in which elements appear in a report.
1. To move an element, click the title bar of the element and drag it to a new position.
   The element positioning under the dragged element shifts as you move the cursor around the report. Red bars appear on either side of the report if the cursor is over an illegal position.
2. When the element is positioned where you want it, drop the element.
3. Click **Save**.

---

### Run a report on a schedule
Create a server task to run a report automatically.
If you want a report to be run without manual intervention, a server task is the best approach. This task creates a server task allowing for automatic, scheduled runs of a given report.
Task

1. Open the Server Task Builder.
   a. On the Queries and Reports page, select a report.
   b. Select Actions | Schedule.

2. Name the task, describe it, and assign a schedule status, then click Next.
   If you want the task to be run automatically, set the Schedule status to Enabled.

3. From the Actions drop-down list, select Run Report. Select the report to run and the target language, then click Next.

4. Choose a schedule type (frequency), dates, and time to run the report, then click Next.
   The schedule information is used only if you enable Schedule status.

5. Click Save to save the server task.
   The new task now appears in the Server Tasks list.

View report output

View the last run version of every report.
Every time a report runs, the results are stored on the server and displayed in the report list.

Whenever a report runs, the prior results are erased and cannot be retrieved. If you are interested in comparing different runs of the same report, archive the output elsewhere.

Task

1. Select Menu | Reporting | Queries & Reports.

2. Select the Report tab

   In the report list, you see a Last Run Result column. Each entry in this column is a link to retrieve the PDF that resulted from the last successful run of that report. Click a link from this column to retrieve a report.

   A PDF opens within your browser, and your browser behaves as you have configured it for that file type.

Configure the template and location for exported reports

You can define the appearance and storage location for tables and dashboards you export as documents.
Using the Printing and Exporting server setting, you can configure:

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

For option definitions, click ? in the interface.

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

---

**Group reports together**

Every report must be assigned to a group.

Reports are assigned to a group when initially created, but this assignment can be changed later. The most common reasons for grouping reports together are to collect similar reports together, or to manage permissions to certain reports.

**Task**

1. Select **Menu | Reporting | Queries & Reports**, then select the **Report** tab.
2. Select a report and click **Actions | Edit**.
3. Click **Name, Description and Group**.
4. Select a group from the **Report Group** drop-down list and click **OK**.
5. Click **Save** to save any changes to the report.

When you select the chosen group from the **Groups** list in the left pane of the report window, the report appears in the report list.
Disaster Recovery helps you quickly recover, or reinstall your McAfee ePO software. Disaster Recovery uses a Snapshot feature that periodically saves your McAfee ePO configuration, extensions, keys, and more to Snapshot records in the McAfee ePO database.

Contents
- What is Disaster Recovery?
- Disaster Recovery components
- How Disaster Recovery works
- Create Snapshot
- Configure Disaster Recovery server settings
- Open a remote console connection
- Plan your disaster recovery

What is Disaster Recovery?

The McAfee ePO Disaster Recovery feature uses a Snapshot process to save specific McAfee ePO server database records to the McAfee ePO Microsoft SQL database.

The records saved by the Snapshot contain the entire McAfee ePO configuration at the specific time the Snapshot is taken. When the Snapshot records are saved to the database, you can use the Microsoft SQL backup feature to save the entire McAfee ePO database and restore it to another SQL server for an McAfee ePO restore.

Restore SQL database connection examples

Using the restored McAfee ePO SQL database server, that includes the Disaster Recovery Snapshot, you can connect it to:

- Restored McAfee ePO server hardware with the original server name and IP address — Allows you to recover from, for example, a failed McAfee ePO software upgrade.

- New McAfee ePO server hardware with the original server name and IP address — Allows you to upgrade, or restore, your server hardware, and quickly resume managing your network systems.

- New McAfee ePO server hardware with a new server name and IP address — Allows you to move your server from one domain to another.

  This example can provide a temporary network management solution while you rebuild and reinstall your McAfee ePO server hardware and software back to its original domain.

- Restored or new McAfee ePO server hardware with multiple network interface cards (NICs) — You must confirm that the correct IP address is configured for the McAfee ePO server NIC.
The Snapshot is configured, depending on your SQL database version, to automatically run every day. If you configure a script to automatically run the SQL Backup and to copy the SQL backup file to your restore SQL database server, then you can more easily restore your McAfee ePO server. In addition, you can manually take a Snapshot or run your scripts to quickly save and backup complex or important McAfee ePO changes.

The Disaster Recovery Snapshot monitor, found on your McAfee ePO dashboard, allows you to manage and monitor your Snapshots in one place.

Disaster Recovery components

Use Disaster Recovery to restore your McAfee ePO software requires certain hardware, software, access permissions, and information.

You need two hardware server platforms:

- Your existing McAfee ePO server hardware, referred to as your “primary” McAfee ePO server.
- Duplicate SQL Server hardware, referred to as your “restore” server, running Microsoft SQL that matches your primary McAfee ePO server database. Keep the restore server up to date with the latest primary McAfee ePolicy Orchestrator SQL database server configuration using Snapshot and Microsoft SQL backup processes.

To avoid backup and restore problems, closely match your primary and restore server hardware and SQL versions.

Snapshot Dashboard monitor

The Server Snapshot monitor, found on your McAfee ePolicy Orchestrator dashboard, allows you to manage and monitor each Snapshot in one place.

If the Snapshot monitor does not appear in your Dashboard, create a dashboard and add the Disaster Recovery monitor.

Using the Server Snapshot monitor allows you to:

- Click **Take Snapshot** to manually save an McAfee ePO server Snapshot.
- Click **See details of last run** to open the **Server Task Log Details** page. This page displays information and log messages about the most recent Snapshot saved.
- Confirm the date and time the last Snapshot was saved to the SQL database, next to **Last Run At**.
- Click the **Disaster Recovery** link to access additional Disaster Recovery information.

The color and title of the Snapshot monitor tells you the status of your latest Snapshot. For example:

- **Blue, Saving Snapshot to Database** — Snapshot process is in progress.
- **Green, Snapshot Saved to Database** — Snapshot process completed successfully and it is up to date.
- **Red, Snapshot Failed** — An error occurred during the Snapshot process.
- **Gray, No Snapshot Available** — No Disaster Recovery Snapshot has been saved.
- **Orange, Snapshot Out of Date** — Changes to the configuration have occurred and a recent Snapshot has not been saved. Changes that trigger a Snapshot Out of Date status include:
  - Any extension changed. For example updated, removed, deleted, upgraded, or downgraded.
  - The **Keystore** folder changed.
• The `conf` folder changed.
• The Disaster Recovery passphrase changed in Server Settings.

**Disaster Recovery Snapshot Server Task**

You can use the Disaster Recovery Snapshot Server Task to disable and enable the Snapshot server task schedule.

> The Snapshot server task schedule is enabled, by default, for the Microsoft SQL Server database and disabled, by default, for the Microsoft SQL Server Express database.

**Disaster Recovery requirements**

To use Disaster Recovery, you need the hardware, software, and information listed in the following table.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware requirements</strong></td>
<td></td>
</tr>
<tr>
<td>Primary McAfee ePO server hardware</td>
<td>The server hardware requirements determine the number of systems managed.  You could have the McAfee ePO server and SQL Server database installed on the same or separate server hardware. See the McAfee ePolicy Orchestrator Installation Guide for detailed hardware requirements.</td>
</tr>
<tr>
<td>Restore McAfee ePO server hardware</td>
<td>For best results, closely mirror your primary McAfee ePO server hardware.</td>
</tr>
<tr>
<td>Primary McAfee ePO server</td>
<td>Run the primary server with a recent Snapshot saved in the SQL database.</td>
</tr>
<tr>
<td>Primary SQL database</td>
<td>The primary SQL database, stores the McAfee ePO server configuration, client information, and Disaster Recovery Snapshot records.</td>
</tr>
<tr>
<td><strong>Software requirements</strong></td>
<td></td>
</tr>
<tr>
<td>Backup file of primary SQL database</td>
<td>Using either the Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command line, you can create a backup file of the primary database including the Snapshot records.</td>
</tr>
<tr>
<td>Restore SQL database software</td>
<td>Using the Microsoft SQL Server Management Studio or the RESTORE (Transact-SQL) command line, you can restore the primary SQL database including the Snapshot records on the restore SQL database server.</td>
</tr>
<tr>
<td>McAfee ePO software</td>
<td>This software, downloaded from the McAfee website, is used to install and configure the restore McAfee ePO server.</td>
</tr>
<tr>
<td><strong>Information requirements</strong></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery Keystore encryption passphrase</td>
<td>This passphrase was added during the initial installation of the McAfee ePO software and decrypts sensitive information stored in the Disaster Recovery Snapshot.</td>
</tr>
<tr>
<td>Administrator rights</td>
<td>You must be able to access both the primary and restore servers and the SQL database as, for example, DBOwner and DBCreator.</td>
</tr>
<tr>
<td>Last known IP address, DNS name, or NetBIOS name of the primary McAfee ePO server</td>
<td>If you change any one of these items during the McAfee ePO server restore, ensure that the agents have a way to locate the server. The easiest method is to create a Canonical Name (CNAME) record in DNS that points requests from the old IP address, DNS name, or NetBIOS name of the primary McAfee ePO server to the restore McAfee ePO server information.</td>
</tr>
</tbody>
</table>
How Disaster Recovery works

To quickly reinstall the McAfee ePO software, create periodic snapshots of the McAfee ePO configuration. You must then back up and restore the database to a restore server, and reinstall the McAfee ePO software using the **Restore** option.

Disaster Recovery Snapshot and backup overview

The Disaster Recovery Snapshot, SQL database backup, and copying processes create a duplicate McAfee ePO database on a restore SQL database server.

This is an overview of the Disaster Recovery Snapshot, SQL database backup, and copying processes.

The following diagram is an overview of the McAfee ePO software Disaster Recovery process and the hardware involved.

In this diagram, the SQL database is installed on the same server hardware as the McAfee ePO server. The McAfee ePO server and SQL database can be installed on different server hardware.

**Figure 5-1  McAfee ePO server Disaster Recovery Snapshot and backup**

The Disaster Recovery configuration includes these general steps performed on the primary McAfee ePO server:
Take a Snapshot of the McAfee ePO server configuration and save it to the primary SQL database. This step can be done manually or via a default server task.

When the Snapshot is taken, these database files are saved:

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\Server\extensions</td>
<td>The default path to McAfee ePO software extension information.</td>
</tr>
<tr>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\Server\conf</td>
<td>The default path to required files used by the McAfee ePO software extensions.</td>
</tr>
<tr>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\Server\keystore</td>
<td>These keys are specifically for McAfee ePO agent-server communication and the repositories.</td>
</tr>
<tr>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\Server\DB\Keystore</td>
<td>The default path to the McAfee product installation server certificates.</td>
</tr>
<tr>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\Server\DB\Software</td>
<td>The default path to the McAfee product installation files.</td>
</tr>
</tbody>
</table>

The Disaster Recovery Snapshot records saved include the paths you have configured for your registered executables. The registered executable files are not backed up and you must replace those executable files when you restore the McAfee ePO server. After you restore the McAfee ePO server, any registered executables with broken paths are red on the Registered Executables page.

Test your registered executable paths after you restore your McAfee ePO server. Some registered executable paths might not appear red, but still fail because of dependency issues related to the registered executables.

Back up the SQL database using the Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line process.

Copy the SQL database backup file to the duplicate restore SQL Server.

The McAfee ePO server Disaster Recovery Snapshot and backup process is complete. You do not need to continue with the McAfee ePO server recovery installation unless you are reinstalling the McAfee ePO software.

**McAfee ePO server recovery installation overview**

Reinstalling the McAfee ePO software is the last step in quickly restoring the McAfee ePO server.

This topic is an overview of reinstalling the McAfee ePO software on the restore McAfee ePO server. For details, see the installation guide.
The following diagram is an overview of the McAfee ePO server reinstallation. In this diagram, the SQL database is installed on the same server hardware as the McAfee ePO server. The McAfee ePO server and SQL database can be installed on different server hardware.

**Figure 5-2 McAfee ePO server recovery installation**

The McAfee ePO software installation using the Disaster Recovery Snapshot file includes these general steps performed on the McAfee ePO restore server:

1. Find the SQL database backup file of the previous section. Use the Microsoft SQL Server Management Studio or the RESTORE (Transact-SQL) command-line process to restore the primary SQL Server configuration to the restore SQL Server.

2. During the McAfee ePO database software installation:
   1. On the Software Welcome dialog box, click restore from Snapshot.
   2. Select Microsoft SQL Server to link the McAfee ePO software to the restore SQL database that had the primary McAfee ePO server configuration.

   After the McAfee ePO software installation is started, the database records saved during the Snapshot process are used in the software configuration instead of creating records in the database.

3. Ensure that the agents can reconnect to the restore McAfee ePO server by creating a CNAME record in DNS. This record redirects requests from the old IP address, DNS name, or NetBIOS name of the primary McAfee ePO server to the new information for the restore McAfee ePO server.

Now the McAfee ePO restore server is running with the exact same configuration as the primary server. The clients can connect to the restore server and you can manage them exactly as before the primary McAfee ePO server was removed.

**Create Snapshot**

Creating frequent Disaster Recovery Snapshots of your primary McAfee ePO server is the first step in quickly restoring a McAfee ePO server.

After you make many configuration changes to McAfee ePO, create a Disaster Recovery Snapshot manually using any of these tasks.

- **Best practice:** Create a Disaster Recovery Snapshot Server task to automate server snapshots.
Tasks

• *Create a snapshot from the McAfee ePO on page 55*
  Use the ePolicy Orchestrator Dashboard to take Disaster Recovery Snapshots of your primary McAfee ePO server and to monitor the Snapshot process as the Dashboard status changes.

• *Create snapshot from Web API on page 55*
  Use the McAfee ePO Web API to take Disaster Recovery snapshots of your primary McAfee ePO server. Doing so enables you to use one command string to complete the process.

**Create a snapshot from the McAfee ePO**

Use the ePolicy Orchestrator Dashboard to take Disaster Recovery Snapshots of your primary McAfee ePO server and to monitor the Snapshot process as the Dashboard status changes.

**Task**

1. Select **Menu** | **Reporting** | **Dashboards** to see the **ePO Server Snapshot** monitor.
   If needed, click **Add Monitor**, select **ePO Server Snapshot** from the list, and drag it to the dashboard.

2. Click **Take Snapshot** to start saving the McAfee ePO server configuration.
   During the Snapshot process, the **Snapshot Monitor** title bar changes to indicate the status of the process. The Snapshot process takes from 10 minutes to more than an hour to complete, depending on the complexity and size of your network. This process does not affect your McAfee ePO server performance.

3. If needed, click **See details of current run** to open the **Server Task Log Details** of the last saved Snapshot.
   After the Snapshot process is complete, you click **See details of current run** to open the Server Task Log Details of the last saved Snapshot.

The latest Disaster Recovery Snapshot is saved to the McAfee ePO server primary SQL database. The database is now ready to back up and copy to the restore SQL database server.

**Create snapshot from Web API**

Use the McAfee ePO Web API to take Disaster Recovery snapshots of your primary McAfee ePO server. Doing so enables you to use one command string to complete the process.

All commands described in this task are typed in your web browser address bar to access your McAfee ePO server remotely.

You are prompted for the administrator user name and password before the output is displayed.

See the *McAfee ePolicy Orchestrator Web API Scripting Guide* for detailed Web API use and examples.

**Task**

1. Use the following McAfee ePO Web API Help command to determine the parameters for running the Snapshot:
   • localhost: — The name of your McAfee ePO server name.
   • 8443 — Destination port, identified as "8443" (the default).
• /remote/core.help?command= — Calls the Web API Help.

• scheduler.runServerTask — Calls the specific server task Help.

The runServerTask command is case-sensitive.

The example command returns this Help.

OK:
scheduler.runServerTask taskName
Runs a server task and returns the task log ID. Use task log ID with the 'tasklog.listTaskHistory' command to view the running task's status. Returns the task log ID or throws on error.
Requires permission to run server tasks.
Parameters:
  [taskId (param 1) | taskName] - The unique id or name of the task

2 Use the following command to list all server tasks and determine the taskName parameter to run the Snapshot server task:

https://localhost:8443/remote/scheduler.listAllServerTasks?:output=terse

The previous example command returns a list that looks similar to the following. The exact list displayed depends on your permissions and the extensions installed.

3 Using the task name, Disaster Recovery Snapshot Server, run the Snapshot server task using this command:


If the task is successful, output similar to the following appears.

OK

102

The Snapshot process can take from 10 minutes to more than an hour to complete, depending on the complexity and size of your network. This process normally does not affect your McAfee ePO server performance.

4 Confirm that the Web API server task Snapshot ran successfully.

a Use this command to find the Disaster Recovery Snapshot Server task log ID:

https://localhost:8443/remote/tasklog.listTaskHistory?taskName=Disaster%20Recovery%20Snapshot%20Server

This command displays all Disaster Recovery Snapshot Server tasks. Find the most recent task and note the ID number. For example, ID: 102 in the following:

ID: 102
Name: Disaster Recovery Snapshot Server
Start Date: [date]
End Date: [date]
User Name: admin
Status: Completed
Source: scheduler
Duration: Less than a minute

b Use this command and that Task ID number 102 to display all task log messages.

https://localhost:8443/remote/tasklog.listMessages?taskLogId=102
Configure Disaster Recovery server settings

You can change the Keystore encryption passphrase used when you installed McAfee ePO and link it to an SQL database restored with Disaster Recovery Snapshot records.

Before you begin
You must have administrator rights to change the Keystore encryption passphrase.

Using Disaster Recovery to create an McAfee ePO server Snapshot provides you with a quick recovery method for the McAfee ePO server.

As an administrator, this setting is helpful if you have lost, or forgotten, the Keystore encryption passphrase configured during McAfee ePO installation. You can change the existing passphrase without knowing the previously configured passphrase.

Task

1. Select Menu | Configuration | Server Settings, select Disaster Recovery from the Setting Categories, then click Edit.

2. From Keystore encryption passphrase, click Change passphrase and type the new passphrase and confirm it.

The Keystore encryption passphrase is used to encrypt and decrypt the sensitive information stored in the server Snapshot. This passphrase is required during the McAfee ePO server recovery process. Make note of this passphrase.

The McAfee ePO database must be periodically copied to a restore Microsoft SQL Database server to create an actual backup database.

Open a remote console connection

Using your McAfee ePO server name, or IP address, and the server communication port number you can connect and configure McAfee ePO from any supported Internet browser.

When you connect to McAfee ePO using a remote connection, some configuration changes are not allowed. For example, you can’t run registered executables from a remote connection.

To configure a remote connection you must determine your McAfee ePO server name, or IP address, and the server communication port number. When you open McAfee ePO, while logged on to your physical McAfee ePO server, notice the address that appears in your browser. Confirm that it is similar to:

https://win-2k8-epo59:8443/core/orionSplashScreen.do

In this example URL:
Task

1. Open any McAfee ePO supported Internet browser. See McAfee ePO Installation Guide for a list of supported browsers.

2. In the browser address bar type either of the following, and click Enter:
   - https://<servername>:8443
   For example, https://win-2k8-epo59:8443

3. Logon to McAfee ePO and you have established a remote console connection.

   See the McAfee ePO Web API Scripting Guide for examples of expanded commands you can run from a remote console connection.

Plan your disaster recovery

Configure the McAfee ePO server for a disaster recovery scenario as soon as possible after you complete your installation.

Disaster Recovery

The Disaster Recovery feature helps you quickly recover or reinstall your McAfee ePO software.

Disaster Recovery uses a Snapshot feature that periodically saves your McAfee ePO configuration, extensions, keys, and more to snapshot records in the McAfee ePO database. For additional information, see KnowledgeBase Article McAfee ePO server backup and disaster recovery procedure, KB66616.

The records saved by the snapshot contain the whole McAfee ePO configuration at the specific time the snapshot is taken. Once the snapshot records are saved to the database, you can use the Microsoft SQL backup feature to save the whole McAfee ePO database and restore it to another SQL Server.

The McAfee ePO software Disaster Recovery configuration includes these general steps performed on the McAfee ePO primary server:

1. Take a snapshot of the McAfee ePO server configuration and save it to the primary SQL database. You can create this snapshot manually or through a default server task provided for this purpose.

2. Back up the SQL database using the Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line process.

3. Copy the SQL database backup file, created in step 2, to the duplicate SQL Server used to restore the database.

4. Reinstall the McAfee ePO software using the Restore option when the McAfee ePO Setup starts.

- win-2k8-epo59 — is the name of the McAfee ePO server
- :8443 — is the console-to-application server communication port number used by McAfee ePO.

The default is port number is "8443" unless you changed it.
Server clusters for disaster recovery

If you require zero downtime when a hardware failure occurs, you can cluster your McAfee ePO server and SQL Servers. However, zero downtime requires additional hardware and increases the cost of implementation.

You might choose to cluster only the SQL Servers to minimize downtime. If the McAfee ePO server fails due to a hardware failure, you can reinstall its operating system, which takes only a few hours, and point the McAfee ePO server to your SQL database.

The full restore procedures are described in McAfee ePO server backup and disaster recovery procedure, KnowledgeBase article KB66616.

Cold and hot spares on one physical site

If your large production environment requires minimal downtime, you can use a cold or hot spare McAfee ePO server. The spare server runs a restored installation of McAfee ePO and points to your SQL database.

If you have only one physical site, cluster your SQL Servers. If your McAfee ePO server fails, you can simply change the IP address of the spare McAfee ePO server to the IP address of the failed McAfee ePO server. This IP address change is transparent to the agents and provides the least downtime in a disaster situation.

⚠️ You must have a last-known-good SQL database backup for this IP address change to work.

Cold and hot spares on two physical sites

For total disaster recovery, use two physical sites, one primary site and one secondary site.

Your primary site has a clustered SQL Server and one McAfee ePO server. McAfee recommends that the secondary site use a hot or cold spare McAfee ePO server and a SQL database. We recommend that you locate the secondary McAfee ePO server at another physical site that has a different IP address and different DNS name. You can use SQL replication or SQL Log Shipping to copy the McAfee ePO database from the primary site to the secondary site's SQL Server on a nightly or weekly basis during non-business hours. Then make sure that your secondary McAfee ePO server is selecting your secondary SQL Server. See the Microsoft article, Types of Replication (http://technet.microsoft.com/en-us/library/ms152531.aspx) for details.

Figure 5-3  Primary and secondary McAfee ePO site configuration

If the primary site fails to communicate, configure all agents previously communicating with the primary McAfee ePO server to communicate with the secondary server. The agents find the McAfee ePO server by communicating to its IP address first, and if that fails they use its DNS name. If the agents find that the primary McAfee ePO server's IP address is not available, these steps occur.

1. The agents query the DNS where you have changed the IP address for the primary server.
2. The agents select the IP address of the secondary server.
3. The agents try to connect to the secondary McAfee ePO server and SQL database.
Using the System Tree and Tags

You can organize, group, and tag your managed systems using the System Tree and Tags features.

Contents
- Organizing systems
- Tags

Organizing systems
Use McAfee ePO to automate and customize your systems’ organization.

The structure you put in place affects how security policies are inherited and enforced throughout your environment.

The System Tree is the graphical representation of this structure. You can organize your System Tree using these methods:

- Manual organization from the console (drag and drop).
- Automatic synchronization with your Active Directory server.
- Criteria-based sorting, using criteria applied to systems manually or automatically.

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, plan your System Tree before adding the systems.

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

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

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

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

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

**Environmental borders and their impact on system organization**

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

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

**Topological borders**

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

**Geographic borders**

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

**Political borders**

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

**Functional borders**

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

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

**Subnets and IP address ranges**

In many cases, organizational units of a network use specific subnets or IP address ranges, so you can create a group for a geographic location and set IP address filters for it.

You can also use network location, such as IP address, as the primary grouping criterion, if your network isn't spread out geographically

**Best practice:** Consider using sorting criteria based on IP address information to automate System Tree creation and maintenance. Set IP address subnet masks or IP address range criteria for applicable groups within the System Tree. These filters automatically populate locations with the appropriate systems.
**Operating systems and software**
Consider grouping systems with similar operating systems to manage 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. Also, by giving these systems a corresponding tag, you can automatically sort them into a group.

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

If possible, use tag-based sorting criteria to automatically populate groups with the appropriate systems. Plus, to help sort your systems, you can create tag groups nested up to four levels deep, with up to 1,000 tag subgroups in each level. For example, if you can organize your systems using geographic location, chassis type (server, workstation, or laptop), platform (Windows, Macintosh, Linux, or SQL), and user, you might have the tag groups in this table.

<table>
<thead>
<tr>
<th>Location</th>
<th>Chassis type</th>
<th>Platform</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Los Angeles</td>
<td>Desktop</td>
<td>Windows</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td>Laptop</td>
<td>Macintosh</td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Server</td>
<td>Linux</td>
<td>Corporate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
<td>Corporate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL</td>
<td>Corporate</td>
</tr>
<tr>
<td>San Francisco</td>
<td>Desktop</td>
<td>Windows</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td>Laptop</td>
<td>Macintosh</td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Server</td>
<td>Linux</td>
<td>Corporate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
<td>Corporate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL</td>
<td>Corporate</td>
</tr>
</tbody>
</table>

**Active Directory synchronization**
If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain parts of the System Tree.
Once defined, the System Tree is updated with any new systems (and subcontainers) in your Active Directory.
Leverage Active Directory integration to perform these system management tasks:

- Synchronize with your Active Directory structure, by importing systems, and the Active Directory subcontainers (as System Tree groups), and keeping them up-to-date with Active Directory. At each synchronization, both systems and the structure are updated in the System Tree to reflect the systems and structure of Active Directory.

- Import systems as a flat list from the Active Directory container (and its subcontainers) into the synchronized group.

- Control what to do with potential duplicate systems.

- Tag newly imported or updated systems.

- Use the system description, which is imported from Active Directory with the systems.

Use this process to integrate the System Tree with your Active Directory systems structure:

1. Configure the synchronization settings on each group that is a mapping point in the System Tree. At the same location, configure whether to:
   - Deploy agents to discovered systems.
   - Delete systems from the System Tree when they are deleted from Active Directory.
   - Allow or disallow duplicate entries of systems that exist elsewhere in the System Tree.

2. Use the Synchronize Now action to import Active Directory systems (and possibly structure) into the System Tree according to the synchronization settings.

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

**Types of Active Directory synchronization**

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

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

- Deploy agents automatically to systems new to ePolicy Orchestrator Cloud. You might not want to configure this setting on the initial synchronization if you are importing many 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 Cloud (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 setting 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, make sure to select not to add systems again if they exist elsewhere in the System Tree. This synchronization type 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 Cloud.
- 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, make sure you select not to add the systems when they exist elsewhere in the System Tree. This setting prevents duplicate entries for systems in the System Tree.

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

**Criteria-based sorting**

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

Systems must match only 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 the criteria and sorting order.

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 and Found.

New systems that call into 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 do disable System Tree sorting on a system, it is excluded from sorting actions, except when the Test Sort action is performed. During a test sort, the sorting status of the system or collection is considered and can be moved or sorted from the Test Sort page.

System Tree sorting settings on the McAfee ePO server

For sorting to take place, it must be enabled on the server and on the systems. By default, once sorting is enabled, 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 are placed during a sort action. The Test Sort page displays the systems and the paths to the location where they are 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** — Prevents other ePolicy Orchestrator Cloud users from mistakenly configuring sorting criteria on groups and moving systems to undesirable locations in the System Tree.

- **Sort systems on each agent-server communication** — Sorts systems 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 not sorted again as long as this setting is selected. You can still sort 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 isn't sorted, regardless of how the sorting action is taken. However, performing the Test Sort action sorts this system. If enabled, systems can be sorted using the manual Sort Now action, and can be sorted at agent-server communication.
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 setting IP address sorting criteria for groups.

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

IP address sorting criteria must not overlap between different groups. Each IP address range or subnet mask in a group's sorting criteria must 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 Group Details tab. You can check for IP address overlap using the Check IP Integrity action in the Group Details tab.

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

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

Group order and sorting
For additional flexibility with System Tree management, configure the order of a group's subgroups, and the order of their placement during sorting.

When multiple subgroups have matching criteria, changing this order can change where a system ends up in the System Tree. 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 group's Sorting Criteria page.

Only subgroups at the last position of the sort order can be catch-all groups. These groups receive all systems that were sorted into the parent group, but were not sorted into any of the catch-all's peers.

How a system is added to the System Tree when sorted
When the McAfee Agent communicates with the server for the first time, the server uses an algorithm to place the system in the System Tree. When it cannot find an appropriate location for a system, it puts the system in the Lost and Found group.

On each agent-server communication, the server attempts to locate the system in the System Tree by McAfee Agent GUID. Only systems whose agents have already called into the server for the first time have a McAfee Agent GUID in the database. If a matching system is found, it is left in its existing location.

If a matching system is not found, the server uses an algorithm to sort the systems into the appropriate groups. Systems can be sorted into any criteria-based group in the System Tree, as long as each parent group in the path does not have non-matching criteria. Parent groups of a criteria-based subgroup must have no criteria or matching criteria.
The sorting order assigned to each subgroup (defined in the **Group Details** tab) determines the order that the server considers subgroups for sorting.

1. The server searches for a system without a McAfee Agent GUID (the McAfee Agent has never before called in) 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 and Found group, and the system is placed there.

3. Properties are updated for the system.

4. The server applies all criteria-based tags to the system if the server is configured to run sorting criteria at each agent-server communication.

5. What happens next depends on whether System Tree sorting is enabled on both the server and the system.
   - If System Tree sorting is disabled on either the server or the system, the system is left where it is.
   - If System Tree sorting is enabled on the server and system, the system is moved based on the sorting criteria in the System Tree groups.

6. Systems that were added using Active Directory or NT Domain synchronization have System Tree sorting disabled by default. With System Tree sorting disabled, systems are not sorted on the first agent-server communication.

7. Once sorted into a group, each of its subgroups is considered for matching criteria according to their sorting order on the Group Details tab.

8. Sorting continues until there is no subgroup with matching criteria for the system, and is placed in the last group found with matching criteria.

9. If such a top-level group is not found, the subgroups of top-level groups (without sorting criteria) are considered according to their sorting.

10. 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.

11. If the server cannot sort the system into any group, it is placed in the Lost and Found group within a subgroup that is named after its domain.

**View system information details**

You can view detailed information and status about a system in the System Tree.
Task

1 Open the System Tree page.
   1 Select Menu | Systems | System Tree.
   2 Click Systems tab and any system row.

2 Click Customize to change the information displayed in the three system information monitors:
   • Summary — Displays the results of the McAfee Agent Communication Summary, by default.
   • Properties — Displays information about the systems location in your network and the agent installed, by default.
   • Query monitor — Displays the system-specific results for the Threat Events in the Last 2 Weeks query, by default.

3 Click one of these tabs, to view additional details about the selected system:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Properties</td>
<td>Displays details about the system. For example, operating system, memory installed, and connection information.</td>
</tr>
<tr>
<td>Products</td>
<td>Lists one of these product states:</td>
</tr>
<tr>
<td></td>
<td>• Installed Product — The state of the installed product for which the McAfee Agent has communicated with the install event.</td>
</tr>
<tr>
<td></td>
<td>• Uninstalled Product — The state of the uninstalled product for which the McAfee Agent has communicated with the uninstall event.</td>
</tr>
<tr>
<td></td>
<td>• Deployment Task status of product — The state of the deployment task of a newer version of an existing product which is getting installed.</td>
</tr>
<tr>
<td></td>
<td>The status of the deployment task of the same version of the product or an older version of the same product is ignored.</td>
</tr>
<tr>
<td>Applied Policies</td>
<td>Displays the name of policies applied to this system and lists them alphabetically.</td>
</tr>
<tr>
<td>Applied Client Tasks</td>
<td></td>
</tr>
<tr>
<td>Threat Events</td>
<td>Lists threat and other events, plus detailed information about those events,</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>List configuration information about the McAfee Agent installed on the system.</td>
</tr>
</tbody>
</table>

**Creating and populating System Tree groups**

To help you visualize your managed systems by geographic or machine-type values, create System Tree groups and populate the groups with systems.

*Best practice:* Drag selected systems to any group in the System Tree to populate groups. Drag and drop to move groups and subgroups in the System Tree.

There is no single way to organize a System Tree. Because every network is different, your System Tree organization can be as unique as your network layout. You can use more than one method of organization.
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. If you have a smaller network, you can create your System Tree by hand and add each system manually.

**Add systems to an existing group manually**
Add specific systems to a selected group.

**Task**

1. Open the New Systems page.
   a. Select **Menu | Systems | System Tree**.
   b. Click **New Systems**.
2. Select whether to deploy the McAfee Agent to the new systems, and whether the systems are added to the selected group, or to a group according to sorting criteria.
3. Next to **Target systems**, type the NetBIOS name for each system in the text box, separated by commas, spaces, or line breaks. Alternatively, click **Browse** to select the systems.
4. Specify additional options as needed.
   If you selected **Push agents and add systems to the current group**, you can enable automatic **System Tree** sorting. Do this to apply the sorting criteria to these systems.
5. Click **OK**.

**Create groups manually**
Create System Tree subgroups.

**Task**

1. Open the New Subgroups dialog box.
   a. Select **Menu | Systems | System Tree**.
   b. Select a group, then click **New Subgroup**.
   ![You can also create more than one subgroup at a time.]
2. Type a name then click **OK**.
   The new group appears in the System Tree.
3. Repeat as necessary until you are ready to populate the groups with systems. Use one of these processes to add systems to your System Tree groups:
   - Typing system names manually.
   - Importing them from NT domains or Active Directory containers. You can regularly synchronize a domain or a container to a group for ease of maintenance.
   - Setting up IP address-based or tag-based sorting criteria on the groups. When agents check in from systems with matching IP address information or matching tags, they are automatically placed in the appropriate group.
Export systems from the System Tree

Export a list of systems from the System Tree to a .txt file for later use. Export at the group or subgroup level while retaining the System Tree organization.

It can be useful to have a list of the systems in your System Tree. You can import this list into your McAfee ePO server to quickly restore your previous structure and organization.

This task does not remove systems from your System Tree. It creates a .txt file that contains the names and structure of systems.

Task

1. Select Menu | Systems | System Tree.

2. Select the group or subgroup containing the systems you want to export, then click System Tree Actions | Export Systems.

3. Select whether to export:
   - **All systems in this group** — Exports the systems in the specified **Source group**, but does not export systems listed in nested subgroups under this level.
   - **All systems in this group and subgroups** — Exports all systems at and below this level.

4. Click OK.

   The Export page opens. You can click the systems link to view the system list, or right-click the link to save a copy of the ExportSystems.txt file.

Create a text file of groups and systems

Create a text file of the NetBIOS names for your network systems that you want to import into a group. You can import a flat list of systems, or organize the systems into groups.

Define the groups and their systems by typing the group and system names in a text file. Then import that information into McAfee ePO.

For large networks, use network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate text files with 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 whole structure into the System Tree.

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

Task

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

   ```
   GroupA\system1
   GroupA\system2
   GroupA\GroupB\system3
   GroupC\GroupD
   ```

2. Verify the names of groups and systems, and the syntax of the text file, then save the text file to a temporary folder on your server.
**Import systems and groups from a text file**
Import systems or groups of systems into the System Tree from a text file you have created and saved.

**Task**

1. Open the New Systems page.
   a. Select Menu | Systems | System Tree.
   b. Click New Systems.
2. Select Import systems from a text file into the selected group, but do not push agents.
3. Select whether the import file contains:
   - Systems and System Tree Structure
   - Systems only (as a flat list)
4. Click Browse, then select the text file.
5. Select what to do with systems that already exist elsewhere in the System Tree.
6. Click OK.

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

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

**Tasks**
- Add sorting criteria to groups on page 72
  Sorting criteria for System Tree groups can be based on IP address information or tags.
- Enable System Tree sorting on the server on page 73
  For systems to be sorted, System Tree sorting must be enabled on both the server and the systems.
- Enable or disable System Tree sorting on systems on page 73
  The sorting status of a system determines whether it can be sorted into a criteria-based group.
- Sort systems manually on page 74
  Sort selected systems into groups with criteria-based sorting enabled.

**Add sorting criteria to groups**
Sorting criteria for System Tree groups can be based on IP address information or tags.

**Task**

1. Select Menu | Systems | System Tree, click the Group Details tab, then select the group in the System Tree.
2. Next to Sorting criteria click Edit. The Sorting Criteria page for the selected group appears.
3. Select Systems that match any of the criteria below, then the criteria selections appear.

Although you can configure multiple sorting criteria for the group, a system only has to match a single criterion to be placed in this group.
4 Configure the criteria. 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** — Click Add Tags and perform these steps in the Add Tags dialog box.
  1. Click the tag name, or names, to add and sort the systems in this parent group.
  2. Click OK.

To select multiple tags, click Ctrl + the tag names.

The tags selected appear in Tags on the Sorting Criteria page and next to Sorting Criteria on the Group Details page.

5 Repeat as needed until sorting criteria is reconfigured for the group, then click Save.

**Enable System Tree sorting on the server**

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

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

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

**Task**

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

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

**Enable or disable System Tree sorting on systems**

The sorting status of a system determines whether it can be sorted into a criteria-based group.

You can change the sorting status on systems in any table of systems (such as query results), and also automatically on the results of a scheduled query.

**Task**

1. Select Menu | Systems | System Tree | Systems, then select the systems you want.

2. Select Actions | Directory Management | Change Sorting Status, then select whether to enable or disable System Tree sorting on selected systems.

3. In the Change Sorting Status dialog box, select whether to disable or enable System Tree sorting on the selected system.

Depending on the setting for System Tree sorting, these systems are sorted on the next agent-server communication. Otherwise, they can only be sorted with the Sort Now action.
Sort systems manually
Sort selected systems into groups with criteria-based sorting enabled.

Task

1. Select Menu | Systems | System Tree | Systems, then select the group that contains the systems.

2. Select the systems then click Actions | Directory Management | Sort Now. The Sort Now dialog box appears.

   If you want to preview the results of the sort before sorting, click Test Sort instead. (However, if you move systems from within the Test Sort page, all selected systems are sorted, even if they have System Tree sorting disabled.)

3. Click OK to sort the systems.

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

Mapping Active Directory containers to groups allows you to:

• Synchronize the System Tree structure to the Active Directory structure so that when containers are added or removed in Active Directory, the corresponding group in the System Tree is added or removed.

• Delete systems from the System Tree when they are deleted from Active Directory.

• Prevent duplicate entries of systems in the System Tree when they exist in other groups.

Task

1. Select Menu | Systems | System Tree | Group Details, then select a group in the System Tree for mapping an Active Directory container to.

   You cannot synchronize the Lost and Found group of the System Tree.

2. Next to Synchronization type, click Edit. The Synchronization Settings page for the selected group appears.


4. Select the type of Active Directory synchronization you want to occur between this group and the Active Directory container (and its subcontainers):

   • Systems and container structure — Select this option if you want this group to truly reflect the Active Directory structure. When synchronized, the System Tree structure under this group is changed to reflect the Active Directory container that it's mapped to. When containers are added or removed in Active Directory, they are added or removed in the System Tree. When systems are added, moved, or removed from Active Directory, they are added, moved, or removed from the System Tree.

   • Systems only — Select this option if you only want the systems from the Active Directory container (and non-excluded subcontainers) to populate this group, and this group only. No subgroups are created when mirroring Active Directory.

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

   If you are using Active Directory synchronization as a starting point for security management, and plan to use System Tree management functionality after mapping your systems, do not select this option.
6 In the Active Directory domain section, you can:
   • Type the fully qualified domain name of your Active Directory domain.
   • Select from a list of already registered LDAP servers.

7 Next to Container, click Add and select a source container in the Select Active Directory Container dialog box, then click OK.

8 To exclude specific subcontainers, click Add next to Exceptions and select a subcontainer to exclude, then click OK.

9 Select whether to deploy the McAfee Agent automatically to new systems. If you do, configure the deployment settings.

   **Best practice:** Because of its size, do not deploy the McAfee Agent during the initial import if the container is large. Instead, import the container, then deploy the McAfee Agent to groups of systems at a time, rather than all at once.

10 Select whether to delete systems from the System Tree when they are deleted from the Active Directory domain. Optionally choose whether to remove agents from the deleted systems.

11 To synchronize the group with Active Directory immediately, click Synchronize Now.

   Clicking Synchronize Now saves any changes to the synchronization settings before synchronizing the group. If you have an Active Directory synchronization notification rule enabled, an event is generated for each system that is added or removed. These events appear in the Audit Log, and are queryable. If you deployed agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the Last Synchronization time is updated, displaying the time and date when the synchronization finished, not when any agent deployments completed.

   **Best practice:** Schedule an NT Domain/Active Directory synchronization server task for the first synchronization. This server task is useful if you are deploying agents to new systems on the first synchronization, when bandwidth is a larger concern.

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

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

   **Best practice:** Set up a recurring NT Domain/Active Directory synchronization server task to keep your System Tree current with any changes to your Active Directory containers.

**Import NT domains into an existing group**

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

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

If the domain is large, you can create subgroups to assist with policy management or organization. To do this, first import the domain into a group of your System Tree, then manually create logical subgroups.

   **To manage the same policies across several domains, import each of the domains into a subgroup under the same group. The subgroups will inherit the policies set for the top-level group.**

When using this method:
• Set up IP address or tag sorting criteria on subgroups to automatically sort the imported systems.
• Schedule a recurring NT Domain/Active Directory synchronization server task for easy maintenance.

**Task**

1. Select **Menu | Systems | System Tree | Group Details** and select or create a group in the **System Tree**.

2. Next to **Synchronization type**, click **Edit**. The **Synchronization Settings** page for the selected group appears.

3. Next to **Synchronization type**, select **NT Domain**. The domain synchronization settings appear.

4. Next to **Systems that exist elsewhere in the System Tree**, select what to do with systems that exist in another group of the **System Tree**.

   **Best practice:** Don’t select **Add systems to the synchronized group and leave them in their current System Tree location**, especially if you are using the NT domain synchronization only as a starting point for security management.

5. Next to **Domain**, click **Browse** and select the NT domain to map to this group, then click **OK**. Alternatively, you can type the name of the domain directly in the text box.

   When typing the domain name, do not use the fully-qualified domain name.

6. Select whether to deploy the McAfee Agent automatically to new systems. If you do so, configure the deployment settings.

   **Best practice:** Because of its size, do not deploy the McAfee Agent during the initial import if the container is large. Instead, import the container, then deploy the McAfee Agent to groups of systems at a time, rather than all at once.

7. Select whether to delete systems from the **System Tree** when they are deleted from the NT domain. You can optionally choose to remove agents from deleted systems.

8. To synchronize the group with the domain immediately, click **Synchronize Now**, then wait while the systems in the domain are added to the group.

   Clicking **Synchronize Now** saves changes to the synchronization settings before synchronizing the group. If you have an NT domain synchronization notification rule enabled, an event is generated for each system added or removed. These events appear in the **Audit Log**, and are queryable. If you selected to deploy agents to added systems, the deployment is initiated to each added system. When the synchronization is complete, the **Last Synchronization** time is updated. The time and date are when the synchronization finished, not when any agent deployments completed.

9. To synchronize the group with the domain manually, click **Compare and Update**.

   a. If you are going to remove any systems from the group with this page, select whether to remove their agents when the system is removed.

   b. Select the systems to add to and remove from the group as necessary, then click **Update Group** to add the selected systems. The **Synchronize Setting** page appears.

10. Click **Save**, then view the results in the **System Tree** if you clicked **Synchronize Now** or **Update Group**.

    Once the systems are added to the **System Tree**, distribute agents to them if you did not select to deploy agents as part of the synchronization.

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

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

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

- Adds new systems on the network to the specified group.
- Adds new corresponding groups when new Active Directory containers are created.
- Deletes corresponding groups when Active Directory containers are removed.
- Deploys agents to new systems.
- Removes systems that are no longer in the domain or container.
- Applies site or group policies and tasks to new systems.
- Prevents or allows duplicate entries of systems that still exist in the System Tree after you moved them to other locations.

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

**Task**

1. Open the Server Task Builder.
   a. Select Menu | Automation | Server Tasks.
   b. Click New Task.
2. On the Description page, name the task and choose whether it is enabled once it is created, then click Next.
3. From the drop-down list, select Active Directory Synchronization/NT Domain.
4. Select whether to synchronize all groups or selected groups. If you are synchronizing only some groups, click Select Synchronized Groups and select specific ones.
5. Click Next to open the Schedule page.
6. Schedule the task, then click Next.
7. Review the task details, then click Save.

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

**Update a synchronized group with an NT domain manually**

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

The update includes the following changes:

- Adds systems currently in the domain.
- Removes systems from your System Tree that are no longer in the domain.
- Removes agents from all systems that no longer belong to the specified domain.
**Task**

1. Select **Menu | Systems | System Tree | Group Details**, then select the group that is mapped to the NT domain.
2. Next to **Synchronization type**, click **Edit**.
3. Select **NT Domain**, then click **Compare and Update** near the bottom of the page.
4. If you are removing systems from the group, select whether to remove the agents from systems that are removed.
5. Click **Add All** or **Add** to import systems from the network domain to the selected group.
   - Click **Remove All** or **Remove** to delete systems from the selected group.
6. Click **Update Group** when finished.

**Move systems within the System Tree**

Move systems from one group to another in the System Tree. You can move systems from any page that displays a table of systems, including the results of a query.

In addition to the steps below, you can also drag and drop systems from the Systems table to any group in the System Tree.

Even in a perfectly organized System Tree that's regularly synchronized, you might need to move systems manually between groups. For example, you might need to periodically move systems from the Lost and Found group.

**Task**

1. Select **Menu | Systems | System Tree | Systems**, then browse to and select the systems.
2. Click **Actions | Directory Management | Move Systems** to open the Select New Group page.
3. Select whether to enable or disable System Tree sorting on the selected systems when they are moved.
4. Select the group to place the systems in, then click **OK**.
   - If you move systems between groups, the moved systems inherit the policies assigned to their new group.

**How Transfer Systems works**

You can use the Transfer Systems command to move managed systems from one McAfee ePO server to another. For example, from an old McAfee ePO server to a new McAfee ePO 5.x server.

You might need to transfer managed systems if:

- You're upgrading the server hardware and operating system.
- You're upgrading the server hardware and the McAfee ePO software version.

This graphic shows the major processes to transfer systems from one McAfee ePO server to another.
Export your security keys from the old server.

1. Export the security keys in the new server.

2. Register the new McAfee ePO server to the old server.

3. Transfer your current systems to the new McAfee ePO server.

4. Confirm that you can view the systems in the new server’s System Tree.

5. Confirm that the systems no longer appear in the old server’s System Tree.

6. Confirm systems moved

Transfer systems from one server to another

Use the Transfer Systems option to move systems from an old McAfee ePO 4.x server to a new McAfee ePO 5.x server.

You might see the following error when you register the servers and enable the Transfer Systems options with Automatic Sitelist Import:

ERROR: Master agent-server keys must be imported into the remote server before importing the sitelist. Go to Server Settings to export security keys from this server. Visiting this link now causes you to lose any unsaved changes to this registered server.

Both keys (1024 and 2048) must be imported for successful registration so the Automatic Sitelist Import can save without issue.
Tasks

- **Export security keys from the old server on page 80**
  Export the 2048-bit and 1024-bit security keys.

- **Import security keys to the new server on page 80**
  Import the 2048-bit and 1024-bit security keys from the old server on the new server.

- **Register the old server to the new server on page 81**
  Register the new server. For example, register a McAfee ePO 5.x server to a McAfee ePO 4.x server.

- **Transfer systems between servers on page 82**
  After you have imported the keys and registered the new server, you can use the old server to initiate the transfer process.

- **Check the status of transferred computers on page 82**
  Verify that your systems now appear on the new server.

**Export security keys from the old server**
Export the 2048-bit and 1024-bit security keys.

**Task**

1. Log on to the console.
2. Select **Menu | Configuration | Server Settings**.
3. Click **Security Keys** under the **Setting Categories** column, click **Edit**.
   
   The Edit Security Keys page opens.
4. Save the 2048-bit keys listed under the Agent-server secure communication keys list.
   a. Click the 2048-bit key and click **Export**.
   b. Click **OK** to confirm the export key confirmation message.
   c. Click **Save**.
   d. Type or browse to a path where you want to save the security key .zip file.
   e. Click **Save** again.
5. Save the 1024-bit keys listed under the Agent-server secure communication keys list.
   a. Click the 1024-bit key and click **Export**.
   b. Click **OK** to confirm the export key confirmation message.
   c. Click **Save**.
   d. Type or browse to a path where you want to save the security key .zip file.
   e. Click **Save** again.

**Import security keys to the new server**
Import the 2048-bit and 1024-bit security keys from the old server on the new server.
Task

1. Log on to the new console.
2. Select Menu | Configuration | Server Settings.
3. Click Security Keys from the Setting Categories column, then click Edit.
4. Click Import.
5. Import the 2048-bit key.
   a. Click Browse, locate the exported 2048-bit security key .zip file.
   b. Click Open.
   c. Click Next.
   d. Confirm that you have selected the correct key on the Summary tab, and click Save.
6. Import the 1024-bit key.
   a. Click Browse, locate the exported 1024-bit security key .zip file.
   b. Click Open.
   c. Click Next.
   d. Confirm that you have selected the correct key on the Summary tab, and click Save.

Register the old server to the new server

Register the new server. For example, register a McAfee ePO 5.x server to a McAfee ePO 4.x server.

Task

1. From the old server, log on to the console.
2. Click Menu | Configuration | Registered Servers.
3. Click New Server.
4. Select ePO from the Server type drop-down list, type a name for this server in the Name section, and click Next.
5. Type the credentials to the new server and click Test Connection.
6. If the test is successful, select Enable for the Transfer systems entry.
7. Ensure that Automatic sitelist import is selected, and click Save.
   • The Manual sitelist import option is also available and can be used if you want to do a manual import by selecting an existing SiteList.xml file.
   • You can obtain the SiteList.xml file to use for this process in the following folder on the server where the agents are being transferred to: <ePO_Installation_Directory>\DB\SiteList.xml
• On a McAfee ePO 4.6 server, you can select only version 4.6 or previous versions as the McAfee ePO version. When you test the connection to the database of the registered server, you see the following warning:

  Database connection successful! Warning Versions mismatch!

  You can safely ignore the warning. The McAfee ePO version selected (4.6) does not match the database (5.x) you have tested.

Transfer systems between servers
After you have imported the keys and registered the new server, you can use the old server to initiate the transfer process.

Task

1. Log on to the old server.
2. Select Menu | Systems | System Tree.
3. Select the systems you want to transfer.
   
   Ensure that the selected systems are communicating to the old server, before you transfer them.
4. Click Actions | Agent | Transfer Systems.
5. Select the new server and click OK to transfer.

   Two agent-server communication intervals must occur before the system appears in the System Tree of the new server. The length of time required depends on your configuration. The default agent-server communication interval is one hour.

Check the status of transferred computers
Verify that your systems now appear on the new server.

Task

1. From the new server, select Menu | System Tree | Systems.
   
   Your systems are listed in the System Tree.
2. From the old server, select Menu | System Tree | Systems.
   
   Your systems are not listed in the System Tree.

How the Automatic Responses feature interacts with the System Tree
Before you plan the implementation for Automatic Responses, understand how this feature works with the System Tree.

This feature does not follow the inheritance model used when enforcing policies.

Automatic Responses use events that occur on systems in your environment and configured response rules. These rules are associated with the group that contains the affected systems and each parent above it. When an event occurs, it is delivered to the server. If the conditions of a rule are met, designated actions are taken.
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 in 10 minutes. But an administrator does not want to be notified unless viruses are detected on 1,000 systems in the whole environment in the same amount of time.

- **Recipients for the notification message.** An administrator for a particular group might want to be notified only if a specified number of virus detection events occur in the group. Or, an administrator wants each group administrator to be notified if a specified number of virus detection events occur in the whole System Tree.

System Tree location does not filter Server events.

### Tags

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

#### Create tags
Use the New Tag Builder to create tags quickly.

**Task**

1. Select **Menu | Systems | Tag Catalog | New Tag.**
2. On the **Description** page, enter a name and meaningful description, then click **Next.** The **Criteria** page appears.
3. Select and configure the criteria, then click **Next.** The **Evaluation** page appears.
   - **To apply the tag automatically, configure criteria for the tag.**
4. Select whether systems are evaluated against the tag's criteria only when the **Run Tag Criteria** action is taken, or also at each agent-server communication, then click **Next.** The **Preview** page appears.
   - These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and have not been excluded from the tag.
5. Verify the information on this page, then click **Save.**
   - If the tag has criteria, this page displays the number of systems that receive this tag when evaluated against its criteria.

The tag is added under the selected tag group in the **Tag Tree** on the **Tag Catalog** page.

#### Manage tags

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

1. Select **Menu | Systems | Tag Catalog**.

2. From the **Tags** list, select a tag or multiple tags, then perform one of these tasks:

   1. **Edit tag** — Click **Actions | Edit**, then from the **Edit Tag Builder**:
      - The number of affected systems is listed at the top of the page.
      - a. On the **Description** page, type a name and meaningful description, then click **Next**.
      - b. Select and configure the criteria, then click **Next**.
      - The information about this page is displayed.

      
      - To apply the tag automatically, you must configure criteria for the tag.
      - 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**.
      - These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and are not excluded from the tag.
      - Verify the information about this page, then click **Save**.

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

      The tag is updated on the **Tag Catalog** page under the selected tag group in the **Tag Tree**.

   2. **Delete tag** — Click **Actions | Delete**, then from the **Delete** dialog-box, click **OK** to delete the tag.

   3. **Move tag to another Tag Group** — Click **Actions | Move Tags**, then from the **Move Tags** dialog-box select the destination tag subgroup for the tag, then click **OK** to move the tag.

      
      - You can also drag and drop the tags into the tag groups in the **Tag Group Tree**.

**Create, delete, and change tag subgroups**

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

**Task**

1. Select **Menu | Systems | Tag Catalog**.

2. Perform one of these tasks for a tag subgroup:

   1. **Create a tag subgroup** — Use these steps:
      - a. In the **Tag Tree**, select the tag group (or parent tag group) where you want to create the tag subgroup.
      - My Tags is the default top-level tag group added during McAfee ePO installation.
      - b. Click **New Subgroup** to see the **New Subgroup** dialog box.
c In the **Name** field, enter a descriptive name for the new tag subgroup.
d Click **OK** to create the tag subgroup.

2 **Rename a tag subgroup** — Use these steps:
a In the **Tag Tree**, select the tag subgroup that you want to rename.
b Click **Tag Tree Actions | Rename Group** to open the **Rename Subgroup** dialog box.
c In the **Name** field, enter the new name for the tag subgroup.
d Click **OK** and the tag subgroup is renamed.

3 **Delete a tag subgroup** — Use these steps:
a In the **Tag Tree**, select the tag subgroup that you want to delete.
b Click **Actions | Delete**. An **Action: Delete** confirmation dialog box appears.
c If you still want to delete the tag subgroup, click **OK** and the tag subgroup is removed.

### Exclude systems from automatic tagging

Prevent systems from having specific tags applied.

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

**Task**

1 Select **Menu | Systems | System Tree | Systems**, then select the group that contains the systems in the **System Tree**.

2 Select one or more systems in the **Systems** table, then click **Actions | Tag | Exclude Tag**.

3 In the **Exclude Tag** dialog box, select the tag group, select the tag to exclude, then click **OK**.

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

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

### Create a query to list systems based on tags

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

**Task**

1 Open the Server Task Builder.
a Select **Menu | Automation | Server Tasks**.
b Click **New Task**.
2 On the Description page, name and describe the task, then click Next.

3 From the Actions drop-down menu, select Run Query.

4 In the Query field, select one of these queries from the McAfee Groups tab, then click OK.
   - Inactive Agents
   - Duplicate Systems Names
   - Systems with High Sequence Errors
   - Systems with no Recent Sequence Errors
   - Unmanaged Systems

5 Select the language for displaying the results.

6 From the Sub-Actions list, select one of these subactions to take based on the results.
   - Apply Tag — Applies a selected tag to the systems returned by the query.
   - Clear Tag — Removes a selected tag on the systems returned by the query. Select Clear All to remove all tags from the systems in the query results.
   - Exclude Tag — Excludes systems from the query results if they have the selected tag applied to them.

7 From the Select Tag window, select a tag group from the Tag Group Tree and optionally filter the list of tags using the Tags text box.

8 Click Next.

9 Schedule the task, then click Next.

10 Verify the configuration of the task, then click Save.

The task is added to the list on the Server Tasks page. If the task is enabled (default), it runs at the next scheduled occurrence. If the task is disabled, it only runs by clicking Run next to the task.

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

Task

1 Select Menu | Systems | System Tree | Systems, then select the group that contains the systems you want.

2 Select the systems, then click Actions | Tag | Apply Tag.

3 In the Apply Tag dialog box, select the tag group, select the tag to apply, then click OK.

   To limit the list to specific tags, type the tag name in the text box under Tags.
Verify that the tags have been applied:

a. Select Menu | Systems | Tag Catalog, then select a tag or tag group from the list of tags.

b. Next to Systems with tag in the details pane, click the link for the number of systems tagged manually. The Systems with Tag Applied Manually page appears.

c. Verify that the systems are in the list.

Clear tags from systems
Remove tags from selected systems.

Task

1. Select Menu | Systems | System Tree | Systems, then select the group that contains the systems you want.

2. Select the systems, then click Actions | Tag | Clear Tag.

3. In the Clear Tag dialog box, perform one of these steps, then click OK.
   - Remove a specific tag — Select the tag group, then select the tag.

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

   - Remove all tags — Select Clear All.

4. Verify that the tags have been removed:
   a. Select Menu | Systems | Tag Catalog, then select a tag or tag group in the list of tags.

   b. Next to Systems with tag in the details pane, click the link for the number of systems tagged manually. The Systems with Tag Applied Manually page appears.

   c. Verify that the systems are not included in the list.

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

Task

1. Select Menu | Systems | Tag Catalog, then select a tag or tag group from the Tags list.

2. Click Actions | Run Tag Criteria.

3. On the Action pane, select whether to reset manually tagged and excluded systems.

   Resetting manually tagged and excluded systems removes the tag from systems that don't match the criteria, and applies the tag to systems that match criteria but were excluded from receiving the tag.

4. Click OK.
5 Verify that the systems have the tag applied:
   a Select Menu | Systems | Tag Catalog, then select a tag or tag group in the list of tags.
   b Next to Systems with tag in the details pane, click the link for the number of systems with the tag applied
      by criteria. The Systems with Tag Applied by Criteria page appears.
   c Verify that the systems are in the list.

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

Apply criteria-based tags on a schedule
Schedule a regular task that applies a tag to all systems that match the tag criteria.

Task

1 Open the Server Task Builder.
   a Select Menu | Automation | Server Tasks.
   b Click New Task.

2 On the Description page, name and describe the task and select whether the task is enabled once it is
   created, then click Next. The Actions page appears.

3 Select Run Tag Criteria from the drop-down list, then select a tag from the Tag drop-down list.

4 Select whether to reset manually tagged and excluded systems.
   Resetting manually tagged and excluded systems does two things:
   ▪ Removes the tag on systems that don't match the criteria
   ▪ Applies the tag to systems that match the criteria but were excluded from receiving the tag

5 Click Next to open the Schedule page.

6 Schedule the task for the times you want, then click Next.

7 Review the task settings, then click Save.

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

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

Contents
- Users
- Authenticating with certificates
- Permission sets

Users

User accounts allow you to control how people access and use McAfee ePO.

You can create user accounts manually, then assign each account an appropriate permission set. You can also configure your McAfee ePO server to allow users to log on using Windows authentication, but this requires configuration and set up of multiple settings and components.

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

Managing McAfee ePO users with Active Directory

Use pre-existing Windows authenticated user credentials to automatically create McAfee ePO users and assign permissions to them.

Authenticate credentials by mapping McAfee ePO permission sets to Active Directory groups in your environment. This feature can reduce the management overhead when you have many McAfee ePO users in your organization. To complete the configuration, use this process:

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

User authentication

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

- Against the domain that your McAfee ePO server is joined to (default).
- Against a list of one or more domain controllers.
- Against a list of one or more DNS-style domain names.
- Using a WINS server to look up the appropriate domain controller.
If you use domain controllers, DNS-style domain names, or a WINS server, configure the Windows authentication server setting.

**Registered LDAP servers**

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

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

The user account used to register the LDAP server with McAfee ePO is trusted through a bidirectional transitive trust. Otherwise, it must physically exist on the domain that the LDAP server belongs to.

**Windows authorization**

The server setting for Windows authorization specifies which Active Directory (AD) server McAfee ePO 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 logon.

McAfee ePO can dynamically assign permission sets to Windows Authenticated users even if Active Directory User Login is not enabled.

**Assigning permissions**

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

**Active Directory User Login**

You can enable the Active Directory User Login server setting, which 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`, supplies these credentials: `eng\jsmith1`, with the appropriate password.

- An Active Directory server that contains information about this user has been registered with McAfee ePO.

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

**Support for Universal Groups**

McAfee ePO partially supports Active Directory Universal Groups.

It restricts its communication to one domain when retrieving group information.

It supports these features when retrieving group memberships for a Universal Group:

- Direct membership lookup in a Universal Group
- Indirect membership lookup through a nested Universal Group
- Indirect membership lookup through Global or Domain Local Groups, if that group resides in the same domain as the Global Catalog being used to perform the lookup

Finally, it does not support indirect membership when that group resides on a different domain from the Global Catalog being used to perform the lookup.
Windows authentication and authorization strategies

You can take several approaches when planning how to register your LDAP servers. Taking the time in advance to plan your server registration strategy helps you get it right the first time and reduce problems with user authentication.

Ideally, authentication and authorization is a process you do once, and only alter if your overall network topology changes. Once servers are registered and Windows authentication is configured, you do not have to modify these settings often.

Authentication versus authorization

Authentication involves verifying the user’s identity by matching as authentic the credentials supplied by the user to something the system trusts. This trust could be a McAfee ePO server account, Active Directory credentials, or a certificate. If you want to use Windows authentication, examine how the domains (or servers) containing your user accounts are organized.

The software completes Authorization after you verify the user’s credentials. You can apply permission sets and determine what the user can do within the system. Windows authentication allows you to set permission for users from different domains. Attach permission sets to groups contained within these domains.

User account network topology

The effort required to fully configure Windows authentication and authorization depends on your network topology, and the distribution of user accounts across your network.

- If the credentials for users are contained in a small set of domains or servers in a single domain tree, register the root of the tree.
- If your user accounts are more spread out, register a number of servers or domains. Determine the minimum number of domain (or server) subtrees you need and register the roots of those trees. Try to register them in the order of usage. Placing the most commonly used domains at the top of the list improves average authentication performance.

Permission structure

For users to be able to log on to a McAfee ePO server using Windows authentication, attach a permission set to the Active Directory group on the domain their account belongs to. When determining how permission sets are assigned, consider the following capabilities:

- Permission sets can be assigned to multiple Active Directory groups.
- Permission sets can be dynamically assigned only to an entire Active Directory group. They cannot be assigned to just some users within a group.

If you want to assign special permissions to an individual user, you can do so by creating an Active Directory group that contains only that user.

Enable Windows authentication in the McAfee ePO server

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

To activate the Windows Authentication page in the server settings, stop the ePolicy Orchestrator Cloud service. Perform this task on the McAfee ePO server.
Task

1. From the server console, select Start | Settings | Control Panel | Administrative Tools
2. Select Services.
3. In the Services window, right-click McAfee ePolicy Orchestrator Applications Server and select Stop.
4. Rename Winauth.dll to Winauth.bak.
   In a default installation, this file is found in C:\Program Files\McAfee\ePolicy Orchestrator \Server\bin.
5. Restart the server.

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

Configure Windows authentication

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

**Before you begin**
You must have first prepared your server for Windows authentication.

How you configure these settings depends on several issues:

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

Users can authenticate using Windows credentials for the domain that the McAfee ePO server is joined to. They can also authenticate to any domain that has a two-way trust relationship with the McAfee ePO server’s domain. If you have users in domains that don't meet that criteria, configure Windows authentication.

Task

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

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

4. Click Save when you are finished adding servers.

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

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

**Task**

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

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

Create a custom logon message

Create and display a custom logon message to be displayed on the Log On page. Your message can be written in plain text, or formatted using HTML. If you create an HTML formatted message, you are responsible for all formatting and escaping.

**Task**

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

Restrict a user session to a single IP address

Restricting logons to a single IP address can prevent attacks that take advantage of persistent session information.

By default, user sessions are maintained across IP addresses. Maintaining user sessions enables users to change locations without having to log on repeatedly.

If your network requires more security, you can restrict user sessions to a single IP address. Doing so forces users to resubmit their credentials every time their IP address changes, such as when they take their laptop to a different location.
Task

1. Select **Menu | Configuration | Server Settings**, select **User Session** from the **Settings Categories**, then click **Edit**.
2. Select **Restrict session to a single IP address**.
3. Click **Save**.

Any time a user changes IP addresses, they must re-enter their credentials to access the McAfee ePO console.

The Audit Log

The Audit Log records all McAfee ePO user actions. Visit the Audit Log to track user actions. For example, you can see who created a product deployment.

Since the Audit Log is a growing list of information, to improve performance, periodically purge the old information.

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

Audit Log entries can be queried against. You can create queries with the Query Builder 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.

- Periodically remove outdated actions from the Audit Log to improve database performance.

Audit Log example

This Audit Log example describes tracking the actions of an individual McAfee ePO user. For example, if an individual user created a product deployment, you can see details about the created deployment, using the Audit Log.

In this figure, the Audit Log is filtered to show a specific user’s recent activities. You can see when the user logged on and off, and what changes they made. To learn more information about a specific action, like the product deployment, you can click on that row.
You can click an Audit Log row to show details about that entry.

**View user actions**
The Audit Log displays past user actions. Use the Audit Log to track access to your McAfee ePO server, and what changes users make.

**Task**

1. Open the Audit Log: select **Menu | Reporting | Audit Log**.
2. Sort and filter the table to focus on relevant entries.
   - To change which columns are displayed, click **Choose Columns**.
   - To order table entries, click a column title.
   - To hide unrelated entries, select a filter from the drop-down list.
3. To view additional details, click an entry.

**Remove outdated actions from the Audit Log**
Periodically remove outdated actions from the Audit Log to improve database performance.

*Items removed from the Audit Log are deleted permanently.*
Task

1. Open the Audit Log: select **Menu | Reporting | Audit Log**.
2. Click **Purge**.
3. In the Purge dialog box, enter a number, then select a time unit.
4. Click **OK**.

Any items of the specified age or older are deleted, including items not in the current view. The number of removed items is displayed in the lower right corner of the page.

Create a server task to automatically remove outdated items.

---

**Authenticating with certificates**

Enable certificate-based authentication to allow your users to access McAfee ePO with a valid client certificate instead of a user name and password.

Client certificate authentication is a type of public-key authentication. It differs from public-key authentication because you grant trust to a trusted third party, known as a **certification authority** (or CA). Certificates are digital documents that combine identity information and public keys. The CA digitally signs the certificates and verifies that the information is accurate.

When a user tries to access McAfee ePO using certificate-based authentication, McAfee ePO checks the client certificate to make sure that it was signed. After the client certificate is verified, the user is granted access.

Certificates have predefined expiration dates, which force the review of user permissions.

For users configured with valid certificates, certificate-based authentication replaces password authentication. All other users continue to use passwords to access McAfee ePO.

Before your organization can use certificate-based authentication, install the CA certificate on McAfee ePO and a signed client certificate on your endpoints.

**Configure McAfee ePO for certificate-based authentication**

Before users access McAfee ePO with certificate-based authentication, enable the authentication method and upload a signed CA certificate.

---

**Before you begin**

You must have a signed certificate in P7B, PKCS12, DER, or PEM format.

---

**Task**

1. Open the Edit Certificate-based Authentication page.
   a. Select **Menu | Configuration | Server Settings**.
   b. From the **Setting Categories** list, select **Certificate-based Authentication**, and click **Edit**.
2. Select **Enable certificate-based Authentication**.
3 Next to CA certificate for client certificate, click Browse, navigate to and select the certificate file, then click OK. When a file is applied, the prompt changes to Replace current CA certificate.

Replace the certificate when it expires, or if your organization's security requirements change. For example, your organization might require SHA-256 certificates for authentication.

4 (Optional) If you provided a PKCS12 certificate, enter a password.

5 Configure any advanced or optional settings as needed.

- If you have a certificate revocation list (CRL), click Browse, navigate to and select the CRL file, then click OK.

The CRL file must be in PEM format.

- (Optional) As an alternative or additional method of checking a certificate's authenticity, configure the Online Certificate Status Protocol (OCSP).

  1 Click Enable OCSP checking.
  2 Type the URL to the OCSP server.
  3 (Optional) Select Enable CRL Distribution Point checks when the McAfee ePO server receives no response from OCSP.

If the connection to the default OCSP URL fails, McAfee ePO tries to connect to the certification authority CRL mentioned within the certificate under CRL Distribution Point Check instead.

  4 (Optional) Select Make the default OCSP URL the primary OCSP URL.

If that connection fails, McAfee ePO falls back to the other OCSP responder, if mentioned in the certificate under Authority Information Access.

- To require certificate-based authentication for all remote users, click Remote users use the certificate to sign in.

- To make the user name the same as the subject Distinguished Name (DN) specified in the certificate, click Default certificate user name is the subject DN.

- Configure Active Directory Integration.

  For these settings to work, you must have Active Directory user logon enabled and the user group added to a permission set.

  - To automatically assign Active Directory users to a permission set, select Automatically assign permission for user logon with an Active Directory certificate.
  
  - To automatically create an McAfee ePO user account for anyone who accesses McAfee ePO with the valid AD certificate, select Automatically create user for Active Directory certificate owners.

6 Click Save.

7 Restart ePolicy Orchestrator Cloud to activate certificate authentication.

**Disable certificate-based authentication**

If certificates are no longer used in your network environment, remove certificate-based authentication as an authentication option.
**Task**

1. Open the Edit Certificate-based Authentication page.
   a. Select **Menu | Configuration | Server Settings**.
   b. From the **Setting Categories** list, select **Certificate-based Authentication**, and click **Edit**.

2. Deselect **Enable Certificate Based Authentication**, then click **Save**.

Once you disable certificate-based authentication, your users can no longer access McAfee ePO with a certificate, and must log on with their user name and password instead. Your previous configuration settings are reset.

Restart the server to complete the configuration change.

**Configure user accounts for certificate-based authentication**

Users must have certificate-based authentication configured before they can authenticate with a client certificate. The client certificates used for certificate-based authentication are typically acquired with a smart card or similar device. Software bundled with the smart card hardware can extract the certificate file. This extracted certificate file is usually the file uploaded in this procedure.

**Task**

1. Open the **Edit User** page.
   a. Select **Menu | User Management | Users**.
   b. From the **Users** list, select a user, then click **Actions | Edit**.

2. Next to **Authentication type**, select **Change authentication or credentials | Certificate-Based Authentication**.

3. Use one of these methods to provide credentials:
   - Copy the DN field from the certificate file and paste it into the **Personal Certificate Subject DN Field** edit box.
   - Upload the signed certificate file: click **Browse** to navigate to and select the certificate file, then click **OK**.

   
   ![This certificate file was uploaded in the procedure, Configure MFS certificate-based authentication.]

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

4. Click **Save** to save changes to the user’s configuration.

The certificate information is verified. A warning appears if the certificate is invalid. If the certificate is valid, the McAfee ePO logon page appears. The user can choose a language and click **Log On** without entering a user name and password.

**Update the certificate revocation list**

To prevent access to McAfee ePO by specific users that were configured for certificate-based authentication, add the user’s client certificate to the certificate revocation list (CRL) installed on your McAfee ePO server.

**Before you begin**

You must already have a CRL file in ZIP or PEM format.
The CRL file is a list of revoked McAfee ePO users and their digital certificate status. The list includes the revoked certificates, the reasons for revocation, dates of certificate issue, and the issuing entity. When a user tries to access the McAfee ePO server, the CRL file is checked and it allows or denies access for that user.

**Task**

1. Select **Menu | Configuration | Server Settings**.
2. Select **Certificate-based Authentication**, then click **Edit**.
3. To update the CRL file, next to **Certificate revocation list file**, click **Choose File**, navigate to the CRL file, then click **OK**.
4. Click **Save** to save all changes.
5. Restart McAfee ePO to activate certificate authentication.

McAfee ePO checks the updated CRL file to confirm that the client certificate has not been revoked every time a user tries to access the McAfee ePO.

You can also use the cURL command line to update the CRL file.

To run cURL commands from the command line, install the cURL and grant remote access to the McAfee ePO server. See the *McAfee ePolicy Orchestrator Web API Scripting Guide* for cURL download details and other examples.

At the cURL command-line type:

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

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

**Troubleshooting certificate-based authentication**

A few problems cause most authentication issues using certificates.

If a user cannot log on with their certificate, try one of these options to resolve the problem:

- Verify that the user has not been disabled.
- Verify that the certificate has not expired or been revoked.
- Verify that the certificate is signed with the correct certificate authority.
- Verify that the DN field is correct on the user configuration page.
- Verify that the browser is providing the correct certificate.
- Check the Audit Log for authentication messages.
Permission sets

Permission sets control the level of access users have to the features available in the software.

To create a more secure environment, specify and control the access users have to different parts of the system for even the smallest installations.

Contents
- How users, groups, and permission sets fit together
- Manage permission sets

How users, groups, and permission sets fit together

McAfee ePO controls access to items using interactions between users, groups, and permission sets.

A user account grants log on access to the McAfee ePO console and when mapped with a permission set, it defines what the user is allowed to access. Administrators can create accounts for individual users and assign permissions, or they can create a permission set that maps to users or groups in your Active Directory/NT server.

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

Administrators

Administrators have read and write permissions and rights to all operations. When you install the server, an administrator account is created automatically. By default, the user name for this account is admin. If the default value is changed during installation, this account is named accordingly.

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

Permissions exclusive to administrators include:
- Create, edit, and delete source and fallback sites.
- Change server settings.
- Add and delete user accounts.
- Add, delete, and assign permission sets.
- Import events into McAfee ePO databases and limit events that are stored there.

Users

Users can be assigned any number of permission sets to define their access levels in McAfee ePO.

User accounts can be created and managed in several ways. You can:
- Create user accounts manually, then assign each account an appropriate permission set.
- Configure your McAfee ePO server to allow users to log on using Windows authentication.

Allowing users to log on using their Windows credentials is an advanced feature that requires configuration and setup of multiple settings and components.

Groups

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

A particular access profile is defined in a permission set. This profile usually involves a combination of access levels to various parts of McAfee ePO. For example, one permission set might grant the ability to read the Audit Log, use public and shared dashboards, and create and edit public reports or queries.

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

Default permission sets

McAfee ePO provides these four default permission sets that provide permissions to its functionality.

- Executive Reviewer — Provides view permissions to dashboards, events, contacts, and can view information that relates to the whole 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.
- Global Admin — Provides view and change permissions across McAfee ePO features. Users that are assigned this permission set each need at least one more permission set that grants access needed products and groups of the System Tree.
- Group Reviewer — Provides view permissions across McAfee ePO features. Users that are assigned this permission set each need at least one more permission set that grants access needed products and groups of the System Tree.

A user group administrator or the global administrator can edit the canned permission sets as required.

When you upgrade a product extension:

- An edited canned permission set for the product is retained with the default canned permission set.
- A deleted permission set for the product is added again.

Manage permission sets

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

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

Task

1. Open the Permission Sets page: select Menu | User Management | Permission Sets.
2. Select one of these actions.
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a permission set</td>
<td>1 Click <strong>New Permission Set</strong>.</td>
</tr>
<tr>
<td></td>
<td>2 Type a unique name for the new permission set.</td>
</tr>
<tr>
<td></td>
<td>3 To immediately assign specific users to this permission set, select their user names in the Users section.</td>
</tr>
<tr>
<td></td>
<td>4 To map any Active Directory groups to this permission set, select the server from the Server Name list, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>5 If you added any Active Directory servers that you want to remove, select them in the Active Directory list box, then click <strong>Remove</strong>.</td>
</tr>
<tr>
<td></td>
<td>6 Click <strong>Save</strong> to create the permission set.</td>
</tr>
<tr>
<td>Edit a permission set</td>
<td>1 Select a permission set to change. Its details appear to the right.</td>
</tr>
<tr>
<td></td>
<td>If you created a permission set, it is already selected for you.</td>
</tr>
<tr>
<td></td>
<td>2 Select a category of permissions to change by clicking <strong>Edit</strong> in that category row.</td>
</tr>
<tr>
<td></td>
<td>3 Change the permissions, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Copy a permission set</td>
<td>1 From the <strong>Permission Sets</strong> list, select a permission set to duplicate, then click <strong>Actions</strong></td>
</tr>
<tr>
<td></td>
<td>2 Type a new name for the duplicate permission set. By default, the software appends (copy) to the existing name.</td>
</tr>
<tr>
<td></td>
<td>3 Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Delete a permission set</td>
<td>1 Select the permission set that you want to delete From the <strong>Permission Sets</strong> list, select the permission set that you want to delete. Its details appear to the right.</td>
</tr>
<tr>
<td></td>
<td>2 Click <strong>Actions</strong></td>
</tr>
<tr>
<td>Export permission sets</td>
<td>Click <strong>Export All</strong>.</td>
</tr>
<tr>
<td></td>
<td>The McAfee ePO server sends an XML file to your browser. What happens next depends on your browser settings. Most browsers ask you to save the file.</td>
</tr>
<tr>
<td></td>
<td>The XML file contains only roles with a defined level of permissions. If, for example, a Permission Set has no permissions for queries and reports, no entry appears in the file.</td>
</tr>
<tr>
<td>Import permission sets</td>
<td>1 Click <strong>Import</strong>.</td>
</tr>
<tr>
<td></td>
<td>2 Click <strong>Browse</strong> to navigate to and select the XML file with the permission sets that you want to import.</td>
</tr>
<tr>
<td></td>
<td>3 Choose whether to keep permission sets with the same name as an imported permission set by selecting the appropriate option. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>If McAfee ePO cannot locate a valid permission set in the indicated file, an error message is displayed and the import process is stopped.</td>
</tr>
<tr>
<td></td>
<td>The permission sets are added to the server and displayed in the Permission Sets list.</td>
</tr>
</tbody>
</table>
Software Manager

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

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

What's in the Software Manager

The Software Manager eliminates the need to access the McAfee Product Download website to obtain new McAfee software and software updates.

You can use the Software Manager to download:

- **Licensed software** is any software your organization has purchased from McAfee. The Software Not Checked In product category provides a list of licensed software that is not currently installed on your server. The number displayed next to each subcategory in the Product Categories list indicates how many products are available.

- **Evaluation software** is software for which your organization does not currently possess a license. You can install evaluation software on your server, but functionality might be restricted until you acquire a product license.

- **Software updates** are a new update for the released software you are using. You can use the Software Manager to check in new packages and extensions. Available software updates are listed in the Updates Available category.

- **Product documentation** is new and updated product documentation you can obtain from the Software Manager. Help extensions can be installed automatically. PDF and HTML documentation such as Product Guides and Release Notes can also be downloaded from the Software Manager.

 DATs and Engines are not available from the Software Manager.

About software component dependencies

Many of the software products you can install for use with your McAfee ePO server have predefined dependencies on other components. Dependencies for product extensions are installed automatically. For all other product components, you must review the dependencies list in the component details page, and install them first.

Software Manager user interface

The Software Manager user interface has these main features to help you view and manipulate your new and existing software.
## Option Definition

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Categories</strong></td>
<td>This is where you search for or select products to view or manipulate in the selected product tables.</td>
</tr>
</tbody>
</table>

**Selected product tables, separated into three parts:**

- **List of products and their status**
  
  Select a product in this list and details and manipulation features appear in the details and component rows.

- **Product details row**
  
  Lists a product description, its status, allows a language filter, and provides these actions:
  
  - **Check In All**
    
    Checks in all new versions and components of the selected product.
  
  - **Update All**
    
    Updates all existing versions and components of the selected product to the latest version.
  
  - **Remove All**
    
    Removes all versions and components of the selected product.

- **Component rows**
  
  Displays all components of the selected product and, depending on the component, allows you to check in, update, remove, or download the individual component.

---

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

From the Software Manager, you can check in, update, and remove managed product components from your server.

Both licensed and evaluation software can be accessed in the Software Manager.

Software availability, and whether it is in the **Licensed** or **Evaluation** category, depends on your license key. For more information, contact your administrator.

---

**Task**

1. Click **Menu | Software | Software Manager**.

2. In the **Software Manager** page **Product Categories** list, select one of the following categories, or use the search box to find your software:
   
   - **Updates Available** — Lists any available updates to licensed software components already installed or checked in to the McAfee ePO server.
   
   - **Checked in Software** — Displays all software (both **Licensed** and **Evaluation**) installed or checked in to this server.

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

   - **Software Not Checked in** — Displays any software that is available, but not installed on this server.
   
   - **Software (by Label)** — Displays software by function as described by McAfee product suites.
3 When you have located the correct software, select an action that applies to all the components in the software, or individual components:

- For all the components in the software, click:
  - Check In All to check in all components of the new product on this server.
  - Update All to update all components of the existing product on this server.
  - Remove All to remove all components of the existing product on this server.

- For individual components in the software, click:
  - Download to download software or product documentation to a location on your network.
  - Check In (branch) to check in a new product package on this server.
  - Check In to check in a new product extension on this server.
  - Update to update an existing package or extension that is already installed or checked in to this server.
  - Remove to uninstall a package or extension that is installed or checked in to this server.

4 In the Check In Software Summary page, review and accept the product details and End User License Agreement (EULA), then click OK to complete the operation.

Checking product compatibility

You can configure a Product Compatibility Check to automatically download a Product Compatibility List from McAfee. This list identifies products that are no longer compatible in your McAfee ePO environment.

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

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

See the McAfee ePolicy Orchestrator Installation Guide for details.

Product Compatibility Check

The Product Compatibility Check uses an XML file, the Product Compatibility List, to determine which product extensions aren't compatible with a version of McAfee ePO.

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

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

Remediation

When you view the list of incompatible extensions through the installer or the Upgrade Compatibility Utility, you are notified if a known replacement extension is available.
In some cases during an upgrade:
• An extension blocks the upgrade and must be removed or replaced before the upgrade can continue.
• An extension is disabled, but you must update it after the McAfee ePO upgrade is complete.

Disabling automatic updates
You might want to disable automatic updates of the Product Compatibility List. The download occurs:
• As part of a background task.
• When the Software Manager content is refreshed (helpful when your McAfee ePO server does not have inbound Internet access).
• When you re-enable the download setting for the Product Compatibility List (also re-enables Software Manager automatic updates of the Product Compatibility List).

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

You can manually download the list:
• When you install McAfee ePO.
• When using Server Settings | Product Compatibility List to manually upload a Product Compatibility List. This list takes effect immediately after upload.

Best practice: Disable automatic updating of the list to prevent overwriting the manually downloaded Product Compatibility List.

Open https://epo.mcafee.com/ProductCompatibilityList.xml to manually download the list.

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setup.exe DISABLEPRODCOMPATUPDATE=1</td>
<td>Disables automatic downloading of the Product Compatibility List from the McAfee website.</td>
</tr>
<tr>
<td>setup.exe PRODCOMPATXML=&lt;full_filename_including_path&gt;</td>
<td>Specifies an alternate Product Compatibility List file.</td>
</tr>
</tbody>
</table>

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

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

Any manually downloaded Product Compatibility List must be a valid XML file provided by McAfee. If you make any changes to the Product Compatibility List XML file, the file is no longer valid.
Task

1. Select **Menu | Configuration | Server Settings**, select **Product Compatibility List** from the **Setting Categories**, then click **Edit**.
   
   A list of disabled incompatible extensions appears.

2. Click **Disabled** to stop automatic and regular downloads of the Product Compatibility List from McAfee.

3. Click **Browse** and navigate to the **Upload Product Compatibility List**, then click **Save**.

Automatic downloading of the Product Compatibility List is disabled. Your McAfee server uses the same list until you upload a new list, or connect your server to the Internet and enable automatic downloading.
Manual package and update management

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

Contents

- Bring products under management
- Check in packages manually
- Delete DAT or engine packages from the Master Repository
- Move DAT and engine packages between branches
- Check in Engine, DAT, and Extra.DAT update packages manually
- Best practice: Automating DAT file testing

Bring products under management

A product’s extension must be installed before McAfee ePO can manage the product.

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

Task

1. From the McAfee ePO console, select **Menu | Software | Extensions | Install Extension**.
   
   You can only have one task updating the Master Repository at once. If you try to install an extension at the same time as a Master Repository update is running, the following error appears:

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

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

2. Browse to and select the extension file, then click **OK**.

3. Verify that the product name appears in the **Extensions** list.

Check in packages manually

Check in the deployment packages to the Master Repository so that the ePolicy Orchestrator software can deploy them.
### Task

1. Open the Check In Package wizard.
   - Select **Menu** | **Software** | **Master Repository**.
   - Click **Check In Package**.

2. Select the package type, then browse to and select the package file.

3. Click **Next**.

4. Confirm or configure the following:
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the branch. If there are requirements in your environment to test new packages before deploying them throughout the production environment, use the **Evaluation** branch whenever checking in packages. Once you finish testing the packages, you can move them to the **Current** branch by selecting **Menu** | **Software** | **Master Repository**.
   - **Options** — Select whether to:
     - **Move the existing package to the Previous branch** — When selected, moves packages in the Master Repository from the **Current** branch to the **Previous** branch when a newer package of the same type is checked in. Available only when you select **Current** in **Branch**.
     - **Package signing** — Specifies if the package is a McAfee or a third-party package.

5. Click **Save** to begin checking in the package, then wait while the package is checked in.

The new package appears in the **Packages in Master Repository** list.

### Delete DAT or engine packages from the Master Repository

Delete DAT or engine packages from the Master Repository. As you check in new update packages regularly, they replace the older versions or move them to the Previous branch, if you are using the Previous branch.

#### Task

1. Click **Menu** | **Software** | **Master Repository**.

2. In the row of the package, click **Delete**.

3. Click **OK**.

### Move DAT and engine packages between branches

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

1. Select Menu | Software | Master Repository.
2. In the row of the package, click Change Branch.
3. Select whether to move or copy the package to another branch.
4. Select which branch receives the package.
   - If you have McAfee® NetShield® for NetWare in your network, select Support NetShield for NetWare.
5. Click OK.

Check in Engine, DAT, and Extra.DAT update packages manually

Check in update packages to the Master Repository to deploy them using the McAfee ePO software. Some packages can only be checked in manually.

Task

1. Open the Check In Package wizard.
   a. Select Menu | Software | Master Repository.
   b. Click Check In Package.
2. Select the package type, browse to and select a package file, then click Next.
3. Select a branch:
   - Current — Use the packages without testing them first.
   - Evaluation — Use the packages in a lab environment first.

   Once you finish testing the packages, you can move them to the Current branch by selecting Menu | Software | Master Repository.
   - Previous — Use the previous version to receive the package.
4. Next to Options, select Move the existing package to the Previous branch to archive the existing 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.

Best practice: Automating DAT file testing

Use the built-in functionality of McAfee ePO to automatically validate DAT file compatibility and content files that are downloaded from the McAfee public site.

McAfee Labs rigorously tests the content, such as DAT and engine files, before they are released on the public update servers. Because every organization is unique, you can perform your own compatibility validation to ensure the compatibility of DATs and content in your unique environment.
The compatibility validation processes vary by organization. The process in this section is meant to automate much of the compatibility validation process and reduce the need for administrator intervention.

**Best practice:** To confirm that only compatible DAT files are distributed in your environment, you might move the content manually from the Evaluation branch into the Current branch of the repository.

**DAT file validation overview**

Figure 9-1  Automatic DAT file testing steps

1. A server task pulls DAT updates from the McAfee public site to the Evaluation branch of the Master Repository.
2. A McAfee Agent policy applies the DAT files from the Evaluation repository branch restricted to a group of systems in a Test group.
3. A McAfee Agent update client task installs the DAT on the Test group systems.
4. An on-demand scan task runs frequently on the Test group.

Depending on the on-demand scan output, one of these scenarios occurs:
If the DAT is not compatible with the test group, an Automatic Response email is sent to the appropriate administrators. The email tells the administrators to stop distribution of the DAT files from the Current repository.

Otherwise, after a specified time, a server task copies the files from the Evaluation branch to the Current branch of the repository. Then those files are automatically sent to the rest of the managed systems.

**Pull and copy DAT updates from McAfee**

To create an automated DAT file testing process requires configuring tasks to pull the DATs from McAfee and copy them to the Current branch of the repository.

The McAfee ePO platform provides three repository branches in your Master and Distributed Repositories:

- **Current branch** — By default, the main repository branch for the latest packages and updates.
- **Evaluation branch** — Used to test new DAT and engine updates before deploying to your whole organization.
- **Previous branch** — Used to save and store prior DAT and engine files before adding the new ones to the Current branch.

You must create two server tasks to automate the DAT file testing.

- One task pulls the DAT files hourly to the Evaluation branch to ensure that the latest DAT is in the Evaluation branch shortly after McAfee releases it to the public.

  ![Best practice: Run the task hourly to get an extra DAT file in case the initial file, released at 11:00 a.m., was replaced later in the day.]

- One server task waits until a few hours after the test group of systems is scanned. Then, unless the administrator stops the server task, it automatically copies the DAT files from the Evaluation branch to the Current branch.

**Tasks**

- **Best practices: Configure task to pull DAT to Evaluation branch on page 113**
  To automate your DAT file testing process, you must create a task to automatically pull DAT files from the McAfee public site into the Evaluation repository branch.

- **Best practices: Configure server task to copy files from Evaluation to Current branch on page 114**
  To automate your DAT file testing process, create a task to automatically copy DAT files from the Evaluation branch of the repository to the Current branch.

**Best practices: Configure task to pull DAT to Evaluation branch**

To automate your DAT file testing process, you must create a task to automatically pull DAT files from the McAfee public site into the Evaluation repository branch.

You might want to configure this task to distribute only DAT files, if your organization tests the engine for a longer time, than the few hours in this example, or restricts their automatic release.

**Task**

1. Select **Menu | Automation | Server Tasks**, then click **Actions | New Task** to display the **Server Task Builder** wizard.
2. In the **Description** tab, type a server task name, for example, **DAT pull hourly to Evaluation repository, and a description to appear on the Server Task page.**
3. In **Schedule status**, click **Enable**, then click **Next**.
4 In the Actions tab, configure these settings:
   • From the Actions list, select Repository Pull.
   • From the Source site list, select the McAfee public site you want to use, McAfeeFtp or McAfeeHttp.
   • From the Branch list, select Evaluation.
   • Deselect Move existing package to Previous branch, if needed.
   • From Package types, click Select packages.

5 From the Available Source Site Packages dialog box, select DAT and Engine, then click OK.
   We recommend that, at minimum, you pull the DAT and engine files from the McAfee public website.
   If you have multiple distributed repositories, you can chain a replication task to the same pull task to
   replicate your Evaluation branch to your distributed repositories.

6 In the Schedule tab, configure these settings:
   • For the Schedule type, click Hourly.
   • For the Start date, select today's date.
   • For the End date, click No end date.
   • From Schedule, configure the task to run every hour at 10 minutes past the hour.

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

To confirm that the automatic DAT file pull is working, go to Menu | Software | Master Repository and use the
Check-In date information to confirm that the Evaluation branch DAT file was updated within the last two hours.

**Best practices: Configure server task to copy files from Evaluation to Current branch**
To automate your DAT file testing process, create a task to automatically copy DAT files from the Evaluation
branch of the repository to the Current branch.

**Before you begin**
You must have created the server task to automatically copy the DAT and content files to the Evaluation branch of the repository.

**Task**

1 Select Menu | Automation | Server Tasks, then click Actions | New Task.

2 In the Server Task Builder Descriptions tab, type a task name and notes, then in Schedule status, click Enabled,
then click Next.

3 In the Actions tab, configure these settings, then click Next:
   • For Actions list, select Change the Branch for a Package, select All packages of type 'DAT' in branch 'Evaluation' as the package to change, Copy as the action, then click Current as the target branch.
   • Click + to create another action, and from the second Actions list, select Change the Branch for a Package, select All packages of type 'Engine' in branch 'Evaluation' as the package to change, Copy as the action, and Current as the target branch.
4 In the Schedule tab, change these settings:
   • For Schedule type, click Daily.
   • For Start date, select today’s date.
   • For End date, click No end date.
   • Change the Schedule settings to configure the task to run at 4:00 or 5:00 p.m.

   Historically, McAfee releases DAT files only once a day, at about 3:00 p.m. Eastern Time (19:00 UTC or GMT). In the rare case that a second DAT file is released later in the day, it requires an administrator to disable the copy task to your Current Branch.

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

To confirm that the DAT file copy from the Evaluation branch to the Current branch is working, go to Menu | Software | Master Repository and use the Check-In date information to confirm that the Evaluation branch DAT file was copied to the Current branch at the time configured in the schedule.

**Best practice: Create a test group of systems**

To safely test DAT and content files, create a test group of systems used to run the files in your Evaluation repository.

Make sure that the test group of systems you use meet the following criteria:

   • Use a representative sampling of system server builds, workstation builds, and operating systems and Service Packs in your environment for validation.
   • Use 20–30 systems for validation for organizations with less than 10,000 nodes. For larger organizations, include at least 50 types of systems.

   You can use VMware images that replicate your operating system builds. Make sure that these systems are in a “clean” state to ensure that no malware has been introduced.

   • Use Tags to apply policies and tasks to individual systems that are scattered throughout your System Tree. Tagging these systems has the same effect as creating an isolated test group, but allows you to keep your systems in their current groups.

**Task**

1 To create a System Tree group, select Menu | Systems Section | System Tree.

2 From the System Tree group list, select where you want to add your new group, then click System Tree Actions | New Subgroups, and in the New Subgroups dialog box, type a name, for example DAT Validation, then click OK.

3 To add systems to your test group, you can drag systems from other groups to your newly created subgroup, add new systems, or add virtual machine systems.

You created a test group as an isolated group of systems. This test group allows you to test new DAT and engine updates before you deploy the updates to all other systems in your organization.

**Best practice: Configure an agent policy for the test group**

Create a McAfee Agent policy with an update task that automatically copies DAT and content files to the systems in your test group.
Task

1 In the System Tree, select Menu | Systems Section | System Tree, then click the test group that you created.

2 To duplicate the existing policy, click the Assigned Policies tab, select McAfee Agent from the Product list, then in the Category list in the General policy row, click My Default.

3 On the My Default page, click Duplicate, and in the Duplicate Existing Policy dialog box, type the name, for example Update from Evaluation, add any notes, then click OK.

   This step adds a policy, Update from Evaluation, to the Policy Catalog.

4 Click the Updates tab to change the repository used by this policy.

5 In the Repository branch to use for each update type, click the DAT and Engine list down-arrows, then change the listed repositories to Evaluation.

6 Click Save.

Now you have created a McAfee Agent policy to use with an update task that automatically copies the DAT and content files to the systems in your test group from the Evaluation repository.

Best practice: Configure an on-demand scan of the test group

Create an on-demand scan task that starts after you update the DAT files to your test group, to scan for any problems that occur in your test group.

Before you begin

You must have created the test group in your System Tree.

This configuration assumes that you are not using user systems as your test systems. If you are using actual user systems, you might need to change some of these scan configurations.

Task

1 To create a new on-demand scan task, select Menu | Policy | Client Task Catalog, then from the Client Task Catalog page in the Client Task Types list, expand VirusScan Enterprise and click On Demand Scan.

2 In the Client Task Catalog page, click New Task, and in the New Task dialog box, confirm that On Demand Scan is selected and click OK.

3 On the Client Task Catalog: New Task page, type a name, for example, Evaluation test group ODS task, and add a detailed description.

4 Click the Scan Locations tab, then configure these settings:
   a For the Locations to scan, configure:
      • Memory for rootkits
      • Running Processes
      • All local disks
      • Windows folder
   b For the Scan options, select Include subfolders and Scan boot sectors.
5 Click the Scan Items tab, then configure these settings:
   a For File types to scan, select All files.
   b For Options, select Detect unwanted programs.
   c For Heuristics, select Find unknown program threats and Find unknown macro threats.

6 In the Actions tab:
   a For When a threat is found, configure Clean files, then Delete files.
   b For When an unwanted program is found, configure Clean files, then Delete files.

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

   ! Do not change any settings on the Reports tab.

8 In the Task tab:
   a For Platforms where this task will run, select Run this task on servers and Run this task on workstations.
   b For User account to use when running task, set your credentials and select the test group domain.

9 Click Save.

Now the on-demand scan task is configured to scan for any problems that might occur in your test group. Next configure a client task to schedule when to launch the task.

**Best practice: Schedule an on-demand scan of the test group**

Schedule your on-demand scan task to run five minutes after each McAfee Agent policy update from the Evaluation repository to the test group.

**Before you begin**
You must have created a test group of systems and an on-demand scan of the test group.

**Task**

1 Select Menu | Policy | Client Task Catalog.

2 On the Client Task Catalog page, select VirusScan Enterprise and On Demand Scan in Client Task Types.

3 Find the on-demand scan you created, click Assign in the Actions column, select the test group of systems that you created to assign the task, then click OK.

4 In the Client task Assignment Builder, configure these settings, then click Next:
   a For Product list, select VirusScan Enterprise.
   b For Task Type list, select On Demand Scan.
   c For Task Name list, select the ODS task you created.

5 In the Schedule tab, configure these settings:
   a For Schedule status, select Enabled.
   b For Schedule type, select Daily from the list.
   c For Effective period, select today's date as the Start date, then select No end date.
d For Start time, configure these settings:
   • Select 9:05 AM from the time lists.
   • Click Run at that time, and then repeat until, then select 2:00 PM from the time lists.
   • For During repeat, start task every, select 5 minute(s) from the lists.

e For Task runs according to, click Local time on managed systems.

f For Options, deselect everything.

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

Your on-demand scan task is now scheduled to run every 5 minutes, from 9:05 a.m. until 2:00 p.m., after each agent policy update, from the Evaluation repository to the test group.

**Best practice: Configure an Automatic Response for malware detection**

If malware is found by the on-demand scan in the test group, you want to block the files from being copied automatically to the Current repository. Set up an automatic notification to the administrator.

**Before you begin**
You must have already created an on-demand scan task to scan for any problems that might occur in your test group.

**Task**

1 To display the Response Builder, select Menu | Automation | Automatic Responses, click New Response, then configure these settings in the Descriptions tab, then click Next.
   a Type a name, for example Malware found in test group, and a detailed description
   b For Language, select a language from the list.
   c For Event Group, select ePO Notification Events from the list.
   d From Event type, select Threat from the list.
   e For Status, select Enabled.

2 Configure these settings in the Filter tab, then click Next.
   a For Available Properties list, select Threat Category.
      Optionally, you can add additional categories, such as an access protection rule being triggered.
   b In the Required Criteria column and the Defined at row, click ... to select the test group of systems that you created in the Select System Tree Group dialog box, then click OK.
   c In the Threat Category row, select Belongs to from the Comparison list and Malware from the Value list.
      Click + to add another category.
   d Select Belongs to from the Comparison list and Access Protection from the Value list.

3 Configure these settings in the Aggregation tab, then click Next.
   a For Aggregation, click Trigger this response for every event.
   b Do not configure any Grouping or Throttling settings.
4 Configure these settings in the **Actions** tab:
   a Select **Send Email** from the **Actions** list.
   b For Recipients, type the email address of the administrator to be notified.
   c For Importance, select **High** from the list.
   d For Subject, type an email header, for example **Malware found in the Test Group!**
   e For Body, type a message, for example **Research this NOW and stop the server task that pulls content into the Current branch!**
   f Following the message body, insert these variables to add to the message, and click **Insert**:
      • **OS Platform**
      • **Threat Action Taken**
      • **Threat Severity**
      • **Threat Type**

5 Click **Next**, confirm that the configuration is correct in the Summary tab, then click **Save**.

Now you have an Automatic Response configured that sends an email to an administrator any time malware is detected in the test group running the Evaluation DAT file.
Manual package and update management

Best practice: Automating BAT file testing
10 Deploying products

Contents
- Product deployment steps
- Choosing a product deployment method
- Benefits of product deployment projects
- Viewing Product Deployment audit logs
- View product deployment
- Deploy products using a deployment project
- Monitor and edit deployment projects
- Global updating
- Deploy update packages automatically with global updating
- New Deployment page

Product deployment steps
You can deploy product software to your managed systems using automatic or manual configuration methods. The method you choose depends on the level of detail you want to configure to complete the process.

The following diagram shows the processes you can use to add and update software on the Master Repository, then deploy that software to your managed systems.
Use the Software Manager to automatically review and update McAfee software and software components.

From the Master Repository, you can manually check in deployment packages then use Product Deployment or client tasks to deploy them to your managed systems.

The Product Deployment feature offers a simplified workflow and increased functionality to deploy products to your McAfee ePO managed systems.

Create client tasks to manually assign and schedule product deployments to groups or individual managed system.

Product deployment is the output process that keeps your security software as current as possible to protect your managed systems.

Choosing a product deployment method

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

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

To maintain and use client tasks and objects created outside of a Product Deployment project, use the client task object library and assignment interfaces. You can maintain existing tasks and object while using the Product Deployment project interface to create new deployments.
Benefits of product deployment projects

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

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

- **Run a deployment continuously** — You can configure your deployment project so that when new systems matching your criteria are added, products are deployed automatically.

- **Stop a running deployment** — If you must stop a deployment once it's started, you can. Then you can resume that deployment when you’re ready.

- **Uninstall a previously deployed product** — If a deployment project has been completed, and you want to uninstall the associated product from the systems assigned to your project, select Uninstall from the Action list.

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

Table 10-1  Product deployment methods compared

<table>
<thead>
<tr>
<th>Client task objects</th>
<th>Function comparison</th>
<th>Product deployment project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and description</td>
<td>Same</td>
<td>Name and description</td>
</tr>
<tr>
<td>Collection of product software to deploy</td>
<td>Same</td>
<td>Collection of product software to deploy</td>
</tr>
<tr>
<td>Use tags to select target systems</td>
<td>Enhanced in Product Deployment project</td>
<td>Select when the deployment occurs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Continuous</strong> — Continuous deployments use System Tree groups or tags which allow you to move systems to those groups or assign systems tags and cause the deployment to apply to those systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Fixed</strong> — Fixed deployments use a fixed, or defined, set of systems. System selection is done using your System Tree or Managed Systems Query output tables.</td>
</tr>
<tr>
<td>Deployment schedule</td>
<td>Similar</td>
<td>Simplified deployment schedule allows you to either run the deployment immediately or run it once at a scheduled time.</td>
</tr>
<tr>
<td>Not specified</td>
<td>New in Product Deployment project</td>
<td>Monitor the current deployment status, for example deployments scheduled but not started, in progress, stopped, paused, or completed.</td>
</tr>
<tr>
<td>Not specified</td>
<td>New in Product Deployment project</td>
<td>(Fixed deployments only) View a historical snapshot of data about the number of systems receiving the deployment.</td>
</tr>
<tr>
<td>Not specified</td>
<td>New in Product Deployment project</td>
<td>View the status of individual system deployments, for example systems installed, pending, and failed.</td>
</tr>
<tr>
<td>Not specified</td>
<td>New in Product Deployment project</td>
<td>Modify an existing deployment assignment using:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create New for modifying an existing deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Duplicate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop and Pause Deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Continue and Resume Deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Uninstall</td>
</tr>
</tbody>
</table>
Viewing Product Deployment audit logs

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

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

View product deployment

During the initial product deployment, McAfee ePO automatically creates a product deployment process. You can use this product deployment process as a base to create other product deployments.

Before you begin
You must run the Getting Started dashboard process to create a product deployment or create a product deployment manually.

Task

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

The initially created product deployment uses the name of the System Tree group you configured in the Getting Started dashboard process and appears in the Deployment summary list with the name Initial Deployment My Group.

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

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

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

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

Deploy products using a deployment project

A deployment project allows you to easily select products to deploy to your target systems, and schedule the deployment.

Expired products appear in the Packages list. You can uninstall them from target systems in Actions.
Task

1 Select Menu | Software | Product Deployment.

2 Select New Deployment to start a new project.

3 Type a name and description for this deployment. This name appears on the Product Deployment page after you save the deployment.

4 Choose the type of deployment:
   • Continuous — Uses your System Tree groups or tags to configure the systems receiving the deployment. This feature allows these systems to change over time as they are added or removed from the groups or tags.
   • Fixed — Uses a fixed (defined) set of systems to receive the deployment. System selection is done using your System Tree or the output of Managed Systems Queries.

5 To automatically update your products, make sure that the Auto Update checkbox is selected.
   If the checkbox is deselected, products are still updated with the latest patches, hotfixes, and content packages, but major and minor releases are ignored.

   During a new deployment, the McAfee Agent checks for new updates, hotfixes, and content packages of all installed products on the client. See the McAfee Agent documentation for details.

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

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

7 From the Actions list, select Install or Uninstall.

8 In the Command line text field, specify any command-line installation options. For information about command-line options, see the product documentation for the software you’re deploying.

9 Under Select the systems, click Select Systems.
   The System Selection dialog box is a filter that allows you to select groups in your System Tree using these tabs:
   • System Tree — Select System Tree groups or subgroups and their associated systems.
   • Tags — Select tag groups or tag subgroups and their associated systems.
   • Selected Systems — Displays the total selections you made in each tab, creating the target systems for your deployment.

   For example, if your System Tree contains Group A, which includes both servers and workstations, you can target the entire group. You can also target only the servers or only the workstations (if they are tagged correctly), or a subset of either system type in Group A.

   For a fixed deployment, the maximum number of systems that can receive the deployment is 500.

   If needed, configure the following:
   • Run at every policy enforcement (Windows only)
   • Allow end users to postpone this deployment (Windows only)
• Maximum number of postponements allowed
• Option to postpone expires after
• Display this text

10 Under Select a start time select a schedule for your deployment:
• Run Immediately — Starts the deployment task during the next ASCI.
• Once or Daily — Opens the scheduler so you can configure the start date, time, and randomization.

11 Click Save at the top of the page. The Product Deployment page opens with your new project added to the list of deployments.

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

---

**Monitor and edit deployment projects**

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

**Task**

1 Select Menu | Software | Product Deployment.

2 Filter the list of deployment projects using the following:
   • Type — Filters the deployments that appear by All, Continuous, or Fixed.
   • Status — Filters the deployments that appear by All, Finished, In Progress, Pending, Running, or Stopped.

3 From the list on the left side of the page, click a deployment to display its details on the right side of the page.
   
   | If a package in this deployment expires, the deployment is invalid. If you mouse-over the deployment, you see this message: “Package(s) in this deployment have been moved, deleted, or expired.” |

4 Use the progress section of the details display to view:
   • Calendar displaying the start date for pending continuous and fixed deployments.
   • Histogram displaying systems and the time to completion for fixed deployments.
   • Status bar displaying system deployment and uninstallation progress.

   | Under the status bar, Task Status lists Successful, Failed, and Pending for the number of target systems in parentheses. |

5 Click Action and one of these actions to modify a deployment:
   • Edit
   • Delete
   • Duplicate
   • Resume
   • Stop
   • Uninstall
   • Mark Finished

6 In the details section, click View Task Details to view and modify the settings for the deployment.
7 In the Systems table, select an option in the Filter list to change which systems appear.

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

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

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

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

---

**Global updating**

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

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

You can also specify which packages and updates initiate a global update. When you specify that certain content initiates a global update, make sure to create a replication task to distribute content that was not selected.

**Best practice:** When using global updating, schedule a regular pull task (to update the Master Repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update.

---

**Global updating process**

1 Contents are checked in to the Master Repository.

2 The server performs an incremental replication to all distributed repositories.

3 The server issues a SuperAgent wake-up call to all SuperAgent in the environment.

4 The SuperAgent broadcasts a global update message to all agents within the SuperAgent subnet.

5 Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed for updating.

6 The agent searches the distributed repositories for a site that has this minimum catalog version.

7 Once a suitable repository is found, the agent runs the update task.

If the agent does not receive the broadcast, the minimum catalog version is supplied at the next agent-server communication.

If the agent receives notification from a SuperAgent, the agent is supplied with the list of updated packages. If the agent finds the new catalog version at the next agent-server communication, it is not supplied with the list of packages to update, and updates all packages available.
Requirements

These requirements must be met to implement global updating:

- A SuperAgent must use the same agent-server secure communication (ASSC) key as the agents that receive its wake-up call.
- A SuperAgent is installed on each broadcast segment. Managed systems cannot receive a SuperAgent wake-up call if there is no SuperAgent on the same broadcast segment. Global updating uses the SuperAgent wake-up call to alert agents that new updates are available.
- Distributed repositories are set up and configured throughout your environment. We recommend SuperAgent repositories, but they are not required. Global updating functions with all types of distributed repositories.
- If using SuperAgent repositories, managed systems must be able to access the repository where its updates come from. Although a SuperAgent is required on each broadcast segment for systems to receive the wake-up call, SuperAgent repositories are not required on each broadcast segment.

Deploy update packages automatically with global updating

You can enable global updating on the server to automatically deploy user-specified update packages to managed systems.

Task

1. Click Menu | Configuration | Server Settings, select Global Updating, then click Edit at the bottom of the page.
2. On the Edit Global Updating page next to Status, select Enabled.
3. Edit the Randomization interval, if wanted.
   
   Each client update occurs at a randomly selected time within the randomization interval, which helps distribute network load. The default is 20 minutes.
   
   For example, if you update 1000 clients using the default randomization interval of 20 minutes, roughly 50 clients update each minute during the interval. This randomization lowers the load on your network and on your server. Without the randomization, all 1000 clients would try to update simultaneously.
4. Next to Package types, select which packages initiate an update.

   Global updating initiates an update only if new packages for the components specified here are checked in to the Master Repository or moved to another branch. Select these components carefully.

   - Signatures and engines — Select Host Intrusion Prevention Content, if needed.

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.

   Make 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.
**New Deployment page**

The New Deployment page is where you define deployment projects to install or uninstall products on managed systems. Product packages must be checked in before deploying them.

This task is divided into the steps required to create a deployment project. The options available in each step are defined in the *Option definitions* tables.

### Table 10-2  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the new deployment configuration.</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the New Deployment page.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the deployment.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description of the new deployment.</td>
</tr>
</tbody>
</table>

#### Choose the type of deployment

<table>
<thead>
<tr>
<th>Type</th>
<th>Specifies the way systems are assigned for deployment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous</td>
<td>Assign the deployment using System Tree groups or tags. This option allows the number of systems inheriting the product to change over time.</td>
</tr>
<tr>
<td>Fixed</td>
<td>Assign specific systems to receive the deployment using your System Tree or Managed Systems Queries table output. Limited to 500 systems.</td>
</tr>
</tbody>
</table>

**Auto Update**: If Auto Update:

- Selected — All products are updated including major version changes with updates, hotfixes and content packages.
- Deselected — Only the individual versions are deployed. No updates, hotfixes, or content packages are updated. Major version changes are ignored.

> During a new deployment, the agent checks for new updates, hotfixes and content packages of all installed products on the client. See McAfee Agent documentation for details.

### Table 10-3  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select your software</td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Specifies which package to deploy or uninstall. Click [+] and [-] to add or remove packages.</td>
</tr>
<tr>
<td>Branch</td>
<td>Specifies which branch the package is stored in.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Current</strong> — Used when you want the package available to managed systems in your production environment.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Evaluation</strong> — Used to test the package on a limited number of systems before making it available to the larger environment.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Previous</strong> — Used when you want to keep previous versions of packages for rollback purposes.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies whether the action is Install or Uninstall.</td>
</tr>
</tbody>
</table>
Table 10-3 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Language</strong></td>
<td>Specifies which interface language to use for the deployment.</td>
</tr>
<tr>
<td></td>
<td><strong>Neutral</strong> allows the multiple language package to query the operating system and install the correct language.</td>
</tr>
<tr>
<td><strong>Command line</strong></td>
<td>Specifies command-line installation options.</td>
</tr>
<tr>
<td></td>
<td><strong>See the product documentation for information on command-line options for the product you are installing.</strong></td>
</tr>
</tbody>
</table>

Table 10-4 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select the systems</strong></td>
<td>Click <strong>Select Systems</strong>, then select the systems to receive the new deployment using these tabs.</td>
</tr>
<tr>
<td></td>
<td><strong>The type of deployment you select, fixed or continuous, determines which tabs appear.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Systems Tree</strong> tab — (Fixed) Selects and displays systems. Used with continuous deployment, selects System Tree groups.</td>
</tr>
<tr>
<td></td>
<td><strong>Selected Systems</strong> tab — (Fixed) Selects individual or System Tree groups of systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Queries</strong> tab — (Fixed) Select the output from preconfigured query output systems tables.</td>
</tr>
<tr>
<td></td>
<td><strong>Tags</strong> tab — (Continuous) Selects systems configured with specific tags.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Run at Every Policy Enforcement</strong> as needed.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Allow end users to postpone this deployment</strong> as needed.</td>
</tr>
<tr>
<td></td>
<td>Enter number for <strong>Maximum number of postponements allowed.</strong></td>
</tr>
<tr>
<td></td>
<td>Enter number of seconds for <strong>Option to postpone expires after.</strong></td>
</tr>
<tr>
<td></td>
<td>Select <strong>Display this text</strong>, if you want text to appear when the deployment begins</td>
</tr>
</tbody>
</table>

Table 10-5 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select a start time</strong></td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td><strong>Run Immediately</strong> — Starts the deployment immediately.</td>
</tr>
<tr>
<td></td>
<td><strong>Once</strong> — Starts the deployment using specified settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Start date</strong> — Specifies the date to start this task.</td>
</tr>
<tr>
<td></td>
<td><strong>Start Time</strong> — Specifies the time to start this task.</td>
</tr>
<tr>
<td></td>
<td><strong>Coordinated Universal Time (UTC)</strong> — Specifies whether the task schedule runs according to the local time on the managed system or UTC.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable randomization</strong> — Specifies that this task runs randomly within the number of hours and minutes you specify. Otherwise, this task starts at the scheduled time regardless if other client tasks are scheduled to run at the same time.</td>
</tr>
</tbody>
</table>
The ePO Support Center extension provides access to important and useful information about your servers and installed products. The Support Center allows you to:

- View live data about your ePO Server Health
- Receive Support Notifications (SNS)
- Search across content portals and knowledge bases
- Access product-specific best practices and how-to information

Support Center requires ePO 5.3.3 or later.

**Contents**

- ePO Server Health
- Support Notifications
- Search Support
- Product Information

### ePO Server Health

ePO Server Health provides useful details about your ePO server and database. The health timeline shows regularly scheduled status updates.

#### ePO Server Details

ePO Server Details provides an overview of your ePO server, ePO version, and database.

- Server Details
- ePO Details
- SQL Server Details
- ePO Database Details
- ePO Event Database Details

#### Server Health Timeline

Server Health Timeline provides a visual display of regularly scheduled health checks over time. By default, these checks run hourly and you can modify the schedule using the Server Task page. You can also run a manual health check.

The color coded icons represent each of the checks. The icons describe the type of check and are color coded to indicate the status. Typically, green means the check was successful, yellow that there was a warning, and red that the check failed. You can hover over an icon to view quick details. Click the icon to view more details.
You can view the details of the default and manual health checks in the **Audit Log** page.

**Health Check Details**

Health Check Details provides a summary of the selected row in the timeline. It also includes detailed information about each of the specific checks.

**Table 11-1  Health check details**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO Database Connection Check</td>
<td>Verifies connectivity between the ePO server and the ePO database server.</td>
<td>Can ePO connect to the database?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — No</td>
</tr>
<tr>
<td>ePO Server machine CPU Check</td>
<td>Verifies the CPU load of the ePO server.</td>
<td>ePO server CPU load is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — More than 90%</td>
</tr>
<tr>
<td>ePO Server Machine Memory Check</td>
<td>Verifies the memory load of the ePO server.</td>
<td>Free memory is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — More than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — Less than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — Less than 10%</td>
</tr>
<tr>
<td>ePO Database CPU Check</td>
<td>Verifies the CPU load of the ePO database server.</td>
<td>ePO database server CPU load is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — More than 90%</td>
</tr>
<tr>
<td>ePO Database Index Fragmentation Check</td>
<td>Verifies the index fragmentation state of the ePO database.</td>
<td>Index fragmentation is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 30%</td>
</tr>
<tr>
<td>ePO Database Memory Check</td>
<td>Verifies the memory load of the ePO database server.</td>
<td>Free memory is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — More than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — Less than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — Less than 10%</td>
</tr>
<tr>
<td>ePO Database Size Check</td>
<td>Verifies the free space available on the ePO database server.</td>
<td>Free space is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — More than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — Less than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — Less than 10%</td>
</tr>
<tr>
<td>ePO Application Server JVM Thread Check</td>
<td>Verifies the thread status of the ePO Application Server JVM.</td>
<td>Threads timed waiting count and blocked count are...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 100 and 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 100 and 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — More than 100 and more than 0</td>
</tr>
</tbody>
</table>
### Table 11-1  Health check details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO Application Server JVM CPU Check</td>
<td>Verifies the CPU load of the ePO Application Server JVM.</td>
<td>ePO Application Server JVM CPU load is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — More than 90%</td>
</tr>
<tr>
<td>ePO Application Server JVM Memory Check</td>
<td>Verifies the memory load of the ePO Application Server JVM.</td>
<td>Free memory is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — More than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — Less than 30%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — Less than 10%</td>
</tr>
<tr>
<td>Data Channel Waiting Queue Check</td>
<td>Verifies the waiting queue load for data channel messages.</td>
<td>Waiting count is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 5</td>
</tr>
<tr>
<td>Event Parser Failing Check</td>
<td>Verifies the ePO Event Parser failing count.</td>
<td>Failing count is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Equal to 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — More than 0</td>
</tr>
<tr>
<td>Event Parser Waiting Check</td>
<td>Verifies the waiting queue load of the ePO Event Parser.</td>
<td>Waiting count is...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — Less than 50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 50</td>
</tr>
<tr>
<td>Failing Server Tasks Check</td>
<td>Verifies whether server tasks have been failing in the last 7 days.</td>
<td>Tasks are failing?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — Yes</td>
</tr>
<tr>
<td>Waiting Server Tasks Check</td>
<td>Verifies whether server tasks have been in a waiting state from more than an hour at the time of the check.</td>
<td>Tasks are in a waiting state for more than an hour?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Successful — No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — Yes</td>
</tr>
</tbody>
</table>

### Manual server health checks

Apart from the scheduled default server health checks that run every hour, you can trigger the health checks manually at any point in time.

### Manual Health Check Details

These are the manual health checks that are not run by default and the detailed information about each of the specific checks.
Table 11-2  Manual Health check details

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO Database Collation</td>
<td>Verifies the database collation match between the ePO database server</td>
<td>Does the database collation match between the ePO database server and the ePO database?</td>
</tr>
<tr>
<td>Check</td>
<td>and the ePO database.</td>
<td>• Successful — Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — No</td>
</tr>
</tbody>
</table>

You can't run the scheduled Default Health Check group manually; but you can run the health check for a group or an individual check manually. However, you can run the default server health checks at any time on the Server Tasks page.

Support Notifications

Support Notifications provides a view of the most recent information posted by the Support Notifications Service (SNS). You can use this feed to view the most up-to-date information on product upgrades, product releases, end-of-life notices, and critical incidents.

The Support Notifications page is a continuously updated news feed that displays notifications received in the last 30 days. The page displays the newest notifications first and updates every hour. When a notification is added to the page for the first time, it is tagged as New. Clicking a link opens the notice in a new browser tab.

In the upper-right corner, you can see when the Support Notification page was updated. By default, the page refreshes hourly. Click the refresh icon to manually refresh the Support Notification page.

Create Support Notification tags

Tags allow you to filter the support notifications based on various criteria such as criticality, software updates, release notifications and so on. You can provide a name of your choice and color code the tags for easy identification. Tagging the notifications helps you to categorize and prioritize the notifications.

**Task**

1. Select Menu | Support Center | Support Notifications.
2. Click Tags and then click Create new tag.
3. Enter a name for the new tag, choose a tag color from the palette and then click Save.

You have created a new tag and now you can apply this tag to the support notifications.

Apply Support Notification tags

You can create and apply tags based on various criteria to categorize the support notifications. You can apply multiple tags to a single notification.

**Task**

1. Select Menu | Support Center | Support Notifications.
2. Select the notifications that you want to tag, then click Tags.
3. You can select from the existing list of tags or create a new tag and then click Apply tags.

You can see the tag under the notification.

The selected notifications are tagged and can be easily filtered based on the tag.
Remove a support notification tag
You can remove a tag that is applied to a support notification if the tag is not applicable to that notification anymore.

Task
1 Select Menu | Support Center | Support Notifications.
   You can view the tags applied to a notification below the notification itself.
2 Click the cross mark on the tag to remove the tag from the notification.
   The tag is removed from the notification.

Delete a support notification tag
Tags are created to categorize and filter notifications. After the notifications are viewed and addressed, you may choose to delete the tags that are of no use anymore.

Task
1 Select Menu | Support Center | Support Notifications.
2 Click Tags and then select the tag that you want to delete and click Delete Tags. You can select multiple tags and delete at once.
   The selected tags are deleted permanently.

Edit a support notification tag
You can edit an existing tag using the Edit tag option. You can change the name of the tag or change the color assigned to the tag or do both.

Task
1 Select Menu | Support Center | Support Notifications.
2 Click Tags and select the tag that you want to edit. Then, click Edit Tag.
3 Make the required changes to the name or the color or both. Then, click Save.
   The changes are applied to the tag.

Filter tagged support notifications
You can filter notifications based on the tags applied. The page displays only the tagged notifications.

Task
1 Select Menu | Support Center | Support Notifications.
2 Click Tags and then select the tag that you want to filter and click Filter Tagged.
   The tagged support notifications are filtered and displayed.

Search Support
The Search McAfee Support feature allows you to search for content on the support services site from within the ePO Console.

Enter a search term in the field to view a list of related articles.
Product Information

Product Information includes a selection of useful topics about your products. The page organizes content by product and topic. Each topic includes high-level information and links to relevant best practices on the documentation portal.

The Product Information page includes content for McAfee ePolicy Orchestrator and McAfee Endpoint Security.
Policies ensure that product features are configured correctly on managed systems.

Policies are organized by product, then by categories in each product. For example, the McAfee Agent product includes categories for General, Repository, and Troubleshooting.

To see policies in a specific policy category, select **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 for products they have permissions to.

Each category includes two default policies, **McAfee Default** and My Default. You can't delete, edit, export, or rename these policies, but you can copy them and edit the copy.

For example, to increase the McAfee ePO response time, some enterprise users change the agent-server communication interval (ASCI) for workstations in the McAfee Agent policy, from the default of every 60 minutes, to every 240–360 minutes.

To change the workstation ASCI setting, duplicate the McAfee Agent, McAfee Default policy, in the General category, and change the ASCI setting. Then you must assign the new policy to a System Tree group or tag that includes all those workstations.
For example, you can increase the McAfee ePO response time from the default value of every 60 minutes. To add time, change the agent-server communication interval (ASCI) for workstations in the McAfee Agent policy to every 240–360 minutes.

To change the workstation ASCI setting, duplicate the McAfee Agent, McAfee Default policy, in the General category, and change the ASCI setting. Then you must assign the new policy to a System Tree group or tag that includes all those workstations.

**When policies are applied and enforced**

Policies are applied to systems according to the agent-server communication and policy enforcement intervals. The policy configuration defines when policy settings are enforced.

**Applying policies**

After you configure policy settings, the new settings are applied to specified managed systems at the next agent-server communication. By default, the agent-server communication occurs every 60 minutes. You can adjust this interval on the General tab of the McAfee Agent policy pages. Or, depending on how you implement agent-server communication, you could change the ASCI using a McAfee Agent Wake-up client task.

For example, if you want to change the settings of the default McAfee VirusScan Enterprise on-demand scan policy, follow these steps:

1. Duplicate the default McAfee VirusScan Enterprise on-demand scan policy and save it with a new name.
2. Change the settings to meet your requirements.
3. Reassign the new policy to the same, or different, managed systems in a group on the System Tree.

The next time an agent-server communication occurs, the new policy is applied to all systems.

**Policy enforcement**

The timing of policy enforcement depends on the configuration of the policies. Enforcement can happen:

- Instantly, for example, the On-Access Scan policy occurs when you start any application.

- At agent-server communication or policy enforcement intervals, for example, the Product Deployment policy runs to confirm that the installed software versions on the managed systems match the versions on the Master Repository. If a new version is available, it is downloaded to all systems.

- At configured Client Task intervals, for example, the on-demand scan policy, by default runs at 12 a.m. every night to scan all your managed systems for threats.

After policy settings are applied on the managed system, the McAfee Agent continues to enforce policy settings according to the policy enforcement interval. By default, the policy enforcement occurs every 60 minutes. You can adjust this interval on the General tab as well.

This figure describes the individual steps needed to run the scheduled McAfee VirusScan Enterprise on-demand scan.
The Policy Based on-demand scan Client Task runs at 12 a.m.

The client task starts the full on-demand scan on the managed systems.

Using the configured settings in the policy, the scans run and if any threats are found they are cleaned, quarantined, or deleted as required.

How policies are assigned to systems

Policies are assigned to systems by one of two methods: inheritance or assignment.

You can assign any policy in the Policy Catalog to any group or system in the System Tree. Assignment allows you to define policy settings once for a specific need, then apply the policy to multiple locations.

Inheritance determines whether the policy settings and client tasks for a group or system in the System Tree are taken from its parent group. By default, inheritance is enabled throughout the System Tree.

When you copy and paste policy assignments, only true assignments are pasted. If the source location inherited a policy that you selected to copy, it is the inheritance characteristic that was pasted to the target. The target then inherits the policy (for that particular policy category) from its parent.

Assignment locking

You can lock the assignment of a policy on any group or system. Assignment locking prevents other users from inadvertently replacing a 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 make sure that no other users move it.

Assignment locking does not prevent the policy owner from changing policy settings. So, if you intend to lock a policy assignment, make sure that you are the owner of the policy.
Policy ownership

Each policy is assigned an owner — the user who created it. You must have the correct permissions to edit a policy you don't own.

If you want to use a policy owned by a different user, we recommend that you duplicate the policy, then use the duplicate. Duplicating policies prevents unexpected policy changes from affecting your network. If you assign a policy that you don't own, and the owner modifies the policy, all systems that were assigned the policy receive the modifications.

You can specify multiple users as owners of a single policy.

Policy assignment rules

Policy assignment rules reduce the overhead of managing numerous policies for individual users or systems that meet specific criteria, while maintaining more generic policies across your System Tree.

This level of granularity in policy assignments limits the instances of broken inheritance in the System Tree to accommodate the policy settings that particular users or systems require. Policy assignments can be based on either user specific or system-specific criteria:

- **User-based policies** — Policies that include at least one user-specific criteria. For example, you can create a policy assignment rule that is enforced for all users in your engineering group. You can then create another policy assignment rule for members of your IT department. This rule allows them to log on to any computer in the engineering network with the access rights to troubleshoot problems on a specific system in that network. User-based policies can also include system-based criteria.

- **System-based policies** — Policies that include only system-based criteria. For example, you can create a policy assignment rule that is enforced for all servers on your network based on the tags you have applied, or all systems in a specific location in your System Tree. System-based policies cannot include user-based criteria.

Policy assignment rule priority

Policy assignment rules can be prioritized to simplify maintenance of policy assignment management. When you set priority to a rule, it is enforced before other assignments with a lower priority.

In some cases, the outcome can be that some rule settings are overridden. For example, consider a system that is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included systems unrestricted access to Internet content. Rule B has priority level 2, and heavily restricts the same system's access to Internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the system has unrestricted access to Internet content.

How multi-slot policies work with policy assignment rule priority

Priority of rules is not considered for multi-slot policies. When a single rule containing multi-slot policies of the same product category is applied, all settings of the multi-slot policies are combined. Similarly, if multiple rules containing multi-slot policy settings are applied, all settings from each multi-slot policy are combined. As a result, the applied policy is a combination of the settings of each individual rule.

When multi-slot policies are aggregated, they are aggregated only with multi-slot policies of the same type. However, multi-slot policies assigned using policy assignment rules are not aggregated with multi-slot policies assigned in the System Tree. Multi-slot policies assigned using policy assignment rules override policies assigned in the System Tree. Furthermore, user-based policies take priority over system-based policies.

Scenario: Using multi-slot policies to control Internet access

In your System Tree, there is a group named "Engineering" which consists of systems tagged with either "IsServer" or "IsLaptop." In the System Tree, policy A is assigned to all systems in this group. Assigning policy B to any location in the System Tree above the Engineering group using a policy assignment rule overrides the
settings of policy A, and allows systems tagged with "IsLaptop" to access the Internet. Assigning policy C to any group in the System Tree above the Engineering group allows users in the Admin user group to access the Internet from all systems, including those in the Engineering group tagged with "IsServer."

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Assignment type</th>
<th>Policy name</th>
<th>Policy settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic policy</td>
<td>Policy assigned in the System Tree</td>
<td>A</td>
<td>Prevents Internet access from all systems to which the policy is assigned.</td>
</tr>
<tr>
<td>System-based</td>
<td>Policy assignment rule</td>
<td>B</td>
<td>Allows Internet access from systems with the tag &quot;IsLaptop.&quot;</td>
</tr>
<tr>
<td>System-based</td>
<td>Policy assignment rule</td>
<td>C</td>
<td>Allows unrestricted Internet access to all users in the Admin user group from all systems.</td>
</tr>
<tr>
<td>User-based</td>
<td>Policy assignment rule</td>
<td>C</td>
<td>Allows unrestricted Internet access to all users in the Admin user group from all systems.</td>
</tr>
</tbody>
</table>

**Excluding Active Directory objects from aggregated policies.**

Because rules that consist of multi-slot policies are applied to assigned systems without regard to priority, you might need to prevent policy setting aggregation in some instances. You can prevent aggregation of user-based multi-slot policy settings across multiple policy assignment rules by excluding a user (or other Active Directory objects such as a group or organizational unit) when creating the rule. For more information on the multi-slot policies that can be used in policy assignment rules, see the product documentation for the managed product you are using.

**User-based policy assignment**

User-based policy assignment rules give you the ability to create user-specific policy assignments. These assignments are enforced at the target system when a user logs on.

When a user logs on to a managed system for the first time, there can be a slight delay while the McAfee Agent contacts its assigned server for the policy assignments specific to this user. During this time, the user has access only to that functionality allowed by the default computer policy, which typically is your most secure policy.

On a managed system, the agent keeps a record of the users who log on to the network. The policy assignments you create for each user are pushed down to the system they log on to, and are cached during each agent-server communication. The McAfee ePO server applies the policies that you assigned to each user.

**System-based policy assignment**

System-based assignments allow you to assign policies based on System Tree location or tags. System-based policies are assigned based on selection criteria you define using the Policy Assignment Builder.

All policy assignment rules require that System Tree location is specified. Tag-based policy assignments are useful when you want all systems of a particular type to have the same security policy, regardless of their System Tree location.

**Scenario: Creating new SuperAgents using tags**

You have decided to create a set of SuperAgents in your environment, but you don't have time to manually identify the systems in your System Tree to host these SuperAgents. Instead, you can use the Tag Builder to tag all systems that meet a specific set of criteria with a new tag: "isSuperAgent." Once you have built the tag, you can create a Policy Assignment Rule that applies your SuperAgent policy settings to every system tagged with "isSuperAgent."
Once the tag is created, you can use the Run Tag Criteria action from the Tag Catalog page to assign the new policy. As each system with the new tag calls in at its regular interval, it is assigned a new policy based on your isSuperAgent Policy Assignment Rule.

Create and manage policies

McAfee ePO provides a number of tools to manage policies, including the Policy Catalog, Policy History, and Policy Comparison.

Tasks

- **Create a policy from the Policy Catalog page** on page 142
  Custom policies created using the Policy Catalog are not assigned to any groups or systems. You can create policies before or after a product is deployed.

- **Enforcing product policies** on page 143
  Policy enforcement is enabled by default, and is inherited in the System Tree, but you can manually enable or disable enforcement on specified systems.

- **Enforce policies for a product in a System Tree group** on page 143
  Enable or disable policy enforcement in a group.

- **Enforce policies for a product on a system** on page 143
  Enable or disable policy enforcement on a managed system.

- **Manage policy history** on page 144
  You can view and compare policy history entries, or revert to a previous version of a policy.

- **Edit policy history permission sets** on page 145
  Configure the permission sets for your products so that users can revert policies to previous versions using the Policy History page.

- **Compare policies** on page 145
  Policy Comparison can help you identify differences between similar policies.

- **Change the owners of a policy** on page 146
  By default, ownership is assigned to the user who creates the policy. If you have the required permissions, you can change the ownership of a policy.

Create a policy from the Policy Catalog page

Custom policies created using the Policy Catalog are not assigned to any groups or systems. You can create policies before or after a product is deployed.

**Task**

1. Open the New Policy dialog box.
   - Select **Menu** | **Policy** | **Policy Catalog**.
   - Select the product and category from the drop-down lists.
     - All created policies for the selected category appear in the Details pane.
   - Click **New Policy**.
2. Select the policy you want to duplicate from the Create a policy based on this existing policy drop-down list.
3. Type a name for the new policy and click **OK**.
   - The policy appears in the Policy Catalog.
4 Click the name of the new policy. The Policy Settings Builder opens.

5 Edit the policy settings as needed.

6 Click Save.

**Enforcing product policies**

Policy enforcement is enabled by default, and is inherited in the System Tree, but you can manually enable or disable enforcement on specified systems.

You can manage policy enforcement from these locations:

- Assigned Policies tab of the System Tree — Choose whether to enforce policies for products or components on the selected group.
- Policy Catalog page — View policy assignments and enforcement. You can also lock policy enforcement to prevent changes below the locked node.

> If policy enforcement is turned off, systems in the specified group don't receive updated site lists during an agent-server communication. As a result, managed systems in the group might not function as expected.

For example, you might configure managed systems to communicate with Agent Handler A. If policy enforcement is turned off, the managed systems do not receive the new site list with this information and the systems report to a different Agent Handler listed in an expired site list.

**Enforce policies for a product in a System Tree group**

Enable or disable policy enforcement in a group.

**Task**

1 Select Menu | Systems | System Tree, click Assigned Policies tab, then select a group in the System Tree.

2 Select the product you want, then click the link next to Enforcement Status.

3 To change the enforcement status, select Break inheritance and assign the policy and settings below.

4 Next to Enforcement status, select Enforcing or Not enforcing accordingly.

5 Choose whether to lock policy inheritance.
   - Locking inheritance for policy enforcement prevents breaking enforcement for groups and systems that inherit this policy.

6 Click Save.

**Enforce policies for a product on a system**

Enable or disable policy enforcement on a managed system.

**Task**

1 Select Menu | Systems | System Tree, click Systems tab, then select the group under System Tree where the system belongs.
   - The list of systems belonging to this group appears in the details pane.
2 Select a system, then click **Actions | Modify Policies on a Single System**. 
   The **Policy Assignment** page appears.

3 Select a **Product**, then click **Enforcing** next to **Enforcement status**. 
   The Enforcement page appears.

4 If you want to change the enforcement status you must first select **Break inheritance and assign the policy and settings below**.

5 Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.

6 Click **Save**.

### Managing policy history

When you change a policy from the Policy Catalog, a Policy History entry is created where you can describe the change for future reference. Policy History entries appear in three places: Policy History, Server Task Log Details, and Audit Log Details.

Only policies you create in the Policy Catalog have Policy History entries. Make sure that you leave a comment when you revise a policy. Consistent commenting creates a strong history of your changes.

To record policy revisions, type a comment in the text field next to **Duplicate**, in the footer of the **Policy Catalog** page.

If you have policy users configured to create and edit policies, the Status column options vary depending on your permissions. For example:
- McAfee ePO administrators have full control of all policy history functions.
- Policy administrators can Approve or Decline changes submitted by policy users.
- Policy users can monitor the status of their policies. Status includes Pending Review, **Approved**, or Declined.

### Manage policy history

You can view and compare policy history entries, or revert to a previous version of a policy.

**Before you begin**

You must have appropriate permissions to revert to a previous policy history entry. You need only view permission to see policy history entries.

**Task**

1 To view the Policy History, select **Menu | Policy | Policy History**.

   No Policy History entries appear for McAfee Default policies. You might need to use the page filter to select a created or duplicated McAfee Default policy.

2 Use the **Product**, **Category**, and **Name** filters to select Policy History entries.
3 To manage a policy or Policy History entry, click **Actions**, then select an action.

- **Choose Columns** — Opens a dialog box that allows you to select which columns to display.
- **Compare Policy** — Opens the Policy Comparison page where you can compare two selected policies. The current version of a policy has the latest date. To compare the current revision of a policy and a previous policy revision, select the latest revision and a previous revision to compare.
- **Export Table** — Opens the Export page where you can specify the package and format of Policy History entry files to export, then email the file.
- **Revert Policy** — Reverts the policy to the selected policy version. You can select only one target policy.

When you revert a policy, you are prompted to add a comment to the Policy History entry.

**Edit policy history permission sets**

Configure the permission sets for your products so that users can revert policies to previous versions using the Policy History page.

**Before you begin**

You must have appropriate permissions to change permission sets.

**Task**

1. Select **Menu | User Management | Permission Sets**.
2. In the right pane, click **Edit** in the Permission row for the product associated with the policy. For example, select **EEFF Policy Permission** to change McAfee® Endpoint Encryption for Files and Folders policy permissions.
3. Click **View and change policy and task settings**, then click **Save**.

Now you can revert existing policies to Policy History entries from the Policy History page.

**Compare policies**

Policy Comparison can help you identify differences between similar policies.

Many of the values and variables included on the Policy Comparison page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the policy you want to compare.

**Task**

1. Select **Menu | Policy Comparison**, then select a product, category, and **Show** settings from the lists.

   ![Best practice: Change the Show setting from All Policy Settings to Policy Differences or Policy Matches to reduce the data displayed.]

   These settings populate the policies to compare in the **Policy 1** and **Policy 2** lists.
2. Select the policies to compare in the **Compare policies** row from the **Policy 1** and **Policy 2** column lists.

   The top two rows of the table display the number of settings that are different and identical.
3 Click Print to open a printer friendly view of the comparison.

**Change the owners of a policy**

By default, ownership is assigned to the user who creates the policy. If you have the required permissions, you can change the ownership of a policy.

**Task**

1 Select Menu | Policy | Policy Catalog, then select the Product and Category. All created policies for the selected category appear in the details pane.

2 Locate the policy you want, then click the owner of the policy. The Policy Ownership page appears.

3 Select the owners of the policy from the list, then click OK.

---

**Move and share policies between McAfee ePO servers**

In environments with multiple McAfee ePO servers, you can move and share policies to avoid re-creating them on each server.

You can move and share policies only with equal or earlier major versions of McAfee ePO. For example, you can share a policy created on a version 5.3 server with a 5.1 server; you can't share a policy from a 5.1 server to a 5.3 server.

**Tasks**

- **Register servers for policy sharing on page 146**
  Register servers to share a policy.

- **Designate policies for sharing on page 146**
  You can designate a policy for sharing among multiple McAfee ePO servers.

- **Schedule server tasks to share policies on page 147**
  The Share Policies server task ensures that any changes you make to shared policies are pushed to sharing-enabled McAfee ePO servers.

**Register servers for policy sharing**

Register servers to share a policy.

**Task**

1 Select Menu | Configuration | Registered Servers, then click New Server. The Registered Server Builder opens to the Description page.

2 From the Server type menu, select ePO, specify a name and any notes, then click Next. The Details page appears.

3 Specify any details for your server and click Enable in the Policy sharing field, then click Save.

**Designate policies for sharing**

You can designate a policy for sharing among multiple McAfee ePO servers.
Task

1. Select **Menu | Policy | Policy Catalog**, then click **Product** menu and select the product whose policy you want to share.

2. In the **Actions** column for the policy to be shared, click **Share**.

Shared policies are automatically pushed to McAfee ePO servers with policy sharing enabled. When you click **Share** in step 2, the policy is immediately pushed to all registered McAfee ePO servers that have policy sharing enabled. Changes to shared policies are similarly pushed.

Schedule server tasks to share policies

The **Share Policies** server task ensures that any changes you make to shared policies are pushed to sharing-enabled McAfee ePO servers.

If you set a long server task interval, or disable the **Share Policies** server task, we recommend manually running the task whenever you edit shared policies.

Task

1. Open the Server Task Builder.
   a. Select **Menu | Automation | Server Tasks**.
   b. Click **New Task**.

2. On the Description page, specify the name of the task and any notes, then click **Next**.
   
   New server tasks are enabled by default. If you do not want this task to be enabled, in the Schedule status field, select **Disabled**.

3. From the Actions drop-down menu, select **Share Policies**, then click **Next**.

4. Specify the schedule for this task, then click **Next**.

5. Review the summary details, then click **Save**.

Create and manage policy assignment rules

Configure policy assignment rules to simplify policy management.

Tasks

- *Create policy assignment rules on page 147*
  
  Creating policy assignment rules allows you to enforce policies for users or systems based on configured rule criteria.

- *Manage policy assignment rules on page 148*
  
  Perform common management tasks when working with policy assignment rules.

Create policy assignment rules

Creating policy assignment rules allows you to enforce policies for users or systems based on configured rule criteria.
Task

1. Open the Policy Assignment Builder.
   a. Select **Menu | Policy | Policy Assignment Rules**.
   b. Click **New Assignment Rule**.

2. Specify the details for this policy assignment rule, including:
   - A unique name and description.
   - The rule type you specify determines which criteria is available on the **Selection Criteria** page.

   By default, the priority for new policy assignment rules is assigned sequentially based on the number of existing rules. After creating the rule, you can edit the priority by clicking **Edit Priority** on the **Policy Assignment Rules** page.

3. Click **Next**.

4. Click **Add Policy** to select the policies that you want to enforce with this policy assignment rule.

5. Click **Next**.

6. Specify the criteria you want to use in this rule. Your criteria selection determines which systems or users are assigned this policy.

7. Review the summary and click **Save**.

Manage policy assignment rules

Perform common management tasks when working with policy assignment rules.

Task

1. Select **Menu | Policy | Policy Assignment Rules**.

2. Perform one of these actions:
   - **Edit a policy assignment rule** — Perform these steps:
     1. Click the selected assignment. The Policy Assignment Builder opens.
     2. Work through each page to change this policy assignment rule, then click **Save**.
   - **Delete a policy assignment rule** — Click **Delete** in the selected assignment row.
   - **Edit the priority of a policy assignment rule** — Perform these steps:
     1. Select **Actions | Edit Priority** and the Edit Priority page opens.
     2. Grab the handle and drag the row up or down in the list to change the priority, then click **Save**.
   - **View the summary of a policy assignment rule** — Click > in the selected assignment row. The row expands to display the summary information.
Policy management users

As a McAfee ePO administrator you can assign different permission sets to different policy users so they can create and modify specific product policies. Some users can approve or deny policy changes from policies submitted by other users.

Policies can be managed by three users with different permissions. The McAfee ePO administrator creates these other two user levels and permissions.

As the McAfee ePO administrator, you can create users with hierarchical levels of policy permissions. For example, you can create these policy users:

• Policy administrator — They can approve policies created and modified by other users.
• Policy user — They can duplicate and create policies that they submit to the policy administrator for approval before they are used.

Overview of creating different policy users

As the McAfee ePO administrator it takes these general steps to create a policy administrator and policy user:

1. In Server Settings, enable Policy Administration.
2. In Permission Sets, create different permission sets for the policy administrator and policy user.
3. In User Management, create policy administrator and policy user then manually assign them the different permission sets.

Overview of policy user and policy administrator processes

Once the policy user and policy administrator are created, they can perform these policy tasks:

• The policy user:
  1. In the Policy Catalog can duplicate, modify, or create policies for their assigned types and submit them to the policy administrator for approval.
  2. In the Policy History, can monitor the approval status by the policy administrator.

• The policy administrator can do everything the policy user can do plus, in the Policy History page, approve or deny the policy changes submitted by policy users.

Best practice: Set policy management globally

As administrator, you can use Server Settings to globally configure Policy Administration to allow users to change or create policies with or without administrator approval.

Before you begin
You must have administrator rights to change Policy Administration.
Task

1. To change the Policy Administration settings, select **Menu | Configuration | Server Settings**, then select **Policy Administration** and click **Edit**.

2. From Edit Policy Administration, select one of the following options, and click **Save**:

   **Table 12-1 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Needs administrator approval</td>
<td>Forces the users to request approval from the administrator before they can save a new or changed policy.</td>
</tr>
<tr>
<td></td>
<td>Administrators can give users permission to approve or deny policy changes in Permission Sets under Policy Management.</td>
</tr>
<tr>
<td>Does not need administrator approval</td>
<td>Allows the user to save a new or changed policy without administrator approval.</td>
</tr>
</tbody>
</table>

3. (Optional) Create policy management permission sets to change policy management for individual users.

Create policy management permission sets

As administrator you can create permission sets for different policy user levels. The Permission Sets allow some policy users to create and modify policies, plus allow some policy users to approve or decline policies created by other users.

**Before you begin**

You must have administrator rights to change Permission Sets.

To help you manage policy creation, you can create permission sets for users who can create and modify specific product policies. For example, you can create permission sets that allow one user to change policies and another user permission to approve or decline those changes.

These steps describe creating two different permission sets:

- Policy User (policyUserPS) permission set — Allows the policy user permission to create and modify specific product policies, but the policy changes must be approved before the policy is saved.

- Policy Administrator (policyAdminPS) permission set — Allows the policy administrator permission to create and modify specific product policies, plus approve or decline the changes created by policy users.

Task

1. To create the two permission sets, select **Menu | User Management | Permission Sets**, then click **New Permission Sets**.

2. To create the policy administrator permission set from the **New Permission Set** page, type the name, for example **policyAdminPS** and click **Save**.

3. With the policyAdminPS permission set selected, scroll down to the Policy Management row and click **Edit**.

4. From Edit Permission Sets policyAdminPS: Policy Management page, select **Can save policy changes directly and approve or decline the policy changes submitted by other users**, and click **Save**.

   This allows the policy administrator user to approve or decline policy changes for other users without administrator approval.
5 With the policyAdminPS permission set still selected, scroll down to a setting, for example the Endpoint Security Common, row and click Edit.

6 From Edit Permission Sets policyAdminPS: Endpoint Security Common page, select View and change policy and task settings and click Save.

   This allows the policy administrator user to make policy changes to Endpoint Security Common policies.

   Continue selecting settings and configuring the edit permissions as needed.

7 To duplicate the policy administrator permission set and create the policy user permission set, click Actions | Duplicate.

8 In the Actions: Duplicate pop-up window, type the policy user permission set name, for example policyUserPS and click OK.

   These two steps create a duplicate of the policy administrator permission set. The one following change creates the policy user (policyUserPS) permission set.

9 From the Permission Sets list, click the policyUserPS permission set created in step 7.

10 Scroll down to the Policy Management row and click Edit.

11 From Edit Permission Sets policyUserPS: Policy Management page, select Policy Approval setting No Permissions, and click Save:

   This setting forces the users assigned this permission set to request approval from the administrator before they can save a new or changed policy.

Now you have created the two permission sets to use when creating the two policy user and policy administrator users.

Create policy management users

As administrator, you can create different policy user levels with different permission sets that allow one user to create and modify policies and an administrator user to approve or decline policy changes.

Before you begin
You must have administrator rights to create Users in User Management.

These steps describe creating two different users:

- Policy User (policyUser) — The policyUser can create and modify specific product policies, but the policy changes must be approved by the policy administrator before the policy is saved.

- Policy Administrator (policyAdmin) — The policyAdmin can create and modify specific product policies, plus approve or decline the changes created by policy users.

Task

1 Open the User Management page: click Menu | User Management | Users.

2 To create the policy user (policyUser), perform these steps.
   a Click New User.
   b Type a user name. For example, policyUser.
   c Select Enable for the logon status of this account.
Select whether the new account uses McAfee ePO authentication, Windows authentication, or Certificate Based Authentication and provide the required credentials or browse and select the certificate.

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

Select the policy user permission set you created in Administrator creates user policy management permission sets. For example, select policyUserPS.

Click Save to return to the Users tab.

The new policy user appears in the Users list of the User Management page.

To create the policy administrator (policyAdmin), perform these steps.

Click New User.

Type a user name. For example, policyAdmin.

Select Enable for the logon status of this account.

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

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

Select the policy user permission set you created in Create policy management permission sets. For example, select policyAdminPS.

Click Save to return to the Users tab.

The new policy administrator appears in the Users list of the User Management page.

Now you have two policy users. One policy user can change policies and a policy administrator user who can approve or decline those changes.

Submit policy changes for acceptance

Non-administrator policy users can create and change policies, but if configured by the administrator, they might need to submit the policy for review by the administrator or a policy administrator.

Before you begin

You must have configured the Server Settings and user permission sets to allow users to submit policies for approval.

Task

1. Create and maintain policies.

   Policy users only have access to policies and setting configured by the administrator in their assigned permission set.

2. When you get to the step in the policy process to save the policy, click Submit for Review.

   That sends the policy to the administrator to approve or decline.

3. To check the status of the policy acceptance, select Menu | Policy | Policy History.
Use the Product, Category, and Name filters to select Policy History entries to check.

In the Status column, one of these entries appears describing the administrator’s action:

- Pending review — Has not been reviewed.
- Declined — Has been declined and not saved.
- Approved — has been approved and saved.

Accept policy changes
As a policy administrator, you need to periodically approve or decline policy user submitted requests.

Before you begin
You must have configured the Server Settings and user permission sets to allow users to submit policies for approval.

Task

1. To change the status of the policy submitted for review, select Menu | Policy | Policy History.
2. Use the Product, Category, and Name filters to select Policy History entries to check.
3. In the Policy Status column, select one of these links related to the submitted policy:
   - Accepted — The policy is saved and now ready to use.
   - Declined — The policy has been declined and not saved.

Assign policies to managed systems
Assign policies to a group or to specific systems in the System Tree. You can assign policies before or after a product is deployed.

We recommend assigning policies at the highest level possible so that the groups and subgroups below inherit the policy.

Tasks

- Assign a policy to a System Tree group on page 153
  Assign a policy to a specific group of the System Tree.
- Assign a policy to a managed system on page 154
  Assign a policy to a specific managed system.
- Assign a policy to systems in a System Tree group on page 154
  Assign a policy to multiple managed systems within a group.

Assign a policy to a System Tree group
Assign a policy to a specific group of the System Tree.
Task

1. Select Menu | Systems | System Tree, click Assigned Policies tab, then select a product.
   Each assigned policy per category appears in the details pane.

2. Locate the policy category you want, then click Edit Assignment.

3. If the policy is inherited, next to Inherited from, select Break inheritance and assign the policy and settings below.

4. Select the policy from the Assigned policy drop-down list.
   
   From this location, you can also edit the selected policy's settings, or create a policy.

5. Choose whether to lock policy inheritance.
   Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

6. Click Save.

Assign a policy to a managed system
Assign a policy to a specific managed system.

Task

1. Select Menu | Systems | System Tree, click Systems tab, then select a group under System Tree.
   All systems within this group (but not its subgroups) appear in the details pane.

2. Select a system, then click Actions | Agent | Modify Policies on a Single System.
   The Policy Assignment page for that system appears.

3. Select a product.
   The categories of selected product are listed with the system's assigned policy.

4. Locate the policy category you want, then click Edit Assignments.

5. If the policy is inherited, next to Inherited from, select Break inheritance and assign the policy and settings below.

6. Select the policy from the Assigned policy drop-down list.
   
   From this location, you can also edit settings of the selected policy, or create a policy.

7. Choose whether to lock policy inheritance.
   Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

8. Click Save.

Assign a policy to systems in a System Tree group
Assign a policy to multiple managed systems within a group.
Task

1. Select Menu | Systems | System Tree, click Systems tab, then select a group in the System Tree. All systems in this group (but not its subgroups) appear in the details pane.

2. Select the systems you want, then click Actions | Agent | Set Policy & Inheritance. The Assign Policy page appears.

3. Select the Product, Category, and Policy from the drop-down lists.

4. Select whether to Reset inheritance or Break inheritance, then click Save.

Copy and paste policy assignments
Copy and paste policy assignments to easily share multiple assignments between groups and systems from different portions of the System Tree.

Tasks

- **Copy policy assignments from a group on page 155**
  You can use Copy Assignments to copy policy assignments from a group in the System Tree.

- **Copy policy assignments from a system on page 155**
  You can use Copy Assignments to copy policy assignments from a specific system.

- **Paste policy assignments to a group on page 156**
  You can paste policy assignments to a group after you copy them from a group or system.

- **Paste policy assignments to a specific system on page 156**
  Paste policy assignments to a specific system after copy the policy assignments from a group or system.

Copy policy assignments from a group
You can use Copy Assignments to copy policy assignments from a group in the System Tree.

Task

1. Select Menu | Systems | System Tree, click Assigned Policies tab, then select a group in the System Tree.

2. Click Actions | Copy Assignments.

3. Select the products or features where you want to copy policy assignments, then click OK.

Copy policy assignments from a system
You can use Copy Assignments to copy policy assignments from a specific system.

Task

1. Select Menu | Systems | System Tree, click Systems tab, then select a group in the System Tree. The systems belonging to the selected group appear in the details pane.
2. Select a system, then click **Actions | Agent | Modify Policies on a Single System**.

3. Click **Actions | Copy Assignments**, select the products or features where you want to copy policy assignments, then click **OK**.

**Paste policy assignments to a group**

You can paste policy assignments to a group after you copy them from a group or system.

**Task**

1. Select **Menu | Systems | System Tree**, click **Assigned Policies** tab, then select the group you want 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.

   ![Information](image)
   When pasting policy assignments, the Enforce Policies and Tasks policy appears in the list. This policy controls the enforcement status of other policies.

3. Select the policy categories you want to replace with the copied policies, then click **OK**.

**Paste policy assignments to a specific system**

Paste policy assignments to a specific system after copy the policy assignments from a group or system.

**Task**

1. Select **Menu | Systems | System Tree**, click **Systems** tab, then select a group in the System Tree.

   All 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.

   ![Information](image)
   When pasting policy assignments, the Enforce Policies and Tasks policy appears in the list. This policy controls the enforcement status of other policies.

4. Confirm the replacement of assignments.

**View policy information**

View detailed information about your policies, including policy owners, assignments, and inheritance.
Tasks

• View groups and systems where a policy is assigned on page 157
  View the Policy Catalog Assignment page to see the group, or system that inherits the policy.

• View policy settings on page 157
  View details for a policy assigned to a product category or system.

• View policy ownership on page 158
  View the owners of a policy.

• View assignments where policy enforcement is disabled on page 158
  View assignments where policy enforcement, per policy category, is disabled.

• View policies assigned to a group on page 158
  View the policies assigned to a System Tree group, sorted by product.

• View policies assigned to a specific system on page 158
  View a list of all policies assigned to a system from one central location, the System Tree.

• View policy inheritance for a group on page 159
  View the policy inheritance of a specific group.

• View and reset broken inheritance on page 159
  Identify the groups and systems where policy inheritance is broken.

• Create policy management queries on page 159
  Retrieve the policies assigned to a managed system, or policies broken in the system hierarchy.

View groups and systems where a policy is assigned

View the Policy Catalog Assignment page to see the group, or system that inherits the policy.

The parent Policy Catalog page lists the number of policy assignments. It does not list the group or system that inherits the policy.

For example, if you view the McAfee Agent product in the Product Catalog you can view the default assignments for each policy. For the McAfee Default policy, the General category is assigned to the Global Root node and Group node type.

Task

1. Select Menu | Policy | Policy Catalog, then select a product and category.
   All created policies for the selected category appear in the details pane.

2. Under Assignments for the row of the policy, click the link.
   The link indicates the number of groups or systems the policy is assigned to (for example, 6 assignments).

On the Assignments page, each group or system where the policy is assigned appears with its node name and node type.

View policy settings

View details for a policy assigned to a product category or system.

The policy assigned to a System Tree group or system can tell you, for example, the policy enforcement interval, the priority event forwarding interval, or if peer-to-peer communication is enabled.

Task

1. Select Menu | Policy | Policy Catalog, then select a product and category.
   All created policies for the selected category appear in the details pane.
2. Click the policy name link. The policy pages and their settings appear.

You can also view this information when accessing the assigned policies of a specific group. To access this information, select Menu | Systems | System Tree, click Assigned Policies tab, then click the link for the selected policy in the Policy column.

View policy ownership

View the owners of a policy.

Task

1. Select Menu | Policy | Policy Catalog, then select a product and category.
   All created policies for the selected category appear in the details pane.
2. The owners of the policy are displayed under Owner.

View assignments where policy enforcement is disabled

View assignments where policy enforcement, per policy category, is disabled.

Normally you want policy enforcement enabled. Use this task to find any policies that are not being enforced and change their configuration.

Task

1. Select Menu | Policy | Policy Catalog, then select a product and category.
   All created policies for the selected category appear in the details pane.
2. Click the link next to Product enforcement status, which indicates the number of assignments where enforcement is disabled, if any.
   The Enforcement for <policy name> page appears.
3. Go to System Tree | Assigned Policies page to change the enforcement policy of the listed policy.

View policies assigned to a group

View the policies assigned to a System Tree group, sorted by product.

For example, if you have different policies assigned to servers and workstation groups, use this task to confirm the policies are set correctly.

Task

1. Select Menu | Systems | System Tree, click Assigned Policies tab, then select a group in the System Tree.
   All assigned policies, organized by product, appear in the details pane.
2. Click any policy link to view its settings.

View policies assigned to a specific system

View a list of all policies assigned to a system from one central location, the System Tree.

For example, if you have different policies assigned to specific systems, use this task to confirm the policies are set correctly.
Task
1. Select Menu | Systems | System Tree, click the Systems tab, then select a group in the System Tree.
   All systems belonging to the group appear in the details pane.

2. Click the name of a system to drill into the System Information page, then click the Applied Policies tab.

**View policy inheritance for a group**
View the policy inheritance of a specific group.
For example, if you have policy inheritance configured for different groups, use this task to confirm the policy inheritance is set correctly.

Task
1. Select Menu | Systems | System Tree.

2. Click Assigned Policies tab.
   All assigned policies, organized by product, appear in the details pane.

   The policy row, under Inherit from, displays the name of the group from which the policy is inherited.

**View and reset broken inheritance**
Identify the groups and systems where policy inheritance is broken.
For example, if you have policies with broken inheritance configured for some groups, use this task to confirm the policies are set correctly.

Task
1. Select Menu | Systems | System Tree, then click Assigned Policies tab.
   All assigned policies, organized by product, appear in the details pane. The policy row, under Broken Inheritance, displays the number of groups and systems where this policy's inheritance is broken.

   This number 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, 1 doesn't inherit appears, regardless of the number of systems within the group.

2. Click the link indicating the number of child groups or systems that have broken inheritance.
   The View broken inheritance page displays a list of the names of these groups and systems.

3. To reset the inheritance of any of these, select the checkbox next to the name, then click Actions and select Reset Inheritance.

**Create policy management queries**
Retrieve the policies assigned to a managed system, or policies broken in the system hierarchy.
You can create either of the following Policy Management queries:

- **Applied Policies** — Retrieves policies assigned to a specified managed system.
- **Broken Inheritance** — Retrieves information on policies that are broken in the system hierarchy.
Task

1. Select Menu | Reporting | Queries & Reports, then click New Query.
   The Query Builder opens.

2. On the Result Type page, select Policy Management from the Feature Group list.

3. Select a Result Type, then click Next to display the Chart page:
   • Applied Client Tasks
   • Applied Policies
   • Client Tasks Assignment Broken Inheritance
   • Policies Assignment Broken Inheritance

4. Select the type of chart or table to display the primary results of the query, then click Next.
   The Columns page appears.
   ![If you select Boolean Pie Chart, configure the criteria that you want to include in the query.]

5. Select the columns to be included in the query, then click Next.
   The Filter page appears.

6. Select properties to narrow the search results, then click Run.
   The Unsaved Query page displays the results of the query, which is actionable.
   ![Selected properties appear in the content pane with operators that can specify criteria, which narrows the data that is returned for that property.]

7. On the Unsaved Query page, take any available action on items in any table or drill-down table.
   • If the query didn't return the expected results, click Edit Query to go back to the Query Builder and edit the details of this query.
   • If you don't want to save the query, click Close.
   • To use this query again, click Save and continue to the next step.

8. In the Save Query page, enter a name for the query, add any notes, and select one of the following:
   • New Group — Enter the new group name and select either:
     • Private group (My Groups)
     • Public group (Shared Groups)
   • Existing Group — Select the group from the list of Shared Groups.

9. Click Save.
Server and client tasks

Use server and client tasks to automate McAfee ePO and managed system processes. McAfee ePO includes preconfigured server tasks and actions. Most of the additional software products you manage with McAfee ePO also add preconfigured server and client tasks.

Contents
- Server tasks
- Client tasks

Server tasks

Server tasks are configurable actions that run on McAfee ePO at scheduled times or intervals. Leverage server tasks to automate repetitive tasks. McAfee ePO includes preconfigured server tasks and actions. Most of the additional software products you manage with McAfee ePO also add preconfigured server tasks.

View server tasks

The Server Task Log provides the status of your server tasks and displays any errors that might have occurred.

Task

2. Sort and filter the table to focus on relevant entries.
   - To change which columns are displayed, click Choose Columns.
   - To order table entries, click a column title.
   - To hide unrelated entries, select a filter from the drop-down list.
3. To view additional details, click an entry.

Server task status

The status of each server task appears in the Status column of the Server Task Log.

<table>
<thead>
<tr>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting</td>
<td>The server task is waiting for another task to finish.</td>
</tr>
<tr>
<td>In Progress</td>
<td>The server task has started, but not finished.</td>
</tr>
<tr>
<td>Paused</td>
<td>A user paused the server task.</td>
</tr>
<tr>
<td>Stopped</td>
<td>A user stopped the server task.</td>
</tr>
<tr>
<td>Status</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed</td>
<td>The server task started, but did not finish successfully.</td>
</tr>
<tr>
<td>Completed</td>
<td>The server task finished successfully.</td>
</tr>
<tr>
<td>Pending Termination</td>
<td>A user requested that the server task end.</td>
</tr>
<tr>
<td>Ended</td>
<td>A user closed the server task manually before it finished.</td>
</tr>
</tbody>
</table>

Create a server task

Create server tasks to schedule various actions to run on a specified schedule.

If you want McAfee ePO to run certain actions without manual intervention, a server task is the best approach.

**Task**

1. Open the Server Task Builder.
   - Select **Menu** | **Automation** | **Server Tasks**.
   - Click **New Task**.

2. Give the task an appropriate name, and decide whether the task has a Schedule status, then click **Next**.
   - If you want the task to run automatically, set Schedule status to **Enabled**.

3. Select and configure the action for the task, then click **Next**.

4. Choose the schedule type (the frequency), start date, end date, and schedule time to run the task, then click **Next**.
   - The schedule information is used only if you enable Schedule status.

5. Click **Save** to save the server task.

The new task appears in the Server Tasks list.

Remove outdated server tasks from the Server Task Log: best practice

Periodically remove old server task entries from the Server Task Log to improve database performance.

- Items removed from the Server Task Log are deleted permanently.

**Task**

1. Open the Server Task Log: select **Menu** | **Automation** | **Server Task Log**.

2. Click **Purge**.

3. In the Purge dialog box, enter a number, then select a time unit.

4. Click **OK**.

Any items of the specified age or older are deleted, including items not in the current view. The number of removed items is displayed in the lower right corner of the page.

- Create a server task to automatically remove outdated items.
Remove outdated log items automatically

Use a server task to automatically remove old entries from a table or log, such as closed issues or outdated user action entries.

⚠️ Items removed from a log are deleted permanently.

Task

1. Open the Server Task Builder.
   a. Select Menu | Automation | Server Tasks.
   b. Click New Task.
2. Type a name and description for the server task.
3. Enable or disable the schedule for the server task, then click Next.
   The server task does not run until it is enabled.
4. From the drop-down list, select a purge action, such as Purge Server Task Log.
5. Next to Purge records older than, enter a number, then select a time unit, then click Next.
6. Schedule the server task, then click Next.
7. Review the details of the server task.
   • To make changes, click Back.
   • If everything is correct, click Save.

The new server task appears on the Server Tasks page. Outdated items are removed from the specified table or log when the scheduled task runs.

Accepted Cron syntax when scheduling a server task

If you select the Schedule type | Advanced option when scheduling a server task, you can specify a schedule using Cron syntax.

Cron syntax is made up of six or seven fields, separated by a space. Accepted Cron syntax, by field in descending order, is detailed in the following table. Most Cron syntax is acceptable, but a few cases are not supported. For example, you cannot specify both the Day of Week and Day of Month values.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Allowed values</th>
<th>Allowed special characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds</td>
<td>0–59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Minutes</td>
<td>0–59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Hours</td>
<td>0–23</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of Month</td>
<td>1–31</td>
<td>, - * ? / L W C</td>
</tr>
<tr>
<td>Month</td>
<td>1–12, or JAN - DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of Week</td>
<td>1–7, or SUN - SAT</td>
<td>, - * ? / L C #</td>
</tr>
<tr>
<td>Year (optional)</td>
<td>Empty, or 1970–2099</td>
<td>, - * /</td>
</tr>
</tbody>
</table>
Allowed special characters

- Commas (,) are allowed to specify more values. For example, "5, 10, 30" or "MON, WED, FRI".
- Asterisks (*) are used for "every." For example, "*" in the minutes field is "every minute".
- Question marks (?) are allowed to specify no specific value in the Day of Week or Day of Month fields.
  The question mark must be used in one of these fields, but cannot be used in both.
- Forward slashes (/) identify increments. For example, "5/15" in the minutes field means the task runs at minutes 5, 20, 35 and 50.
- The letter "L" means "last" in the Day of Week or Day of Month fields. For example, "0 15 10 ? * 6L" means the last Friday of every month at 10:15 am.
- The letter "W" means "weekday". So, if you created a Day of Month as "15W", this means the weekday closest to the 15th of the month. Also, you can specify "1W", which means the last weekday of the month.
- The pound character "#" identifies the "Nth" day of the month. For example, using "6#3" in the Day of Week field is the third Friday of every month, "2#1" is the first Monday, and "4#5" is the fifth Wednesday.
  If the month does not have a fifth Wednesday, the task does not run.

Client tasks

Create and schedule client tasks to automate endpoint tasks in your network.

For information about which client tasks are available and what they can do to help you, see the documentation for your managed products.

Client task example

When you initially start McAfee ePO, some preconfigured client tasks are automatically installed to help manage your McAfee products. These client tasks provide basic security for most users, and run by default.

Client tasks are configured to run using different criteria. For example, some client tasks run:

- Continuously — These client tasks automatically scan programs and files for threats as they occur.
- At configured events — These client tasks run at agent-server communication interval (ASCI) or policy enforcement interval.
- On schedule — These client tasks run at a time configured in the product deployment or policy.

This preconfigured client task, named Initial Deployment Update My Group, deploys the McAfee software on your managed systems.

This client task runs continuously to keep the McAfee software on all your systems up to date.

This graphic describes how the "Initial Deployment Update My Group" client task works.
The client task starts when you run the Smart Installer URL on a system.

The client task looks at the list of software saved in the Master Repository and, using a Product Deployment named "Initial Deployment My Group," automatically starts downloading the software to all your managed systems.

Once the software is installed, it is run periodically using other client task requests sent from McAfee ePO to protect your systems.

By default, every 60 minutes at the agent-server communication interval (ASCI), the latest versions of all software installed on your managed systems are sent to the McAfee ePO.

The client task continuously compares the software versions installed in the Master Repository to the list of software versions installed on your managed systems. If a more recent version of software exists in the Master Repository, that software is automatically downloaded using Product Deployment to your managed systems.

How the Client Task Catalog works

Use the Client Task Catalog to create client task objects you can reuse to help manage systems in your network. The Client Tasks Catalog applies the concept of logical objects to McAfee ePO client tasks. You can create client task objects for various purposes without the need to assign them immediately. As a result, you can treat these objects as reusable components when assigning and scheduling client tasks.

You create client task assignments to:

- Link System Tree groups or tagged systems to a client task.
- Schedule the client task to run.
- Set stop tasks, randomization, and rerun delays for the client task.

Client tasks can be assigned at any level in the System Tree. Groups and systems lower in the tree inherit client tasks. As with policies and policy assignments, you can break the inheritance for an assigned client task.
Client task objects can be shared across multiple registered McAfee ePO servers in your environment. When client task objects are set to be shared, each registered server receives a copy after your Share Client Task server task runs. Any changes made to the task are updated each time it runs. When a client task object is shared, only the owner of the object can modify its settings.

Administrators on the target server that receives a shared task is not an owner for that shared task. None of the users on the target server is owner for any shared task objects the target receives.

Deployment tasks
Deployment tasks are client tasks that are used to deploy managed security products to your managed systems from the Master Repository.

You can create and manage individual deployment task objects using the Client Task Catalog, then assign them to run on groups or individual system. Alternatively, you can create Product Deployment projects to deploy products to your systems. Product Deployment projects automate the process of creating and scheduling client task objects individually. They also provide additional automated management functionality.

Important considerations
When deciding how to stage your Product Deployment, consider:

- Package size and available bandwidth between the Master Repository and managed systems. In addition to potentially overwhelming the McAfee ePO server or your network, deploying products to many systems can make troubleshooting problems more complicated.

- A phased rollout to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred clients at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

Deploying products on selected systems
If you are deploying McAfee products or components that are installed on a subset of your managed systems:

1. Use a tag to identify these systems.
2. Move the tagged systems to a group.
3. Configure a Product Deployment client task for the group.

Deployment packages for products and updates
The McAfee ePO software deployment infrastructure supports deploying products and components, as well as updating both.

Each product that McAfee ePO can deploy provides a product deployment package .zip file. The .zip file contains product installation files, which are compressed in a secure format. McAfee ePO can deploy these packages to any of your managed systems.

The software uses these .zip files for both detection definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. We recommend configuring policy settings before deploying the product to network systems. Configuring policy settings saves time and ensures that your systems are protected as soon as possible.

These package types can be checked in to the Master Repository with pull tasks, or manually.
Supported package types

<table>
<thead>
<tr>
<th>Package type</th>
<th>Description</th>
<th>Origination</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuperDAT files (SDAT.exe) files</td>
<td>The SuperDAT files contain both DAT and engine files in a single update package. If bandwidth is a concern, we recommend updating DAT and engine files separately.</td>
<td>McAfee website. Download and check SuperDAT files into the Master Repository manually.</td>
</tr>
<tr>
<td>Supplemental detection definition (Extra.DAT) files</td>
<td>The Extra.DAT 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 Extra.DAT files immediately, rather than wait until the signature is added to the next DAT file. Extra.DAT files are from the McAfee website. You can distribute them through McAfee ePO. Pull tasks do not retrieve Extra.DAT files.</td>
<td>McAfee website. Download and check supplemental DAT files into the Master Repository manually.</td>
</tr>
<tr>
<td>Product deployment and update packages</td>
<td>A product deployment package contains installation software.</td>
<td>Product CD or downloaded product .zip file. Check product deployment packages into the Master Repository manually. For specific locations, see the documentation for that product.</td>
</tr>
<tr>
<td>McAfee Agent language packages</td>
<td>A McAfee Agent language package contains files necessary to display McAfee Agent information in a local language.</td>
<td>Master Repository — Checked in at installation. For future versions of the McAfee Agent, you must check McAfee Agent language packages into the Master Repository manually.</td>
</tr>
</tbody>
</table>

Package signing and security

All packages created and distributed by McAfee are signed with a key pair using the DSA (Digital Signature Algorithm) signature verification system. The packages 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 McAfee has not signed. 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 previously described, but McAfee ePO signs them when they are checked in.

The McAfee Agent only trusts package files signed by McAfee ePO or McAfee. This feature protects your network from receiving packages from unsigned or untrusted sources.

Package ordering and dependencies

If one product update depends on another update, check in the update packages to the Master Repository in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them in again, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.
Product and update deployment
The McAfee ePO repository infrastructure allows you to deploy product and update packages to your managed systems from a central location. Although the same repository is used, there are differences.

Product deployment vs. update packages

<table>
<thead>
<tr>
<th>Product deployment packages</th>
<th>Update packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must be manually checked in to the Master Repository.</td>
<td>DAT and Engine update packages can be copied from the source site automatically with a pull task. All other update packages must be checked in to the Master Repository manually.</td>
</tr>
<tr>
<td>Can be replicated to the Master Repository and installed automatically on managed systems using a deployment task.</td>
<td>Can be replicated to the Master Repository and installed automatically on managed systems with global updating.</td>
</tr>
<tr>
<td>If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.</td>
<td>If not implementing global updating for product updating, an update client task must be configured and scheduled for managed systems to retrieve the package.</td>
</tr>
</tbody>
</table>

Product deployment and updating process
Follow this high-level process for distributing DAT and Engine update packages.

1. Check in the update package to the Master Repository with a pull task, or manually.

2. Do one of the following:
   - If you are using global updating, create and schedule an update task for laptop systems that leave the network.
   - If you are not using global updating, perform the following tasks.
     1. Use a replication task to copy the contents of the Master Repository.
     2. Create and schedule an update task for agents to retrieve and install the update on managed systems.

Deployment tags
When a deployment task is created, a tag with the task name is automatically created and applied to the systems on which the task is enforced. These tags are only created for a fixed deployment. Does not apply to continuous deployment.

These tags are added to the Deployment Tags group on the Tag Catalog page every time a deployment task is created and enforced to systems. This group is a read-only group, and tags in this group can’t be manually applied, changed, deleted, or used in a criteria configuration to filter systems.

Use the Product Deployment task to deploy products to managed systems
Deploy products to managed systems with the Product Deployment client task.
You can create this task for a single system, or for groups of the System Tree.

Tasks
- Configure a deployment task for groups of managed systems on page 169
  Configure a product deployment task to deploy products to groups of managed systems in the System Tree.
- Configure a deployment task to install products on a managed system on page 170
  Deploy products to a single system using a product deployment task.
Configure a deployment task for groups of managed systems

Configure a product deployment task to deploy products to groups of managed systems in the System Tree.

**Task**

1. Open the New Task dialog box.
   
   a. Select **Menu | Policy | Client Task Catalog**.
   
   b. Under Client Task Types, select a product, then click **New Task**.

2. Select **Product Deployment**, then click **OK**.

3. Type a name for the task you are creating and add any notes.

4. Next to Target platforms, select the types of platform to use the deployment.

5. Next to Products and components, set the following:
   
   • Select a product from the first drop-down list. The products listed are products that you have checked in to the Master Repository. If you do not see the product you want to deploy listed here, check in the product package.
   
   • Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
   
   • To specify command-line installation options, type the options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

   ![You can click + or – to add or remove products and components from the list displayed.]

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

   ![If you set your security product to update automatically, you cannot set the Action to Remove.]

7. (Windows only) Next to Options, select whether you want to run this task for every policy process, then click **Save**.

8. Select **Menu | Systems Section | System Tree | Assigned Client Tasks**, then select the required group in the System Tree.

9. Select the **Preset** filter as **Product Deployment (McAfee Agent)**.

   Each assigned client task per selected category appears in the details pane.

10. Click **Actions | New Client Task Assignment**.

11. On the Select Task page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select the task you created to deploy your product.

12. Next to Tags, select the platforms you are deploying the packages to, then click **Next**:

   • **Send this task to all computers**
   
   • **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.

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

---

McAfee ePolicy Orchestrator 5.9.0 Product Guide

13

169
On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

Review the summary, then click Save.

At every scheduled run, the deployment task installs the latest sensor package to systems that meet the specified criteria.

**Configure a deployment task to install products on a managed system**

Deploy products to a single system using a product deployment task.

Create a product deployment client task for a single system when that system requires:

- A product installed that other systems within the same group do not require.
- A different schedule than other systems in the group. For example, if a system is located in a different time zone than its peers.

**Task**

1. Open the New Task dialog box.
   a. Select **Menu** | **Policy** | **Client Task Catalog**.
   b. Under Client Task Types, select a product, then click **New Task**.
2. Ensure that **Product Deployment** is selected, then click **OK**.
3. Type a name for the task you are creating and add any notes.
4. Next to **Target platforms**, select the types of platform to use the deployment.
5. Next to **Products and components** set the following:
   - Select a product from the first drop-down list. The products listed are those products for which you have already checked in a package to the Master Repository. If you do not see the product you want to deploy listed here, check in that product’s package.
   - Set the **Action** to **Install**, then select the **Language** and **Branch** of the package.
   - To specify command-line installation options, type the command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

   You can click + or – to add or remove products and components from the list displayed.

6. If you want to automatically update security products that are already deployed, including hotfixes and patches, select **Auto Update**.

   If you set your security product to update automatically, you cannot set the **Action** to **Remove**.

7. Next to **Options**, select if you want to run this task for every policy enforcement process (Windows only), then click **Save**.

8. Select **Menu** | **Systems** | **System Tree** | **Systems**, select the system on which you want to deploy a product, then click **Actions** | **Agent** | **Modify Tasks on a single system**.

9. Click **Actions** | **New Client Task Assignment**.

10. On the **Select Task** page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select the task you created for deploying product.
11 Next to Tags, select the platforms to which you are deploying the packages, then click Next:

- Send this task to all computers
- Send this task to only computers that have the following criteria — Click edit, select the tag group and tags to use in the criteria, then click OK.

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

12 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

13 Review the summary, then click Save.

### Updating tasks

If you do not use global updating, determine when agents on managed systems go for updates.

You can create and update client tasks to control when and how managed systems receive update packages.

If you use global updating, this task is not needed, although you can create a daily task for redundancy.

### Considerations when creating or updating client tasks

Consider the following when scheduling client update tasks:

- Create a daily update client task at the highest level of the System Tree, so that all systems inherit the task. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact. For networks with offices in different time zones, balance network load by running the task at the local system time of the managed system, rather than at the same time for all systems.
- If you are using scheduled replication tasks, schedule the task at least an hour after the scheduled replication task.
- Run update tasks for DAT and Engine files at least once a day. Managed systems might be logged off from the network and miss the scheduled task. Running the task frequently ensures that these systems receive the update.
- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one task to update only DAT files, then create another to update both DAT and Engine files weekly or monthly (Engine packages are released less frequently).
- Create and schedule more tasks to update products that do not use the McAfee Agent for Windows.
- Create a task to update your main workstation applications, to ensure that they all receive the update files. Schedule it to run daily or several times a day.

### View assigned client task

During the Initial Product Deployment process, McAfee ePO automatically creates a product deployment client task. You can use this assigned client task as a basis for creating other product deployment client tasks.

**Before you begin**

You must run the Initial Product Deployment to create the initial product deployment client task.
Task

1. To see the initial product deployment client task, select Menu | Client Task Catalog.

2. Find the initial product deployment client task: from the Client Task Types list, select McAfee Agent | Product Deployment.

   The initially created product deployment client task uses the name of the System Tree group that you configured in the Agent Deployment URL as InitialDeployment_<groupName>. For example, "InitialDeployment_AllWindowsSystems." This task appears in the Name column of the McAfee Agent | Product Deployment table.

3. To open the client task and view its details, click the name of the task configured in the Agent Deployment URL.

4. To close the page, click Cancel.

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

Update managed systems regularly with a scheduled update task

Create and configure update tasks. If you use global updating, we recommend using a daily update client task to ensure systems are current with the latest DAT and engine files.

Task

1. Open the New Task dialog box.
   a. Select Menu | Policy | Client Task Catalog.
   b. Under Client Task Types, select a product, then click New Task.

2. Verify that Product Update is selected, then click OK.

3. Type a name for the task you are creating and add any notes.

4. Next to the Update in Progress dialog box, select if you want the users to be aware an update is in process, and if you want to allow them to postpone the process.

5. Select a package type, then click Save.

   When configuring individual signatures and engines, if you select Engine and deselect DAT, when the new engine is updated a new DAT is automatically updated to ensure complete protection.

6. Select Menu | Systems | System Tree, click the Systems tab, then select the system where you want to deploy the product update, then click Actions | Agent | Modify Tasks on a single system.

7. Click Actions | New Client Task Assignment.

8. On the Select Task page, make the following selections:
   • Product — Select McAfee Agent.
   • Task Type — Select Product Update.

Then select the task you created to deploy the product update.
Next to Tags, select the platforms where you are deploying the packages, then click **Next**:  

- **Send this task to all computers.**
- **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.

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

On the **Schedule** page, select whether the schedule is enabled, and specify the schedule details, then click **Next**.

Review the summary, then click **Save**.

The task is added to the list of client tasks for the groups and systems where it is applied. Agents receive the new update task information the next time they communicate with the server. If the task is enabled, the update task runs at the next occurrence of the scheduled day and time.

Each system updates from the appropriate repository, depending on how the policies for that client's agent are configured.

**Evaluate new DATs and engines before distribution**

You might want to test DAT and engine files on a few systems before deploying them to your entire organization. You can test update packages using the Evaluation branch of your Master Repository.

The McAfee ePO software provides three repository branches for this purpose.

**Task**

1. Create a scheduled Repository Pull task that copies update packages in the Evaluation branch of your Master Repository. Schedule it to run after McAfee releases updated DAT files.

2. Create or select an evaluation group in the System Tree, then create a McAfee Agent policy for the systems to use only the Evaluation branch.
   a. Select the Evaluation branch on the **Updates** tab in the **Repository Branch Update Selection** section.

   The policies take effect the next time the McAfee Agent calls into the server. The next time the agent updates, it retrieves them from the Evaluation branch.

3. Create a scheduled update client task for the evaluation systems that updates DAT and engine files from the Evaluation branch of your repository. Schedule it to run one or two hours after your Repository Pull task is scheduled to begin.
   
   The evaluation update task created at the evaluation group level causes it to run only for that group.

4. Monitor the systems in your evaluation group until satisfied.

5. Move the packages from the Evaluation branch to the Current branch of your Master Repository. Select **Menu** | **Software** | **Master Repository** to open the **Master Repository** page.

   Adding them to the Current branch makes them available to your production environment. The next time any client task retrieves packages from the Current branch, the new DAT and engine files are distributed to systems that use the task.

**Manage client tasks**

Create and maintain client tasks.
Tasks

- Create client tasks on page 174
  Use client tasks to automatically perform product updates. The process is similar for all client tasks.

- Edit client tasks on page 174
  You can edit any previously configured client task settings or schedule information.

- Compare client tasks on page 175
  The Client Task Comparison tool determines which client task settings are different and which are the same.

- View client tasks assigned to a specific system on page 175
  View a list of all client tasks assigned to a system from one central location, the System Tree.

Create client tasks

Use client tasks to automatically perform product updates. The process is similar for all client tasks.

In some cases, you must create a new client task assignment to associate a client task to a System Tree group.

Task

1. Open the New Task dialog box.
   a. Select Menu | Policy | Client Task Catalog.
   b. Under Client Task Types, select a product, then click New Task.

2. Select a task type from the list, then click OK to open the Client Task Builder.

3. Enter a name for the task, add a description, then configure the settings specific to the task type you are creating.

   The configuration options depend on the task type selected.

4. Review the task settings, then click Save.

The task is added to the list of client tasks for the selected client task type.

Edit client tasks

You can edit any previously configured client task settings or schedule information.

Task

1. Select Menu | Policy | Client Task Catalog.

2. Select the Client Task Type from the navigation tree on the left.

   The available client tasks appear in the window on the right.

3. Click the client task name to open the Client Task Catalog dialog box.

4. Edit the task settings as needed, then click Save.

The managed systems receive the changes you configured the next time the agents communicate with the server.
**Compare client tasks**
The Client Task Comparison tool determines which client task settings are different and which are the same. Many of the values and variables included on this page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the client task that you want to compare.

**Task**

1. Select **Menu | Client Task Comparison**, then select a product, client task type, and show settings from the lists. These settings populate the client tasks to compare in the Client Task 1 and Client Task 2 lists.

2. Select the client tasks to compare in the **Compare Client Tasks** row from the **Client Task 1** and the **Client Task 2** column lists. The top two rows of the table display the number of settings that are different and identical. To reduce the amount of data, change the **Show** setting from **All Client Task Settings** to **Client Task Differences** or **Client Task Matches**.

3. Click **Print** to open a printer-friendly view of this comparison.

**View client tasks assigned to a specific system**
View a list of all client tasks assigned to a system from one central location, the System Tree.

**Task**

1. Select **Menu | Systems | System Tree**, click the **Systems** tab, then select a group in the System Tree. All systems belonging to the group appear in the details pane.

2. Click the name of a system to drill into the System Information page, then click the **Applied Client Tasks** tab.
Setting up automatic responses

Take immediate action against threats and outbreaks by automatically starting McAfee ePO processes when events occur.

McAfee ePO responds when the conditions of an automatic response rule are met. You specify the actions that make up the response, and the type and number of events that must meet the condition to trigger the response.

By default, an automatic response rule can include these actions:

• Create an issue.
• Execute server tasks.
• Run external commands.
• Run system commands.
• Send an email message.
• Send SNMP traps.

You can also configure external tools installed on the McAfee ePO server to run an external command.

Managed products increase the number of actions you can select.

The products that you manage with McAfee ePO determine the types of events you can create an automatic response rule for.

Here are some typical conditions that might trigger an automatic response:

• Detection of threats by your anti-virus software.
• Outbreak situations. For example, 1,000 virus-detected events are received in five minutes.
• High-level compliance of McAfee ePO server events. For example, a repository update or a replication task failed.

Contents

• Using Automatic Responses
• Event thresholds
• Default automatic response rules
• Response planning
• Determine how events are forwarded
• Configure Automatic Responses
• Choose a notification interval
• Create and edit Automatic Response rule
• Actions page (Response Builder)
• Aggregation page (Response Builder)
• Automatic Responses page
• Description page (Automatic Response Builder)
• Edit Email Server page
• Edit Event Filtering page
• Edit Event Notifications page
Using Automatic Responses

You can specify which events trigger a response, and what that response is. The complete set of event types for which you can configure an automatic response depends on the software products you are managing with McAfee ePO.

By default, your response can include these actions:

- Create issues.
- Run system commands.
- Execute server tasks.
- Send email message to multiple recipients.
- Execute server tasks.
- Send SNMP traps.

You can also configure external tools installed on the McAfee ePO server to run an external command.

This feature is designed to create user-configured notifications and actions when the conditions of a rule are met. These conditions include, but are not limited to:

- Detection of threats by your anti-virus software product.
- Outbreak situations. For example, 1000 virus-detected events are received in five minutes.
- High-level compliance of McAfee ePO server events. For example, a repository update or a replication task failed.

Event thresholds

Setting event thresholds lets you tailor the frequency of automatic responses to fit the needs and realities of your environment.

Aggregation

Use aggregation to set the number of events that occur before triggering an automatic response. For example, you can configure an automatic response rule to send an email message when either one of these thresholds is met:

- In one hour, the server receives 1,000 or more virus detection events from different systems.
- In one hour, the server receives 100 or more virus detection events from one 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 securing a large network, you might receive tens of thousands of events in an hour, generating thousands of email messages. Throttling allows you to limit the number of notification messages you receive based on one rule. For example, you can specify in a response 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 one group. Grouping provides these benefits:

- Respond to all events with the same or higher severity at once.
- Prioritize events that are generated.

Default automatic response rules

Enable the default McAfee ePO response rules for immediate use while you learn more about the feature.

Before enabling any of the default rules, perform these actions:

- Specify the email server (select Menu | Configuration | Server Settings) that sends the notification messages.
- Make sure that the recipient email address is correct. This address is configured on the Actions page of the Automatic Response Builder.

<table>
<thead>
<tr>
<th>Rule name</th>
<th>Associated events</th>
<th>Email sent when...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed repository update or replication</td>
<td>Distributed repository update or replication failed</td>
<td>Any update or replication fails.</td>
</tr>
<tr>
<td>failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware detected</td>
<td>Any events from any unknown products</td>
<td>These criteria are met:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The number of events is at least 1,000 in an hour.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The number of selected distinct values is 500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At most, once every 2 hours.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The email includes the source system IP address, threat names, product information, and other parameters.</td>
</tr>
<tr>
<td>Master Repository update or replication</td>
<td>Master Repository update or replication failed</td>
<td>Any update or replication fails.</td>
</tr>
<tr>
<td>failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Noncompliant computer detected</td>
<td>Noncompliant Computer Detected events</td>
<td>Any events are received from the Generate Compliance Event server task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Response planning

Before creating automatic response rules, think about the actions you want the McAfee ePO server to take.

Plan for these items:

- The event types that trigger messages in your environment.
- Who receives which messages. For example, you might not need to notify all administrators about a failed product upgrade, but you might want them to know that an infected file was discovered.
- The types and levels of thresholds that 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 send one message for every 1,000 events.
- The commands or registered executables you want to run when the conditions of a rule are met.
- The server task you want to run when the conditions of a rule are met.
Determine how events are forwarded

Determine when events are forwarded and which events are forwarded immediately.

The server receives event notifications from agents. You can configure McAfee Agent policies to forward events either immediately to the server or only after agent-server communication intervals.

If you choose to send events immediately (as set by default), the McAfee Agent forwards all events when they are received.

If you choose not to have all events sent immediately, the McAfee Agent forwards immediately only events that are designated by the issuing product as high priority. Other events are sent only at the agent-server communication.

Tasks

• Determine which events are forwarded immediately on page 180
  Determine whether events are forwarded immediately or only during agent-server communication.

• Determine which events are forwarded to the server on page 180
  You can determine which events are forwarded to the server using server settings and event filtering.

Determine which events are forwarded immediately

Determine whether events are forwarded immediately or only during agent-server communication.

If the currently applied policy is not set for immediate uploading of events, either edit the currently applied policy or create a McAfee Agent policy. This setting is configured on the Threat Event Log page.

Task

1  Select Menu | Policy | Policy Catalog, then select Product as McAfee Agent and Category as General.

2  Click an existing agent policy.

3  On the Events tab, select Enable priority event forwarding.

4  Select the event severity.
   Events of the selected severity (and greater) are forwarded immediately to the server.

5  To regulate traffic, type an Interval between uploads (in minutes).

6  To regulate traffic size, type the Maximum number of events per upload.

7  Click Save.

Determine which events are forwarded to the server

You can determine which events are forwarded to the server using server settings and event filtering.

These settings affect the bandwidth used in your environment, as well as the results of event-based queries.
Task

1. Select Menu | Configuration | Server Settings, select Event Filtering, then click Edit at the bottom of the page.

2. Select the events you want forwarded, either all or individual events.
   - To forward all available events, select All events to the server.
   - To forward only the events you specified, select Only selected events to the server.

3. Select where you want the selected events stored.
   - To store all selected events in the server:
     - Click Store selected in ePO — Store all selected events in the McAfee ePO database.
     - Click Store selected in SIEM — Store all selected events in security information and event management (SIEM) database.
     - Click Store selected in both — Store all selected events in both the McAfee ePO and the SIEM databases. This is the default setting.
   - To store the selected events in individually selected servers:
     - Click Store in ePO — Store event in the McAfee ePO database.
     - Click Store in SIEM — Store event in SIEM database.
     - Click Store in both — Store event in McAfee ePO and SIEM databases.

   If a product extension provides an event storage option for an event type during registration, that event storage option is saved. If a product extension does not provide an event storage option for an event type during registration, the default is to save the events in both McAfee ePO and SIEM databases.

4. Select event source.
   - Events from any source — Any source includes the McAfee Agent, McAfee ePO, and more.
   - Events that were generated by the sending agent — Only events generated by the McAfee Agent.

5. Click Save.

Changes to these settings take effect after all agents have communicated with the McAfee ePO server.

---

Configure Automatic Responses

Contents

- Assign permissions to notifications
- Assign permissions to Automatic Responses
- Manage SNMP servers
- Manage registered executables and external commands

Assign permissions to notifications

Notifications permissions enable users to view, create, and edit registered executables.
Task

1. Select **Menu | User Management | Permission Sets**, then either create a permission set or select an existing one.
2. Next to **Event Notifications**, click **Edit**.
3. Select the notifications permission you want:
   - No permissions
   - View registered executables
   - Create and edit registered executables
   - View rules and notifications for entire System Tree (overrides System Tree group access permissions)
4. Click **Save**.
5. If you created a permission set, select **Menu | User Management | Users**.
6. Select a user to assign the new permission set to, then click **Edit**.
7. Next to **Permission sets**, select the checkbox for the permission set with the notifications permissions you want, then click **Save**.

Assign permissions to Automatic Responses
Assign permissions to responses when you need to limit the types of responses users can create.

**Before you begin**
To create a response rule, users need permissions for the Threat Event Log, System Tree, Server Tasks, and Detected Systems features.

Task

1. Select **Menu | User Management | Permission Sets**, then create a permission set or select an existing one.
2. Next to **Automatic Response**, click **Edit**.
3. Select an **Automatic Response** permission:
   - No permissions
   - View Responses; view Response results in the Server Task Log
   - Create, edit, view, and cancel Responses; view Response results in the Server Task Log
4. Click **Save**.
5. If you created a permission set, select **Menu | User Management | Users**.
6. Select a user to assign the new permission set to, then click **Edit**.
7. Next to **Permission sets**, select the checkbox for the permission set with the **Automatic Response** permissions you want, then click **Save**.
Manage SNMP servers
Configure responses to use your SNMP (Simple Network Management Protocol) server.
You can configure responses to send SNMP traps to your SNMP server. You can receive SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment.

You do not need to make other configurations or start any services to configure this feature.

SNMP server actions
1. Select Menu | Configuration | Registered Servers.
2. From the list of registered servers, select an SNMP server, then click Actions and a change available from the Registered Servers page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edit the server information as needed, then click Save.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected SNMP server. When prompted, click Yes.</td>
</tr>
</tbody>
</table>

Import .MIB files
Import .mib files before you set up rules to send notification messages to an SNMP server using an SNMP trap.
You must import three .mib files from \Program Files\McAfee\ePolicy Orchestrator\MIB. The files must be imported in the following order:
1. NAI-MIB.mib
2. TVD-MIB.mib
3. EPO-MIB.mib

These files allow your network management program to decode the data in the SNMP traps into meaningful text. The EPO-MIB.mib file depends on the other two files to define the following traps:
- **epoThreatEvent** — This trap is sent when an Automatic Response for an McAfee ePO Threat Event is triggered. It contains variables that match properties of the Threat event.
- **epoStatusEvent** — This trap is sent when an Automatic Response for an McAfee ePO Status Event is triggered. It contains variables that match the properties of a (Server) Status event.
- **epoClientStatusEvent** — This trap is sent when an Automatic Response for an McAfee ePO Client Status Event is triggered. It contains variables that match the properties of the Client Status event.
- **epoTestEvent** — This is a test trap that is sent when you click Send Test Trap in the New SNMP Server or Edit SNMP Server pages.

For instructions on importing and implementing .mib files, see the product documentation for your network management program.

Manage registered executables and external commands
The registered executables you configure are run when the conditions of a rule are met. Automatic Responses trigger the registered executable commands to run.

You can run registered executable commands only on console applications.
Task

1. Select Menu | Configuration | Registered Executables.
2. Select one of these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a registered executable</td>
<td>1. Click Actions</td>
</tr>
<tr>
<td></td>
<td>2. Type a name for the registered executable.</td>
</tr>
<tr>
<td></td>
<td>3. Type the path and select the registered executable that you want a rule to execute when triggered.</td>
</tr>
<tr>
<td></td>
<td>4. Modify the user credentials, if needed.</td>
</tr>
<tr>
<td></td>
<td>5. Test the executable and confirm that it worked using the Audit Log.</td>
</tr>
<tr>
<td></td>
<td>6. Click Save.</td>
</tr>
<tr>
<td></td>
<td>The new registered executable appears in the Registered Executables list.</td>
</tr>
</tbody>
</table>

| Edit a registered executable   | 1. Find the registered executable to edit in the Registered Executable page, then click Edit. |
|                                | 2. Change the information as needed and click Save.                  |

| Duplicate a registered executable | 1. Find the registered executable to duplicate in the Registered Executable page, then click Duplicate. |
|                                 | 2. Type a name for the registered executable, then click OK.         |
|                                 | The duplicated registered executable appears in the Registered Executables list. |

| Delete a registered executable  | 1. Find the registered executable to delete in the Registered Executable page, then click Delete. |
|                                | 2. When prompted, click OK.                                         |
|                                | The deleted registered executable no longer appears in the Registered Executables list. |

Choose a notification interval

This setting determines how often the automatic response system is notified that an event has occurred. These events generate notifications:

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

An automatic response can be triggered only after the automatic response system receives a notification. Specify a short interval for sending notifications, and choose an evaluation interval that is frequent enough to ensure that the automatic response system can respond to an event in a timely manner, but infrequent enough to avoid excessive bandwidth consumption.
Task

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

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

Create and edit Automatic Response rule

**Contents**
- Define a rule
- Set filters for the rule
- Set Aggregation and grouping criteria for the rule
- Configure the actions for an automatic response rule

**Define a rule**
When creating a rule, include information that other users might need to understand the purpose or effect of the rule.

**Task**

1. Select **Menu | Automation | Automatic Responses**, then click **New Response**, or click **Edit** next to an existing rule.

2. On the **Description** page, type a unique name and any notes for the rule. A good name gives users a general idea of what the rule does. Use notes to provide a more detailed description.

3. From the **Language** menu, select the language that the rule uses.

4. Select the **Event group** and **Event type** that trigger this response.

5. Next to **Status**, select **Enabled** or **Disabled**. The default is Enabled.

6. Click **Next**.

**Set filters for the rule**
To limit the events that can trigger the response, set the filters for the response rule on the Filters page of the Response Builder.

**Task**

1. From the **Available Properties** list, select a property and specify the value to filter the response result.
   
   Available Properties depend on the event type and event group selected on the Description page.

2. Click **Next**.

**Set Aggregation and grouping criteria for the rule**
Define when events trigger a rule on the Aggregation page of the Response Builder.

A rule's thresholds are a combination of aggregation, throttling, and grouping.
Task

1. Next to **Aggregation**, select an aggregation level.
   - To trigger the response for every event, select **Trigger this response for every event**.
   - To trigger the event after multiple events occur, perform these steps.
     1. Select **Trigger this response if multiple events occur within**, then define the amount of time in seconds, minutes, hours, or days.
     2. Select the aggregations conditions.
        - **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.
          For example, you can set the response to occur when an instance of the selected event property exceeds 300, or when the number of events exceeds 3,000, whichever threshold is crossed first.

2. Next to **Grouping**, select whether to group the aggregated events. If you do, specify the property of the event on which they are grouped.

3. As needed, next to **Throttling**, select **At most, trigger this response once every** and define an amount of time that must pass before this rule can send another notification message.
   - The amount of time can be defined in minutes, hours, or days.

4. Click **Next**.

**Configure the actions for an automatic response rule**
Configure the responses triggered by the rule on the Actions page of the Response Builder.
Configure multiple actions by using the + and - buttons next to the drop-down list for the type of notification.

**Task**

1. Configure each action that occurs as part of the response.
   - After configuring the options for an action, click **Next** if finished, or click + to add another action.
     - To send an email as part of the response, select **Send Email** from the drop-down list.
       1. Next to **Recipients**, click ... and select the recipients for the message. This list of available recipients is taken from Contacts (Menu | User Management | Contacts). Or, you can manually type email addresses, separated by a comma.
       2. Select the importance of the email.
       3. Type the **Subject** of the message or insert any of the available variables directly into the subject.
       4. Type any text that you want to appear in the body of the message or insert any of the available variables directly into the body.
To send an SNMP trap, select **Send SNMP Trap** from the drop-down list.

1. Select an SNMP server from the drop-down list.
2. Select the value types that you want to send in the SNMP trap. Some events do not include all information specified. If a selection you made is not represented, the information was not available in the event file.

To run an external command, select **Run External Command** from the drop-down list.

1. Select the Registered Executables and type any arguments for the command.

To create an issue, select **Create issue** from the drop-down list.

1. Select the type of issue that you want to create.
2. Type a unique name and any notes for the issue or insert any of the available variables directly into the name and description.
3. Select the **State**, **Priority**, **Severity**, and **Resolution** for the issue from the respective drop-down list.
4. Type the name of the assignee in the text box.
5. Click **Next** if finished, or click + to add another notification.

To run a scheduled task, select **Execute Server Task** from the drop-down list.

1. Select the task that you want to run from the **Task to execute** drop-down list.
2. Click **Next** if finished, or click + to add another notification.

2. On the Summary page, verify the information, then click **Save**.

The new rule appears in the Responses list.

---

**Actions page (Response Builder)**

Specify one or more actions to take in response to an event. The event type you specified in the Description page of the Response Builder determines available actions. You can specify multiple actions to take by clicking +. Each action must be configured using the action options defined in the table.

**Create Issue action**

**Table 14-1 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create issue of the type</td>
<td>Select the type of issue that you want to create.</td>
</tr>
<tr>
<td>Name</td>
<td>Type a name for the issue.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description for the issue.</td>
</tr>
<tr>
<td>State</td>
<td>Select a state from the list.</td>
</tr>
</tbody>
</table>

Using the Insert variable lists you can insert variables in the email with descriptions of the event.

---

Automatic response rules do not have a dependency order.
Table 14-1 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Select a priority from lowest to highest from the list.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select a severity from lowest to highest from the list.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Select a resolution from the list.</td>
</tr>
<tr>
<td>Assignee</td>
<td>Type the email of the assignee of the issue.</td>
</tr>
</tbody>
</table>

Execute Server Task action

Table 14-2 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task to execute</td>
<td>Select the task that you want to occur when this response is triggered.</td>
</tr>
</tbody>
</table>

Run External Command action

Table 14-3 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered executable</td>
<td>Select the registered executable that you want to run when this response is triggered. Create the registered executable before adding it to this response action.</td>
</tr>
<tr>
<td>Arguments</td>
<td>Type arguments into the Arguments field.</td>
</tr>
</tbody>
</table>

| Note | Make sure you use the correct syntax for your executable. |

Send System Command action

Table 14-4 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Tag</td>
<td>Runs the system command to assign tags based on the following:</td>
</tr>
<tr>
<td>• Server</td>
<td>Applies the tag on all managed servers.</td>
</tr>
<tr>
<td>• Workstation</td>
<td>Applies the tag on all managed workstations.</td>
</tr>
<tr>
<td>Assign Policy</td>
<td>Runs the system command to assign a policy based on the following:</td>
</tr>
<tr>
<td>• Product</td>
<td>The product selected.</td>
</tr>
<tr>
<td>• Category</td>
<td>The category selected.</td>
</tr>
<tr>
<td>• Policy</td>
<td>Assigns the policy by resetting the policy inheritance and using the product and category configured, or breaking the policy inheritance and using the policy selected from the drop-down list.</td>
</tr>
<tr>
<td>Clear Tag</td>
<td>Runs the system command to remove the following tags:</td>
</tr>
<tr>
<td>• Server</td>
<td>Managed server tags.</td>
</tr>
<tr>
<td>• Workstation</td>
<td>Managed workstation tags.</td>
</tr>
<tr>
<td>• Clear all</td>
<td>All tags.</td>
</tr>
<tr>
<td>Delete Systems</td>
<td>Runs the system command to remove agents and delete systems from management.</td>
</tr>
</tbody>
</table>
Table 14-4  Option definitions *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy McAfee Agent</td>
<td>Runs the system command to deploy the McAfee Agent using the following:</td>
</tr>
<tr>
<td></td>
<td>• Abort after — Specifies the number of minutes before canceling the attempt.</td>
</tr>
<tr>
<td></td>
<td>• Agent version — Specifies the version of the agent to send and install on the selected systems. Agent versions available depend on which agent installation packages are checked in to the Master Repository.</td>
</tr>
<tr>
<td></td>
<td>• Credentials for agent installation — Specifies the domain name, user name, and password of the user account with which to install the agent on selected systems.</td>
</tr>
<tr>
<td></td>
<td>• Installation options — Specifies the systems to deploy the McAfee Agent to based on the following:</td>
</tr>
<tr>
<td></td>
<td>• Install only on systems that do not have an agent — Sends the agent installation package only to systems without an agent installed. When deselected, sends the agent installation package to all selected systems, regardless of whether the agent is already installed on them.</td>
</tr>
<tr>
<td></td>
<td>• Force installation over existing version — Replaces existing agents within the selected group with the selected versions. This option is not available when you select Install only on systems that do not have an agent.</td>
</tr>
<tr>
<td></td>
<td>• Installation path — Specifies the path on the client system (default is <code>&lt;system_drive&gt;\McAfee\Common Framework</code>) where you want to install the agent. The location you specify must exist on managed systems.</td>
</tr>
<tr>
<td></td>
<td>• Number of attempts — Specifies the number of attempts before canceling the attempt.</td>
</tr>
<tr>
<td></td>
<td>• Push Agent using — Specifies the Agent Handler to use based on the following selection:</td>
</tr>
<tr>
<td></td>
<td>• Using the selected Agent Handler from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• Using all Agent Handlers</td>
</tr>
<tr>
<td></td>
<td>• Retry interval — Specifies the number of seconds between attempts to install the agent.</td>
</tr>
</tbody>
</table>
Table 14-4  Option definitions *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deploy McAfee Agent</strong></td>
<td>Runs the system command to deploy the McAfee Agent using the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Abort after</strong> — Specifies the number of minutes before canceling the attempt.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Agent version</strong> — Specifies the version of the agent to send and install on the selected systems. Agent versions available depend on which agent installation packages are checked in to the Master Repository.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Credentials for agent installation</strong> — Specifies the domain name, user name, and password of the user account with which to install the agent on selected systems.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Installation options</strong> — Specifies the systems to deploy the McAfee Agent to based on the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Install only on systems that do not have an agent</strong> — Sends the agent installation package only to systems without an agent installed. When deselected, sends the agent installation package to all selected systems, regardless of whether the agent is already installed on them.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force installation over existing version</strong> — Replaces existing agents within the selected group with the selected versions. This option is not available when you select <strong>Install only on systems that do not have an agent</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Installation path</strong> — Specifies the path on the client system (default is <code>&lt;system_drive&gt;\McAfee\Common Framework</code>) where you want to install the agent. The location you specify must exist on managed systems.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Number of attempts</strong> — Specifies the number of attempts before canceling the attempt.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Push Agent using</strong> — Specifies the Agent Handler to use based on the following selection:</td>
</tr>
<tr>
<td></td>
<td>• Using the selected Agent Handler from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• Using all Agent Handlers</td>
</tr>
<tr>
<td></td>
<td>• <strong>Retry interval</strong> — Specifies the number of seconds between attempts to install the agent.</td>
</tr>
<tr>
<td><strong>Exclude Tag</strong></td>
<td>Runs the system command to exclude server and workstation tags.</td>
</tr>
<tr>
<td><strong>Move Systems</strong></td>
<td>Runs the system command to move managed systems using the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>System Tree group</strong> — Browse to the group to move.</td>
</tr>
<tr>
<td></td>
<td>• When these systems are moved to the new location — Specify the System Tree sorting using the following:</td>
</tr>
<tr>
<td></td>
<td>• Disable System Tree sorting on these systems.</td>
</tr>
<tr>
<td></td>
<td>• Enable System Tree sorting on these systems.</td>
</tr>
<tr>
<td></td>
<td>• Do not change the System Tree sorting status for any of these systems.</td>
</tr>
<tr>
<td><strong>Resort Systems</strong></td>
<td>Runs the system command to resort the managed systems.</td>
</tr>
</tbody>
</table>
### Table 14-4  Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Run Client Task Now</strong></td>
<td>Runs the system command to run a client task using the following:</td>
</tr>
<tr>
<td></td>
<td>• Abort after — Specifies the number of minutes before canceling the task.</td>
</tr>
<tr>
<td></td>
<td>• Connect Using — Specifies the handler to use for the task.</td>
</tr>
<tr>
<td></td>
<td>• Number of attempts — Specifies the number of attempts before canceling the task.</td>
</tr>
<tr>
<td></td>
<td>• Product — The product selected.</td>
</tr>
<tr>
<td></td>
<td>• Randomization — Specifies the randomization intervals, in minutes, to mitigate the bandwidth impact.</td>
</tr>
<tr>
<td></td>
<td>• Retry interval — Specifies the number of seconds between attempts to run the task.</td>
</tr>
<tr>
<td></td>
<td>• Stop Task on the Client After — Specifies the number of minutes before the attempt to run the task is canceled.</td>
</tr>
<tr>
<td></td>
<td>• Task — Select the task from the list.</td>
</tr>
<tr>
<td></td>
<td>• Task Type — Select the task type from the list.</td>
</tr>
<tr>
<td><strong>Sensor Blacklist Management</strong></td>
<td>Runs the system command to add or remove sensors from the blacklist.</td>
</tr>
<tr>
<td><strong>Set User Properties</strong></td>
<td>Runs the system command to set the description.</td>
</tr>
<tr>
<td><strong>Transfer Systems</strong></td>
<td>Runs the system command to transfer systems between McAfee ePO servers.</td>
</tr>
<tr>
<td><strong>Wake Up Agents</strong></td>
<td>Runs the system command to wake up agents using the following:</td>
</tr>
<tr>
<td></td>
<td>• Abort after — Specifies the number of minutes or hours before canceling the wake-up attempt.</td>
</tr>
<tr>
<td></td>
<td>• Force complete policy and task update — Forces policy and task updates during the agent wake-up.</td>
</tr>
<tr>
<td></td>
<td>• Get full product properties in addition to system properties — Select to retrieve all agent properties. Otherwise, only minimal product properties and system properties are sent.</td>
</tr>
<tr>
<td></td>
<td>• Number of attempts — Specifies the number of attempts before canceling the agent wake-up.</td>
</tr>
<tr>
<td></td>
<td>• Randomization — Specifies the randomization intervals, in minutes, to mitigate the bandwidth impact.</td>
</tr>
<tr>
<td></td>
<td>• Retry interval — Specifies the amount of time between attempts to run the wake-up task. The interval can be provided in seconds, minutes, and hours.</td>
</tr>
<tr>
<td></td>
<td>• Wake up Agent using — Specifies the Agent Handler to use based on the following selection:</td>
</tr>
<tr>
<td></td>
<td>• Using the last connected Agent Handler</td>
</tr>
<tr>
<td></td>
<td>• Using all Agent Handlers</td>
</tr>
<tr>
<td></td>
<td>• Wake-up call type — Specifies the call type as either:</td>
</tr>
<tr>
<td></td>
<td>• Agent Wake-Up Call</td>
</tr>
<tr>
<td></td>
<td>• SuperAgent Wake-Up Call</td>
</tr>
</tbody>
</table>
### Send Email action

**Table 14-5  Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients</td>
<td>Enter or select the recipient of the event email.</td>
</tr>
<tr>
<td>Importance</td>
<td>Select the importance of the email.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject that appears in the event email. Using the Insert variable lists, you can insert variables in the email with descriptions of the event.</td>
</tr>
<tr>
<td>Body</td>
<td>Enter the text that appears in the event email. Using the Insert variable lists, you can insert variables in the email with descriptions of the event.</td>
</tr>
</tbody>
</table>

### Send SNMP trap action

**Table 14-6  Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Servers</td>
<td>Select an SNMP server from the preconfigured list. Using the Insert variable lists, you can insert variables in the email with descriptions of the event.</td>
</tr>
<tr>
<td>Available Types</td>
<td>Select the SNMP trap type value to send using the &gt;&gt; button to move it to the Selected Types list.</td>
</tr>
</tbody>
</table>

Before using this feature, add your SNMP servers to Automatic Responses, and import the .mib files.
Aggregation page (Response Builder)

Use the Aggregation page of the Response Builder to specify how many times you want the response to be triggered by the event, and whether you want to group the events using a specific filter.

Table 14-7  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation</td>
<td>Specifies how many events must occur before the response is triggered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trigger this response for every event</strong> — The response occurs every time the event occurs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trigger this response if multiple events occur within</strong> — The response is triggered only when the event occurs more than once within the specified time period. The time period can be specified in seconds, minutes, hours, or days. Optionally, you can also select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>When the number of distinct values for an event property is at least a certain value</strong> — If you want the response triggered only when a distinct event property occurs a minimum number of times, you can use this option to specify the event property and the number of events that must occur before the response is triggered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>When the number of events is at least</strong> — If you want the response triggered only when multiple events occur, you can use this option to specify the minimum number of events that must occur before the response is triggered.</td>
</tr>
<tr>
<td>Grouping</td>
<td>When multiple events are aggregated, this option allows you to specify whether to group the events, and if so, what criteria to use.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do not group aggregated events</strong> — Aggregated events are not grouped according to any specific criteria.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Group aggregated events by</strong> — Specifies that you want to group aggregated events, and set the criteria by which to group them.</td>
</tr>
<tr>
<td>Throttling</td>
<td>Specifies how often this response is triggered. The shorter the interval, the more often responses to this event are generated. Set this interval based on the event this rule is in response to. For example, in an outbreak scenario, an interval set too long might allow an outbreak to spread before a response is triggered, but setting it too short could overwhelm your server with response events.</td>
</tr>
</tbody>
</table>

Automatic Responses page

Create, edit, view, or delete automatic responses for specific types of events.

Not all McAfee products have or support events. Check your product documentation for information about events and automatic responses.

If a response status displays Invalid, the associated product extension might have been uninstalled, or the user might not have permissions to the response.

Table 14-8  Option definitions

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>New Response</td>
<td>Opens the Response Builder where you can create a response.</td>
</tr>
<tr>
<td>actions</td>
<td>Import Responses</td>
<td>Opens the Import Response Details page where you can import a previously exported response rule .xml file.</td>
</tr>
<tr>
<td>Filter</td>
<td>Show Filter/Hide Filter</td>
<td>Shows or hides the filter options used to filter the displayed responses.</td>
</tr>
<tr>
<td>options</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 14-8 Option definitions (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preset</td>
<td>Filter the displayed responses. The McAfee products that you have installed determine the selections in this list. These filters are included by default:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• All — Displays all responses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ePO Notification Events — Displays only those responses for McAfee ePO notification events.</td>
<td></td>
</tr>
<tr>
<td>Quick Find</td>
<td>To filter the displayed responses to the search results, enter a search term. Click <strong>Apply</strong> to perform the search.</td>
<td></td>
</tr>
<tr>
<td>Clear</td>
<td>Removes all filter settings.</td>
<td></td>
</tr>
<tr>
<td>Show selected rows</td>
<td>Select to restrict the displayed list of responses to only selected responses.</td>
<td></td>
</tr>
<tr>
<td>Actions column</td>
<td><strong>View</strong></td>
<td>Opens the Response details page where you can review the details of the selected response.</td>
</tr>
<tr>
<td></td>
<td><strong>Edit</strong></td>
<td>Opens the Response Builder where you can edit the response.</td>
</tr>
<tr>
<td></td>
<td><strong>Duplicate</strong></td>
<td>Creates a copy of the selected response.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
<td>Deletes the selected response.</td>
</tr>
<tr>
<td></td>
<td><strong>Disable Responses</strong></td>
<td>Disables the selected responses.</td>
</tr>
<tr>
<td></td>
<td><strong>Duplicate</strong></td>
<td>Creates a copy of the selected response.</td>
</tr>
<tr>
<td></td>
<td><strong>Edit</strong></td>
<td>Opens the Response Builder where you can edit the response.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable Responses</strong></td>
<td>Enables the selected responses.</td>
</tr>
<tr>
<td></td>
<td><strong>Export Responses</strong></td>
<td>Downloads the selected response as an .xml file.</td>
</tr>
<tr>
<td></td>
<td><strong>Export Table</strong></td>
<td>Opens the Export page where you can specify the format and details about how to download your responses.</td>
</tr>
<tr>
<td></td>
<td><strong>View</strong></td>
<td>Opens the Response details page where you can review the details of the selected response.</td>
</tr>
</tbody>
</table>
Description page (Automatic Response Builder)

Use the Description page of the Response Builder to specify a name, a description, event group and type, and status for an automatic response.

Table 14-9 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Allows you to type a description of this response.</td>
</tr>
<tr>
<td>Event</td>
<td>Specifies information about the event that triggers this automatic response. Event groups and their event types include:</td>
</tr>
<tr>
<td></td>
<td>• Examples of server events include: Active directory synchronization failed (or succeeded); or Repository pull succeeded (or failed).</td>
</tr>
<tr>
<td></td>
<td>• An example of a threat event is: Virus detected.</td>
</tr>
<tr>
<td></td>
<td>• An example of a client event is: Product update succeeded (or failed).</td>
</tr>
<tr>
<td></td>
<td>Event groups are not necessarily a part of every product. Check the product documentation for information about events and automatic responses.</td>
</tr>
<tr>
<td>McAfee ePO Notification Events</td>
<td>Specifies the available McAfee ePO notification event types, including:</td>
</tr>
<tr>
<td></td>
<td>• Client — Events that occur on managed systems. For example, &quot;Product update succeeded.&quot;</td>
</tr>
<tr>
<td></td>
<td>• Server — Events that occur on the McAfee ePO server. For example, &quot;Repository pull failed.&quot;</td>
</tr>
<tr>
<td></td>
<td>• Threat — Events that indicate a possible threat are detected. For example, &quot;Virus detected.&quot;</td>
</tr>
<tr>
<td>Language</td>
<td>Allows you to select the language of response from the list.</td>
</tr>
<tr>
<td>Name</td>
<td>Allows you to type a name for the response. Spaces, underscores, and special characters are allowed.</td>
</tr>
<tr>
<td>Status</td>
<td>Allows you to select whether the response is enabled or disabled. The default is Enabled.</td>
</tr>
</tbody>
</table>

Edit Email Server page

Configure the email server that ePolicy Orchestrator Cloud uses to send automatic email messages from the cloud to selected individuals.

Table 14-10 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Specifies the credentials required to authenticate to the email server.</td>
</tr>
<tr>
<td>From address</td>
<td>Specifies the email address that appears in the From text box in email messages that are sent from the ePolicy Orchestrator Cloud server.</td>
</tr>
<tr>
<td>SMTP server name</td>
<td>Specifies the IP address or name of the SMTP server.</td>
</tr>
<tr>
<td>SMTP server port</td>
<td>Specifies the port number used to communicate with the SMTP server.</td>
</tr>
</tbody>
</table>
## Edit Event Filtering page

Use this page to specify which events are forwarded to the McAfee ePO server.

### Table 14-11 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The agent forwards</strong></td>
<td>Specifies, globally, which events the agent processes and forwards to the McAfee ePO server. Options include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>All events to the server</strong> — Process and forward all events to the server.</td>
</tr>
<tr>
<td></td>
<td>To <em>individually</em> select the server or servers to receive the events, select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store in ePO</strong>—Stores the event in the McAfee ePO database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store in SIEM</strong>—Stores the event in the SIEM database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store in both</strong>—Stores the event in McAfee ePO and SIEM databases.</td>
</tr>
<tr>
<td></td>
<td>To <em>globally</em> select the server or servers to receive the events, select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store selected in ePO</strong>—Store all selected events in McAfee ePO database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store selected in SIEM</strong>—Store all selected events in SIEM database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store selected in both</strong>—Store all selected events in McAfee ePO and SIEM databases. The default setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Select All</strong> and <strong>Deselect All</strong> are disabled when you select <strong>All events to the server</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Only selected events to the server</strong> — Process and forward only those events selected from the list of available events.</td>
</tr>
<tr>
<td></td>
<td>To <em>individually</em> select the server or servers to receive the individual events, select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store in ePO</strong>—Stores the event in the McAfee ePO database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store in SIEM</strong>—Stores the event in the SIEM database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store in both</strong>—Stores the event in McAfee ePO and SIEM databases.</td>
</tr>
<tr>
<td></td>
<td>To <em>globally</em> select the server or servers to receive the individually selected events, select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store selected in ePO</strong>—Store all selected events in McAfee ePO database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store selected in SIEM</strong>—Store all selected events in SIEM database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Store selected in both</strong>—Store all selected events in McAfee ePO and SIEM databases. The default setting.</td>
</tr>
<tr>
<td></td>
<td><strong>You can use Select All and Deselect All, with Only selected events to the server, to select or deselect the all event checkboxes.</strong></td>
</tr>
<tr>
<td></td>
<td>These settings do not take effect until the next agent-server communication.</td>
</tr>
</tbody>
</table>

| **The server accepts**        | Specifies, globally, events accepted by the McAfee ePO server. Options include:                                                          |
|                               | • **Events from any source** — All events sent by any agent are process by the McAfee ePO server. The default setting.                   |
|                               | • **Events that were generated by the sending agent** — The McAfee ePO server processes only those events sent by the source agent.    |
**Edit Event Notifications page**

Use this page to specify the startup of Notification Events, and the interval between the Notifications to check for new events.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation Interval</td>
<td>Specifies how often you want McAfee ePO Notification Events to be sent to Automatic Responses.</td>
</tr>
</tbody>
</table>

**Edit Response Configuration page**

Use this page to configure the ePolicy Orchestrator Cloud response server settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Specifies how often you want ePolicy Orchestrator Cloud to check for new notifications.</td>
</tr>
<tr>
<td>Startup Delay</td>
<td>Specifies how long ePolicy Orchestrator Cloud should wait after startup before processing events.</td>
</tr>
</tbody>
</table>

**Filter page (Response Builder)**

Use the Filter page of the Response Builder to specify the criteria to use for filtering events.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Properties</td>
<td>Properties that can be selected and configured as criteria to narrow the response results. Available properties depend on the event type and event group selected on the Description page.</td>
</tr>
<tr>
<td>Property</td>
<td>Lists the name of the property being used to specify selection criteria.</td>
</tr>
<tr>
<td>Comparison</td>
<td>Lists comparison operators you can select from the drop-down list.</td>
</tr>
<tr>
<td>Value</td>
<td>Type or select a value from the list to use for system selection.</td>
</tr>
<tr>
<td>+</td>
<td>Adds another entry for the same property for which you can specify an AND or OR logical operator.</td>
</tr>
<tr>
<td>-</td>
<td>Removes an entry for a property.</td>
</tr>
</tbody>
</table>

**Import Response Rules page**

Review the rules and their details, and choose whether they are enabled before importing. Rules are displayed in the pane on the left, details on the right. Click each rule to review the details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name defined for this rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies any details provided about this rule.</td>
</tr>
<tr>
<td>Language</td>
<td>Specifies the language of the interface used when creating this rule.</td>
</tr>
<tr>
<td>Event</td>
<td>Specifies the Event group and Event type categories that trigger this rule.</td>
</tr>
</tbody>
</table>
Table 14-15  Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Specifies whether this rule was enabled or disabled when exported.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Specifies whether this rule triggers an event at every occurrence, or after a user-defined number of occurrences. Aggregation can be used to reduce the amount of bandwidth consumed by a particular response rule.</td>
</tr>
<tr>
<td>Grouping</td>
<td>Specifies whether events of this type, when aggregated, are grouped. You can specify criteria for grouping events.</td>
</tr>
<tr>
<td>Throttling</td>
<td>Specifies how often this response is triggered. The shorter the interval, the more often the responses to this event are generated.</td>
</tr>
<tr>
<td>Actions</td>
<td>Specifies which actions are defined for this response rule.</td>
</tr>
<tr>
<td>Enable response rule</td>
<td>Specifies whether this rule is enabled when imported into your server.</td>
</tr>
</tbody>
</table>

Import Response Rule page

Use this page to import a previously exported response rule. The default format of the exported response rule file is `Rule_<ResponseRuleName>.xml`.

Response Details page

Use this page to view response details.

Table 14-16  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the response.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description of the selected response.</td>
</tr>
<tr>
<td>Event</td>
<td>Specifies the event group and the event type for which response is generated.</td>
</tr>
<tr>
<td>Actions</td>
<td>Specifies the actions you can take in response to an event.</td>
</tr>
</tbody>
</table>

Table 14-17  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Specifies the actions you can take in response to an event.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Specifies how many events must occur before the response is triggered.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description of the selected response.</td>
</tr>
<tr>
<td>Event</td>
<td>Specifies the event group and the event type for which response is generated.</td>
</tr>
<tr>
<td>Grouping</td>
<td>Specifies the criteria on which the aggregated multiple events are grouped.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the response.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies whether the response is enabled or disabled.</td>
</tr>
<tr>
<td>Throttling</td>
<td>Specifies how often this response is triggered.</td>
</tr>
</tbody>
</table>
Summary page (Response Builder)

Allows you to review the information for the automatic response to an event.

Click Save to save the settings, or Back to make additional changes.

Client Events page

Use this page to check for client events for the selected system.

Table 14-18 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Options</td>
<td>Shows or hides the following options used to filter which entries to display based on predefined criteria, including:</td>
</tr>
<tr>
<td></td>
<td>• Show selected rows — Select this box to display only the rows you have selected.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Unique identifier of the event.</td>
</tr>
<tr>
<td>Event Type</td>
<td>The type of the event.</td>
</tr>
<tr>
<td>Event Received Time</td>
<td>Time when the event was received by the McAfee ePO Cloud server.</td>
</tr>
<tr>
<td>Product Name</td>
<td>The product associated with the client event.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the product.</td>
</tr>
<tr>
<td>Actions</td>
<td>Specifies the actions that you can perform on the selected events, including:</td>
</tr>
<tr>
<td></td>
<td>• Choose Columns — Opens the Select the Columns to Display page. Use this to select which columns of data to display on the Threat Event Log page.</td>
</tr>
<tr>
<td></td>
<td>• Delete — Deletes the selected event.</td>
</tr>
<tr>
<td></td>
<td>• Export — Opens the Export page. From the Export page, you can specify the format of the files to be exported, how they are packaged, and what to do with them. For example, files could be exported in .pdf format, packaged into a .zip file, and mailed to an administrator as an email attachment.</td>
</tr>
<tr>
<td></td>
<td>• Show Related Systems — Takes you to a page where you can view and take action on the systems where selected events occurred.</td>
</tr>
</tbody>
</table>
Manage registered executables and external commands

The registered executables you configure are run when the conditions of a rule are met. Automatic Responses trigger the registered executable commands to run.

You can run registered executable commands only on console applications.

Task

1. Select Menu | Configuration | Registered Executables.
2. Select one of these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a registered executable</td>
<td>1. Click Actions</td>
</tr>
<tr>
<td></td>
<td>2. Type a name for the registered executable.</td>
</tr>
<tr>
<td></td>
<td>3. Type the path and select the registered executable that you want a rule to execute when triggered.</td>
</tr>
<tr>
<td></td>
<td>4. Modify the user credentials, if needed.</td>
</tr>
<tr>
<td></td>
<td>5. Test the executable and confirm that it worked using the Audit Log.</td>
</tr>
<tr>
<td></td>
<td>6. Click Save.</td>
</tr>
<tr>
<td></td>
<td>The new registered executable appears in the Registered Executables list.</td>
</tr>
</tbody>
</table>

| Edit a registered executable  | 1. Find the registered executable to edit in the Registered Executable page, then click Edit. |
|                               | 2. Change the information as needed and click Save.                   |

| Duplicate a registered executable | 1. Find the registered executable to duplicate in the Registered Executable page, then click Duplicate. |
|                                   | 2. Type a name for the registered executable, then click OK.           |
|                                   | The duplicated registered executable appears in the Registered Executables list. |

| Delete a registered executable   | 1. Find the registered executable to delete in the Registered Executable page, then click Delete. |
|                               | 2. When prompted, click OK.                                           |
|                               | The deleted registered executable no longer appears in the Registered Executables list. |
Manage registered executables and external commands
Agent-server communication

Client systems use the McAfee Agent and agent-server communications to communicate with your McAfee ePO server. For version-specific information about your agents, see the McAfee Agent Product Guide.

Contents
- How agent-server communication works
- Best practices: Estimating and adjusting the ASCI
- Managing agent-server communication
- Agent Deployment Settings page

How agent-server communication works
McAfee Agent communicates with the McAfee ePO server periodically using agent-server communication to send events and ensure that all settings are up to date.

During each agent-server communication, the McAfee Agent collects its current system properties, and events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the McAfee Agent, and the repository list if it has changed since the last agent-server communication.

See the McAfee Agent Product Guide for details about:
- How agent-server communication works
- How SuperAgents work to use bandwidth and McAfee ePO performance
- Collect McAfee Agent statistics
- Queries provided by the McAfee Agent

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

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

To determine whether to change your ASCI, ask how often changes occur to endpoint policies on your McAfee ePO server. For most organizations, once your policies are in place, they don't often change. Some organizations change an endpoint policy less frequently than once every few months. That means a system
calling in every 60 minutes looking for a policy change, about eight times in a typical work day, might be excessive. If the agent does not find any new policies to download, it waits until the next agent-server communication, then checks again at its next scheduled check-in time.

To estimate the ASCI, your concern is not wasting bandwidth because agent-server communications are only a few kilobytes per communication. The concern is the strain put on the McAfee ePO server with every communication from every agent in larger environments. All your agents need at least two communications a day with the McAfee ePO server. This requires a 180–240 minute ASCI in most organizations.

For organizations with fewer than 10,000 nodes, the default ASCI setting is not a concern at 60 minutes. But for organizations with more than 10,000 nodes, change the default setting of 60 minutes setting to about 3–4 hours.

For organizations with more than 60,000 nodes, the ASCI setting is much more important. If your McAfee ePO server is not having performance issues, you can use the 4-hour ASCI interval. If there are any performance issues, consider increasing your ASCI to 6 hours; possibly even longer. This change significantly reduces the number of agents that are simultaneously connecting to the McAfee ePO server and improves the server performance.

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

This table lists basic ASCI guidelines.

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

**Configure the ASCI setting: best practice**

After you estimate the best ASCI setting, reconfigure the setting in the McAfee ePO server.

The ASCI is set to 60 minutes by default. If that interval is too frequent for your organization, change it.

**Task**

1. Select **Menu | Policy | Policy Catalog**, then select **McAfee Agent** from the **Product** list and **General** from the **Category** list.

2. Click the name of the policy you want to change and the **General** tab.

3. Next to **Agent-to-server communication interval**, type the number of minutes between updates.
   
   This example shows the interval set to 60 minutes.

   **Click Save.**

   If you send a policy change or add a client task immediately, you can execute an agent wake-up call.
Allow agent deployment credentials to be cached

Administrators must provide credentials to successfully deploy agents from your McAfee ePO server to systems in your network. You can choose whether to allow agent deployment credentials to be cached for each user. Once a user's credentials are cached, that user can deploy agents without having to authenticate again. Credentials are cached per user, so a user who has not previously provided credentials can't deploy agents without providing their own credentials first.

**Task**

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

2. Select the checkbox to allow agent deployment credentials to be cached.

Change agent communication ports

You can change some of the ports used for agent communication on your McAfee ePO server. You can modify the settings for these agent communication ports:

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

**Task**

1. Select **Menu | Configuration | Server Settings**, select **Ports** from the **Setting Categories**, then click **Edit**.

2. Select whether to enable port 443 for agent-server communications, enter the ports to be used for agent wake-up calls and broadcasts, then click **Save**.

### Agent Deployment Settings page

Use this page to specify the deployment options for the McAfee Agent.

**Table 16-1 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent version</td>
<td>Specifies the version of the agent to deploy on the selected systems. Available agent versions depend on which agent installation packages are checked in to the master repository.</td>
</tr>
<tr>
<td>Credentials for agent installation</td>
<td>Specifies the domain name, user name, and password of the user account with which to install the agent on selected systems.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Installation path</td>
<td>Specifies the path on the client system (default is <code>&lt;system_drive&gt;\McAfee\Common Framework</code>) where you want to install the agent. The location you specify must exist on managed systems.</td>
</tr>
<tr>
<td>Installation options</td>
<td>• Install only on systems that do not have an agent managed by this McAfee ePO server — Sends the agent installation package only to systems without an installed agent managed by this McAfee ePO server. Be careful using this option if there are systems in your environment managed by another McAfee ePO server.</td>
</tr>
<tr>
<td></td>
<td>• Suppress agent installation user interface — Hides the installation of the agent from the end user.</td>
</tr>
<tr>
<td></td>
<td>• Force installation over existing version — Within the selected group, replaces existing agents with the selected versions. McAfee recommends using this option only when downgrading agents. This option is not available when you select Install only on systems that do not have an agent managed by this McAfee ePO server.</td>
</tr>
</tbody>
</table>
Automating and optimizing McAfee ePO workflow

You can create queries and tasks to automatically run for improved server performance, easier maintenance, and to monitor threats.

When you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change.

Contents

- Best practice: Find systems with the same GUID
- Best practices: Purging events automatically
- Best practice: Creating an automatic content pull and replication
- Best practices: Filtering 1051 and 1059 events
- Best practice: Finding systems that need a new agent
- Finding inactive systems: best practice
- Measuring malware events best practice
- Finding malware events per subnet: best practice
- Create an automatic compliance query and report best practice

Best practice: Find systems with the same GUID

You can use preconfigured server tasks that runs queries and targets systems that might have the same GUIDs. This task tells the agent to regenerate the GUID and fix the problem.

Task

1. Select Menu | Automation | Server Tasks to open the Server Tasks Builder.
2. Click Edit in the Actions column for one of the following preconfigured server tasks.
   - Duplicate Agent GUID - Clear error count
   - Duplicate Agent GUID - Remove systems that potentially use the same GUID
3. On the Description page, select Enabled, then click:
   - Save — Enable the server task and run it from the Server Task page.
   - Next — Schedule the server task to run at a specific time and perform the task.

This clears the error count and removes any systems with the same GUID, and assigns the systems a new GUID.
Best practices: Purging events automatically

Periodically purge the events that are sent daily to your McAfee ePO server. These events can eventually reduce performance of the McAfee ePO server and SQL Servers.

Events can be anything from a threat being detected, to an update completing successfully. In environments with a few hundred nodes, you can purge these events on a nightly basis. But in environments with thousands of nodes reporting to your McAfee ePO server, it is critical to delete these events as they become old. In these large environments, your database size directly impacts the performance of your McAfee ePO server, and you must have a clean database.

You must determine your event data retention rate. The retention rate can be from one month to an entire year. The retention rate for most organizations is about six months. For example, six months after your events occur, on schedule, they are deleted from your database.

McAfee ePO does not come with a preconfigured server task to purge task events. This means that many users never create a task to purge these events and, over time, the McAfee ePO server SQL database starts growing exponentially and is never cleaned.

Create a purge events server task best practice

Create an automated server task that deletes all events in the database that are older and no longer needed.

Some organizations have specific event retention policies or reporting requirements. Make sure that your purge event settings conform to those policies.

Task

1. To open the Server Task Builder dialog box, select Menu | Automation | Server Tasks, then click Actions | New Task.
2. Type a name for the task, for example Delete client events, add a description, then click Next.
3. On the Actions tab, configure these actions from the list:
   - Purge Audit Log — Purge after 6 months.
   - Purge Client Events — Purge after 6 months.
   - Purge Server Task Log — Purge after 6 months.
   - Purge Threat Event Log — Purge every day.
   - Purge SiteAdvisor Enterprise Events — Purge after 10 days.

   You can chain the actions all in one task so that you don’t have to create multiple tasks.

   This example purges SiteAdvisor Enterprise events because they are not included in the normal events table and require their own purge task. The SiteAdvisor Enterprise events are retained for only 10 days because they collect all URLs visited by managed systems. These events can save a large amount of data in environments with more than 10,000 systems. Therefore, this data is saved for a much shorter time compared to other event types.

4. Click Next and schedule the task to run every day during non-business hours.
5. Click the Summary tab, confirm that the server task settings are correct, then click Save.
Purge events by query

You can use a custom configured query as a base to delete client events.

**Before you begin**

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

There are reasons why you might need to purge data or events based on a query. For example, there can be many specific events overwhelming your database. In this example, you might not want to wait for the event to age out if you are keeping your events for six months. Instead you want that specific event deleted immediately or nightly.

Purging these events can significantly improve the performance of your McAfee ePO server and database.

Configure purging data based on the results of a query.

**Task**

1. Select **Menu | Automation | Server Tasks**, then click **Action | New Task** to open the Server Task Builder.

2. Type a name for the task, for example **Delete 1059 client events**, then on the **Actions tab**, click **Purge Client Events** from the Actions list.

3. Click **Purge by Query**, then select the custom query that you created.

   ![This menu is automatically populated when table queries are created for client events.]

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

**Best practice: Creating an automatic content pull and replication**

Pulling content daily from the public McAfee servers is a primary functions of your McAfee ePO server. Regularly pulling content keeps your protection signatures up to date for McAfee products.

Pulling the latest DAT and content files keeps your protection signatures up to date for McAfee products like VirusScan Enterprise and Host Intrusion Prevention.

The primary steps are:

1. Pull content from McAfee into your Master Repository, which is always the McAfee ePO server.

2. Replicate that content to your distributed repositories. This ensures that multiple copies of the content are available and remain synchronized. This also allows clients to update their content from their nearest repository.

The most important content are the DAT files for VirusScan Enterprise, released daily at approximately 3 p.m. Eastern Time (19:00 UTC or GMT).

Optionally, many users with larger environments choose to test their DAT files in their environment before deployment to all their systems.
Pull content automatically: best practice

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

You must schedule your pull tasks to run at least once a day after 3 p.m. Eastern Time (19:00 UTC or GMT). In the following example, the pull is scheduled for twice daily, and if there is a network problem at 5 p.m., the task occurs again at 6 p.m.. Some users like to pull their updates more frequently, as often as every 15 minutes. Pulling DATs frequently is aggressive and unnecessary because DAT files are typically released only once a day. Pulling two or three times a day is adequate.

![Testing your DAT files before deployment requires a predictable pull schedule.](image)

Task

1. Select **Menu | Automation | Server Tasks**, then click **Actions | New task**.
2. In the Server Task Builder dialog box, type a task name and click **Next**.
3. Specify which signatures to include in the pull task.
   a. In the Actions dialog box, from the Actions list, select **Repository Pull**, then click **Selected packages**.
   b. Select the signatures that apply to your environment.

   ![Best practice: When you create a pull task for content, select only the packages that apply to your environment instead of selecting All packages. This keeps the size of your Master Repository manageable. It also reduces the bandwidth used during the pull from the McAfee website and during replication to your distributed repositories.](image)

4. Click **Next**.
5. Schedule your pull task to run at least once a day after 3 p.m. Eastern Time, then click **Next**.
6. Click the **Summary** tab, confirm that the server task settings are correct, then click **Save**.

Now you have created a server task that automatically pulls the McAfee DAT files and content from the public McAfee servers.

Best practices: Filtering 1051 and 1059 events

1051 and 1059 events can make up 80 percent of the events stored in your database. If enabled, make sure that you periodically purge these events.

If you have not looked at Event Filtering on your McAfee ePO server in a long time, run the custom Event Summary Query and check the output.

The two most common events seen in customer environments are:
• 1051 — Unable to scan password-protected file
• 1059 — Scan timed out

These two events can be enabled on the McAfee ePO server. If you never disabled them, you might find a significant number of these events when you run the Event Summary Query. These two events can, for some users, make up 80 percent of the events in the database, use a tremendous amount of space, and impact the performance of the database.

The 1059 events indicate that a file was not scanned, but the user was given access. Disabling the 1059 event means that you lose visibility of a security risk.

So why are these events in there? These events have historic significance and go back several years and are meant to tell you that a file was not scanned by VirusScan Enterprise. This failure to scan the file might be due to one of two reasons:
• The scan timed out due to the size of the file, which is a 1059 event.
• It was inaccessible due to password protection or encryption on the file, which is a 1051 event.

Disable these two events under event filtering, to prevent a flood of these events into your database. By disabling these events, you are effectively telling the agent to stop sending these events to McAfee ePO.

VirusScan Enterprise still logs these events in the On-access scanner log file for reference on the local client.

Optionally, you can disable additional events, but this is not typically needed because most of the other events are important and are generated in manageable numbers. You can also enable additional events, as long as you monitor your event summary query to make sure that the new event you enabled does not overwhelm your database.

**Best practice: Filter 1051 and 1059 events**
Disable 1051 and 1059 events if you find a significant number of them when you run the Event Summary Query.
Task

1. Select Menu | Configuration | Server Settings, in the Setting Categories list select Event Filtering, then click Edit.

2. In The agents forwards list on the Edit Event Filtering page, scroll down until you see these events, then deselect them:
   - 1051: Unable to scan password protected (Medium)
   - 1059: Scan Timed Out (Medium)

   This figure shows the 1051 and 1059 events deselected on the Server Settings page.

3. Click Save.

Now these two events are no longer saved to the McAfee ePO server database when they are forwarded from the agents.

Best practice: Finding systems that need a new agent

If you suspect some of your managed systems might not have the same McAfee Agent installed, perform these tasks to find the systems with the older agent versions, then select those systems for a McAfee Agent upgrade.

Create an Agent Version Summary query best practice

Find systems with old McAfee Agent versions using a query to generate a list of all agent versions that are older than the current version.
Task

1. To duplicate the Agent Versions Summary query, select **Menu | Reporting | Queries & Reports**, then find the **Agent Versions Summary** query in the list.

2. In the Actions column of the Agent Versions Summary query, click **Duplicate**. In the Duplicate dialog box, change the name, select a group to receive the copy of the query, then click **OK**.

3. Navigate to the duplicate query that you created, then click **Edit** in the Actions column to display the preconfigured Query Builder.

4. In the Chart tab, in the **Display Results As** list, expand **List** and select **Table**.

5. To configure the Sort by fields, in the **Configure Chart: Table** page, select **Product Version (Agent)** under Agent Properties in the list, click **Value (Descending)**, then click **Next**.

6. In the Columns tab, remove all preconfigured columns except **System Name**, then click **Next**.

7. In the Filter tab, configure these columns, then click **Run**:
   a. For the Property column, select **Product Version (Agent)** from the Available Properties list.
   b. For the Comparison column, select **Less than**.
   c. For the Value column, type the current McAfee Agent version number.

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

**Update the McAfee Agents with a product deployment project best practice**

Update the old McAfee Agent versions found using an Agent Version Summary query and a Product Deployment task.

**Task**

1. Select **Menu | Software | Product Deployment**, then click **New Deployment**.

2. From the New Deployment page, configure these settings:
   a. Type a name and description for this deployment. This name appears on the **Product Deployment** page after the deployment is saved.
   b. Next to **Type**, select **Fixed**.
   c. Next to **Package**, select the McAfee Agent that you want installed on the systems. Select the language and repository branch (Evaluation, Current, or Previous) that you want to deploy from.
   d. Next to **Command line**, specify any command-line installation options. See the **McAfee Agent Product Guide** for information on command-line options.
In the **Select the systems** group, click **Select Systems**, and from the dialog box, click the **Queries** tab and configure these options, then click **OK**:

- Select the Agent Version Summary table query that you created.
- Select the system names displayed in the Systems list.

The Total field displays the number of systems selected.

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

3 Click **Save**.

The Product Deployment project starts running and allows you to monitor the deployment process and status.

---

**Finding inactive systems: best practice**

Most environments are changing constantly, new systems are added and old systems removed. These changes create inactive McAfee Agent systems that, if not deleted, can ultimately skew your compliance reports.

As systems are decommissioned, or disappear because of extended travel, users on leave, or other reasons, remove them from the System Tree. An example of a skewed report might be your DAT report on compliance. If you have systems in your System Tree that have not reported into the McAfee ePO server for 20 days, they appear as out of date by 20 days and ultimately skew your compliance reports.

**Initial troubleshooting**

Initially, when a system is not communicating with the McAfee ePO server, try these steps:

1 From the System Tree, select the system and click **Actions | Agents | Wake Up Agents**.

   **Configure a Retry interval of**, for example, 3 minutes.

2 To delete the device from McAfee ePO, but not remove the agent in the System Tree, select the system and click **Actions | Directory Management | Delete**. Do not select **Remove agent on next agent-server communication**.

3 Wait for the system to communicate with McAfee ePO again.

   **The system appears in the System Tree Lost and Found group.**

**Dealing with inactive systems**

You can create a query and report to filter out systems that have not communicated with the McAfee ePO server in X number of days. Or your query and report can delete or automatically move these systems.

It's more efficient to either delete or automatically move these inactive systems. Most organizations choose a deadline of between 14–30 days of no communication to delete or move systems. For example, if a system has not communicated with the McAfee ePO server after that deadline you can:

- Delete that system.
- Move that system to a group in your tree that you can designate as, for example, **Inactive Agents**.

A preconfigured Inactive Agent Cleanup Task exists, disabled by default, that you can edit and enable on your server.
Change the Inactive Agents query: best practice

If the default Inactive Agents query is not configured to match your needs, you can duplicate the query and use it as a base to create your custom query.

Deleting the inactive agents that have not communicated in last month is the default setting for the preconfigured Inactive Agents query. If you want to change the default timer setting, make a copy of the Inactive Agents query.

The instructions in this task describe how to create a copy of the existing Inactive Agents query to change the deadline to 2 weeks.

**Task**

1. To duplicate the Inactive Agents query, select **Menu | Reporting | Queries & Reports**, then find the Inactive Agents query in the list.

2. In the Actions column of the Inactive Agents query, click **Duplicate**.

3. In the Duplicate dialog box change the name, select a group to receive the copy of the query, then click **OK**.

4. Navigate to the duplicate query that you created and, in the Actions column, click **Edit** to display the preconfigured Query Builder.

5. To change the Filter tab settings from once a month to every two weeks, set the Last Communications property, *Is not within the last* comparison, to **2 Weeks** value.

   **Don't change the and Managed State property, Equals comparison, or the Managed value.**

6. Click **Save**.

Now your new Inactive Agents query is ready to run from a server task to delete systems with an inactive agent.

Delete inactive systems: best practice

Use the Inactive Agent Cleanup server task with the preconfigured query named Inactive Agents to automatically delete inactive systems.

**Before you begin**

You must have enabled or duplicated the Inactive Agents query.

Deleting a system from the System Tree deletes only the record for that system from the McAfee ePO database. If the system physically exists, it continues to perform normally with the last policies it received from the McAfee ePO server for its applicable products.

**Task**

1. To create a duplicate of the Inactive Agent Cleanup Task, select **Menu | Automation | Server Tasks**, then find the Inactive Agent Cleanup Task in the server tasks list.

2. Click the preconfigured Inactive Agent Cleanup Task, click **Actions | Duplicate**.

3. In the Duplicate dialog box, change the server task name, then click **OK**.

4. In the server task row you created, click **Edit** to display the Server Task Builder page.

5. From the Descriptions tab, type any needed notes, click **Enabled** in **Schedule status**, then click **Next**.
6 From the Actions tab, configure these settings:
   a From the Actions list, select Run Query,
   b For Query, click ... to open the Select a query from the list dialog box.
   c Click the group tab where you saved your copy of the Inactive Agents query, select your query, then click OK.
   d Select your language.
   e In Sub-Actions, select Delete Systems from the list.

   Do not click Remove agent. This setting causes McAfee ePO to delete the McAfee Agent from the inactive systems when they are removed from the System Tree. Without the agent installed, when the removed system reconnects to the network it cannot automatically start communicating with the McAfee ePO server and reinsert itself back into the System Tree.

   (Optional) Instead of using the default subaction Delete Systems, you can select Move Systems to another Group. This moves the systems found by the query to a designated group, for example, Inactive Systems in your System Tree.

7 Click Next, schedule when you want this server task to run, then save the server task.

Now any inactive systems are automatically removed from the McAfee ePO server, and your system compliance reports provide more accurate information.

Measuring malware events best practice

Counting malware events provides an overall view of attacks and threats being detected and stopped. With this information, you can gauge the health of your network over time and change it as needed.

Creating a query that counts total infected systems cleaned per week is the first step in creating a benchmark to test your network malware status. This query counts each system as a malware event occurs. It counts the system only once even if it generated thousands of events.

Once this query is created, you can:

- Add it as a dashboard to quickly monitor your network malware attacks.
- Create a report to provide history of your network status.
- Create an Automatic Response to notify you if a threshold of systems is affected by malware.

Create a query that counts systems cleaned per week best practice

Creating a query to count the number of systems cleaned per week is a good way to benchmark the overall status of your network.

Task

1 Select Menu | Reporting | Queries & Reports, then click Actions | New.
2 On the Query Wizard Result Types tab for the Feature Group, select Events, then in the Result Types pane, click Threat Events, then click Next.
3 On the Chart tab, in the Display Results As list, select Single Line Chart.
4 In the Configure Chart: Single Line Chart pane, configure these settings, then click Next:
   • In Time base is, select Event Generated Time.
   • In Time unit, select Week.
   • In Time Sequence is, select Oldest First.
   • In Line values are, select Number of.
   • Select Threat Target Host Name.
   • Click Show Total.

5 In the Columns tab, in the Available Columns list select these columns to display, then click Next:
   • Event Generated Time
   • Event Category
   • Threat Target Host Name
   • Threat Severity
   • Threat Target IPv4 Address
   • Threat Name

6 In the Filter tab, Available Properties list, configure this Required Criteria:
   • For Event Generated Time, select these settings from the Is within the last list, 3 and Months.
   • For Event Category, select these settings from the Belongs to list, Malware.
   • For Action Taken, select these settings from the lists Equals and Deleted.

7 Click Save to display the Save Query page, then configure these settings:
   • For Query Name, type a query name, for example, Total Infected Systems Cleaned Per Week.
   • For Query Description, type a description of what this query does.
   • For Query Group, click New Group, type the query group name, then click Public.

8 Click Save.

When you run this query, it returns the number of infected systems cleaned per week. This information provides a benchmark of the overall status of your network.

---

**Finding malware events per subnet: best practice**

Finding threats by subnet IP address shows you whether a certain group of users needs process changes or additional protection on your managed network.

For example, if you have four subnets, and only one subnet is continuously generating threat events, you can narrow down the cause of those threats. Perhaps users on that subnet have been sharing infected USB drives.

**Create a query to find malware events per subnet best practice**

Create a query to find malware events and sort them by subnet. This query helps you find networks in your environment that are under attack.
Task

1. To duplicate the existing Threat Event Descriptions in the Last 24 Hours query, select Menu | Reports | Queries & Reports, then find and select the Threat Target IP Address query in the list.

2. Click Actions | Duplicate and in the Duplicate dialog box, edit the name, select the group to receive the copy, then click OK.

3. In the Queries list, find the new query that you created and click Edit.

   The duplicated query is displayed in the Query Builder with the Chart tab selected.

4. In the Display Results As list, select Table under List.

5. In the Configure Chart: Table dialog box, select Threat Target IPv4 Address from the sort by list and Value (Descending), then click Next.

6. In the Columns tab, you can use the preselected columns.

   **Tip:** It might help to move the Threat Target IPv4 Address closer to the left of the table, then click Next.

   Don't change the default Filter tab settings.

7. Click the Summary tab, confirm that the query settings are correct, then click Save.

8. In the Queries list, find the query that you created, then click Run.

   Now you have a query to find malware events and sort them by IP subnet address.

---

Create an automatic compliance query and report best practice

You can create a compliance query and report to find which of your managed systems meet specific criteria. For example, you can find systems that don't have the latest DATs or have not contacted the McAfee ePO server in over 30 days.

To find this important information automatically, use these tasks.

**Tasks**

- **Create a server task to run compliance queries best practice on page 218**
  You must create a server task to run your compliance queries weekly to automate generating your managed systems' compliance report.

- **Create a report to include query output best practice on page 220**
  Once you have the query data saved, you must create a report to contain the information from the queries you ran before you can send it to the administrator team.

- **Create a server task to run and deliver a report: best practice on page 220**
  You must create a server task to automatically run the report and send the compliance report to your administrators.

---

**Create a server task to run compliance queries best practice**

You must create a server task to run your compliance queries weekly to automate generating your managed systems' compliance report.

Follow these steps to create a server task that runs your compliance queries every Sunday morning at 2:00 a.m. Running the queries on Sunday morning allows you to run the report on Monday morning at 5:00 a.m. and deliver it by email to the administrators.
Task

1. Select Menu | Automation | Server Tasks, then click Actions | New Task.

2. In the Server Task Builder:
   a. In the Descriptions tab, type a name and notes.
   b. In the Schedule status, click Enabled.
   c. Click Next.

3. In the Actions tab, configure these settings.
   a. In the Actions list, select Run Query and configure these settings:
      • For Query, select VSE: Compliance Over the Last 30 Days.
      • Select your language.
      • For Sub-Actions, select Export to File then click OK.
      • For C:\reports\, type a valid file name.
      • For If file exists, select Overwrite.
      • For Export, select Chart data only.
      • For Format, select CSV.
   b. Click + to create another action, and in the second Actions list, select Run Query and configure these settings, then Next.
      • For Query, select Inactive Agents.
      • Select your language.
      • For Sub-Actions, select Export to File.
      • For C:\reports\, type a valid file name.
      • For If file exists, select Overwrite.
      • For Export, select Chart data only.
      • For Format, select CSV.

4. In the Schedule tab, change these settings, then click Next.
   a. For Schedule type, click Weekly.
   b. For Start date, select today's date.
   c. For End date, click No end date.
   d. Change the Schedule settings to configure the task to run on Monday at 2:00 AM.
      You can set the schedule to run when and as often as you want.
   e. Confirm that all settings are correct in the Summary tab, then click Save.

That completes creating the server task to automatically run the two compliance queries, then save the output of the queries to CSV files.
Create a report to include query output best practice

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

Before you begin
You must know the format of the queries you are adding to the report.

In this example the queries have these formats:

• VSE: Compliance Over the Last 30 Days — Chart
• Inactive Agents — Table

Create a report that contains the data captured from your compliance queries, which is run automatically using a server task, then emailed to the administrators every Monday morning.

Task

1. Select Menu | Reporting | Queries & Reports, then select the Report tab.
2. Click Actions | New.
   A blank Report Layout page appears.
3. Click Name and type a name for the report, click Description and, optionally, type a description, click Group, and select an appropriate group to receive the report, then click OK.
4. In the Report Layout pane, drag and drop these query input formats from the Toolbox list:
   • For the VSE: Compliance Over the Last 30 Days chart query, drag the Query Chart tool into the Report Layout pane, then from the Query Chart list select VSE: Compliance Over the Last 30 Days, then click OK.
   • For the Inactive Agents table query, drag the Query Table tool into the Report Layout pane, then from Query table list, select Inactive Agents, then click OK.
5. Click Save, and the new compliance report is listed in the Reports tab.
6. To confirm that your report is configured correctly, click Run in the Actions column for your report, then verify that the Last Run Status displays Successful.
7. To see the report, click the link in the Last Run Result column, then open or save the report.

That completes creating the report to display the two compliance queries and save their output to a PDF file.

Create a server task to run and deliver a report: best practice

You must create a server task to automatically run the report and send the compliance report to your administrators.

Before you begin
You must have already:
• Created and scheduled a server task that runs the compliance queries.
• Created the report that includes the output of these queries.

Follow these steps to:
• Automatically run a report that contains the data captured from your compliance queries.
• Use a server task to email the report to the administrators every Monday morning at 5:00 a.m.

**Task**

1. Select **Menu | Automation | Server Tasks**, then click **Actions | New Task**.
2. In the Server Task Builder, configure these settings, then click **Next**.
   a. In the **Descriptions** tab, type a name and notes.
   b. In the **Schedule status**, click **Enabled**.
3. In the **Actions** tab, select **Run Report**, configure these settings, then click **Next**.
   a. For **Select a report to run**, select the compliance report you configured.
   b. Select your language.
   c. For **Sub-Actions**, select **Email file**.
   d. For **Recipients**, type the email addresses of your administrators.
      - Separate multiple email addresses with commas.
   e. For **Subject**, type the information you want to appear in the subject line of the email.
4. In the **Schedule** tab, change these settings, then click **Next**.
   a. For **Schedule type**, click **Weekly**.
   b. For **Start date**, select today’s date.
   c. For **End date**, click **No end date**.
   d. Change the Schedule settings to configure the task to run on **Monday at 5:00 AM**.
      - You can set the schedule to run when and as often as you want.
   e. Confirm that all settings are correct in the Summary tab, then click **Save**.

That completes the final task to create a compliance report that runs automatically and is delivered to your administrators every Monday morning at 5 a.m.
Automating and optimizing McAfee ePO workflow
Create an automatic compliance query and report best practice
Repositories house your security software packages and their updates for distribution to your managed systems.

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

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

Contents

- What repositories do
- Repository types and what they do
- Repository branches and their purposes
- Using repositories
- Setting up repositories for the first time
- Manage source and fallback sites best practice
- Verify access to the source site best practice
- Configure settings for global updates best practice
- Configure agent policies to use a distributed repository best practice
- Use SuperAgents as distributed repositories
- Create and configure repositories on FTP or HTTP servers and UNC shares
- Using UNC shares as distributed repositories
- Use local distributed repositories that are not managed
- Work with the repository list files
- Change credentials on multiple distributed repositories
- Pulling tasks
- Replication tasks
- Repository selection

What repositories do

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

Repository content can include the following:

- Managed software to deploy to your clients
- Security content such as DATs and signatures
- Patches and any other software needed for client tasks that you create using McAfee ePO
One common misconception is that a repository is created by installing a McAfee ePO server on a system. Unlike your server, repositories do not manage policies, collect events, or have code installed on them. A repository is nothing more than a file share located in your environment that your clients can access.

**Repository types and what they do**

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

**How repository components work together**

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

![Diagram of source sites and repositories delivering packages to systems]

**Figure 18-1 Source sites and repositories delivering packages to systems**

1. **Source site** — The source site is updated daily by McAfee.
2. **Master Repository** — The Master Repository regularly pulls DAT and engine update files from the source site.
3. **Distributed repositories** — The Master Repository replicates the packages to distributed repositories in the network.
4. **Managed systems** — The managed systems in the network retrieve updates from a distributed repository.
5. **Fallback site** — If managed systems can’t access the distributed repositories or the Master Repository, they retrieve updates from the fallback site.

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

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

We recommend using the McAfee http or McAfee ftp update sites as your source site.

Source sites are not required. You can download updates manually and check them into your Master Repository. But, 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, and some language packs. Manually check in all other packages and updates, including service packs and patches, to the Master Repository.

Master Repository

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

By default, McAfee ePO uses Microsoft Internet Explorer proxy settings.

Distributed repositories

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

As you update your Master Repository, McAfee ePO replicates the contents to the distributed repositories. Replication can occur:

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

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

A large organization can have multiple locations with limited bandwidth connections between them. Distributed repositories help reduce updating traffic across low-bandwidth connections, or at remote sites with many endpoints. If you create a distributed repository in the remote location and configure the systems in 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, when selected updates and packages are checked in to the Master Repository. Update tasks are not needed. But, if you want automatic updating, create SuperAgents in your environment. Create and configure repositories and the update tasks.

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

**Fallback site**

The fallback site is a source site enabled as the backup site. Managed systems can retrieve updates when their usual repositories are inaccessible. For example, when network outages or virus outbreaks occur, accessing the established location might be hard. Managed systems can remain up-to-date using a fallback site. The default fallback site is the McAfee http update site. You can enable only one fallback site.

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

**Repository branches and their purposes**

You can use the three McAfee ePO repository branches to maintain up to three versions of the packages in your master and distributed repositories.

The repository branches are Current, Previous, and Evaluation. By default, McAfee ePO 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.

**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 few 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 few 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. If 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. McAfee ePO 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.

This flowchart describes when to use these three different branches of the Master Repository.

---

### Using Master Repository branches

1. Decide if you want to check in new software or update existing software version.
2. Check in or update software?
   - **A** Check in
   - **Update**
   - **Yes** Test software before deployment?
     - **No**
     - **Yes** Install updated or checked in software on **Evaluation** branch of Master Repository
   - **No**
   - **Yes** Deploy software to test systems and confirm no problems occur
   - **No** Deploy software to larger network?
     - **Yes**
     - **No**
   - **Yes**
   - **No**
3. **Download or move software to Current branch of Master Repository**
4. **Use Product Deployment or client task to deploy software to managed systems**
5. **Done**

---

**Repositories**

**Repository branches and their purposes**

- **Current branch**
  - Used for testing and deployment of software.
  - Software is installed and deployed after testing.
- **Previous branch**
  - Used for storing previously tested software.
  - Software is moved here when new versions are tested and deployed.
- **Evaluation branch**
  - Used for testing new software updates.
  - Software is installed and tested here before being moved to the Current branch.

---

**McAfee ePolicy Orchestrator 5.9.0 Product Guide**

227
Using repositories

Distributed repositories work as file shares that store and distribute security content for your managed endpoints. Repositories play an important role in your McAfee ePO infrastructure. How you configure repositories and deploy them depends on your environment.

Distributed repository types

Before you create distributed repositories, it is important to understand which type of repository to use in your managed environment. The McAfee ePO server always acts as the Master Repository. It keeps the master copy of all content needed by your agents. The server replicates content to each of the repositories distributed throughout your environment. As a result, your agents can retrieve updated content from an alternate and closer source.

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

Distributed repository types include:

- FTP repositories
- HTTP repositories
- UNC share repositories
- SuperAgents

Consider the following when planning your distributed repositories:

- The McAfee ePO server requires that you use certain protocols for the repositories, but any server vendor can provide those protocols. For example, if you use an HTTP repository, you can use either Microsoft Internet Information Services (IIS) or Apache server (Apache is the faster option).

- There is no operating system requirement for the systems that host your repository. As long as your McAfee ePO server can access the folders you specify to copy its content to, and as long as the agents can connect to these folders to download their updates, everything works as expected.

- Your agent updates and McAfee ePO replication tasks are only as good as your repositories. If you are already using one of these repositories and your environment works well, do not change the configuration.

If you are starting with a new installation with no repositories, use a SuperAgent because they are easy to configure and are reliable.

Unmanaged repositories

If you are unable to use managed systems as distributed repositories, you can create and maintain unmanaged distributed repositories but a local administrator must keep the distributed files up-to-date manually.

Once the distributed repository is created, use McAfee ePO to configure managed systems of a specific System Tree group to update from it.

Manage all distributed repositories through McAfee ePO. This ensures your managed environment is up to date. Use unmanaged distributed repositories only if your network or organization’s policy doesn’t allow managed distributed repositories.

FTP repositories

FTP servers can host a distributed McAfee ePO server repository. You might already have FTP servers in your environment, and you can store McAfee content there as well.

FTP repositories are:
- Fast
- Able to manage extensive loads from the clients pulling data
- Helpful in a DMZ where HTTP might not be optimal and UNC shares can't be used

Using FTP servers, your clients do not need authentication and can use an anonymous log on pull their content. No authentication reduces the chance that a client fails to pull its content.

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 folder and site location for the distributed repository. See your web server documentation for details.

**HTTP repositories**

HTTP servers can host a distributed McAfee ePO server repository. You might already have HTTP servers in your environment.

HTTP servers can be fast serving out files to large environments. Your HTTP servers allow clients to pull their content without authentication, which reduces the chance that a client might fail to pull its content.

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

**UNC share repositories best practice**

Universal Naming Convention (UNC) shares can host your McAfee ePO server repository.

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

> The correct permissions must be set to access the folder.

Because most administrators are familiar with the concept of UNC shares, UNC shares might seem like the easiest method to choose, but that's not always the case.

If you use UNC shares to host your McAfee ePO server repository, you must correctly configure the account and shares. See the *Recommendations for download credentials when using UNC shares as software repositories in ePolicy Orchestrator*, KB70999, for details.

If you choose to use UNC shares, you must:

1. Create the folder.
2. Adjust share permissions.
3  Change the NTFS permissions.

4  Create two accounts, one with read access and one with write access.

If your IT group has password rules, such as changing a password every 30 days even for service accounts, changing those passwords in McAfee ePO can be cumbersome. You must change the password for access to each of the distributed repository shares in the Windows operating system and in the configuration settings for each of the UNC Distributed Repositories in McAfee ePO. Access the McAfee ePO UNC Distributed Repositories settings using Menu | Software | Distributed Repositories.

![Figure 18-2 UNC repository credentials page](image)

All these tasks increase the chance of failure because these processes must be completed manually. Your agents might not properly update if your agents cannot authenticate to your UNC share because they are not part of the domain or the credentials are incorrect.

**Best practice: SuperAgent repositories**

You can create a SuperAgent repository to act as an intermediary between the McAfee ePO server and other agents.

The SuperAgent caches information received from a McAfee ePO server, the Master Repository, or a mirrored Distributed Repository, and distributes it to the nearest agents. The Lazy Caching feature allows SuperAgents to retrieve data from McAfee ePO servers only when requested by a local agent node. Creating a hierarchy of SuperAgents along with lazy caching further saves bandwidth and minimizes the wide-area network traffic.

A SuperAgent also broadcasts wake-up calls to other agents using that SuperAgent repository. When the SuperAgent receives a wake-up call from the McAfee ePO server, it wakes up the agents using its repository connection.

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

For detailed information about SuperAgents and how to configure them, see the *McAfee Agent Product Guide*.
SuperAgent repositories

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

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

Although functionality of SuperAgent broadcast wake-up calls requires a SuperAgent in each broadcast segment, broadcast wake-up calls are not a requirement for the SuperAgent repository. But, managed systems must have access to the system hosting the repository.

SuperAgent considerations

When you configure systems as SuperAgents, follow these guidelines.

- Use existing file repositories in your environment, for example Microsoft System Center Configuration Manager (SCCM).
- You don’t need a SuperAgent on every subnet.
- Turn off Global Updating to prevent unwanted updates of new engines or patches from the Master Repository.

SuperAgent and its hierarchy

A hierarchy of SuperAgents can serve agents in the same network with minimum network traffic utilization. A SuperAgent caches the content updates for the McAfee ePO server or distributed repository and distributes content updates to the agents in the network, reducing the wide area network traffic. It is always ideal to have more than one SuperAgent to balance the network load.

You use the Repository policy to create the SuperAgent hierarchy. We recommend that you have a three-level hierarchy of SuperAgents in your network.

See McAfee Agent Product Guide for details about creating a hierarchy of SuperAgents, SuperAgent caching (lazy caching), and communication interruptions.

Create a SuperAgent

Creating a SuperAgent requires these tasks.

1. Create a new SuperAgents policy.
2. Create a new group in the System Tree, for example named SuperAgents.
3. Assign the new SuperAgent policy to the new SuperAgents group.
4. Drag a system into the new SuperAgents group.

Once you have created the new SuperAgents group, you can drag any system into that group and it becomes a SuperAgent the next time it communicates with the McAfee ePO server.

Create SuperAgent policy

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

1. Select **Menu | Policy | Policy Catalog** to open the Policy Catalog page.
2. To duplicate the **My Default** policy from the **Product** drop-down list, select **McAfee Agent**, and from the **Category** drop-down list, select **General**.
3. In the **My Default** policy row, in the **Actions** column, click **Duplicate**.
   
   *The McAfee Default policy cannot be changed.*
4. In the **Duplicate Existing Policy** dialog box, change the policy name, add any notes for reference, and click **OK**.
5. From the Policy Catalog page, click **SuperAgents** tab, select **Convert agents to SuperAgents** to convert the agent to a SuperAgent and update its repository with the latest content.
6. Select **Use systems running SuperAgents as distributed repositories** to use the systems that host SuperAgents as update repositories for the systems in its broadcast segment, then provide the **Repository path**.
7. Select **Enable Lazy caching** to allow the SuperAgents to cache content when it is received from the McAfee ePO server.
8. Click **Save**.

**Best practice: Create a group in the System Tree**
Adding a SuperAgent group to your System Tree allows you to assign a SuperAgent policy to the group.

Task

1. Select **Menu | Systems Section | System Tree**, click **System Tree Actions | New Subgroups**, and give it a distinctive name, for example **SuperAgents**.
2. Click **OK**. The new group appears in the System Tree list.

**Best practice: Assign the new SuperAgents policy to the new SuperAgent group**
Assigning the SuperAgent policy to the new group completes the configuration of the SuperAgent group.

Task

1. In the **System Tree**, select the SuperAgent group that you created, select the **Assigned Policies** tab, then select **McAfee Agent** from the Product list.
2. From the **Actions** column for the **General** category, click **Edit Assignment**.
3. From the **McAfee Agent: General** page, click **Break inheritance and assign the policy and settings below**. Select the SuperAgent policy that you created from the **Assigned Policy** list, then click **Save**.

**Best practice: Assign a system to the new SuperAgent group**
After the SuperAgent group is configured, you can assign the SuperAgent policies to individual endpoints by dragging them into that group. These policies convert the endpoints into SuperAgents.
**Task**

1. In the **System Tree**, click the **Systems** tab and find the system that you want to change to a SuperAgent repository.

2. Drag that row with the system name and drop it into the new SuperAgent group you created in the System Tree.

   Once the system communicates with the McAfee ePO server, it changes to a SuperAgent repository.

3. To confirm that the system is now a SuperAgent repository, select **Menu | Software | Distributed Repositories** and select **SuperAgent** from the **Filter** list. The new SuperAgent repository appears in the list.

   > Before the system appears as a SuperAgent in the group, two agent-server communications must occur. First, the system must receive the policy change and second, the agent must respond back to the McAfee ePO server that is now a SuperAgent. This conversion might take some time depending on your ASCI settings.

**Repository list files**

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

The repository list include 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 McAfee Agent during agent-server communication.

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

- **SiteList.xml file**
  - Import to a McAfee Agent during installation.

- **SiteMgr.xml file**
  - Back up and restore your distributed repositories and source sites if you have to reinstall the server.
  - Import the distributed repositories and source sites from a previous installation of the McAfee ePO software.

**Best practice: Where to place repositories**

You must determine how many repositories are needed in your environment and where to locate them.

To answer these questions, you must look at your McAfee ePO server managed systems and your network geography.

Consider the following factors:

- How many nodes do you manage with the McAfee ePO server?
- Are these nodes located in different geographic locations?
- What connectivity do you have to your repositories?

Remember, the purpose of a repository is to allow clients to download the large amount of data in software updates locally instead of connecting to the McAfee ePO server and downloading the updates across the slower WAN links. At a minimum, your repository is used to update your signature, or DAT files for VirusScan Enterprise daily. In addition, your repository is used by your agents to download new software, product patches, and other content, for example Host Intrusion Prevention content.
Typically you can create a repository for each large geographic location, but there are several caveats. Plus, you must avoid the most common mistakes of having too many or too few repositories and overloading your network bandwidth.

**How many repositories do you need?**

How many repositories you need depends on the server hardware, node count, network topology, and where the repositories are installed.

Repositories have no hard technical limit to how many nodes they can handle. With a properly crafted update task for your clients, repositories can update a significant number of nodes.

The following table is an estimate of the updates a repository can handle and the hardware needed. Many factors can influence these specifications, for example how you update content, products, and patches.

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

Disk space needed for a repository is rarely a concern with today's storage standards. Even if you checked in several McAfee endpoint products, for example McAfee Endpoint Encryption, SiteAdvisor Enterprise, and Policy Auditor, your repository disk space is in the 1-GB range.

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

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

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

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

This example describes the repository specifics for an organization with 3,000 nodes in one office. The organization has these characteristics:

- Approximately 3,000 nodes of workstations and servers.
- Uses VirusScan Enterprise, Host Intrusion Prevention, McAfee Endpoint Encryption, and Host Data Loss Prevention.
- Has a small data center in the same building where the devices reside, so there are no WAN links and all clients are on a 100 MB LAN.

In this example, you can use the primary McAfee ePO server to act as the only repository. The McAfee ePO server is always the Master Repository by default. For 3,000 clients, the McAfee ePO server can handle:

- Policy deployment
- Event collection
- Distributing all updates and software

**Example 2—15,000–20,000 node organization with four offices**

This example describes the repository specifics for an organization with 15,000–20,000 nodes and four offices. The organization has these characteristics:
• Approximately 15,000–20,000 nodes of workstations and servers.
• Has one data center in New York where all traffic destined for the Internet is routed.
• Four offices in the U.S. located in New York, San Francisco, Dallas, and Orlando.
• Each office has approximately 3,000–4,000 nodes and a T1 connection (1.544 Mb/s) back to the New York office.

The McAfee ePO server, located in New York, manages all 20,000 nodes for policies and events for McAfee Endpoint Encryption, VirusScan Enterprise, Host Intrusion Prevention, and Application Control.

A dedicated SuperAgent repository is placed in each of the three major offices that connect to the data center. These repositories are dedicated SuperAgent repositories that connect to the New York data center with medium hardware class servers, for example a single processor 3 GHz CPU and 4 GB of RAM. The SuperAgents only job is to serve out files to the McAfee Agent at each office. When you have multiple repositories, you can specify the order in which agents access repositories. In this example, you would order the repositories so that the dedicated SuperAgent repositories that connect to the New York data center are accessed first. You can even disable access to other repositories you don’t want the agents to use.

**Example 3 – 40,000–60,000 node organization with multiple global offices**

This example describes the repository specifics for an organization with 40,000–60,000 node organization with multiple global offices. The organization has these characteristics:

• Approximately 40,000–60,000 nodes of workstations and servers.
• Three major regions of the U.S. offices, with one data center in New York and three additional offices across the country.
• Each office has approximately 5,000–7,000 nodes.
• The one McAfee ePO server in the New York data center runs VirusScan Enterprise, Host Intrusion Prevention, and SiteAdvisor Enterprise.
• The largest office in the U.S., other than the New York Data Center, has an Agent Handler installed.

The Europe, Middle East, and Africa (EMEA) offices have another data center in the UK with several other offices across EMEA. These other offices range from 200 nodes 3,000 nodes.

The Asia-Pacific (APAC) offices include two smaller offices.

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

**U.S. region servers**

Put one server class client, for example dual processor 3 GHz and 8 GB of RAM, at each site in the U.S.
EMEA region servers

Use the Systems Management Server (SMS) and install the SuperAgents at each office in the EMEA because they are smaller sites. Your repository does not have to be dedicated to McAfee as long as it’s not serving files to several thousand agents.

APAC region servers

The small offices in the APAC region use slow WAN links back to the McAfee ePO server in the New York. Plus these WAN links are already saturated with traffic. These links mean replication from the McAfee ePO server to an APAC repository is not feasible unless it is done during off hours. This option is reasonable if you want to put SuperAgents in APAC.

Fortunately, the APAC offices each have their own fast dedicated connections out to the Internet and do not have to route Internet traffic back to the data center in New York. That provides two potential solutions:

- You can adjust the client tasks in APAC to have them go to the next nearest repository, which might be in California.

  You must completely randomize the agents updating schedule so you spread their updates throughout the day.

- You can put a SuperAgent in the DMZ (publicly accessible on the Internet) at one of the data centers. Then adjust the APAC client tasks forcing them to only update from this SuperAgent in the DMZ. Because the SuperAgent is local to the data center, replication from McAfee ePO is fast. Because the agents don’t have to use a WAN link and can go straight to the Internet and your slow WAN bandwidth concerns are solved.

Disable server Master Repository

In large environments, you can improve performance of your McAfee ePO server by excluding the Master Repository from providing agent updates.

Before you begin

You must have another repository configured before you can disable the Master Repository on the McAfee ePO server.

In large environments, the McAfee ePO server is already busy distributing policies and collecting events. You can improve performance by changing your McAfee Agent policy so that agents do not pull content from the McAfee ePO server directly. Instead of pulling content from the Master Repository, agents access dedicated repositories that are created for local access. This change forces the agents to use only the repositories you created manually. You can specify which repositories agents access when selecting a repository within a policy.

In smaller environments, where fewer nodes are managed, there is no need for this change. The server can handle all these tasks without impacting performance.

Task

1. To open the Policy Catalog, select Menu | Policy | Policy Catalog.

2. From the Product list, select McAfee Agent, then from the Category list, select Repository, and click the policy name to modify.

3. Click the Repositories tab.
4 In the Repository list, click **Disable** in the Actions column for the McAfee ePO server.

This diagram shows the McAfee ePO server disabled.

![Diagram showing the McAfee ePO server disabled](image)

**Figure 18-3 Repositories with McAfee ePO server disabled**

5 Click **Save**.

Now you have improved the McAfee ePO server performance because the agents are no longer accessing it for updates.

**Best practice: Global Updating restrictions**

Global Updating is a powerful feature, but if used incorrectly it can have a negative impact in your environment. Global Updating is used to update your repositories as quickly as possible when the Master Repository changes. Global Updating is great if you have a smaller environment (fewer than 1,000 nodes) with no WAN links. Global Updating generates a huge amount of traffic that could impact your network bandwidth. If your environment is on a LAN, and bandwidth is not a concern, then use Global Updating. If you are managing a larger environment and bandwidth is critical, disable Global Updating.

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

To confirm the Global Updating setting, select **Menu | Configuration | Server Settings** and select **Global Updating** from the Setting Categories list. Confirm that the status is disabled. If not, click **Edit** and change the status.

If you are a user with a large environment and where bandwidth is critical, you can saturate your WAN links if you have Global Updating enabled. You might think having Global Updating enabled makes you receive their DATs quickly. But eventually, McAfee, for example releases an update to its McAfee Endpoint Security engine that can be several megabytes, compared to the 400-KB DAT files. This engine update typically occurs twice a year. When that release occurs the McAfee ePO server pulls the engine from McAfee, starts replicating it to the distributed repositories, and starts waking up agents to receive the new engine immediately. This engine update can saturate your WAN links and roll out an engine that you might prefer to upgrade in a staged release.

If you have a large environment, you can still use Global Updating, but you must disable it when a new engine or product patch is released or the updates could saturate your WAN links.
For additional information see these KnowledgeBase articles:

- How to prevent McAfee ePO 5.X from automatically updating to the latest posted Engine, KB77901
- ePolicy Orchestrator Cloud prematurely deploys McAfee product software patch, KB77063

**How Global Updating works**

If your McAfee ePO server is scheduled to pull the latest DATs from the McAfee website at 2 p.m. Eastern time (and the scheduled pull changes the contents of your Master Repository), your server automatically initiates the Global Update process to replicate the new content to all your distributed repositories.

The Global Updating process follows this sequence of events:

1. Content or packages are checked in to the Master Repository.
2. The McAfee ePO server performs an incremental replication to all distributed repositories.
3. The McAfee ePO server issues a wake-up call to all SuperAgents in the environment.
4. The SuperAgent broadcasts a global update message to all agents in the SuperAgent subnet.
5. Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed.
6. The agent searches the distributed repositories for a site that has this minimum catalog version.
7. Once a suitable repository is found, the agent runs the update task.

**Setting up repositories for the first time**

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

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

**Manage source and fallback sites best practice**

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

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

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

**Tasks**

- **Create source sites on page 239**
  Create a source site from Server Settings.
- **Switch source and fallback sites best practice on page 240**
  Use Server Settings to change source and fallback sites.
- **Edit source and fallback sites best practice on page 240**
  Use Server Settings to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.
- **Delete source sites or disabling fallback sites best practice on page 240**
  If a source or fallback site is no longer in use, delete or disable the site.
Create source sites
Create a source site from Server Settings.

Task

1. Select Menu | Configuration | Server Settings, then select Source Sites.
2. Click Add Source Site. The Source Site Builder wizard appears.
3. On the Description page, type a unique repository name and select HTTP, UNC, or FTP, then click Next.
4. On the Server page, provide the web address and port information of the site, then click Next.
   **HTTP or FTP server type:**
   • From the URL drop-down list, select DNS Name, IPv4, or IPv6 as the type of server address, then enter the address.
     | Option | Definition |
     |--------|------------|
     | DNS Name | Specifies the DNS name of the server. |
     | IPv4 | Specifies the IPv4 address of the server. |
     | IPv6 | Specifies the IPv6 address of the server. |
     • Enter the port number of the server: FTP default is 21; HTTP default is 80.
   **UNC server type:**
   • Enter the network directory path where the repository resides. Use this format: \<COMPUTER>\<FOLDER>.
5. On the Credentials page, provide the Download Credentials used by managed systems to connect to this repository.
   Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository.
   **HTTP or FTP server type:**
   • Select Anonymous to use an unknown user account.
   • Select FTP or HTTP authentication (if the server requires authentication), then enter the user account information.
   **UNC server type:**
   • Enter domain and user account information.
6. Click Test Credentials. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information. If credentials are incorrect, check the:
   • User name and password.
   • URL or path on the previous panel of the wizard.
   • The HTTP, FTP or UNC site on the system.
7. Click Next.
8. Review the Summary page, then click Save to add the site to the list.
Switch source and fallback sites best practice

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

**Task**

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

Edit source and fallback sites best practice

Use Server Settings to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.

**Task**

1. Select **Menu | Configuration | Server Settings**.
2. Select **Source Sites**, then click **Edit**.
3. Locate the site in the list, then click the name of the site.
4. From the Source Site Builder, edit the settings on the builder pages as needed, then click **Save**.

Delete source sites or disabling fallback sites best practice

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

**Task**

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

The site is removed from the Source Sites page.

Verify access to the source site best practice

You must make sure that the McAfee ePO Master Repository and managed systems can access the Internet when using the McAfeeHttp and McAfeeFtp sites as source and fallback sites.

This section describes the tasks for configuring the connection the McAfee ePO **Master Repository** and the McAfee Agent use to connect to the download site directly or via a proxy. The default selection is **Do not use proxy**.
Tasks

- **Configure proxy settings on page 241**
  To update your repositories, configure proxy settings to pull DATs.

- **Configure proxy settings for the McAfee Agent on page 241**
  Configure the proxy settings the McAfee Agent uses to connect to the download site.

**Configure proxy settings**

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

**Task**

1. Select Menu | Configuration | Server Settings.
2. From the list of setting categories, select Proxy Settings, then click Edit.
3. Select Configure the proxy settings manually.
   a. Next to Proxy server settings, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Type the IP address or fully-qualified domain name and the port number of the proxy server.

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

   b. Next to Proxy authentication, configure the settings according to whether you pull updates from HTTP repositories, FTP repositories, or both.

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

   d. Next to Exclusions, select Bypass Local Addresses, then specify distributed repositories that the server can connect to directly by typing the IP addresses or the fully-qualified domain name of those systems, separated by semicolons.
4. Click Save.

**Configure proxy settings for the McAfee Agent**

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

**Task**

1. Select Menu | Policy | Policy Catalog, then from the Product list click McAfee Agent, and from the Category list, select Repository.
   A list of agents configured for the McAfee ePO server appears.
2. On the My Default agent, click Edit Settings.
   The edit settings page for the My Default agent appears.
3. Click the Proxy tab.
   The Proxy Settings page appears.
4 Select **Use Internet Explorer settings (Windows only)** for Windows systems, and select **Allow user to configure proxy settings**, if appropriate.

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

5 Select **Configure the proxy settings manually** to configure the proxy settings for the agent manually.

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

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

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

9 Click **Save**.

---

**Configure settings for global updates best practice**

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

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

**Task**

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

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

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

When using global updating, schedule 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.

**Configure agent policies to use a distributed repository best practice**

Customize how agents select distributed repositories to minimize bandwidth use.
Task

1. Select Menu | Policy | Policy Catalog, then select the Product as McAfee Agent and Category as Repository.
2. Click an existing agent policy, then select the Repositories tab.
3. From Repository list selection, select either Use this repository list or Use other repository list.
4. 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 endpoints 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.
   • You can set the Maximum number of hops.
   • User order in repository list — Selects repositories based on their order in the list.
5. Modify settings in the Repository list as needed:
   • Disable repositories by clicking Disable in the Actions field.
   • Click Move to Top or Move to Bottom to specify the order in which you want endpoints to select distributed repositories.
6. Click Save when finished.

Use SuperAgents as distributed repositories

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

- To convert an agent to a SuperAgent, the agent must be part of a Windows domain.

Tasks

- Create SuperAgent distributed repositories on page 243
  To create a SuperAgent repository, the SuperAgent system must have a McAfee Agent installed and running. We recommend using SuperAgent repositories with global updating.
- Replicate packages to SuperAgent repositories on page 244
  Select which repository-specific packages are replicated to distributed repositories.
- Delete SuperAgent distributed repositories on page 244
  Remove SuperAgent distributed repositories from the host system and the repository list (SiteList.xml). New configurations take effect during the next agent-server communication.

Create SuperAgent distributed repositories

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

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

1. From the McAfee ePO console, select Menu | Policy | Policy Catalog, then from the Product list click McAfee Agent, and from the Category list, select General.

A list of available general category policies available for use on your McAfee ePO server appears.

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

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

4. Select Use systems running SuperAgents as distributed repositories, then type a folder path location for the repository. This location is where the Master Repository copies updates during replication. You can use a standard Windows path, such as C:\SuperAgent\Repo.

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

5. Click Save.

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

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

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

Replicate packages to SuperAgent repositories

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

Task

1. Select Menu | Software | Distributed Repositories.

A list of all distributed repositories appears.

2. Locate and click the SuperAgent repository.

The Distributed Repository Builder opens.

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

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

4. Click Save.

Delete SuperAgent distributed repositories

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

1. From the McAfee ePO console, click Menu | Policy | Policy Catalog, then click the name of the SuperAgent policy you want to modify.

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

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

The SuperAgent repository is deleted and removed from the repository list. However, the agent still functions as a SuperAgent as long as you leave the Convert agents to SuperAgents option selected. Agents that have not received a new site list after the policy change continue to update from the SuperAgent that was removed.

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

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

Tasks

- Create a folder location on page 246
  Create the folder that hosts repository contents on the distributed repository system. Different processes are used for UNC share repositories and FTP or HTTP repositories.

- Add the distributed repository to McAfee ePO on page 246
  Add an entry to the repository list and specify the folder the new distributed repository uses.

- Avoid replication of selected packages on page 247
  If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. Depending on your requirements for testing and validating, you might want to avoid replicating some packages to your distributed repositories.

- Disable replication of selected packages on page 248
  If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. To disable the impending replication of a package, disable the replication task before checking in the package.

- Enable folder sharing for UNC and HTTP repositories on page 248
  On an HTTP or UNC distributed repository, you must enable the folder for sharing across the network, so that your McAfee ePO server can copy files to the repository.

- Edit distributed repositories on page 248
  Edit a distributed repository configuration, authentication, and package selection options as needed.

- Delete distributed repositories on page 249
  Delete HTTP, FTP, or UNC distributed repositories. Doing so also deletes the contents of the distributed repositories.
Create a folder location
Create the folder that hosts repository contents on the distributed repository system. Different processes are used for UNC share repositories and FTP or HTTP repositories.

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

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

Do not configure distributed repositories to reference the same directory as your Master Repository. Doing so locks files on the Master Repository, causing pulls and package check-ins to fail and leaving the Master Repository in an unusable state.

Task

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

2. On the Description page, type a unique name and select HTTP, UNC, or FTP, then click Next. The name of the repository does not need to be the name of the system hosting the repository.

3. On the Server page, configure one of the following server types.
   - **HTTP server type 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.
     - Enter the port number of the server: HTTP default is 80. FTP default is 21.
     - For HTTP server types, 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:
   - 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 Builder
  - 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 Builder
  - HTTP, FTP, or UNC site on the system

7 Click **Next**. The Package Types page appears.

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

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

Avoid replication of selected packages

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

1. Select Menu | Software | Distributed Repositories, then click a repository. The Distributed Repository Builder wizard opens.

2. On the Package Types page, deselect the package that you want to avoid being replicated.

3. Click Save.

**Disable replication of selected packages**

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

Task

1. Click Menu | Automation | Server Tasks, then select Edit next to a replication server task.

   The Server Task Builder opens.

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

**Enable folder sharing for UNC and HTTP repositories**

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

You enable the folder sharing for replication purposes only. Managed systems configured to use the distributed repository use the appropriate protocol (HTTP, FTP, or Windows file sharing) and do not require folder sharing.

Task

1. On the managed system, locate the folder you created using Windows Explorer.

2. Right-click the folder, then select Sharing.

3. On the Sharing tab, select Share this folder.

4. Configure share permissions as needed.

   Systems updating from the repository require only read access, but administrator accounts, including the account used by the McAfee ePO server service, require write access. See your Microsoft Windows documentation to configure appropriate security settings for shared folders.

5. Click OK.

**Edit distributed repositories**

Edit a distributed repository configuration, authentication, and package selection options as needed.

Task

1. Select Menu | Software | Distributed Repositories, then click a repository.

   The Distributed Repository Builder wizard opens, displaying the details of the distributed repository.
2 Change configuration, authentication, and package selection options as needed.

3 Click Save.

**Delete distributed repositories**

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

**Task**

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

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

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

Deleted repositories are removed from the repository list.

**Using UNC shares as distributed repositories**

Follow these guidelines when using UNC shares as distributed repositories.

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

**Correctly configure the share**

Make sure that the UNC share is correctly configured.

- **Use an alternate method to write to your repository** — Log on to the server using other methods (another share, RDP, locally) to write to your repository. Do not mix the repository you read from with the repository you write to. Read credentials are shared with endpoints, and write credentials are used exclusively by the McAfee ePO server to update your distributed repository content.

- **Do not use a share on your Domain Controller** — Create a share off your domain controller. A local user on a domain controller is a domain user.

**Secure the account you use to read from the UNC share**

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

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

> The McAfee ePO server Master Repository must be able to write files to the UNC share account.

- **Create the account locally** — Create the account on the file share, not on the domain. Accounts created locally do not grant rights to systems in the domain.

- **Use a specific account** — Create an account specifically for sharing repository data. Do not share this account with multiple functions.

- **Make the account low privilege** — Do not add this account to any groups it does not need, which includes "Administrators" and "Users" groups.
• **Disable extraneous privileges** — This account does not need to log on to a server. It is a placeholder to get to the files. Examine this account’s permissions and disable any unnecessary privileges.

• **Use a strong password** — Use a password with 8–12 characters, using multiple character attributes (lowercase and uppercase letters, symbols, and numbers). We recommend using a random password generator so that your password is complex.

**Protect and maintain your UNC share**

• **Firewall your share** — Always block unnecessary traffic. We recommend blocking outgoing and incoming traffic. You can use a software firewall on the server or a hardware firewall on the network.

• **Enable File Auditing** — Always enable security audit logs to track access to your network shares. These logs display who accesses the share, and when and what they did.

• **Change your passwords** — Change your password often. Make sure that the new password is strong, and remember to update your McAfee ePO configuration with the new password.

• **Disable the account and share if it's no longer used** — If you switch to a different repository type other than UNC, remember to disable or delete the account, and close and remove the share.

---

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

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

Once an unmanaged repository is created, you must manually configure managed systems to go to the unmanaged repository for files.

**Task**

1. **Copy all files and subdirectories in the Master Repository folder from the server.**
   For example, using a Windows 2008 R2 Server, this path is the default path on your server: `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Software`

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

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

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

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

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

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

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

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

h. Configure authentication credentials as needed.
Click OK to add the new distributed repository to the list.

Select the new repository in the list.

The type Local indicates it is not managed by the McAfee ePO software. When an unmanaged repository is selected in the Repository list, the Edit and Delete buttons are enabled.

Click Save.

Any system where this policy is applied receives the new policy at the next agent-server communication.

---

**Work with the repository list files**

You can export the repository list files.

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

**Tasks**

- **Export the repository list SiteList.xml file on page 251**
  Export the repository list (SiteList.xml) file for manual delivery to systems, or for import during the installation of supported products.

- **Export the repository list for backup or use by other servers on page 252**
  Use the exported SiteMgr.xml file to restore distributed repositories and source sites. Restore when you reinstall the McAfee ePO server, or when you want to share distributed repositories or source sites with another McAfee ePO server.

- **Import distributed repositories from the repository list on page 252**
  Import distributed repositories from the SiteMgr.xml file after reinstalling a server, or when you want one server to use the same distributed repositories as another server.

- **Import source sites from the SiteMgr.xml file on page 252**
  After reinstalling a server, and when you want two servers to use the same distributed repositories, import source sites from a repository list file.

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

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

**Task**

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

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

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

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

Use the exported SiteMgr.xml file to restore distributed repositories and source sites. Restore when you reinstall the McAfee ePO server, or when you want to share distributed repositories or source sites with another McAfee ePO server.

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

Task

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

Import distributed repositories from the repository list

Import distributed repositories from the SiteMgr.xml file after reinstalling a server, or when you want one server to use the same distributed repositories as another server.

Task

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

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

Import source sites from the SiteMgr.xml file

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

Task

1. Select Menu | Configuration | Server Settings, then from the Setting Categories list select Source Sites and click Edit.
2. Click Import.
3. Browse to and select the exported SiteMgr.xml file, then click OK.
4. Select the source sites to import into this server, then click OK.

   The selected source sites are added to the list of repositories on this server.
Change credentials on multiple distributed repositories

Change credentials on multiple distributed repositories of the same type. Doing so is valuable in environments where there are many distributed repositories.

Task

1. Select **Menu | Distributed Repositories**.
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**.
4. Select the distributed repositories you want, then click **Next**.
5. Edit the credentials as needed, then click **Next**.
6. Review the information, then click **Save**.

Pulling tasks

Use pull tasks to update your Master Repository with DAT and Engine update packages from the source site. DAT and Engine files must be updated often. McAfee releases new DAT files daily, and Engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.

You can specify which packages are copied from the source site to the Master Repository.

Extra.DAT files must be checked in to the Master Repository manually. They are available from the McAfee website.

A scheduled repository pull server task runs automatically and regularly at the times and days you specify. For example, you can schedule a weekly repository pull task at 5:00 a.m. every Thursday.

You can also use the Pull Now task to check updates into the Master Repository immediately. For example, when McAfee alerts you to a fast-spreading virus and releases a new DAT file to protect against it.

If a pull task fails, you must check the packages into 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 variables 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. Make sure that all your distributed repositories are up-to-date.

If you are using global updating for all 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.

Schedule a daily incremental replication task. Schedule a weekly full replication task if it is possible for files to be deleted from the distributed repository outside of the replication functionality of the McAfee ePO software.

Repository selection

New distributed repositories are added to the repository list file containing all available distributed repositories. The agent of a managed system updates this file each time it communicates with the McAfee ePO server. The agent performs repository selection each time the agent (McAfee Framework Service) service starts, and when the repository list changes.

Selective replication provides more control over the updating of individual repositories. When scheduling replication tasks, you can choose:

- Specific distributed repositories to which the task applies. Replicating to different distributed repositories at different times lessens the impact on bandwidth resources. These repositories can be specified when you create or edit the replication task.
- Specific files and signatures that are replicated to the distributed repositories. Selecting only those types of files that are necessary to each system that checks in to the distributed repository lessens the impact on bandwidth resources. When you define or edit your distributed repositories, you can choose which packages you want to replicate to the distributed repository.

This functionality is intended for updating only products that are installed on several systems in your environment, like VirusScan 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 algorithms 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. Do not disable repositories in the policy settings. Allowing agents to update from any distributed repository ensures that they receive the updates.
Agent Handlers route communication between agents and your McAfee ePO server. Each McAfee ePO server contains a master Agent Handler. Additional Agent Handlers can be installed on systems throughout your network.

Setting up more Agent Handlers provides the following benefits.

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

**Contents**

- How Agent Handlers work
- Agent Handler details
- Agent Handler functionality
- Best Practices: Agent Handler installation and configuration
- Best Practices: Adding an Agent Handler in the DMZ
- Connect an Agent Handler in the DMZ to a McAfee ePO server in a domain
- Handler groups and priority
- Assign McAfee agents to Agent Handlers
- Manage Agent Handler assignments
- Create Agent Handler groups
- Manage Agent Handler groups
- Move agents between handlers
- Frequently asked questions

**How Agent Handlers work**

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

The handler provides updated sitelists, policies, and policy assignment rules, just as the McAfee ePO server does. The handler also caches the contents of the Master Repository, so that agents can pull product update packages, DATs, and other needed information.

If the handler doesn't have the updates needed when an agent checks in, the handler retrieves them from the assigned repository and caches them, while passing the update through to the agent.
This diagram shows some of the typical connections between Agent Handlers, the McAfee ePO server, and the McAfee ePO SQL Server.

**New York**

- McAfee ePO server
- Administrator
- SQL server
- High-speed links
- Failover support

**Boston**

- 1,000s of nodes
- Load balanced

**Philadelphia**

- 1,000s of nodes
- Load balanced

**Washington DC**

- 1,000s of nodes

---

**Figure 19-1 Agent Handlers in an enterprise network**

In this diagram, all Agent Handlers:

- Are connected to the McAfee ePO SQL Server using low-latency high-speed links
- Are located close to the database they write to
- Have failover configured between Agent Handlers
- Are managed from the McAfee ePO server

The Agent Handlers in these cities have specific configurations.

> A low-latency high-speed link’s round-trip latency must be less than about 10 ms. Use the Windows `tracert` command to confirm the round-trip time (RTT) from the Agent Handler to the McAfee ePO SQL Server.

- **Boston** — The Agent Handler for Boston is configured with failover support to the Agent Handler for Philadelphia.
- **Philadelphia** — The two Agent Handlers have load balancing configured.
- **Washington DC** — The Agent Handler uses specific ports to connect to the McAfee ePO server from behind a firewall.
The Agent Handler must be able to authenticate domain credentials. Or the Agent Handler uses SQL authentication to authenticate to the database. For more information about Windows and SQL authentication, see the Microsoft SQL Server documentation.

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

Run the query Systems per Agent Handler to display all Agent Handlers installed and the number of agents managed by each Agent Handler.

When an Agent Handler is uninstalled, it is not displayed in this chart. If an Agent Handler assignment rule exclusively assigns agents to an Agent Handler and if that Agent Handler is uninstalled, it is displayed in the chart with Uninstalled Agent Handler and the number of agents still trying to contact this Agent Handler.

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

**Multiple Agent Handlers**

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

---

**Agent Handler details**

Agent Handlers provide specific features that can help grow your network to include many more managed systems.

**When to use Agent Handlers**

There are many reasons to use Agent Handlers in your network.

- **Hardware is cheaper** — The mid-range server hardware used for Agent Handlers is less expensive than the high-end servers used for McAfee ePO servers.
- **Scalability** — As your network grows, Agent Handlers can be added to reduce the load on your McAfee ePO server.

  > Connect no more than five Agent Handlers to one McAfee ePO server with a maximum of 50,000 nodes connected to each Agent Handler.

- **Network topology** — Agent Handlers can manage your agent requests behind a firewall or in an external network.
- **Failover** — Agents can failover between Agent Handlers using a configured fallback priority list.
- **Load Balancing** — Multiple Agent Handlers can load balance the McAfee Agent requests in a large remote network.

**When not to use Agent Handlers**

There are some instances not to use Agent Handlers.
• **As distributed repositories** — Repositories, for example SuperAgents, distribute large files throughout an organization. Repositories do not contain any logic. Agent Handlers use logic to communicate events back to the database. These events tell the McAfee Agent when to download new products from the distributed repositories. Agent Handlers can cache files from the distributed repositories, but don’t use them to replace distributed repositories. Agent Handlers are used to reduce the event management load on the McAfee ePO server.

• **Through a slow or irregular connection** — Agent Handlers require a relatively high speed, low latency connection to the database to deliver events sent by the agents.

• **To save bandwidth** — Agent Handlers do not save bandwidth. They actually increase bandwidth use over the WAN connection that connects the clients to the Agent Handler. Use distributed repositories to save bandwidth.

### How Agent Handlers work

Agent Handlers use a work queue in the McAfee ePO database as their primary communication mechanism. Agent Handlers check the server work queue every 10 seconds and perform the requested action. Typical actions include wake-up calls, requests for product deployment, and data channel messages. These frequent communications to the database require relatively high speed, low latency connection between the Agent Handler and the McAfee ePO database.

An Agent Handler installation includes only the Apache Server and Event Parser services. You can deploy Agent Handlers on separate hardware, or virtual machines, that coexist in one logical McAfee ePO infrastructure.

![Agent Handler functional diagram](image.png)

**Figure 19-2 Agent Handler functional diagram**

This diagram shows two different network configurations and their Agent Handlers.
• **Simple network** — The primary Agent Handler is installed as a part of the McAfee ePO server. This is sufficient for many small McAfee ePO installations; typically additional Agent Handlers are not required.

• **Complex network** — Multiple remote Agent Handlers are installed on separate servers connected to the McAfee ePO server. Once installed, the additional Agent Handlers are automatically configured to work with the McAfee ePO server to distribute the incoming agent requests. The McAfee ePO console is also used to configure Agent Handler Assignment rules to support more complex scenarios. For example, an Agent Handler behind the DMZ, firewall, or using network address translation (NAT).

Administrators can override the Agent Handler default behavior by creating rules specific to their environment.

**Best practice: Agent Handlers eliminate multiple McAfee ePO servers**

Use Agent Handlers in different geographic regions instead of multiple McAfee ePO servers.

- Multiple McAfee ePO servers cause management, database duplication, and maintenance problems.

Use Agent Handlers to:

- Expand the existing McAfee ePO infrastructure to handle more agents, more products, or a higher load due to more frequent agent-server communication.

- Ensure that agents continue to connect and receive policy, task, and product updates even if the McAfee ePO server is unavailable.

- Expand McAfee ePO management into disconnected network segments with high-bandwidth links to the McAfee ePO database.

Usually, it is more efficient and less expensive to add an Agent Handler rather than a McAfee ePO server.

- Use a separate McAfee ePO server for separate IT infrastructures, separate administrative groups, or test environments.

**Agent Handler functionality**

Agent Handlers provide horizontal network scalability, failover protection, load balancing, and allow you to manage clients behind a DMZ, firewall, or using network address translation (NAT).

**Providing scalability**

Agent Handlers can provide scalability for McAfee ePO managed networks as the number of clients and managed products grow.

One McAfee ePO server can easily manage up to 200,000 systems with only the VirusScan Enterprise product installed. But, as the systems managed and the number of products integrated with your McAfee ePO server increase the attempts to receive policies or send events to your server increase. This load increase also decreases the maximum number of systems manageable with the same McAfee ePO server hardware.

Agent Handlers allow you to scale your McAfee ePO infrastructure to manage more clients and products. You do this by adding Agent Handlers to manage an equivalent or larger number of agents with one logical McAfee ePO deployment. By default, when you install the Agent Handlers software on a server, all Agent Handlers are used at the same order level unless custom assignment rules are created.
**Failover protection with Agent Handlers best practice**

Agent Handlers allow any McAfee Agent to receive policy and task updates and report events and property changes if the McAfee ePO server is unavailable. For example, an upgrade or network problem.

Once multiple Agent Handlers are deployed, they are available to agents as failover candidates. As long as the Agent Handler is connected to the database, it can continue serving agents. This includes any policy or task changes resulting from agent properties or from administrator changes before the McAfee ePO server goes offline.

The configuration file shared with the McAfee Agent contains a configurable fallback list of Agent Handlers. If needed, the McAfee Agent tries to connect through the list of Agent Handlers until the list ends or it can contact a valid, enabled Agent Handler.

Failover between Agent Handlers is configured in one of two ways.

**Simple deployment failover**

In the simple deployment failover, two Agent Handlers can be deployed as primary and secondary. All agents initiate communications with the primary Agent Handler, and only use the secondary Agent Handler if the primary is unavailable. This deployment makes sense if the primary Agent Handler has better hardware, and can handle the whole load of the infrastructure.

*Figure 19-3 Simple Agent Handler failover*
Failover with load balancing

The second deployment combines failover with load balancing. Multiple Agent Handlers are configured into the same Agent Handler group. The McAfee ePO server inserts each Agent Handler in the group into the list of Agent Handlers at the same order level. The McAfee Agent randomizes Agent Handlers at the same order level, which results in an equal load across all Agent Handlers in a particular group.

Figure 19-4  Failover with Agent Handler load balancing

Agents failover between all Agent Handlers in a group before failing through to the next Agent Handler in the assignment list. Using Agent Handler groups results in both load balancing and failover benefits.

Best practices: Network topology and deployment considerations

Agent Handlers allow flexibility in your network configuration, but additional planning can improve your network performance.

Using Agent Handlers behind a DMZ, firewall, or in NAT networks: best practices

Without Agent Handlers, any McAfee Agent behind a DMZ, firewall, or in a NAT network can be viewed with the McAfee ePO server. But you can’t manage or directly manipulate those systems in the NAT network.

With an Agent Handler behind the DMZ, you can address systems within the NAT region for wake-up calls, data channel access, and more.

This Agent Handler connection requires access to both the SQL database and the McAfee ePO server. Some firewall rules are necessary for this configuration.
This diagram shows an Agent Handler with managed systems behind the DMZ and these connections:

- Data Channel connection to the McAfee ePO server
- Low-latency high-speed connection to the SQL database
- Failover connection between the Agent Handlers

Figure 19-5  Agent Handler behind the DMZ

This table lists all ports used by the McAfee ePO server and the other network components.

⚠️ The ports connecting the Agent Handler to the McAfee ePO server and SQL database must be open to connect to the Agent Handler through a firewall.

Table 19-1  Default ports used

<table>
<thead>
<tr>
<th>Server</th>
<th>Direction</th>
<th>Connection</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>To</td>
<td>Web browser</td>
<td>HTTPS 8443</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>To</td>
<td>SQL database</td>
<td>JDBC/SSL 1433</td>
</tr>
<tr>
<td>Agent Handler</td>
<td>From</td>
<td>McAfee ePO</td>
<td>HTTPS 8443 (install), HTTPS 8444</td>
</tr>
<tr>
<td>Agent Handler</td>
<td>Both</td>
<td>McAfee ePO</td>
<td>HTTP 80</td>
</tr>
<tr>
<td>Agent Handler</td>
<td>To</td>
<td>SQL database</td>
<td>ADO/SSL 1433</td>
</tr>
<tr>
<td>Agent Handler</td>
<td>To</td>
<td>Clients</td>
<td>HTTP 8081</td>
</tr>
<tr>
<td>Agent Handler</td>
<td>From</td>
<td>Clients</td>
<td>HTTP 80, HTTPS 443</td>
</tr>
</tbody>
</table>
Roaming with Agent Handlers

Agent Handlers allow users who roam between enterprise network sites to connect to the nearest Agent Handler.

Roaming is possible only if the Agent Handlers from all locations are configured in the McAfee Agent failover list. You can modify policy and system sorting so that roaming systems can receive a different policy in each location.

Repository cache and how it works

Agent Handlers automatically cache content and product updates if a McAfee Agent can’t access the content directly from the Master Repository on the McAfee ePO server.

The McAfee Agent, by default, uses the primary McAfee ePO server (same server as Tomcat) as the Master Repository. Agents fail back to the Agent Handler if they are unable to communicate with their configured remote repository to pull content and product updates. Since the Agent Handler might not be running on the same server as the true Master Repository (on the McAfee ePO server), the Agent Handler manages these requests. Agent Handlers transparently handle requests for software and cache the required files after downloading them from the Master Repository. No configuration is necessary.

This diagram shows how Agent Handlers cache product update content if the configured remote repository is unavailable to remote systems.

Figure 19-6 Agent Handler repository caching
1. Systems 1 and 2 attempt to pull content or product updates from their configured remote repository and the attempt fails.

2. For System 1, the McAfee Agent is configured, by default, to use Primary Agent Handler 1 that is part of the McAfee ePO server. If the connection to the remote repository fails, System 1 requests the content or product updates directly from the Master Repository on the McAfee ePO server.

3. For System 2, the McAfee Agent is configured to use Secondary Agent Handler 2, if the connection to the remote repository fails.

4. Secondary Agent Handler 2 requests the content or product updates from the Master Repository.

5. Secondary Agent Handler 2 caches those updates, for any subsequent requests, and delivers them to System 2.

---

### Best Practices: Agent Handler installation and configuration

You can configure mid-range servers, located within your network, as Agent Handlers by simply installing the Agent Handler software and assigning systems for management.

You can also group Agent Handlers, set their failover priority, and create virtual Agent Handlers behind a DMZ, firewall, or in NAT networks.

> Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change.

### Deployment considerations

Before you deploy Agent Handlers in your extended network, consider the health of your existing McAfee ePO server and database hardware. If this hardware is already overloaded, adding Agent Handlers actually decreases McAfee ePO performance.

A fully configured Agent Handler has about the same hardware and database requirements as a McAfee ePO server. When determining how many Agent Handlers you need, first examine the database usage. If the database serving your McAfee ePO server is under a heavy load, adding Agent Handlers does not improve your performance. Upgrade your SQL Server hardware to take advantage of multiple Agent Handlers. If the database is currently running at a moderate to low load, then additional Agent Handlers can help you expand your logical McAfee ePO infrastructure.

McAfee testing shows that adding Agent Handlers improves performance until your McAfee ePO database CPU load exceeds 70 percent. Since each Agent Handler adds some overhead, for example database connections and management queries to the database, adding Agent Handlers beyond 70 percent database CPU load does not help performance.

### Agent Handler configuration overview

Agent Handlers can be configured to load balance in groups and as virtual Agent Handlers.

Priority assignment rules enable clients to find Virtual Agent Handlers when the Agent Handlers are using different IP address on multiple network segments.

The *McAfee ePolicy Orchestrator Installation Guide* provides instructions for installing remote Agent Handler software.
Agent Handlers configuration page

To configure all Agent Handler management tasks, select Menu | Configuration | Agent Handlers.

1. Handler Status — Provides the number of installed Agent Handlers and if they are active.

2. New Assignment — Opens the Agent Handler Assignment page to create an Agent Handler assignment.

3. Edit Priority — Opens the Edit Priority page to change priority of the Agent Handler assignments.

4. Systems per Agent Handler — Specifies the number of agents assigned to each Agent Handler.

To see a detailed list of the agents assigned to an Agent Handler, click the Agent Handler name in the list or the color associated with the Agent Handler segment in the pie chart.
• **Handler Groups** — Specifies the number of Agent Handler groups that the McAfee ePO server manages.

• **Handler Assignment Rules** — Displays the list of Agent Handler assignments in your environment, their priority, and details about rule settings.

### Configure Agent Handlers list

To see a list of your Agent Handlers and their detailed information, use the Handlers List accessed through the dashboard.

**Task**

1. Select **Menu | Configuration | Agent Handlers**, to configure an Agent Handler.

2. Click the Agent Handlers number in the **Handler Status** of the dashboard, to see a list of your Agent Handlers and their detailed information.

3. Click the setting in the **Actions** column, to disable, enable, and delete Agent Handlers.

4. Click the Agent Handler name in the **Handler DNS Name** column to configure Agent Handler Settings.

5. From the Agent Handler Settings page, configure these properties.
   - **Published DNS Name**
   - **Published IP Address**

6. Click **Save**

### Configure Agent Handlers groups and virtual groups

You can configure your Agent Handlers into groups and create virtual handlers to use behind a DMZ, firewall, or in NAT networks.

**Task**

1. Select **Menu | Configuration | Agent Handlers** and, in the **Handler Group** dashboard, click **New Group** to create Agent Handler groups.

2. From the Agent Handlers Add/Edit Group page, configure these group settings:
   - **Group Name** — Type a name for the Agent Handler group.
   - **Included Handlers** — Allows you to:
     - Click **Use load balancer** to use a third-party load balancer, then type the **Virtual DNS Name** and **Virtual IP address** in the fields (both are required).
     - Click **Use custom handler list** and use + and – to add and remove additional Agent Handlers. Use the drag-and-drop handle to change the priority of Agent Handlers.

3. Click **Save**
Configure Agent Handlers priority

You can configure the failover priority of your Agent Handlers by setting their failover priorities. When you have multiple Agent Handlers, configure the primary Agent Handler in the McAfee ePO Server as the lowest priority Agent Handler. This priority:

- Forces systems to connect to all other Agent Handlers before connecting to the primary McAfee ePO Server Agent Handler
- Reduces the McAfee ePO Server load so that it can perform other tasks like displaying the McAfee ePO console user interface and running reports and server tasks

**Task**

1. Select **Menu | Configuration | Agent Handlers**, then click **Edit Priority** to create Agent Handler groups.

2. Click and drag the Agent Handlers to create the priority list you need for your network.

   This screenshot shows the McAfee ePO Server, shown as "ePO 1," configured as priority 2 and "Agent Handler 1" configured as priority 1.

   ![Agent Handlers Priority Configuration](image)

3. Click **Save**.

Configure assignments for Agent Handlers

You can assign agents to use Agent Handlers individually or as groups.

- **When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.**

**Task**

1. Select **Menu | Configuration | Agent Handlers**, then click **New Assignment** to change the assignments for Agent Handlers.

2. From the Agent Handler Assignment page, configure these settings:
   - **Assignment Name** — Type a name for the assignment.
   - **Agent Criteria** — Choose one of these methods to assign agents to Agent Handlers:
     - **System Tree location** — Click **System Tree**, select the System Tree Group from the dialog box, then click **OK**.
     - **Agent Subnet** — Type the IPv4/IPv6 address, IPv4/IPv6 address ranges, subnet masks, or subnet masks range.
• **Handler Priority** — To configure the priority used by the McAfee Agent, select:
  
  • **Use all agent handlers** — Agents randomly select which handler to communicate with.
  
  • **Use custom handler list** — Use + and – to add more or remove Agent Handlers. Use the drag-and-drop handle to change the priority of handlers.

3 Click **Save**.

---

**Best Practices: Adding an Agent Handler in the DMZ**

Agent Handlers in the DMZ allow you to directly manage systems with a McAfee Agent installed. Without an Agent Handler installed in the DMZ, you can only view those systems with your McAfee ePO server.

The Agent Handler you install in the DMZ has specific hardware and software requirements. These requirements are similar to the McAfee ePO server requirements. See this information before you begin:

• See the **Best Practices Guide for server hardware requirements** for Agent Handler hardware and operating system requirements.

These are the major steps to configure an Agent Handlers in the DMZ.

1 Install the Windows Server hardware and software in the DMZ between your networks that are internal and external to McAfee ePO.

2 Configure all ports on your firewall between your McAfee ePO server and SQL database and the Agent Handler.

3 Install the McAfee ePO remote Agent Handler software using the information in the **McAfee ePolicy Orchestrator Installation Guide**.

4 If needed, create a subgroup of systems to communicate with the McAfee ePO server through the Agent Handler.

5 Create an Agent Handlers assignment.

6 Configure the Agent Handlers priority list and enable the Agent Handler in the DMZ.

**Configure hardware, operating system, and ports**

Installing the Agent Handler server hardware and software, and configuring the firewall ports are the first steps before using McAfee ePO to manage systems behind a DMZ.

*Before you begin*

Make sure that your Agent Handler server meets all hardware and software requirements.

**Task**

1 Build the Agent Handler server hardware with the Microsoft Windows Server operating system.

2 Install the server in the DMZ behind the firewall in the protected network.

3 Configure your Domain Name System (DNS) server to add the Agent Handler server behind the firewall in the protected network.
4 Configure these ports on the internal-facing firewall to communicate between the McAfee ePO server and the Agent Handler in DMZ:
   - Port 80 — Bidirectional
   - Port 8443 — Bidirectional
   - Port 8444 — Bidirectional
   - Port 443 — Bidirectional

5 Optional — If your SQL database is installed on a different server than your McAfee ePO server, configure these two ports on the internal-facing firewall for that connection to the Agent Handler:
   - Port 1433 TCP — Bidirectional
   - Port 1434 UDP — Bidirectional

6 Configure these ports on the public-facing firewall to communicate between the McAfee ePO server and the Agent Handler in the DMZ:
   - Port 80 TCP — Inbound
   - Port 443 TCP — Inbound
   - Port 8081 TCP — Inbound
   - Port 8082 UDP — Inbound

Install software and configure the Agent Handler

When you complete the McAfee ePO Agent Handler software installation and configuration, your Agent Handler allows you to directly manage systems behind the DMZ.

Before you begin
- You must have installed the Agent Handler hardware and operating system in the DMZ of your external network.
- You must have access to the McAfee ePO executable files located in the downloaded McAfee ePO installation files.

Task

1 Install the McAfee ePO remote Agent Handler software. See the McAfee ePolicy Orchestrator Installation Guide.

2 Use one of these methods to communicate through the Agent Handler to the McAfee ePO server:
   - Create a subgroup of systems. This task uses a subgroup, NAT Systems, in the System Tree behind the DMZ.
   - In Agent Subnet, type IP addresses, IP address ranges, or subnet masks, separated by commas, spaces, or new lines.

3 To start the Agent Handler configuration on the McAfee ePO server, select Menu | Configuration | Agent Handlers.
4 To open the Agent Handler Assignment page, select **New Assignment**.

![Agent Handlers Configuration](image)

**Figure 19-8 Agent Handler Assignment page**

5 Configure these settings:

a Type an **Assignment Name**. For example, **NAT Systems Assignment**.

b Next to Agent Criteria, click **Add Tree Locations** and the "..." to select a System Tree group (for example, **NAT Systems**) and click **OK**. For example, select the NAT Systems group.

c Next to Handler Priority, click **Use custom handler list** and **Add Handlers**.

d From the list, select the Agent Handler to handle these selected systems. Disregard the warning that appears.

e Click **Save**.

6 To configure the Agent Handler as the highest priority for the systems behind the DMZ, click **Edit Priority** and configure these settings, from the Agent Handler Configuration page:

a Move the Agent Handler to the top of the priority list by moving the Agent Handler names.

b Click **Save**.
From the Agent Handler configuration page, in the Handler Status dashboard, click the number of the Agent Handler to open the Agent Handlers List page.

![Agent Handlers Settings page](image)

**Figure 19-9  Agent Handler Settings page**

From the Agent Handler Settings page, configure these settings and click **Save**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published DNS Name</td>
<td>Type the configured name for the Agent Handler.</td>
</tr>
<tr>
<td>Published IP Address</td>
<td>Type the configured IP address for the Agent Handler.</td>
</tr>
</tbody>
</table>

From the Handlers List page, in the row for the Agent Handler in the DMZ, click **Enable** in the Actions column.

The systems designated to use the Agent Handler begin getting their changes during the next few agent-server communications.
10 Confirm that the Agent Handler in the DMZ is managing the systems behind the DMZ:
   a. From the Agent Handlers Configuration page, in the Systems per Agent Handler dashboard, click the Agent Handler name in the list or its corresponding color in the pie chart.
   b. From the Agents for Agent Handler page, confirm that the correct systems appear in the list.
      It might take multiple instances of the agent-server communication before all systems appear in the list.

With the Agent Handlers in the DMZ and configured with the McAfee ePO server, you can now directly manage systems with a McAfee Agent installed behind the DMZ.

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

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

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

**Task**

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

**d**  Right-click the database instance name and click **Properties**.

The system administrator account is enabled.

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

**a**  Open a web browser and go to `https://localhost:8443/core/config-auth`.

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

**b**  Log on with your McAfee ePO credentials.

**c**  Delete the entry in the **User Domain** field, then type `sa`.

**d**  Provide a password for the system administrator account, then click **Test Connection**.

**e**  If the test is successful, click **Apply**.

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

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

---

**Handler groups and priority**

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

**Handler groups**

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

Grouping handlers and assigning priority is customizable, so you can meet the needs of your specific environment. Two common scenarios for grouping handlers are:
• Using multiple handlers for load balancing
  You might have many 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 uses 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 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.

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

Task

1. Select Menu | Configuration | Agent Handlers, then click Actions | New Assignment.

2. Specify a unique name for this assignment.

3. Specify the agents for this assignment using one or both of the following Agent Criteria options:
   • Browse to a System Tree location.
   • Type the IP address, IP range, or subnet mask of managed systems in the Agent Subnet field.

4. Specify Handler Priority by deciding whether to:
   • Use all Agent Handlers — Agents randomly select which handler to communicate with.
   • Use custom handler list — When using a custom handler list, select the handler or handler group from the
     drop-down menu.

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

Complete common management tasks for Agent Handler assignments.
To perform these actions, select Menu | Configuration | Agent Handlers, then in Handler Assignment Rules, click Actions.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a handler assignment</td>
<td>Click Delete in the selected assignment row.</td>
</tr>
<tr>
<td>Edit a handler assignment</td>
<td>Click Edit for the selected assignment. The Agent Handler Assignment page opens, where you can specify:</td>
</tr>
<tr>
<td></td>
<td>• Assignment name — The unique name that identifies this handler assignment.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Use the drag-and-drop handle to quickly change the priority of handlers in your custom handler list.</td>
</tr>
<tr>
<td>Export handler assignments</td>
<td>Click Export. The Download Agent Handler Assignments page opens, where you can view or download the AgentHandlerAssignments.xml file.</td>
</tr>
<tr>
<td>Import handler assignments</td>
<td>Click Import. The Import Agent Handler Assignments dialog box opens, where you can browse to a previously downloaded AgentHandlerAssignments.xml file.</td>
</tr>
<tr>
<td>Edit the priority of handler assignments</td>
<td>Click Edit Priority. The Agent Handler Assignment</td>
</tr>
<tr>
<td>View the summary of handler assignments details</td>
<td>Click &gt; in the selected assignment row.</td>
</tr>
</tbody>
</table>

Create Agent Handler groups

Handler groups make it easier to manage multiple handlers throughout your network, and can play a role in your fallback strategy.

Task

1. Select 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:
   • Click Use load balancer to use a third-party load balancer, then enter the Virtual DNS Name and Virtual IP address (both are required).
   • Click Use custom handler list to specify which Agent Handlers are included in this group.

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

Manage Agent Handler groups

Complete common management tasks for Agent Handler groups.
To perform these actions, select Menu | Configuration | Agent Handlers, then click the Handler Groups monitor.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a handler group</td>
<td>Click Delete in the selected group row.</td>
</tr>
<tr>
<td>Edit a handler group</td>
<td>Click the handler group. The Agent Handler Group Settings page opens, where you can specify:</td>
</tr>
<tr>
<td></td>
<td>• Virtual DNS Name — The unique name that identifies this handler group.</td>
</tr>
<tr>
<td></td>
<td>• Virtual IP address — The IP address associated with this group.</td>
</tr>
<tr>
<td></td>
<td>• Included handlers — Choose whether to use a third-party load balancer or a custom handler list.</td>
</tr>
</tbody>
</table>

Use a custom handler list to specify which handlers, and in what order, agents assigned to this group communicate with.

Enable or disable a handler group Click Enable or Disable in the selected group row.

Move agents between handlers

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

Tasks

- Group agents using Agent Handler assignments on page 278
  Create Agent Handler assignments to group McAfee Agents together.
- Group agents by assignment priority on page 279
  Group agents together and assign them to an Agent Handler that is using assignment priority.
- Group agents using the System Tree on page 280
  Group agents together and assign them to an Agent Handler using the System Tree.

Group agents using Agent Handler assignments

Create Agent Handler assignments to group McAfee Agents together.
Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

💡 When assigning agents to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.
Task

1. Select **Menu | Configuration | Agent Handlers**, then click the required Handler Assignment Rule. The Agent Handler Assignment page appears.

   ![Information icon]
   If the Default Assignment Rules is the only assignment in the list, you must create an assignment.

2. Type a name for the **Assignment Name**.

3. You can configure **Agent Criteria** by System Tree locations, by agent subnet, or individually using the following:
   - **System Tree Locations** — Select the group from the **System Tree location**.
     
     ![Information icon]
     You can browse to select other groups from the Select System Tree Group dialog box and use + and - to add and remove System Tree groups that are displayed.
   
   - **Agent Subnet** — In the text field, type IP addresses, IP address 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.

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

5. Click **Save**.

**Group agents by assignment priority**

Group agents together and assign them to an Agent Handler that is using assignment priority. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers. This list defines the order in which agents attempt to communicate using a particular Agent Handler.

![Information icon]
When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

Task

1. Select **Menu | Configuration | Agent Handlers**.

   ![Information icon]
   If 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**.
As needed, modify the priority or hierarchy of the assignments by clicking **Actions | Edit Priority**.

Moving one assignment to a priority lower than another assignment creates a hierarchy where the lower assignment is actually part of the higher assignment.

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 **Quick Actions**, click **Move to Top** to automatically move the selected assignment to the top priority.

When assignment priority is configured correctly, click **Save**.

**Group agents using the System Tree**

Group agents together and assign them to an Agent Handler using the System Tree. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

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

**Task**

1. Select **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**.

**Frequently asked questions**

Here are answers to frequently asked questions.

**What data is sent to the McAfee ePO server and what is sent to the database?**

A data channel is a mechanism for McAfee products to exchange messages between their endpoint plug-ins and their management extensions. The data channel provides most data sent from the Agent Handler to the application server. It is used internally by the McAfee ePO server for agent deployment and wake-up progress messaging. Other functions such as agent properties, tagging, and policy comparisons are performed directly against the McAfee ePO database.

**If the McAfee ePO server is not defined in my repository list, does replication still occur?**

Yes, if the agent contacts the Agent Handler for software packages, the Agent Handler retrieves them from the McAfee ePO server Master Repository.

**How much bandwidth is used for communication between the database and the Agent Handler?**

Bandwidth between the Agent Handler and the database varies based on the number of agents connecting to that Agent Handler. But, each Agent Handler places a fixed load on the database server for:
• Heartbeat (updated every minute)
• Work queue (checked every 10 seconds)
• Database connections held open to the database (two connections per CPU for EventParser plus four connections per CPU for Apache)

How many agents can one Agent Handler support?

Agent Handlers for scalability are not required until a deployment reaches 100,000 nodes. Agent Handlers for topology or failover might be required at any stage. A good rule is one Agent Handler per 50,000 nodes.

What hardware and operating system should I use for an Agent Handler?

Use the Microsoft Server Operating System (2008 SP2+ server or 2012 64-bit server).

Non-server Operating System versions have severe (~10) limits set on the number of incoming network connections.
Once your McAfee ePO server is configured and protecting your systems there are some tasks to perform to keep your server running at peak efficiency.

Contents

- Maintaining your McAfee ePO server
- Managing SQL databases
- Bandwidth usage

Maintaining your McAfee ePO server

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

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

Best practices: Monitoring server performance

Periodically check how hard your McAfee ePO server is working so that you can create benchmarks and avoid performance problems.

If you suspect your McAfee ePO server is having performance problems, use Windows Task Manager and Windows Server Reliability and Performance Monitor to check the performance.

Using Windows Task Manager

The first steps to take if your McAfee ePO server is having performance problems are to start Windows Task Manager on the server and check McAfee ePO server performance.

- Is there excessive paging?
- Is the physical memory over-utilized?
- Is the CPU over-utilized?

See How to use and troubleshoot issues with Windows Task Manager (http://support.microsoft.com/kb/323527), for details.
Using the Windows Reliability and Performance Monitor
When you install McAfee ePO server, custom counters are added to the built-in Windows Reliability and Performance Monitor. Those counters are informative and can give you an idea of how hard the McAfee ePO server is working.

You must use the 32-bit version of the Reliability and Performance Monitor found at `C:\Windows\SysWOW64\perfmon.exe`. The default 64-bit version of Reliability and Performance Monitor does not have the custom McAfee ePO counters added.

See these links for Microsoft Windows Performance Monitor information:

Finding and using Performance Monitor
To use the custom McAfee ePO counters with the Windows Performance Monitor, you must use the 32-bit version of the tool.

This diagram shows how to find and use Windows Performance Monitor.

![Figure 20-1 Windows Performance Monitor showing the ePolicy Orchestrator Server counters](image)

1. To find the 32-bit version of the Windows Performance Monitor, use Windows Explorer and navigate to `C:\Windows\SysWOW64`, then find and double-click `perfmon.exe`.
2. To confirm that you opened the 32-bit version of Performance Monitor, click Monitoring Tools | Performance Monitor, Add Counters, then click the + sign to open the Add Counters dialog box.
3. To find the McAfee ePO server counters, scroll down the list of counters, find ePolicy Orchestrator Server, and expand the list.

Now you can start using the counters to test and create benchmarks for your McAfee ePO server performance.
Use perfmon with McAfee ePO: best practice
The 32-bit Windows Reliability and Performance Monitor (perfmon) is a tool to develop server benchmarks, which can help you manage your server performance.

Task
1 Start the Windows Performance Monitor.
2 In the Add Counters list, browse or scroll down to the ePolicy Orchestrator Server counters selection, then click + to expand the list of counters.
3 To view the output as a report, click the Change Graph Type icon and select Report from the list.
   For example, the Open ePO Agent Connections counter tells you how many agents are communicating with the McAfee ePO server simultaneously. A healthy McAfee ePO server keeps this number fairly low, usually under 20. For a McAfee ePO server that is struggling, this number is over 200 (the maximum is 250) and stays high, and rarely drops below 20.
4 Click Add to move the selected counter into the Added counters list, then click OK.
5 To determine the stress on your McAfee ePO server and how quickly it can process events from all your agents, add the following counters, then click OK.
   • Completed Agent Requests/sec
   • Currently Running Event Parser Threads
   • Data Channel saturation
   • Data channel threads
   • Event Queue Length
   • Max Event Parser Threads
   • Open ePO Agent Connections
   • Processor Events/sec
   • Static event queue length

The tests listed here are just a few that you can perform with the McAfee ePO server using the Windows Performance Monitor. For additional Windows Performance Monitor information, see these Microsoft websites:

Check event processing: best practice
The number of events appearing in the McAfee ePO database events folder can indicate the performance of your McAfee ePO server.

Task
1 Using Windows Explorer, navigate to this folder:
   C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events
   At any time, this folder might display a few dozen or a few hundred events.
   In larger environments, this folder is constantly processing thousands of events per minute.
2 Click the Refresh icon multiple times, then look at the status bar to see the number of files in this folder changing quickly.

If there are thousands of files in this folder and McAfee ePO is unable to process them, the server is probably struggling to process the events at a reasonable rate.

It is normal for this Events folder to fluctuate depending on the time of day. But, if there are thousands of files in this folder and it is constantly increasing then that probably indicates a performance issue.

3 Confirm that the events are not occurring faster than the event parser can process them. This causes this folder to grow quickly. Use these steps to confirm the event parser is running.
   a To open the Windows Services Manager and confirm that the event parser is running, click Start, Run, type services.msc and click OK.
   b In the Services Manager list, find McAfee ePolicy Orchestrator 5.9.0 Event Parser and confirm it is Started.

4 Check the event parser log file for any errors, using these steps.
   a Go to the log file folder at this path: 
      C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Logs
   b Open this log file and check for errors:
      eventparser_<servername>.log

5 Use these steps if the events are still occurring faster than the event parser can process them.
   a Open the Services Managers list again and temporarily stop all three of these McAfee ePO services:
      • McAfee ePolicy Orchestrator 5.9.0 Application Server
      • McAfee ePolicy Orchestrator 5.9.0 Event Parser
      • McAfee ePolicy Orchestrator 5.9.0 Server
   b Move the contents of the C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events\ folder to another location, or delete the events, if you're not worried about losing the data.

### Maintaining your SQL database

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

### Maintaining the McAfee ePO SQL database best practice

The SQL database requires regular maintenance and back ups to ensure that McAfee ePO functions correctly. The McAfee ePO SQL database houses everything that McAfee ePO uses to function; your System Tree structure, policies, administrators, client tasks, and configuration settings.

Perform these tasks regularly to maintain your SQL Server:
   • Regularly back up the McAfee ePO SQL database and its transaction log.
   • Reindex your database regularly.
• Rebuild your database regularly.
• Purge older events using server tasks.

Back up your SQL database regularly, in case your SQL database or your McAfee ePO server environment fails. If the McAfee ePO server must be rebuilt or restored, current back ups ensure that a safe copy is available. In addition, if you are using the information in the Microsoft website, *Full Database Backups (SQL Server)* ([https://msdn.microsoft.com/en-us/library/ms186289.aspx](https://msdn.microsoft.com/en-us/library/ms186289.aspx)), your transaction log can continue to grow indefinitely until a full backup is performed.

**Table data fragmentation**

One of the most significant performance problems found in databases is table data fragmentation. For example, table fragmentation can be compared to an index at the end of a large book. One index entry in this book might select several pages scattered throughout the book. You must then scan each page for the specific information you are looking for.

This fragmented index is different from the index of the telephone book that stores its data in sorted order. A typical query for the name "Jones" might span multiple consecutive pages, but they are always in a sorted order.

For a database, you start with the data looking like a telephone book and, over time, end up with the data looking more like a large book index. You must occasionally resort the data to re-create the phone book order. This is where reindexing and rebuilding your McAfee ePO SQL database is critical. Over time your database becomes more fragmented, especially if it manages a larger environment where thousands of events are written to it daily.

Setting up a maintenance task to automatically reindex and rebuild your McAfee ePO SQL database takes only a few minutes and is essential to maintain proper performance on the McAfee ePO server. You can include the reindexing as part of your regular backup schedule to combine everything in one task.

**Do not** shrink your database. Data file shrink causes serious index fragmentation. Shrinking the database is a common mistake that many administrators make when building their maintenance task.

**Learn more**

For details about creating your maintenance task, see KnowledgeBase article *Recommended maintenance plan for McAfee ePO database using SQL Server Management Studio*, KB67184.

To learn more about database fragmentation and how to determine the fragmentation of your database, use the DBCC command found in the *Understanding SQL Server’s DBCC SHOWCONTIG* ([http://www.sql-server-performance.com/2002/dt-dbcc-showcontig/](http://www.sql-server-performance.com/2002/dt-dbcc-showcontig/)).

To learn more about maintaining and optimizing your SQL database, see these documents:

• **Improving McAfee ePO Performance by Optimizing SQL** ([https://community.mcafee.com/docs/DOC-2926](https://community.mcafee.com/docs/DOC-2926))

• **McAfee ePO Maintenance Utility** ([https://community.mcafee.com/docs/DOC-4021](https://community.mcafee.com/docs/DOC-4021))

**Best practice: Test SQL database connectivity with test.udl file**

For database connection issues, you can use the test.udl file to confirm the database credentials used to access the SQL database from the McAfee ePO server.

**Before you begin**

You must know the SQL database server name and database name on the server. Use the [https://<localhost>:8443/core/config-auth](https://<localhost>:8443/core/config-auth) URL to learn this information.
20

Maintaining your McAfee ePO server, SQL databases, and bandwidth
Maintaining your McAfee ePO server

If you are troubleshooting McAfee ePO database connection problems, you might see this error in the orion.log
file:
Login failed for user ''. The user is not associated with a trusted SQL Server connection
Task

1

On the McAfee ePO server, create a file named test.udl.

2

Double-click the file you created to display the Data Link Properties user interface.

3

Click the Provider tab, select Microsoft OLE DB Provider for SQL Server from the OLE DB Provider(s) list, then click
Next.

4

On the Connection tab, configure this information:
•

Select or enter a server name — Type the server name, instance, and port using this format:
<servername>\<instancename>,<port>.
If no named database instance is used, use this format: <servername>,<port>

5

•

Enter information to log on to the server — Type the SQL database credentials.

•

Select the database on the server — Type the database name.

Click Test Connection.

The Microsoft Data Link dialog box should display Test connection succeeded.

Best practices: Recommended tasks
McAfee recommends that you perform certain tasks daily, weekly, and monthly to ensure that your managed
systems are protected and your McAfee ePO server is working efficiently.
Because all networks are different, your environment might require more detailed steps, or only some of the
steps, described in this section.
These are suggested best practices and do not guarantee 100-percent protection against security risks.

The processes outlined share these features:

288

•

Once you learn the processes, they don't take too long to perform.

•

They are repeatable, manageable, and effective practices.

•

They are based on input from McAfee experts and IT managers.

McAfee ePolicy Orchestrator 5.9.0 Product Guide


Recommended daily tasks: best practice

Perform these McAfee recommended tasks at least once a day to ensure that your McAfee ePO server-managed systems are safe from threats and your McAfee ePO server is functioning normally.

Before you make any major changes to policies or tasks, McAfee recommends that you back up the database or create a snapshot of the records in the McAfee ePO database.

Figure 20-2 Suggested McAfee ePO daily tasks

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

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.
### Table 20-1  Recommended McAfee ePO daily tasks details

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Daily threat tasks</strong></td>
<td><strong>Task</strong>                                                                                                                                  <strong>Description</strong></td>
</tr>
<tr>
<td>Periodically check McAfee ePO Dashboards for threat events.</td>
<td>Throughout the day, review your dashboards for threats, detections, and trends. Set up automated responses to send emails to administrators when threat activity thresholds are met.</td>
</tr>
<tr>
<td><strong>Examine product specific reports, such as VirusScan Enterprise, Endpoint Security, Access Protection, or McAfee Host IPS, for threat events</strong></td>
<td>Examine reports for any events that might indicate a new vulnerability in the environment. Create a server task to schedule queries and send the results to you. Using this data, you might create policies or edit existing policies.</td>
</tr>
</tbody>
</table>
| React to alerts.                               | If new alerts are found, follow your company’s internal procedure for handling malware. Collect and send samples to McAfee and work toward cleaning up the environment. Ensure that signature files are updated and run on-demand scans as needed. See Troubleshooting procedure for finding possible infected files, KB53094.

Run queries or review dashboards periodically to check for alerts collected from your managed devices. Also watch for these threat signs:
- High CPU usage on undetermined processes
- Unusually high increases in network traffic
- Services added or deleted by someone other than you
- Inability to access network or administrative shares
- Applications or files that stop functioning
- Unknown registry keys added to start an application
- Any browser home page that changed outside your control
- Examine the VSE: Trending Data Dashboard and look at the VSE: DAT Deployment information to determine whether your signature files are up to date.
- Files being created or changed on an endpoint (review Access Protection Rules).

| **Review the McAfee Global Threat Intelligence (GTI) at McAfee Labs Threat site at least once a day.** | To access the McAfee Labs Threat site, select Menu | Reporting | Dashboards. Select the ePO Summary dashboard and in McAfee Links, click Global Threat Intelligence.                                                                                                                                                                                                 |
| **Examine Top 10 reports for infections at the site, group, system, and user level.** | McAfee ePO provides preconfigured Top 10 reports that display statistics on infections in your environment. Determine which users, systems, and parts of the network have the most infections or vulnerability. These reports might reveal weakness in the network, where policies must be adjusted. |
| **Daily security maintenance tasks**          | **Task**                                                                                                                                  **Description**                                                                                                               |
| Examine the DAT deployment reports.          | It is important to have 100 percent deployment of the most recent DAT file to all managed systems. Make sure that clients have an update task configured to run multiple times a day to keep the DAT file current.

Run the VSE: DAT Adoption, VSE: DAT Adoption Over the Last 24 Hours, queries or the VSE: DAT Deployment query frequently throughout the day to ensure that systems are running the latest DATs. |
Table 20-1  Recommended McAfee ePO daily tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check compliance queries and reports.</td>
<td>In Queries &amp; Reports, find the compliance queries that identify systems that have not updated a managed product version with an engine, hotfix, or patch. Create a process to make sure that systems are up to date. For example, run an update or deployment task to ensure compliance.</td>
</tr>
<tr>
<td></td>
<td>Out-of-compliance system numbers drop until all systems have checked in and updated their software.</td>
</tr>
</tbody>
</table>
| Review the inactive agents log to determine which systems are not reporting to McAfee ePO. | In Server Tasks, run the Inactive Agent Cleanup Task. This task identifies systems that have not connected to the McAfee ePO server for a specific number of days, weeks, or months. You can use this task to move inactive systems to a new group in the System Tree, tag the systems, delete the systems, or email a report. If the systems are on the network but having difficulty checking into the McAfee ePO server, you might perform one of these actions:  
  • Use a Ping Agent or Agent Wake-Up Call to check if a system is online and able to perform an agent-server communication with the McAfee ePO server.  
  • Reinstall the McAfee Agent to ensure that the system is communicating with the McAfee ePO server. |
| Ensure that Active Directory or NT Synchronization is working. | Active Directory or NT Domain synchronization pulls in a list of new systems and containers that must be managed by McAfee ePO. If they are used, confirm that the Sync task can be configured to run at least once a day and is working. |
|                                           | If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection.                                  |
| Confirm that a Memory Process Scan occurs at least daily. | Using the Threats Dashboard, confirm that the results of these scans don't indicate an increase in threats. |
|                                           | Run memory process scans frequently, because they are quick and unobtrusive.                                                             |
| Check Rogue System Detection              | Rogue System Detection tells you which devices are attached to the network. It reports unmanaged systems, so they can be quickly found and removed from the network. |
| Daily SQL database tasks                  | Use the Microsoft SQL Enterprise Manager to back up the McAfee ePO database. Verify that the back up was successful after it has completed. |
| Perform an incremental backup of the McAfee ePO database. | You can use the McAfee ePO Disaster Recovery feature to create a snapshot of the records in the McAfee ePO database to quickly recover or reinstall your software, if needed. |
|                                           | You can use the McAfee ePO Disaster Recovery feature to create a snapshot of the records in the McAfee ePO database to quickly recover or reinstall your software, if needed. |
|                                           | See these documents for additional information:  
  • This guide for Disaster Recovery details.  
  • How to back up and restore the ePO database using SQL Server Management Studio, KB52126  
  • McAfee ePO server backup and disaster recovery procedure, KB66616 |
Recommended weekly tasks: best practice

Perform the McAfee suggested tasks at least once a week to ensure that your McAfee ePO server-managed systems are safe from threats and your McAfee ePO server is functioning normally.

Figure 20-3  Suggested McAfee ePO weekly tasks

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

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.
### Table 20-2  Recommended McAfee ePO weekly tasks details

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Weekly McAfee ePO tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Check for McAfee product hotfixes, extensions, and patch updates on the McAfee website or from the Software Manager.</td>
<td>McAfee periodically releases patches and hotfixes, as well as DATs and Engine updates. Check the McAfee website and McAfee ePO Software Manager frequently for new updates to check in to the McAfee ePO console for local environment testing. You can also use the Software Manager to download and check in these updates.</td>
</tr>
<tr>
<td>Run a full replication to all distributed repositories.</td>
<td>Distributed repositories can become corrupt because of an incomplete replication task. Remove corrupt files in the repositories by running a full replication to all distributed repositories once a week. Full replication tasks delete the existing repository contents and replace them with new files.</td>
</tr>
<tr>
<td>Run Distributed Repository Status.</td>
<td>Select <strong>Menu</strong></td>
</tr>
</tbody>
</table>
| Schedule an On-Demand Scan of all systems in your environment. | Schedule an on-demand scan of all systems in your environment that runs during off-hours.  
  
  See these documents for additional information:  
  • Best Practices for On-Demand Scans in VirusScan Enterprise 8.8, KB74059  
  • Best Practices for On-Demand Scans in VirusScan Enterprise 8.8, TU30280 — Tutorial.  
  • VirusScan Enterprise 8.8 Product Guide for details about configuring on-demand scans  
  • How to create a McAfee ePO validation report for the event '1203, KB69428. |
| **Weekly SQL database tasks**                  |                                                                                                                                                                                                           |
| Back up the McAfee ePO SQL database.           | Use the Microsoft SQL Enterprise Manager to back up the McAfee ePO database. Verify that the back-up was successful after it has completed.  
  
  You can use the McAfee ePO Disaster Recovery feature to create a snapshot of the records in the McAfee ePO database to quickly recover, or reinstall your software, if needed.  
  
  See these documents for additional information:  
  • How to back up and restore the ePO database using SQL Server Management Studio, KB52126  
  • McAfee ePO server backup and disaster recovery procedure, KB66616 |
| **Weekly Windows Server operating system tasks** |                                                                                                                                                                                                           |
| Remove inactive systems from Active Directory.  | Active Directory pulls in a list of new systems and containers that must be managed by McAfee ePO. Confirm that the synchronization task is configured to run at least once a day and is working.  
  
  If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection. |
**Recommended monthly tasks: best practice**

Perform the McAfee suggested tasks at least once a month to ensure that your McAfee ePO server managed systems are safe from threats and your McAfee ePO server is functioning normally.

![Diagram](image)

*Figure 20-4  Suggested McAfee ePO monthly tasks*

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

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

**Table 20-3  Recommended McAfee ePO monthly tasks details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monthly McAfee ePO tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Purge events to reduce database size.</td>
<td>Purge events automatically.</td>
</tr>
</tbody>
</table>
| Remove and update duplicate GUIDs. | Run the Duplicate Agent GUID server tasks to find and fix any duplicate GUIDs in your environment.  
   Also, run these server tasks:  
   • Duplicate Agent GUID - clear Error Count  
   • Duplicate Agent GUID - remove systems with potentially duplicated GUIDs |
Table 20-3  Recommended McAfee ePO monthly tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Audit Logs.</td>
<td>Review the McAfee ePO Audit Logs to ensure that individuals with administrative rights are making only approved changes to system configurations, tasks, and policies.</td>
</tr>
<tr>
<td>Validate McAfee ePO Administrator and Reviewer IDs</td>
<td>Confirm that only employees authorized to have administrative access have properly configured IDs, with the proper permission sets in the McAfee ePO system.</td>
</tr>
</tbody>
</table>

**SQL database tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run your McAfee ePO SQL database Maintenance Plan.</td>
<td>Set up and run your SQL Monthly Maintenance Plan. See Recommended maintenance plan for McAfee ePO database using SQL Server Management Studio, KB67184.</td>
</tr>
</tbody>
</table>

**Monthly Windows Server operating system tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Confirm that the Microsoft Operating System and other vendor patch levels on the McAfee ePO server are current. | Review and implement all Microsoft patches to eliminate vulnerabilities and mitigate risk.  
[INFO] Other vendor patches might also be released and need updating to reduce vulnerabilities in the environment. |

**Periodic tasks: best practice**

Performing periodic maintenance is important to ensure proper McAfee ePO server operations. Performing every task daily, weekly, or monthly, is not required. But periodic tasks are important to ensure that overall site health, security, and disaster recovery plans are up to date.

Create a periodic maintenance log to document dates that maintenance was conducted, by whom, and any maintenance-related comments about the task conducted.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess your environment, policies, and policy assignments periodically to confirm that they are still applicable.</td>
<td>Organizational needs can change. Periodically review both existing policies and policy assignments to ensure that they still make sense in the environment. Fewer policies simplify server administration.</td>
</tr>
<tr>
<td>Review existing client tasks and task assignments periodically to confirm that they are still needed.</td>
<td>Client tasks run scans, deploy product updates, product patches and hotfixes, and more to systems managed by McAfee ePO. Clean out unused tasks to reduce system complexity which can ultimately affect database size.</td>
</tr>
<tr>
<td>Review existing tags and tag criteria to ensure that they are still relevant to your environment.</td>
<td>Use tags as an alternative to System Tree groups to combine, or select a group of systems to operate on. For example, to send updates, deploy McAfee managed products, or run scans. Tagging is useful, but you must monitor tags to ensure that they are useful and have the impact needed.</td>
</tr>
<tr>
<td>Review product exclusions (for example, VirusScan Enterprise) and includes/excludes (for example, Access Protection rules) periodically to validate relevancy.</td>
<td>You must keep exclusions as specific as possible in your environment. Products changes can affect the exclusions that you have configured. Periodically review exclusions to ensure that they still accomplish what is needed. Plus, you can use High and Low Risk OnAccess scanning configurations to augment exclusions. Structure the System Tree, or use tags as another method to control exclusions.</td>
</tr>
<tr>
<td>Make any hardware changes or remove any repositories that you want to decommission.</td>
<td>As your network and organization changes, you might find that changing the location and type of repositories you use provides more efficient and effective coverage.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Validate that you have the required software, such as the latest version of the McAfee Agent.</td>
<td>Always use the most current version of McAfee managed products to ensure that you have technical support for those products. Plus, you have the latest features and fixes available.</td>
</tr>
<tr>
<td>Remove any unsupported software or software for products you aren’t using from the master and distributed repositories.</td>
<td>Keeps disk space to a minimum and removes clutter from the McAfee ePO server and distributed repositories. Only keep those products currently in use in your environment in the Master Repository.</td>
</tr>
<tr>
<td>Validate your System Tree and remove any agents that have not communicated with the McAfee ePO server in 30 days or that are de-commissioned.</td>
<td>Keep the System Tree organized and delete systems that are no longer in use, or reporting to McAfee ePO. A clean System Tree ensures that reports do not contain extraneous information. Set up a server task to delete inactive systems.</td>
</tr>
<tr>
<td>Remove server tasks that are no longer used.</td>
<td>Keep only those server tasks that you intend to use in the task listing. You can always disable an unused task that you want to keep, but don’t use regularly. Keeping a minimum list of tasks that you use regularly reduces McAfee ePO complexity.</td>
</tr>
<tr>
<td>Remove Automated Responses that are no longer relevant.</td>
<td>Automated responses are configured to alert individuals, particularly system administrators; when malware event threats, client treats, or compliance issues must be resolved.</td>
</tr>
<tr>
<td>Delete shell systems using a McAfee ePO server task.</td>
<td>Delete systems with incomplete or missing system and product properties from the System Tree. Those systems skew reports and queries, and waste space in the McAfee ePO database.</td>
</tr>
<tr>
<td>Monitor database size</td>
<td>Check the size of the McAfee ePO database and determine whether, and how often, to purge events reported to McAfee ePO. See How to identify why the ePolicy Orchestrator database is large, KB76720. To purge events from the database, see How to remove old events and shrink the ePolicy Orchestrator Cloud database, KB68961 and how to purge the Audit Log, Server Task Log, and Threat Event Log.</td>
</tr>
</tbody>
</table>

**Managing SQL databases**

Back up and restore, maintain, and manage your SQL Server databases.

**Best practice: Maintaining SQL databases**

Your McAfee ePO databases require regular maintenance to promote optimal performance and to protect your data.

Use the Microsoft management tool appropriate for your version of SQL:

<table>
<thead>
<tr>
<th>SQL version</th>
<th>Management tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL 2008 and 2012</td>
<td>SQL Server Management Studio</td>
</tr>
<tr>
<td>SQL Express</td>
<td>SQL Server Management Studio Express</td>
</tr>
</tbody>
</table>

Depending on your deployment of the McAfee ePO software, plan on spending a few hours each week on regular database backups and maintenance. Perform these tasks regularly, either weekly or daily. But, these tasks are not the only maintenance tasks available. See your SQL documentation for details about what else you can do to maintain your database.
Use a remote command to determine the Microsoft SQL database server and name

The following McAfee ePO remote command is used to determine the Microsoft SQL database server and database name.

**Task**

1. Type this remote command in your browser address bar:
   
   `https://<localhost>:8443/core/config`

   In this command:
   - `<localhost>` — Is the name of your McAfee ePO server.
   - `:8443` — Is the default McAfee ePO server port number. Your server might be configured to use a different port number.

2. Save the following information that appears in the **Configure Database Settings** page:
   - Host name or IP address
   - Database name

Configure a Snapshot and restore the SQL database

To quickly reinstall a McAfee ePO server, configure a Disaster Recovery Snapshot to save, or confirm that a snapshot is being saved to the SQL database. Then back up that SQL database, which includes the Snapshot, and copy the database backup file to an SQL Server to create the restoration.

A quick reinstallation of the McAfee ePO server requires these tasks.

**Tasks**

- *Configure Disaster Recovery Server Task on page 297*
  Use the Disaster Recovery Snapshot Server Task to modify the scheduled automatic Snapshots of your McAfee ePO server configuration saved to the SQL database.

- *Use Microsoft SQL to back up and restore the database on page 298*
  To save the Disaster Recovery Snapshot with the McAfee ePO server configuration information, use Microsoft SQL Server procedures.

**Configure Disaster Recovery Server Task**

Use the Disaster Recovery Snapshot Server Task to modify the scheduled automatic Snapshots of your McAfee ePO server configuration saved to the SQL database.

The preconfigured status of your Disaster Recovery Server Snapshot Task depends on the SQL database your McAfee ePO server uses. Disaster Recovery Snapshot is enabled, by default, on all Microsoft SQL Servers.

You can only run one Disaster Recovery Snapshot at a time. If you run multiple Snapshots, only the last Snapshot creates any output and the previous Snapshots are overwritten.

You can modify the default Disaster Recovery Server Task as needed.
Task

1. Select Menu | Automation | Server Tasks, select Disaster Recovery Snapshot Server from the Server Tasks list, and click Edit.

2. From the Disaster Recovery Server Task builder Descriptions tab Schedule status, click Enabled or Disabled as needed.

3. From the Schedule tab, change the following settings as needed:
   - Schedule type — Set the frequency when the Snapshot is saved.
   - Start Date and End Date — Set the start and end dates the Snapshots are saved, or click No End Date to have the task run continuously.
   - Schedule — Set the time when the Snapshot is saved. By default, the Snapshot task runs at 1:59 a.m. daily.

   **Best practice:** Run the Disaster Recovery Server Task during off hours to minimize the changes to the database during the Snapshot creation process.

4. From the Summary tab, confirm that the server task is configured correctly and click Save.

Use Microsoft SQL to back up and restore the database

To save the Disaster Recovery Snapshot with the McAfee ePO server configuration information, use Microsoft SQL Server procedures.

**Before you begin**

To complete this task, you must have connectivity and authorization to copy files between your primary and restore McAfee ePO SQL Servers.

After you create a Snapshot of the McAfee ePO server configuration, you must:

Task

1. Create a Microsoft SQL Server backup of the database using:
   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL

   See your Microsoft SQL Server documentation for details to complete these processes.

2. Copy the backup file created to your restore SQL Server.

3. Restore the backup of the primary SQL database that includes the Disaster Recovery Snapshot records using:
   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL

   See your Microsoft SQL Server documentation for details to complete these processes.

This creates a duplicate SQL Server ready for restoration, if needed, by connecting it to a new McAfee ePO installation using the Restore option.
Use Microsoft SQL Server Management Studio to find McAfee ePO server information

From the Microsoft SQL Server Management Studio, determine your existing McAfee ePO server information.

**Task**

1. Use a Remote Desktop Connection to log on to the Microsoft SQL database server with host name or IP address.

2. Open the Microsoft SQL Server Management Studio and connect to the SQL Server.

3. From the **Object Explorer** list, click `<Database Server Name> | Databases | <Database name> | Tables`.

4. Scroll down to find the **EPOServerInfo** table, right-click the table name, and select **Edit top 200 Rows** from the list.

5. Find and save the information in these database records.
   - ePOVersion — For example `<three-digit ePolicy Orchestrator version>`.
   - DNSName — For example `epo-2k8.servercom`.
   - ComputerName — For example `EPO-2K8`.
   - LastKnownTCPIP — For example `172.10.10.10`.
   - RmdSecureHttpPort — For example `8443`.

Make sure that you have this information in case you ever have to restore your McAfee ePO software.

**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 fields include:

- **Action Taken** — Action that the product took 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 McAfee ePO received the event.
• **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 that 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.
• **UserName** — Threat source user name or email address.

**View and purge the Threat Event Log**
You should periodically view and purge your threat events.

**Task**

1. Select **Menu | Reporting | Threat Event Log**.
2. Select one of these actions.
### Action | Steps
---|---
**View Threat Event Log.** | 1 Click any of the column titles to sort the events. You can also select Actions | Choose Columns and the Select Columns to Display page appears.
2 From the Available Columns list, select different table columns that meet your needs, then click Save.
3 Select events in the table, then click Actions and select Show Related Systems to see the details of the systems that sent the selected events.

**Purge Threat Events.** | 1 Select Actions | Purge.
2 In the Purge dialog box, next to Purge records older than, type a number and select a time unit.
3 Click OK.
Records older than the specified age are deleted permanently.

---

**Best practice: Schedule purging the Threat Event Log**

You can create a server task to automatically purge the Threat Event Log.

**Task**

1. Open the Server Task Builder.
   a. Select Menu | Automation | Server Tasks.
   b. Click New Task.
2. Name and describe the task. Next to Schedule Status, select Enabled, then click Next.
3. Select Purge Threat Event Log from the drop-down list.
4. Select whether to purge by age or from a queries result. If you purge by query, pick a query that results in a table of events.
5. Click Next.
6. Schedule the task as needed, then click Next.
7. Review the task's details, then click Save.

---

**Bandwidth usage**

The McAfee ePO server uses your LAN and WAN bandwidth to receive events from your managed clients and download software to your managed clients. It’s important to understand these requirements to configure your McAfee ePO server to use the bandwidth efficiently.
**Best practice: Agent deployment and bandwidth**

When installing a McAfee ePO server in your environment, you must distribute agents, components, and security products to manage and protect the systems on the network.

During the initial setup of your managed environment, deploying the McAfee Agent generates enough network traffic that we recommend planning the deployment. Although the installation package for the McAfee Agent is smaller than other products (such as VirusScan Enterprise), the agent must be deployed to each client system that you want to manage.

McAfee Agent deployment traffic occurs directly between the McAfee ePO server and the client systems where the agent is deployed.

This table shows the total bandwidth used on a McAfee Agent server, client system, and McAfee Agent SQL database server for McAfee Agent 4.8 deployment.

<table>
<thead>
<tr>
<th>Table 20-4 McAfee Agent bandwidth usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent deployment</strong></td>
</tr>
<tr>
<td>McAfee ePO server</td>
</tr>
<tr>
<td>SQL database server</td>
</tr>
<tr>
<td>Client system</td>
</tr>
</tbody>
</table>

**Actual deployment**

The first and most extensive use of bandwidth occurs when the McAfee Agent installation package is deployed to client systems. You can deploy the McAfee Agent installation package from the McAfee ePO server console to sites, groups, or selected systems in the System Tree. Regardless of the method you use, deploying the agent installation package over the network generates traffic to each system.

How you deploy the McAfee Agent depends on three variables.

- The number of client systems to manage
- Their location in the network topology
- The bandwidth available between the McAfee ePO server and those systems

McAfee recommends deploying agents:

- **In stages** — Do not push network utilization over 80% at any time for a given segment of resources.
- **To individual sites or groups** — This is important if you have more bandwidth-limiting factors such as slower connections between geographic locations.

**Calculating client updates bandwidth best practice**

New product updates use additional bandwidth. Calculate the requirements before you update your products. You can calculate the bandwidth if you know the size of the patch or product being downloaded. To find the exact size of the product installation files in Windows Explorer, right-click the Install folder and click Properties. The product files are at this default path:

C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software\Current\<ProductName>\Install\n
At a minimum, each of your clients must download, on average, 400 KB a day for DAT files. The following examples show how to calculate the bandwidth used for the client updates using this formula:

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

The following examples use this formula to calculate the amount of data pulled a day and describe if creating a local repository reduces the bandwidth.
Example 1 — A small office in India
The small office in India must download the 400 KB a day for DAT files to its 200 nodes. Using the formula:

$(400 \text{ KB}) \times (200 \text{ nodes}) = \text{about 80 MB of data randomly pulled a day to India}$

In the small office in India, you can add a repository, but you must replicate the DAT file from the McAfee ePO server to the repository. This file replication uses about 70 MB of bandwidth a day over a slow WAN link that can negatively affect the WAN link to India because it occurs all at once.

Instead, have the agents connect across the WAN link to the next closest repository to download their DAT file updates. The next repository might be in a larger office, for example Tokyo. The agents can randomly pull their DAT files throughout the day, and their total bandwidth use is only 80 MB.

In this case, do not use a repository in India.

Example 2 — A large office in Tokyo
The large office in Tokyo must download 400 KB a day for DAT files to its 4,000 nodes. Use the formula:

$(400 \text{ KB}) \times (4,000 \text{ nodes}) = \text{about 1.6 GB of data randomly pulled a day to Tokyo}$

The large office in Tokyo, with 4,000 nodes, uses 1.6 GB of bandwidth a day just to update the DAT files alone. Because replication of the DAT file to Tokyo only uses 70 MB of bandwidth a day, it is much more efficient to have a repository in the Tokyo office. Now all DATs are pulled across the LAN instead of across the slower WAN link.

Example 3 — A large office in New York City
The large office in New York City must download a 23-MB patch update for VirusScan Enterprise to its 1,000 nodes. Use the formula:

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

This 23-MB patch is larger than the 400-KB daily DAT files. You probably have a repository in New York depending on the speed of the WAN link to New York and how quickly the patch must be pushed out. You might find a balance if you carefully craft your client tasks to pull updates and patches at a gradual pace instead of deploying the patch to all nodes in one day.

Conclusions
Some McAfee ePO users put a repository at geographic sites that have only a few dozen nodes. If your site does not have at least 200–300 nodes, it cannot benefit from the bandwidth saved using a repository. If there is no local repository, the agents go to the next nearest repository for their updates. This repository might be connecting to the server across a WAN link, but it still uses less bandwidth because you don’t have to replicate the whole repository across the WAN.

The exception to this rule is if you are deploying a larger software package. For example, the VirusScan Enterprise client software is 56 MB. In this case, it is more efficient to place a repository temporarily at a smaller site so that the client’s software can download the 56-MB file locally. Then disable this repository once the client is rolled out.

Best practices: Bandwidth recommendations for repository distribution
If the McAfee ePO server is managing systems across a Wide Area Network (WAN), we recommend that you create at least one distributed repository per Local Area Network (LAN) for client updates.
You must configure when these actions occur, after you install the distributed repository.
• When the repositories are updated from the McAfee ePO server Master Repository
• When the managed systems pull the updates from the distributed repository

These tasks need randomization intervals configured to avoid network bandwidth saturation.

**Number of repositories needed per LAN**

This table lists the suggested number of repositories needed depending on the systems in the LAN and the network bandwidth.

<table>
<thead>
<tr>
<th>Systems in LAN</th>
<th>Network bandwidth (LAN)</th>
<th>100 Mbps</th>
<th>1 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>1 repository</td>
<td>1 repository</td>
<td></td>
</tr>
<tr>
<td>2,000</td>
<td>2 repositories</td>
<td>1 repository</td>
<td></td>
</tr>
<tr>
<td>3,000</td>
<td>3 repositories</td>
<td>1 repository</td>
<td></td>
</tr>
<tr>
<td>4,000</td>
<td>4 repositories</td>
<td>1 repository</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>5 repositories</td>
<td>1 repository</td>
<td></td>
</tr>
<tr>
<td>10,000</td>
<td>10 repositories</td>
<td>2 repositories</td>
<td></td>
</tr>
<tr>
<td>20,000</td>
<td>20 repositories</td>
<td>2 repositories</td>
<td></td>
</tr>
<tr>
<td>30,000</td>
<td>30 repositories</td>
<td>3 repositories</td>
<td></td>
</tr>
</tbody>
</table>

**Repository replication randomization interval setting by WAN bandwidth**

You must consider WAN bandwidth before you set a randomization interval to automate repository replication.

Use these steps in this information to automate repository replication in your network.

1. Create an incremental replication task for each distributed repository in each LAN.
2. According to WAN bandwidth in Mbps, set each task to run sequentially at the minimum of the minutes of the corresponding randomization interval, to avoid overlap.

<table>
<thead>
<tr>
<th>WAN bandwidth Mbps</th>
<th>Randomization interval (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Mbps</td>
<td>1</td>
</tr>
<tr>
<td>5 Mbps</td>
<td>2</td>
</tr>
<tr>
<td>4 Mbps</td>
<td>3</td>
</tr>
<tr>
<td>3 Mbps</td>
<td>4</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>5</td>
</tr>
<tr>
<td>1 Mbps</td>
<td>6</td>
</tr>
</tbody>
</table>

**Randomization interval for client update task**

The client update task you create ensures that systems are current with the latest DAT and engine files. This task requires a randomization interval, with these variables:
To create the client update task, perform these steps.

1. Add the local distributed repository to the repository list in the agent policy.
2. Select the closest repository using **Ping Time**.
3. Create an agent update task with a randomization interval set according to these tables.

### Table 20-7  Recommended interval (minutes) for network bandwidth of 1 Gbps

<table>
<thead>
<tr>
<th>Systems in LAN</th>
<th>Distributed repositories in LAN</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recommended randomization interval (minutes)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2,000</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3,000</td>
<td>15</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4,000</td>
<td>20</td>
<td>15</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>10,000</td>
<td>60</td>
<td>40</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>20,000</td>
<td>120</td>
<td>80</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>30,000</td>
<td>180</td>
<td>120</td>
<td>60</td>
<td></td>
</tr>
</tbody>
</table>

### Table 20-8  Recommended interval (minutes) for network bandwidth of 100 Mbps

<table>
<thead>
<tr>
<th>Systems in LAN</th>
<th>Distributed repositories in LAN</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recommended randomization interval (minutes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>60</td>
<td>30</td>
<td>20</td>
<td>15</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2,000</td>
<td>120</td>
<td>60</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3,000</td>
<td>180</td>
<td>90</td>
<td>60</td>
<td>45</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>4,000</td>
<td>240</td>
<td>120</td>
<td>80</td>
<td>60</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>300</td>
<td>150</td>
<td>100</td>
<td>75</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

### Calculating bandwidth for repository replication and product updates best practice

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

If your enterprise network has geographically diverse networks and WAN network connection speeds that vary, you must calculate the update bandwidth needed from your McAfee ePO server to your managed systems. These are two system update requirements.

- Relatively small, daily, DAT file updates
- Large, infrequent, product software updates
Calculating DAT file bandwidth usage

If you are replicating only DAT files, the bandwidth used is about 70 MB of replication per day. Agents don't use all DAT files that are copied to the repository, but there are 35 incremental DAT files that must be available to all agents in case they are behind on DATs. When determining if you need a repository in a specific location, determine what is more costly in terms of bandwidth usage. You can replicate 70-MB worth of data to a repository, or tell the agents to go to the next nearest repository that might not be located near the agents.

The following example uses updating the DAT files for VirusScan Enterprise, that are released daily. The numbers used to determine if a repository is needed at a site are:

- **400 KB** — The average size of the daily DAT file to download
- **100** — The number of system agents that must download those daily DAT files

**Example 1: Downloading directly from the central McAfee ePO server**

To download the daily DAT file randomly, from the central McAfee ePO server, to the system agents takes the following bandwidth: 100 agents * 400-KB file = about **40 MB of bandwidth**

**Example 2: Downloading the DAT file to the local repository**

For the McAfee ePO server to replicate the DAT file to each repository every day takes at least **70 MB of bandwidth**.

In the previous examples, it is a waste to use 70 MB of bandwidth to download a DAT file to a repository for only 100 system agents. Those 100 system agents can download the same file using only 40 MB of bandwidth.

**Calculating product update bandwidth usage**

Always calculate how much bandwidth the deployment needs by taking the size of the deployment package, multiplied by the number of nodes targeted, divided by the number of repositories used. For example, VirusScan Enterprise 8.8, which is 56 MB, deployed to 1,000 nodes, pulled across three repositories, equals about 56 GB of data. That 56 GB of data is being pulled across three repositories which equal about 19 GB per repository.

```
56 MB (VSE) * 1,000 (nodes) = 56 GB (total) / 3 (repositories) = about 19 GB per repository
```

The following formula calculates the bandwidth to move the 19 GB of data per repository randomly over a 9-hour workday. The total equals about 2.1 GB of data per hour pulled from each repository.

```
19 GB (per repository) / 9 (hours) = about 2.1 GB per hour
```
McAfee ePO provides built-in querying and reporting capabilities. These are highly customizable, flexible, and easy to use.

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

Contents
- Reporting features
- Best practices: How to use custom queries
- Multi-server rollup querying
- Best practices: Running reports with the web API

Reporting features

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

Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change.

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

- Save the output as a report.
- Duplicate the query and change the output.
- View results in the query system.
- Take action on the results as you normally would in the System Tree.

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

Reporting lag time

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

Report lag-time example:
You run a query hourly and the query takes 10 minutes to run.

Events that occur during the 10 minutes, while the query is being run, are not included in that report, but are written to the database.

Those events appear in the next query report run an hour later.

Best practices: How to use custom queries

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

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

You can approach custom queries two ways:

1. You can determine exactly which kind of query that you want to create before you create it.

2. You can explore the Query Builder wizard and try different variables to see the different types of available queries.

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

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

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

Create custom event queries

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

Task

1. Select Menu | Reporting | Queries & Reports, then New Query. The Query wizard opens and displays the Result Types tab.
The result types are organized into groups on the left side of the page. Depending on what extensions have been checked in to McAfee ePO, these groups vary. Most of the result types are self-explanatory, but two of the more powerful result types are Threat Events and Managed Systems. You can access these two events types as shown in the following examples.

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

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

   To create a pie chart, in the Chart type, click **Pie Chart**.

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

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

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

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

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

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

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

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

Only include systems with an older version of VirusScan Enterprise.

Only return systems that have communicated with the McAfee ePO server in the past 14 days.

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

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

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

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

**How event summary queries work best practice**

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

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

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

**Best practice: Create client event summary queries**

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

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

**Task**

1. To create a client events summary query, select **Menu | Reporting | Queries & Reports**.
2. From the Queries page, click **New Query**.
3 From the Query Builder, starting with the **Result Types** tab, click **Events** in the Features Group, **Client Events** in Result Types, then click **Next**.

![Figure 21-3 Query Builder with Client Events selected](image)

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

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

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

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

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

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

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

![Figure 21-4 Query Builder output](image)

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

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

Create a threat events summary query: best practice

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

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

**Task**

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

2. From the Queries page, click New Query.

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

4. From the Chart page, under Summary, click Single Group Summary Table, to display a total count of all threat events in the events table.
5 To create a filter with a good human-readable description of the events, click **Event Description**, in the Labels are list, under Threat Event Descriptions.

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

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

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

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

\[
(10,000 \text{ nodes}) \times (5 \text{ million events}) = \text{estimated number of events}
\]

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

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

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

- Are you purging your events regularly?
- Is there a specific event in the query that comprises most of your events?

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

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

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

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

- Create a query that shows all events you are questioning, then use the information in this section to analyze these threat events.
- Determine if anyone is looking at these excessive events in the first place.
- If events are not being analyzed, change your policy to stop the event forwarding.
- If the event is important, make sure that you are monitoring the number of events.

If no one is looking at these events, you might consider disabling them completely in the VirusScan Enterprise access protection policy to stop them from being sent to the McAfee ePO server. Or, you can adjust your policy to send only the access protection events that you are concerned with instead of excessive events that are not being analyzed. If you do want to see these events, you can leave the policy as configured, but confirm that you are following the rules about purging events from the McAfee ePO server so that these events do not overrun your database.
Create custom table queries: best practice

Create a query that displays the results in a table so that you can act on the query results.

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

A table query is used to return data in a simple table format, without graphs or charts. Server tasks can act on simple table data. For example, you can automatically delete this data.

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

**Task**

1. To open the Queries dialog box, select **Menu** | **Reporting** | **Queries & Reports**, then click **New Query**.
2. Click **Events** in the Features Group and **Client Events** in the Result Types, and click **Next**.
3. In the **Display Results As** pane, click **List**, then click **Table**, then click **Next**.
4. Click **Next** to skip the Columns dialog box.
   
   ![You can skip this step because McAfee ePO does not use the columns you choose in the server task.](image)

5. In **Available Properties** under **Client Events**, click **Event ID** to create an Event ID filter.
   
   An Event ID row is added in the Filter pane.

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

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

   ![Instead of purging the events in real time during business hours, you can create a server task that runs the purge nightly during off hours.](image)

8. To create a server task, select **Menu** | **Automation** | **Server Tasks** and click **Actions** | **New Task**.
9. Give the task an appropriate name and description; then click **Next**.
   
   For example, Purge of 1051 and 1059 Events Nightly.

10. Click **Purge Threat Event Log** from the Actions list, then click **Purge by Query**.
11. In the list, find and click the custom query that you created.
12. Schedule the task to run every night, then click **Save**.

---

**Multi-server rollup querying**

McAfee ePO includes the ability to run queries that report on summary data from multiple databases. Use these result types in the Query Builder for this type of querying:
Rolled-Up Threat Events | Rolled-Up Managed Systems
Rolled-Up Client Events | Rolled-Up Applied Policies
Rolled-Up Compliance History

Action commands cannot be generated from rollup result types.

**How it works**

To roll up data for use by rollup queries, you must register each server (including the local server) that you want to include in the query.

Once the servers are registered, you must configure Roll Up Data server tasks on the reporting server (the server that performs the multi-server reporting). Roll Up Data server tasks retrieve the information from all databases involved in the reporting, and populate the EPORollup_ tables on the reporting server. The rollup queries target these database tables on the reporting server.

As a prerequisite to running a Rolled-Up Compliance History query, you must take two preparatory actions on each server whose data you want to include:

- Create a query to define compliance.
- Generate a compliance event.

**Create a Rollup Data server task**

Rollup Data server tasks draw data from multiple servers at the same time.

**Before you begin**

- Register each McAfee ePO reporting server that you want to include in rollup reporting. Registering each server is required to collect summary data from those servers to populate the EPORollup_ tables of the rollup reporting server.
- The reporting server must also be registered to include its summary data in roll up reporting.

You can't roll up data from registered McAfee ePO servers at versions that are no longer supported. For example, you can't aggregate data from McAfee ePO servers at version 4.5 or earlier.

**Task**

1. Open the Server Task Builder.
   a. Select **Menu | Automation | Server Tasks**.
   b. Click **New Task**.

2. On the Description page, type a name and description for the task, and select whether to enable it, then click **Next**.

3. Click **Actions**, then select **Roll Up Data**.

4. From the **Roll up data from** drop-down menu, select **All registered servers** or **Select registered servers**.

5. If you chose **Select registered servers**, click **Select**. Choose the servers you want data from in the Select Registered Servers dialog box, then click **OK**.
6 Select the data type to be rolled up, then click Next. To select multiple data types, click the + at the end of the table heading.

The data types Threat Events, Client Events, and Applied Policies can be further configured to include the properties Purge, Filter, and Rollup Method. To do so, click Configure in the row that describes the available properties.

7 Schedule the task, then click Next.
The Summary page appears.

If you are reporting on rolled-up compliance history data, make sure that the time unit of the Rolled-Up Compliance History query matches the schedule type of the Generate Compliance Event server tasks on the registered servers.

8 Review the settings, then click Save.

**Create a query to define compliance**
Compliance queries are required on McAfee ePO servers whose data is used in rollup queries.

**Task**

1 Select Menu | Reporting | Queries & Reports, then click New Query.

2 On the Result Type page, select System Management for Feature Group and Managed Systems for Result Types, then click Next.

3 Select Boolean Pie Chart from the Display Result As list, then click Configure Criteria.

4 Select the properties to include in the query, then set the operators and values for each property. Click OK. When the Chart page appears, click Next.

   These properties define compliance for systems managed by this McAfee ePO server.

5 Select the columns to be included in the query, then click Next.

6 Select the filters to be applied to the query, click Run, then click Save.

**Generate compliance events**
Compliance events are used in rollup queries to aggregate data in a single report.

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

1 Select Menu | Automation | Server Tasks, then click Actions | New Task.

2 On the Description page, type a name for the new task, then click Next.

3 From the Actions drop-down menu, select Run Query.

4 Click browse (…) next to the Query field and select a query. The Select a query from the list dialog box appears with the My Groups tab active.

5 Select the compliance-defining query. This could be a default query, such as McAfee Agent Compliance Summary in the McAfee Groups section, or a user-created query, such as one described in *Creating a query to define compliance*. 
6 From the **Sub-Actions** drop-down menu, select **Generate Compliance Event** and specify the percentage or number of target systems, then click **Next**.

> You can generate events using the generate compliance event task if noncompliance rises above a set percentage or set number of systems.

7 Schedule the task for the time interval needed for Compliance History reporting. For example, if compliance must be collected on a weekly basis, schedule the task to run weekly. Click **Next**.

8 Review the details, then click **Save**.

**Export query results to other formats**

Query results can be exported to these formats: HTML, PDF, CSV, and XML.

Exporting query results differs from creating a report. First, no additional information is added to the export output as you do when you create a report; only the output data is added to the report. Second, more formats are supported. The exported query results can be used for further processing using the supported machine-friendly formats such as XML and CSV. Reports are designed to be human readable, and as such are only output as PDF files.

Unlike query results in the console, exported data is not actionable.

**Task**

1 Select **Menu** | **Reporting** | **Queries & Reports**, select a query, then click **Run**.

2 After the query runs, click **Options** | **Export Data**.
   
   The Export page appears.

3 Select what to export. For chart-based queries, select **Chart data only** or **Chart data and drill-down tables**.

4 Select whether the data files are exported individually or in a single archive (.zip) file.

5 Select the format of the exported file.
   - **CSV** — Saves the data in a spreadsheet application (for example, Microsoft Excel).
   - **XML** — Transforms the data for other purposes.
   - **HTML** — Use this report format to view the exported results as a webpage.
   - **PDF** — Print the results.

6 If exporting to a PDF file, configure the following:
   - Select the **Page size** and **Page orientation**.
   - (Optional) **Show filter criteria**.
   - (Optional) **Include a cover page with this text** and enter the needed text.

7 Select whether the files are emailed as attachments to selected recipients, or they are saved to a location on the server to which a link is provided. You can open or save the file to another location by right-clicking it.

8 Click **Export**.

The files are either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.
Best practices: Running reports with the web API

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

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

Use the web URL API or the McAfee ePO user interface

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

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

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

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

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

Or you can paste this web URL query in your browser address bar.
McAfee ePO command framework: best practice

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

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

The *AppliedTag* command is accessed from the System Tree page in the McAfee ePO user interface.

You can find valid *AppliedTag* command parameters using this core.listTables web URL command:

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

The following Web URL command structure, and its parts, are used to find the *AppliedTags* command.

```
https://<localHost:8443/remote/core.listDatatypes?type=applied_tags
```

Following are the parts of the web URL command.

- **Basic URL** — Your remote console connection URL.
  
  The default port number is 8443.

- **Command name** — Appears before the `?` and is listed in the web API Help.

- **Command argument** — Appears after the `?` and is separated by `&` (ampersands).
  
  You can also add S-Expressions to your commands.

Using the web URL Help: best practice

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

Use these Help commands when creating web URL queries:

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

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

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

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

Using the core.help command

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

Type this command to see the Help.

`https://<localHost>:8443/remote/core.help?`
Using the `core.listQueries` Help command

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

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

Type the following command to query with an ID:

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

Using the `core.executeQuery` Help command

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

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

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

This table lists `core.executeQuery` Help.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Arguments</th>
<th>Parameters</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>core.executeQuery</code></td>
<td>queryId</td>
<td>—</td>
<td>—</td>
<td>Executes a SQUID query. Returns the data from the execution of the query or displays on error.</td>
</tr>
<tr>
<td></td>
<td>[database=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The name of the remote database; if blank, the default database for the given database type is used.</td>
</tr>
<tr>
<td></td>
<td>target=</td>
<td>—</td>
<td>—</td>
<td>The SQUID target type to query. Optionally, you can add &quot;.&quot; and the database type before the target. For example, <code>databaseType.target</code>.</td>
</tr>
<tr>
<td></td>
<td>[select=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The SQUID select clause of the query; if blank, all columns are returned.</td>
</tr>
<tr>
<td></td>
<td>[where=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The SQUID where clause of the query; if blank, all rows are returned.</td>
</tr>
<tr>
<td></td>
<td>[order=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The SQUID order-by clause of the query; if blank, database order is returned.</td>
</tr>
<tr>
<td></td>
<td>[group=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The SQUID group-by clause of the query; if blank, no grouping is performed.</td>
</tr>
<tr>
<td></td>
<td>[database=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The name of the remote database; if blank, the default database for the given database type is used.</td>
</tr>
<tr>
<td></td>
<td>[depth=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The SQUID depth to fetch sub-results. (default: 5).</td>
</tr>
<tr>
<td></td>
<td>[joinTables=&lt;&gt;]</td>
<td>—</td>
<td>—</td>
<td>The comma-separated list of SQUID targets to join with the target type; &quot;**&quot; means join all types.</td>
</tr>
</tbody>
</table>

Using the `core.listTables` Help command

To create a McAfee ePO web URL query or to change query parameters exported from an existing query, you must know the names of the SQL tables and their parameters. These three commands provide that information.
Reporting with queries
Best practices: Running reports with the web API

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

Type this command to see the core.listTables Help.
https://<localHost>:8443/remote/core.listTables?:output=terse

To list only the parameters for a specific table, use this command:
https://<localHost>:8443/remote/core.listTables?table=<tableName>

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

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

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

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

Figure 21-6  Web URL query with S-Expression

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

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

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

Find the valid parameters for the target tables and confirm the table relationships.

Group, sort, order, and filter web URL query output
Within your web URL query S-Expressions, you can group, sort, order, and filter web URL query using the arguments listed for the core.executeQuery command.

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

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


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

OK:
Name: Groups
Target: EPOBranchNode
Type: join
Database Type:
Description: null
Columns:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Select?</th>
<th>Condition?</th>
<th>GroupBy?</th>
<th>Order?</th>
<th>Number?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoID</td>
<td>group</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>NodeName</td>
<td>string</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>L1ParentID</td>
<td>group</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>L2ParentID</td>
<td>group</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>BranchState</td>
<td>int</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Notes</td>
<td>string</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>NodePath</td>
<td>string</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>NodeTextPath</td>
<td>string_lookup</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>NodeTextPath2</td>
<td>string_lookup</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

Related Tables:
Name
- ---
Foreign Keys: None

Grouping the output

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

This is the command output.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent handlers</td>
<td>1</td>
</tr>
<tr>
<td>Lost&amp;Found</td>
<td>1</td>
</tr>
<tr>
<td>NAT Systems</td>
<td>3</td>
</tr>
<tr>
<td>Servers</td>
<td>1</td>
</tr>
<tr>
<td>SuperAgents</td>
<td>1</td>
</tr>
</tbody>
</table>

Filtering the output using a string

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

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

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

<table>
<thead>
<tr>
<th>System Name</th>
<th>Tags</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-2K8ER2EPO510 Server</td>
<td>Servers</td>
<td></td>
</tr>
<tr>
<td>DP-2K8AGTHDLR   Server, test Agent handlers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

<table>
<thead>
<tr>
<th>System Name</th>
<th>Tags</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-W7PIP-1</td>
<td>7, Workstation</td>
<td>Workstation</td>
</tr>
<tr>
<td>DP-W7PIP-2</td>
<td>7, Workstation</td>
<td>Workstation</td>
</tr>
<tr>
<td>DP-W7PIP-3</td>
<td>7, Workstation</td>
<td>Workstation</td>
</tr>
</tbody>
</table>

Filtering the output using common attributes

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

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

This is the command output with 4 common attributes.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Tags</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-W7PIP-1</td>
<td>7, Workstation</td>
<td>Workstation</td>
</tr>
<tr>
<td>DP-W7PIP-2</td>
<td>7, Workstation</td>
<td>Workstation</td>
</tr>
<tr>
<td>DP-W7PIP-3</td>
<td>7, Workstation</td>
<td>Workstation</td>
</tr>
</tbody>
</table>

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

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

Parentheses must be matched.

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

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

Parsing query export data to create web URL queries best practice

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

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

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

<table>
<thead>
<tr>
<th>URL-encoded characters</th>
<th>Web URL query characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>%22</td>
<td>quotation marks &quot;&quot;&quot;&quot;</td>
</tr>
<tr>
<td>%20</td>
<td>space &quot; &quot;</td>
</tr>
</tbody>
</table>
Table 21-2 Convert URL-encoded characters to web URL query characters (continued)

<table>
<thead>
<tr>
<th>URL-encoded characters</th>
<th>Web URL query characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>%28</td>
<td>opening parenthesis &quot;(&quot;</td>
</tr>
<tr>
<td>%29</td>
<td>closing parenthesis &quot;)&quot;</td>
</tr>
<tr>
<td>&amp;amp</td>
<td>ampersand &quot;&amp;&quot;</td>
</tr>
<tr>
<td>az (in an order command)</td>
<td>&quot;asc&quot; = ascending order</td>
</tr>
<tr>
<td>za (in an order command)</td>
<td>&quot;desc&quot; = descending order</td>
</tr>
</tbody>
</table>

XML query data file structure

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

**Figure 21-7 Exported query and web URL query data comparison**

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

This table lists the numbers shown in the figure, the major sections of the exported query and the final web URL query, and how they are used.
Table 21-3  Convert URL-encoded characters to web URL query characters

<table>
<thead>
<tr>
<th>Number</th>
<th>Exported query</th>
<th>Web URL query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt;target&gt;...&lt;/target&gt;</td>
<td>target=...</td>
<td>Lists the table parsed in the query.</td>
</tr>
<tr>
<td>2</td>
<td>sexp=...</td>
<td>select=(select...</td>
<td>Lists the S-Expressions command objects, their parameters, and joint tables.</td>
</tr>
<tr>
<td>4</td>
<td>order=...</td>
<td>order=(order(...</td>
<td>Lists the sort order used in the output.</td>
</tr>
</tbody>
</table>

Web URL query separated into parts

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

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

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

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

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

Following is the output of the web URL query.

<table>
<thead>
<tr>
<th>System Name</th>
<th>DAT Version (VirusScan Enterprise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-W7PIP-3</td>
<td>7465.0000</td>
</tr>
<tr>
<td>DP-W7PIP-2</td>
<td>7429.0000</td>
</tr>
<tr>
<td>DP-W7PIP-1</td>
<td>7437.0000</td>
</tr>
<tr>
<td>DP-EN-W7E1XP-2</td>
<td>7465.0000</td>
</tr>
<tr>
<td>DP-2K8ER2EPO510</td>
<td>7437.0000</td>
</tr>
<tr>
<td>DP-2K8AGTHDLR</td>
<td>7437.0000</td>
</tr>
<tr>
<td>DP-2K12R2S-SRVR</td>
<td></td>
</tr>
</tbody>
</table>

Run query with ID number: best practice

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

**Before you begin**

You must have administrator permissions to run the query.

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

For example, to access the query New Agents Added to ePO per Week using the McAfee ePO user interface, select **Menu | Reports | Queries & Reports**, select the **New Agents Added to ePO per Week** query, and click **Actions | Run**.
This web URL output is similar to the query output with the user interface, plus it allows you to use the output in another script or manipulate it as needed.

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

1. Use your browser to log on to your McAfee ePO server.
2. To get a list of the preconfigured queries and their ID numbers, type this URL into the browser address bar, then press Enter.
   
   `https://<localHost>:8443/remote/core.listQueries?:output=terse`

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

**Run query with XML data best practice**
Exporting existing query XML definitions is a great way to learn how to create web URL queries.

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

**Task**
1. Export the existing query definition XML file and open it in a text editor.

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

   ```xml
   <list id="1">
   <query id="2">
   <dictionary id="3"/>
   <name>VSE: DAT Deployment</name>
   <description>Displays the three highest DAT versions, and a slice for all the other versions.</description>
   <target>EPOLeafNode</target>
   <table-uri>query:table?orion.table.columns=EPOComputerProperties.ComputerName%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComputerProperties.Description%3AEPOLeafNode.Tags%3AEPOProdPropsView_VIRUSCAN.productversion%3AEPOProdPropsView_VIRUSCAN.hotfix%3AEPOProdPropsView_VIRUSCAN.servicepack%3AEPOProdPropsView_VIRUSCAN.enginever%3AEPOProdPropsView_VIRUSCAN.enginever64%3AEPOProdPropsView_VIRUSCAN.datver%3AEPOLeafNode.LastUpdate%3Aorion.table.order=az</table-uri>
   <condition-uri>query:condition?orion.condition.sexp=%28+where+%28+version_ge+EPOProdPropsView_VIRUSCAN.productversion+%228%22+%29+%29</condition-uri>
   <summary-uri>query:summary?pie.slice.title=EPOProdPropsView_VIRUSCAN.datver%3Aorion.sum.count.title=EPOLeafNode%3Aorion.query.type=pie.pie%3Aorion.sum.query=true%3Aorion.sum.group.by=EPOProdPropsView_VIRUSCAN.datver%3Aorion.sum.order=desc%3Aorion.show.other=true%3Aorion.sum.aggregation=count%3Aorion.sum.aggregation.showTotal=true</summary-uri>
   </query>
   </list>
```
2 Open an existing web URL query file to use as a template, then save it with a new name. For example, `URL_template`.

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

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

3 From the query definition XML file, find the query target listed between the target tags. For example, `<target>EPOLeafNode</target>` and paste the target table name in `target=` of your template URL.

This is the template with the target table name added.

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

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

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

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

b Add the sort order function. For example, to sort the output by system name, add the string `&order=(order(desc EPOProdPropsView_VIRUSCAN.datver))` in the existing S-Expression. The following example sorts the output by the VirusScan Enterprise DAT version.

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

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

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

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

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

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

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

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

Confirm that your output is similar to the following example.

```
OK:
System Name     DAT Version (VirusScan Enterprise)
--------------- ----------------------------------
DP-2K12R2S-SRVR
DP-EN-W7E1XP-2  7429.0000
DP-W7PIP-2     7437.0000
DP-W7PIP-1     7437.0000
DP-2K8AGTHDLR   7437.0000
DP-2K8ER2EPOS10 7465.0000
DP-W7PIP-3     7465.0000
```

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

### Run query using table objects, commands, and arguments: best practice

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

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

- System name
- McAfee Agent version
- VirusScan Enterprise product family
- VirusScan Enterprise version
- Displays the information as a table

**Task**

1. To find the name of the SQL table with most of your information, use this Help command.
   ```
   https://<localHost>:8443/remote/core.listTables?:output=terse
   ```

2. Using your text editor, type this web URL template command.
   ```
   https://<localHost>:8443/remote/core.executeQuery?target=<tableName>&select=(select <columns>)
   ```

3. Use the information from this command to find the arguments for the system names, McAfee Agent version, and when it was last updated.
   ```
   https://<localHost>:8443/remote/core.listTables?:output=terse&table=EPOLeafNode
   ```
   This command displays this information, which you need for your web URL query:
   - Query "target" — `EPOLeafNode`
   - System name — `EPOLeafNode.NodeName`
   - McAfee Agent version — `EPOLeafNode.AgentVersion`
- When the agent was last updated — EPOLeafNode.LastUpdate
- Products installed on each system — EPOProductPropertyProducts

**OK:**
Name: Managed Systems
Target: EPOLeafNode
Type: target
Database Type:
Description: Retrieves information about systems that have been added to your System Tree.

<table>
<thead>
<tr>
<th>Columns</th>
<th>Name</th>
<th>Type</th>
<th>Select?</th>
<th>Condition?</th>
<th>GroupBy?</th>
<th>Order?</th>
<th>Number?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoID</td>
<td>int</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>Tags</td>
<td>string</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>ExcludedTags</td>
<td>string</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>AppliedTags</td>
<td>applied_tags</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>LastUpdate</td>
<td>timestamp</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>os</td>
<td>string</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>products</td>
<td>string</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>NodeName</td>
<td>string</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>ManagedState</td>
<td>enum</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>AgentVersion</td>
<td>string_lookup</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>AgentGUID</td>
<td>string</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>ParentID</td>
<td>int</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>ResortEnabled</td>
<td>boolean</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>ServerKeyHash</td>
<td>string</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>NodePath</td>
<td>string_lookup</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>TransferSiteListsID</td>
<td>isNotNull</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>SequenceErrorCount</td>
<td>int</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>SequenceErrorCountLastUpdate</td>
<td>timestamp</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>LastCommSecure</td>
<td>string_enum</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>TenantId</td>
<td>int</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
</tbody>
</table>

**Related Tables:**
Name
--------------------------
EPOProdPropsView_EEFF
EPOProdPropsView_VIRUSCAN
EPOProductPropertyProducts
EPOProdPropsView_PCR
EPOBranchNode
EPOProdPropsView_EPOAGENT
EPOComputerProperties
EPOComputerLdapProperties
EPOTagAssignment
EPOProdPropsView_TELEMETRY

**Foreign Keys:**
Source table Source Columns Destination table Destination columns Allows inverse? One-to-one? Many-to-one?

<table>
<thead>
<tr>
<th>Source table</th>
<th>Source Columns</th>
<th>Destination table</th>
<th>Destination columns</th>
<th>Allows inverse?</th>
<th>One-to-one?</th>
<th>Many-to-one?</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPOLeafNode</td>
<td>AutoID</td>
<td>EPOComputerProperties</td>
<td>ParentID</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
<td>EPOTagAssignment</td>
<td>LeafNodeID</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
<td>EPOBranchNode</td>
<td>AutoNodeID</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
<td>EPOComputerLdapProperties</td>
<td>LeafNodeID</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
<td>EPOProductPropertyProducts</td>
<td>ParentID</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>
4 Add the arguments from step 3 to the web URL template command and test it. Confirm that your command looks similar to this example.

```
```

Confirm that your output is similar to this example.

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

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

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

5 Use the `core.listTables` Help command again, but with the `EPOProdPropsView_VIRUSCAN` table. This table lists the VirusScan Enterprise products and versions installed on each system. Confirm that your command looks similar to this example.

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

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

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

Confirm that your example looks similar to the following.

```
```

Confirm that your example output looks similar to the following.

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

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

System Name: DP-EN-W7E1XP-2
Agent Version (deprecated): null
Last Communication: null
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise): 
```
Finally, to show the output as a table, add the command `:output=terse&` after the first `&` and rerun the command.

Confirm that your example command looks similar to the following.

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

Confirm that your example output looks similar to the following.

```
OK:
System Name     Agent Version (deprecated) Last Communication
ProdProps.productFamily (VirusScan Enterprise) Product Version (VirusScan Enterprise)
--------------- -------------------------- ----------------------- ---------------------------------------------- --------------------------------------
DP-2K8ER2EPO510 4.8.0.887                  6/13/14 10:21:50 AM PDT
VIRUSCAN                                       8.8.0.1266
VIRUSCAN
DP-EN-W7E1XF-2 null                       null
VIRUSCAN
DP-W7PIP-1      4.8.0.887                  6/13/14 10:37:20 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-W7PIP-2      4.8.0.887                  6/13/14 10:36:56 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-W7PIP-3      4.8.0.887                  6/13/14 10:37:00 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-2K8AGTHDLR   4.8.0.887                  6/13/14 10:25:10 AM PDT
VIRUSCAN                                       8.8.0.1266
```
Adding systems connected over a VPN

All systems that connect to McAfee ePO using a VPN server use the MAC address of the VPN server. This causes some of the VPN connected systems to disappear from the System Tree because they appear as duplicate MAC addresses.

This diagram and its description explain why some systems connecting to McAfee ePO over a VPN disappear from the System Tree because they have the same MAC address.

1. Client A connects to McAfee ePO over the VPN connection.

2. McAfee ePO associates the MAC address of the VPN server, 00:12:3F:11:11:11, to Client A rather than the client’s actual MAC address.

3. Client B connects to McAfee ePO over the VPN connection.

4. McAfee ePO associates the MAC address of the VPN server, also 00:12:3F:11:11:11, to Client B. Now two clients have the same VPN server MAC address.

Client A is deleted from the System Tree because both clients appear to have the same MAC address.

To stop McAfee ePO from using the VPN server MAC addresses as valid matching criteria and deleting the systems, you must:
Find the VPN server MAC address to learn the Organizationally Unique Identifier (OUI), or vendor identifier. The OUI is the first six digits of the VPN server MAC address.

Use SQL Server Management Studio to insert the VPN server OUI in the McAfee ePO virtual MAC vendor values to stop that OUI being used as the first valid matching criteria. This change causes McAfee ePO to use the client GUID as valid matching criteria instead of the MAC address for all systems connecting with the VPN server OUI.

Contents
- Determining connected VPN server’s OUI
- Use the System Tree to find VPN server MAC address
- Create report to find VPN server MAC address best practice
- Best practice: Use SQL Server Management Studio to add virtual MAC vendor ID value

Determining connected VPN server's OUI
You must determine the OUI for the VPN server to stop McAfee ePO from using the server's MAC addresses as valid matching criteria.

The Organizationally Unique Identifier (OUI) is the first six digits of the VPN server MAC address. These are two ways to determine the OUI of the VPN server.

Use the System Tree to find VPN server MAC address
The best way to find the VPN server MAC address is to find a system connecting to McAfee ePO through that VPN server.

Before you begin
You must have a remote connection to the system connecting to McAfee ePO through that VPN server.

Task

1. Remotely connect to a system connecting to McAfee ePO through that VPN server.
2. Use one of these processes to display the McAfee Agent Status Monitor:
   - If the McAfee Agent icon appears in the system tray, click the icon.
   - If the McAfee Agent Icon does not appear in the notification area, use the following command-line steps to display the McAfee Agent Status Monitor:
     1. From the command prompt, change directories to this default folder:
        C:\Program Files\McAfee\Common Framework\
     2. To display the McAfee Agent Status Monitor, type this command:
        CmdAgent.exe /s
3. From the McAfee Agent Status Monitor, click Collect and Send Props.
   This process collects the system properties and sends them to the McAfee ePO server.
4. From the McAfee ePO console, select Menu | Systems | System Tree.
To display the system information, locate the system that connects to McAfee ePO over the VPN connection and double-click the system name.

Click the System Properties tab, then click Customize on the right of the display.

From the Properties list, find MAC Address, click Move to Top, then click Save.

The VPN connected system's MAC address appears at the top of the list of the system information display.

Make a note of the first six digits of the system MAC address, which is the OUI for the VPN server.

Create report to find VPN server MAC address best practice

You can create a report to list systems with the same MAC address.

**Task**

1. Select Menu | Reporting | Queries & Reports.

2. Click New Query to display the Result Type tab, configure these settings, then click Next.
   - In the Feature Group list, select System Management.
   - In Result Types pane, select Managed Systems.

3. From the Chart tab, configure these settings, then click Next.
   - In the Display Results As list, select Single Group Summary Table.
   - In the Labels are list, under Computer Properties, select MAC Address.

4. In the Columns tab, from the Available Columns list under Computer Properties, select MAC Address, then click Next.

5. In the Filters tab, configure these settings, then click Run.
   - In the Available Properties list, expand Managed Systems and click Managed State.
   - In the Managed State settings, select Equals from the Comparison drop-down list and Managed from the Values drop-down list.
   - In the Available Properties list, expand Computer Properties and click MAC Address.
   - In the MAC Address settings, select Value is not Blank from the Comparison drop-down list.

6. In the output of the query, find any two systems with the same MAC address.
   This MAC address probably belongs to the VPN server connecting the systems to McAfee ePO.

7. Make a note of the first six digits of the system MAC address, which is the OUI of the VPN server.
Best practice: Use SQL Server Management Studio to add virtual MAC vendor ID value

To stop the McAfee ePO server from deleting systems that connect over a VPN server, you must add the VPN server OUI to the McAfee ePO Virtual MAC Vendor values using SQL Server Management Studio.

Before you begin
- You must know the first six-digit OUI.
- You need permission to access SQL Server Management Studio.

Task

1. Type this command in your browser to learn your McAfee ePO server and database name.
   
   https://<ServerName>:8443/core/config-auth

   Replace <ServerName> with the name of your McAfee ePO server and your server communication port number, if it is not the default 8443.

2. Open SQL Server Management Studio and connect to the McAfee ePO SQL database server using your database authentication method.

   Typically the McAfee ePO SQL database server name is <McAfee_ePO_server_name>

   EPOSERVER.

3. In Object Explorer, click these objects:

   - <McAfee_ePO_server_name>\EPOSERVER
   - Databases
   - ePO_<McAfee_ePO_server_name>
   - Tables

4. Scroll down the list to the dbo.EPOVirtualMacVendor table, right-click the table name, and select Script Table as | INSERT to | New Query Editor Window.

   An SQLQuery1.sql file opens in the right pane of the display with the ePOVirtualMacVendor table default value.
5 The default query value, listed between parentheses, is `<VendorID, nvarchar(8),>`. Change that value to the VPN server vendor ID.

Enclose the six-digit hexadecimal value in single quotes.

This is an example of the default table value and the changed `'00123F'` table value.

**Default table value**

```sql
INSERT INTO [<ePO_Server_Name>].[dbo].[EPOVirtualMacVendor] ([VendorID]) VALUES (<VendorID, nvarchar(8),>)
GO
```

**Changed table value**

```sql
INSERT INTO [<ePO_Server_Name>].[dbo].[EPOVirtualMacVendor] ([VendorID]) VALUES ('00123F')
GO
```

6 To run the query and add the VPN server OUI value to the EPOVirtualMacVendor table, click *Query* | *Execute* in the menu bar.

7 Confirm that this status appears in the *Messages* pane below the query that you updated:

(1 Row(s) affected)

Now McAfee ePO uses the client GUID as valid matching criteria instead of the MAC address for all systems connecting with the VPN server OUI.
Adding systems connected over a VPN
Best practice: Use SQL Server Management Studio to add virtual MAC vendor ID value
Registered servers

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

McAfee ePO can communicate with:

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

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

We recommend that you use certificates with RSA public key lengths of 2048 bits or greater for the registered servers that connect to McAfee ePO. For more information, including additional supported public key algorithms and key lengths, see KnowledgeBase article, KB87731.

Contents

- Register McAfee ePO servers
- Using database servers
- Register SNMP servers
- Register syslog servers
- Register LDAP servers
- Mirroring an LDAP server
- Sharing objects between servers

Register McAfee ePO servers

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

Before you begin

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

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

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

**Task**

1. Select **Menu | Configuration | Registered Servers** and click **New Server**.
2. From the Server type menu on the Description page, select **ePO**, specify a unique name and any notes, then click **Next**.
3. Specify the following options to configure the server:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>Specifies the type of authentication to use for this database, including:</td>
</tr>
<tr>
<td></td>
<td>• Windows authentication</td>
</tr>
<tr>
<td></td>
<td>• SQL authentication</td>
</tr>
<tr>
<td>Client task sharing</td>
<td>Specifies whether to enable or disable client task for this server.</td>
</tr>
<tr>
<td>Database name</td>
<td>Specifies the name for this database.</td>
</tr>
<tr>
<td>Database port</td>
<td>Specifies the port for this database.</td>
</tr>
<tr>
<td>Database server</td>
<td>Specifies the name of the database for this server. You can specify a</td>
</tr>
<tr>
<td></td>
<td>databaseMcAfee ePO using DNS Name or IP address (IPv4 or IPv6).</td>
</tr>
<tr>
<td>ePO Version</td>
<td>Specifies the version of the server being registered.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password for this server.</td>
</tr>
<tr>
<td>Policy sharing</td>
<td>Specifies whether to enable or disable policy sharing for this server.</td>
</tr>
<tr>
<td>SQL Server instance</td>
<td>Allows you to specify whether this is the default server or a specific instance, by providing the Instance name.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the SQL browser service is running before connecting to a specific SQL instance using its instance name. Specify the port number if the SQL browser service is not running. Select the Default SQL server instance and type the port number to connect to the SQL server instance.</td>
</tr>
<tr>
<td>SSL communication with database server</td>
<td>Specifies whether McAfee ePO uses SSL (Secure Socket Layer) communication with this database server including:</td>
</tr>
<tr>
<td></td>
<td>• Try to use SSL</td>
</tr>
<tr>
<td></td>
<td>• Always use SSL</td>
</tr>
<tr>
<td></td>
<td>• Never use SSL</td>
</tr>
<tr>
<td>Test connection</td>
<td>Verifies the connection for the detailed server.</td>
</tr>
</tbody>
</table>

If you register a server with a different McAfee ePO version, this information-only warning appears: **Warning Version mismatch!**
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer systems</td>
<td>Specifies whether to enable or disable the ability to transfer systems for this server. When enabled, select Automatic sitelist import or Manual sitelist import.</td>
</tr>
<tr>
<td></td>
<td>When choosing Manual sitelist import, it is possible to cause older versions of McAfee Agent (version 4.0 and earlier) to be unable to contact their Agent Handler. This can happen when:</td>
</tr>
<tr>
<td></td>
<td>• Transferring systems from this McAfee ePO server to the registered McAfee ePO server</td>
</tr>
<tr>
<td></td>
<td>• An Agent Handler name appears alpha-numerically earlier than the McAfee ePO server name in the supplied sitelist</td>
</tr>
<tr>
<td></td>
<td>• Older agents use that Agent Handler</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>Optionally choose to use NT LAN Manager authentication protocol. Select this option when the server you are registering uses this protocol.</td>
</tr>
<tr>
<td>User name</td>
<td>Specifies the user name for this server.</td>
</tr>
</tbody>
</table>

4 Click Save.

**Using database servers**

McAfee ePO can retrieve data from not only its own databases, but from some extensions as well. You might need to register several different server types to accomplish tasks within McAfee ePO. These can include authentication servers, Active Directory catalogs, McAfee ePO servers, and database servers that work with specific extensions you have installed.

**Database types**

An extension can register a database type, otherwise known as a schema or structure, with McAfee ePO. If it does, that extension can provide data to queries, reports, dashboard monitors, and server tasks. To use this data, you must first register the server with McAfee ePO.

**Database server**

A database server is a combination of a server and a database type installed on that server. A server can host more than one database type, and a database type can be installed on multiple servers. Each specific combination of the two must be registered separately and is referred to as a database server.

After you register a database server, you can retrieve data from the database in queries, reports, dashboard monitors, and server tasks. If more than one database using the same database type is registered, you are required to select one of them as the default for that database type.

**Register a database server**

Before McAfee ePO can retrieve data, you must register it with the database server.

**Task**

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

2. Select **Database server** in the **Server type** drop-down list, enter a server name and an optional description, then click **Next**.
Choose a **Database type** from the drop-down list of registered types. Indicate if you want this database type to be as the default.

If there is already a default database assigned for this database type, it is indicated in the **Current Default database for database type** row.

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

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

6. To verify that all connection information and logon credentials are entered correctly, click **Test Connection**.

   A status message indicates success or failure.

7. Click **Save**.

### Modify a database registration

If connection information or logon credentials for a database server changes, you must modify the registration to reflect the current state.

**Task**

1. Open the Registered Servers page by selecting **Menu | Configuration | Registered Servers**.

2. Select a database to edit, then click **Actions | Edit**.

3. Change the name or notes for the server, then click **Next**.

4. Modify the information as appropriate. To verify the database connection, click **Test Connection**.

5. Click **Save** to save your changes.

### Remove a registered database

You can remove databases from the system when they are no longer needed.

**Task**

1. Open the **Registered Servers** page: select **Menu | Configuration | Registered Servers**.

2. Select a database to delete, and click **Actions | Delete**.

3. When the confirmation dialog appears, click **Yes** to delete the database.

The database has been deleted. Any queries, reports, or other items within McAfee ePO that used the deleted database is designated as invalid until updated to use a different database.

### Register SNMP servers

To receive an SNMP trap, you must add the SNMP server's information, so that McAfee ePO knows where to send the trap.
Task

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

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

3. From the URL drop-down list, select one of these types of server address, then enter the address:
   - DNS Name — Specifies the DNS name of the registered server.
   - IPv4 — Specifies the IPv4 address of the registered server.
   - IPv6 — Specifies the DNS name of the registered server which has an IPv6 address.

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

5. Click Send Test Trap to test your configuration.

6. Click Save.

The added SNMP server appears on the Registered Servers page.

Register syslog servers

You can enable McAfee ePO to synchronize with your syslog server. A syslog is a way for network devices to send event messages to a separate logging server. For example, you can use syslog to collect information about specific threat events.

Before you begin
You must have the domain name or IP address for your syslog server.

Task

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

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

3. From the Registered Server Builder page, configure these settings:
   a. Server name — Use DNS-style domain names (for example, internaldomain.com) and fully qualified domain names or IP addresses for servers. (for example, server1.internaldomain.com or 192.168.75.101)
   b. TCP port number — Type the syslog server TCP port. The default is 6514.
c Enable event forwarding — Click to enable event forwarding from Agent Handler to this syslog server.

d Test — Click Test Connection to verify the connection to your syslog server.

4 Click Save.

After you register the syslog server, you can set McAfee ePO to send events to your syslog server. These events are saved, by default, on your Agent Handler at this path: \C:\Program Files (x86)\McAfee\Agent Handler\DB\Logs\server_<servername>.log. This log file includes any syslog server errors that might occur.

Register LDAP servers

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

Register LDAP servers

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

Task

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

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

3 Choose whether you are registering an OpenLDAP or Active Directory server in the LDAP server type list. The rest of these instructions assume that an Active Directory server is being configured. OpenLDAP-specific information is included where required.

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

Using domain names gives failover support, and allows you to choose only servers from a specific site if wanted.

You must use server names with OpenLDAP servers. You can’t use domain names with OpenLDAP servers.

5 Choose if you want to Use Global Catalog. This option is deselected by default. Selecting Use Global Catalog can provide significant performance benefits. Only select this option if the registered domain is the parent of only local domains. If non-local domains are included, chasing referrals could cause significant non-local network traffic, possibly severely impacting performance.

Use Global Catalog is not available for OpenLDAP servers.

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

7 Choose whether to Use SSL when communicating with this server or not.
8 If you are configuring an OpenLDAP server, enter the Port.

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

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

11 Click Test Connection to verify communication with the server as specified. Change information as needed.

12 Click Save to register the server.

Mirroring an LDAP server

LDAP server mirroring to the McAfee ePO database increases performance on any product which uses user-based policies (UBP) and allows LDAP access to Agent Handlers behind a DMZ.

This diagram shows the default LDAP server to Agent Handler connection process and the mirrored LDAP connection process.

Figure A-1 Default and LDAP mirrored connection processes

1 Default connection process from the configured LDAP server to the Agent Handler.

2 Mirrored LDAP connection with the LDAP Synchronize server task requesting user information from the LDAP server.
Shows the LDAP server user information mirrored to the McAfee ePO database.

Shows an Agent Handler behind the DMZ accessing the mirrored LDAP server information in the McAfee ePO database.

Why use LDAP mirroring?

When the LDAP server user information is mirrored to the McAfee ePO database:

- Medium to large organizations can access that user information used by the Agent Handler from the database faster to satisfy LDAP requests for UBPs.
- Agent Handlers behind a DMZ can access the LDAP user information.

The LDAP information in the database can't be accessed or queried from the McAfee ePO user interface.

By default, the LDAP information in the database is updated every 8 hours by the LdapSync: Sync across users from LDAP server task unless:

- An "LDAP change notification" is sent to the Agent Handler from the McAfee ePO server.

By default, the LDAP user information cache in the Agent Handler is updated every 30 minutes.

- You manually run the server task.

Sharing objects between servers

Contents

- Export objects and data from your McAfee ePO server
- Importing items into McAfee ePO

Export objects and data from your McAfee ePO server

Exported objects and data can be used for backing up important data, and to restore or configure the McAfee ePO servers in your environment.

Most objects and data used in your server can be exported or downloaded for viewing, transforming, or importing into another server or applications. The following table lists the various items you can act on. To view data, export the tables as HTML or PDF files. To use the data in other applications, export the tables or to CSV or XML files.

An exported XML file usually contains an element named `<list>` in the event multiple items are being exported. If only one object is exported, this element might be named after the object. (For example `<query>`).

Any more detailed contents are variable depending on the exported item type.

The following items can be exported. Installed extensions can add items to this list. Check the extension documentation for details.

- Dashboards
- Permission Sets
- Queries
- Reports
- Server Tasks
- Users
- Automatic Responses
You can also export items from:

- Policy Catalog
- Client Task Catalog
- Tag Catalog

The following items can have a table of their current contents exported.

- Audit Log
- Issues

**Task**

1. From the page displaying the objects or data, click **Actions** and select an option. For example, when exporting a table, select **Export Table**, then click **Next**.

2. When exporting content that can be downloaded in multiple formats, such as Query data, an **Export** page with configuration options appears. Specify your preferences, then click **Export**.

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

**Importing items into McAfee ePO**

Items exported from a McAfee ePO server can be imported into another server.

McAfee ePO exports items into XML. These XML files contain exact descriptions of the exported items.

**Importing items**

When importing items into McAfee ePO, certain rules are followed:

- All items except users are imported with private visibility by default. You can apply other permissions either during or after import.

- If an item exists with the same name, "(imported)" or "(copy)" is appended to the imported item's name.

- Imported items requiring an extension or product that does not exist on the new server is designated as invalid.

McAfee ePO only import XMLs files exported by McAfee ePO.

Specific details on how to import different kinds of items can be found in the documentation for the individual items.
Registered servers
Sharing objects between servers
Issues

Issues are action items that can be prioritized, assigned, and tracked.

Contents

- Issues and how they work
- View issues
- Remove closed issues from the Issues table
- Create issues manually
- Configure responses to automatically create issues
- Manage issues
- Use tickets with McAfee ePO

Issues and how they work

Issues are managed by users with proper permissions and the installed managed product extensions. An issue’s state, priority, severity, resolution, assignee, and due date are all user-defined, and can be changed at any time. You can also specify default issue responses from the Automatic Responses page. These defaults are automatically applied when an issue is created, based on a user-configured response. Responses also allow multiple events to be aggregated into a single issue so that the McAfee ePO server is not overwhelmed with large numbers of issues.

Issues can be deleted manually, and closed issues can be manually purged based on their age and automatically purged through a user-configured server task.

View issues

The Issues page provides a list of current and closed issues.

Task

2. Sort and filter the table to focus on relevant entries.
   • To change which columns are displayed, click Choose Columns.
   • To order table entries, click a column title.
   • To hide unrelated entries, select a filter from the drop-down list.
3. To view additional details, click an entry.
Remove closed issues from the Issues table

Periodically remove closed issues from the Issues table to improve database performance.

⚠️ Items removed from the Issues table are deleted permanently.

Task

2. Click Purge.
3. In the Purge dialog box, enter a number, then select a time unit.
4. Click OK.

Any items of the specified age or older are deleted, including items not in the current view. The number of removed items is displayed in the lower right corner of the page.

💡 Create a server task to automatically remove outdated items.

Create issues manually

Create an issue when you have an item for administrators to address. Provide enough information so that other users understand why you created the issue.

Task

1. Select Menu | Automation | Issues, then click New Issue.
2. In the New Issue dialog box, select an issue type from the Create issue of type drop-down list, then click OK. If you are unsure which issue type to select, choose Basic.
3. Configure the new issue. Any due dates you specify must be in the future.
4. Click Save.

Configure responses to automatically create issues

Use responses to automatically create issues when certain events occur.

Task

1. Open the Response Builder.
   a. Select Menu | Automation | Automatic Responses.
   b. Click New Response.
2. Complete the fields, then click Next.
3. Select properties to narrow the events that trigger the response, then click Next.
4 Specify these additional details, then click Next.
   • The frequency of events required to generate a response.
   • A method to group events.
   • The maximum time period that you want this response to occur.
5 Select Create issue from the drop-down list, then select the type of issue to create.
   This choice determines the options that appear on this page.
6 Type a name and description for the issue. Optionally, select one or more variables for the name and description.
   This feature provides a number of variables providing information to help fix the issue.
7 Type or select any additional options for the response, then click Next.
8 Review the details for the response, then click Save.

Manage issues

You can add comments, assign, delete, edit, and view details of issues.

Task

1 Select Menu | Automation | Issues.
2 Perform any of the following tasks.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding comments to issues</td>
<td>1 Select the checkbox next to each issue you want to comment, then click Action</td>
</tr>
<tr>
<td></td>
<td>2 In the Add comment panel, type the comment you want to add to the selected issues.</td>
</tr>
<tr>
<td></td>
<td>3 Click OK to add the comment.</td>
</tr>
<tr>
<td>Assigning issues</td>
<td>Select the checkbox next to each issue you want to assign, then click Assign to user.</td>
</tr>
<tr>
<td>Display required columns on issues page</td>
<td>Click Actions</td>
</tr>
<tr>
<td>Deleting issues</td>
<td>1 Select the checkbox next to each issue you want to delete, then click Delete.</td>
</tr>
<tr>
<td></td>
<td>2 Click OK to delete the selected issues.</td>
</tr>
<tr>
<td>Editing issues</td>
<td>1 Select the checkbox next to an issue, then click Edit.</td>
</tr>
<tr>
<td></td>
<td>2 Edit the issue as needed.</td>
</tr>
<tr>
<td></td>
<td>3 Click Save.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Exporting the list of issues | 1. Click **Actions** | **Export Table** to open the Export page.  
2. From the Export page, you can specify the format of files to be exported, as well as how they are packaged.                                                                                          |
| Viewing issue details      | • Select an issue.  
The Issue Details page shows all settings for the issue as well as the Issues Activity Log.                                                                                                          |

**Use tickets with McAfee ePO**

To integrate automatic ticketing with McAfee ePO, you or McAfee Professional Services can use issue APIs to configure a remote server.

See the *McAfee ePolicy Orchestrator Web API Scripting Guide* for detailed Web API use and examples.
SSL certificates

Browsers supported by McAfee ePO warn about a server’s SSL certificate if the browser cannot verify whether a TrustedSource signed the certificate. Creating a self-signed certificate with OpenSSL stops the browser warning. Creating a self-signed certificate can provide the basic security and functionality needed for systems used on internal networks, or if you don’t want to wait for a certification authority to authenticate a certificate.

Contents
- Create a self-signed certificate with OpenSSL
- Other useful OpenSSL commands
- Convert an existing PVK file to a PEM file
- Migrate SHA-1 certificates to SHA-2 or higher
- Security keys and how they work
- Master Repository key pair
- Other repository public keys
- Manage repository keys
- Agent-server secure communication (ASSC) keys
- Back up and restore keys

Create a self-signed certificate with OpenSSL

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

Before you begin

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


To create and self-sign a certificate to use with your McAfee ePO server, use OpenSSL for Windows software. There are many tools you can use to create a self-sign a certificate. This task describes the process using OpenSSL.

To have a third party, for example Verisign or Microsoft Windows Enterprise Certificate Authority, create a signed certificate for McAfee ePO, see How to generate a custom SSL certificate for use with ePO using the OpenSSL toolkit, KB72477.

The file structure used in the following task is:

OpenSSL does not create these folders by default. They are used in these examples and can be created to help you find your output files.
SSL certificates
Create a self-signed certificate with OpenSSL

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

We recommend that you use certificates with RSA public key lengths of 2048 bits or greater.

Task

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

   C:\ssl\bin> openssl genrsa -des3 -out C:/ssl/keys/ca.key 2048

   The following screen appears.

   Loading 'screen' into random state - done
   Generating RSA private key, 2048 bit long modulus
   ++++++ ++++++ ++++++ unable to write 'random state'
   e is 65537 (0x10001)
   Enter pass phrase for keys/ca.key:
   Verifying - Enter pass phrase for keys/ca.key:

   C:\ss\bin>

2. Enter a passphrase at the initial command prompt and verify the passphrase at the second command prompt.

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

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

   The key looks similar to the following example.

   -----BEGIN RSA PRIVATE KEY-----
   Proc-Type: 4:ENCRYPTED
   DEK-Info: DES-EDE3-CBC,CE327E8DD510D1882
   4Ev9bqeteKbo60Wy0cFh6o8u8cU7T8n/cdppSeykv8BAsEuFFe+CsuHLort8Kks
   b39WDAqczf65dKmo58bi9m57X/PZ7oTH7yFXXskfoqED7/VZXktAEHAIwVw+wij
   .
   ...
   im2DEkLWqHkI+6Hd1Gn5GMw959mZJzAaU0F66lBUNULLpDe3yvaGeMi68lfAF9C3
   4kD1t1R1F3plP0kU+6L1Dp0g5FC723Zi0rDrUw6rEuyD1QwIw--
   -----END RSA PRIVATE KEY-----

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

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

   The following screen appears.
Enter pass phrase for ca.key

Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

-----

Country Name [2 letter code] [AU]: US
State or Province Name [full name] [Some-State]: Oregon
Locality Name (eg, city) []: Beaverton
Organization Name (eg, company) [Internet Widgits Pty Ltd]: McAfee
Organizational Unit Name (eg, section) []: Enterprise
Common Name (eg, YOUR name) []: ePO_Server
Email Address []: tester@mcafee.com

C:\ssl\bin>

Type the information needed after the following command prompts:

• Country Name (two letter code) [AU]:
• State or Province Name (full name) [Some-State]:
• Locality Name (for example, city) []:
• Organization Name (for example, company) [Internet Widgits Pty Ltd]:
• Organizational Unit Name (for example, section) []:
• Common Name (for example, YOUR name) []:

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

• Email Address []:

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

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

----BEGIN CERTIFICATE----
MIIDTCCTAqAwIBAgIJAJelid-Ih0dMA0GCSqGSIb3DQEBAQUAA4XgYMBYEBTCAwFQYIKwYBBQUHAgEIfFjFg
VQQGezEwJzEUMDA0V29tZS0wEwYDVQQLDE12UECWJUTQJ0xNRIxkCRIwD3NoWkrTVJUtQJU4xNRIwFw
----END CERTIFICATE----

4 To upload the self-signed certificate, open the Edit Server Certificate page.

a  Select Menu | Configuration | Server Settings.

b  From the Setting Categories list, select Server Certificate, and click Edit.
SSL certificates

Other useful OpenSSL commands

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

Commands to use with PKCS12 certificates

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

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

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

<table>
<thead>
<tr>
<th>Description</th>
<th>OpenSSL command format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extracts the .pem key out of .pfx</td>
<td>openssl pkcs12 -in pkcs12ExampleKey.pfx -out pkcs12ExampleKey.pem</td>
</tr>
<tr>
<td>Removes password on key</td>
<td>openssl rsa -in pkcs12ExampleKey.pem -out pkcs12ExampleKeyNoPW.pem</td>
</tr>
</tbody>
</table>

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

Command to convert a password protected private key PEM file

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

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

In the previous example, C:\ssl\keys is the input and output paths for the file names key.pem and keyNoPassword.pem.
Convert an existing PVK file to a PEM file

The McAfee ePO software supports PEM-encoded private keys, including both password protected and non-password protected private keys. Using OpenSSL you can convert a PVK-formatted key to a PEM format.

**Before you begin**

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

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

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

**Task**

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

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

   In this example, -passin and -passout arguments are optional.

2. If prompted, type the password used when you originally created the PVK file.

   If the -passout argument is not used in the example, the newly created PEM-formatted key is not password protected.

Migrate SHA-1 certificates to SHA-2 or higher

To remediate vulnerabilities in your McAfee ePO environment, migrate your existing certificates to more secure algorithm certificates or regenerate them.

The SHA-1 algorithm has reached end-of-life (EOL). Many organizations are deprecating TLS/SSL certificates signed by the SHA-1 algorithm. If you continue to use SHA-1 certificates, browsers such as Google Chrome or Microsoft Internet Explorer will flag the McAfee ePO console as an unsecure HTTPS site.

If you have upgraded McAfee ePO from an older version, migrate McAfee ePO certificates to the latest hash algorithm. A fresh installation of McAfee ePO installs the latest hash algorithm certificates.

The Certificate Manager allows you to:

- Migrate certificates that are signed by older signing algorithm to the new algorithm such as SHA-1 to SHA-256.
- Regenerate your certificates when your existing certificates are compromised due to vulnerabilities in your environment.
- Migrate or regenerate certificates for managed products that are derived from McAfee ePO root CA.
This task replaces certificates that are used for all these McAfee ePO operations:

- Agent-server communication
- Authenticating to browsers
- Certificate-based user authentication

Read these instructions carefully before proceeding with the steps. If you activate the new certificates before they are populated on the systems in your network, those systems won't be able to connect to your McAfee ePO server until the agents on those systems are re-installed.

**Task**

1. Log on as an administrator, then click **Menu | Configuration | Certificate Manager**.
   
   The Certificate Manager page provides information about the installed Root Certificate, Agent Handler certificates, server certificates, and other certificates that are derived from McAfee ePO root Certificate Authority (CA).

2. Click **Regenerate Certificate**, then click **OK** to confirm the certificate generation.
   
   The McAfee ePO root CA and other certificates that are derived from the root CA are regenerated and stored in a temporary location on the server. The time required to complete the regeneration process depends on the number of Agent Handlers and extensions that derive certificates from McAfee ePO root CA.

3. After the certificates regenerate, wait for sufficient saturation of the new certificates throughout your environment.
   
   As agents communicate to the McAfee ePO server, they are given the new certificate. The percentage of agents that have received the newly-generated certificates is provided in the **Certificate Manager** under Product: Agent Handler | Status.
   
   This distribution percentage is based on the number of agent-server communications that have occurred since the certificates were regenerated. Unmanaged inactive systems will affect this percentage.

4. Once you've achieved a distribution percentage close to 100%, click **Activate Certificates** to carry out all future operations using the new certificates.
   
   A backup of the original certificates is created, and a message appears.

5. Click **OK**. You must re-install any agents that still use the old certificates to restore agent-to-server communication.

6. Once activation of certificates is complete, perform these steps.
   a. Stop the Agent Handler services (including the Remote Agent Handler services).
   b. Restart the McAfee ePO services.
   c. Start the Agent Handler services.
Monitor your environment and make sure that your agents are successfully communicating. You can cancel the migration at this point to roll back the certificate and restore agent-to-server communication; however, this is not possible after you have completed the next step.

Click **Finish Migration** to complete the certificate migration. The certificate backup taken during activation is deleted.

For any issues during the migration, click **Cancel Migration** to revert to the previous certificates. If you cancel the migration, stop the Agent Handler services, restart the McAfee ePO service, and start the Agent Handler service again.

You can start the certificate migration again after fixing any issues.

---

**Security keys and how they work**

The McAfee ePO server relies on three security key pairs.

The three security pairs are used to:

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

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

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

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

**Local master repository key pairs**

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

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

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

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

Master Repository key pair

The Master Repository private key signs all unsigned content in the Master Repository. Agents use the public key to verify the repository content that originates from the Master Repository on this McAfee ePO server. If the content is unsigned, or signed with an unknown repository private key, the downloaded content is considered invalid and deleted.

This key pair is unique to each server installation. However, by exporting and importing keys, you can use the same key pair in a multi-server environment. Doing so ensures that agents can always connect to one of your Master Repositories, even when another repository is down.

Other repository public keys

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

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

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

Manage repository keys

You can manage repository keys using these tasks.

Tasks

- **Use one Master Repository key pair for all servers** on page 362
  You can ensure that all McAfee ePO servers and agents use the same Master Repository key pair in a multi-server environment using Server Settings.

- **Use Master Repository keys in multi-server environments** on page 363
  Make sure that agents can use content originating from any McAfee ePO server in your environment using Server Settings.

Use one Master Repository key pair for all servers

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

This process 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

1. Select Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.

2. From the Edit Security Keys page next to Local master repository key pair, click Export Key Pair.

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

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

5. Next to Import and back up keys, click Import.

6. Browse to the .zip file containing the exported Master Repository key files, then click Next.

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

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

**Use Master Repository keys in multi-server environments**

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

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

The Master Repository key pair is unique for each installation of McAfee ePO. If you use multiple servers, each uses a different key. If your agents can download content that originates from different Master Repositories, you must make sure that agents recognize the content as valid.

You can complete this process in two ways:

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

This task exports the key pair from one McAfee ePO server to a target McAfee ePO server, then, at the target McAfee ePO server, imports, and overwrites the existing key pair.

**Task**

1. On the McAfee ePO server with the Master Repository key pair, select Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.

2. Next to Local master repository key pair, click Export Key Pair, then click OK.

3. In the File Download dialog box, click Save.

4. Browse to a location on the target McAfee ePO server to save the .zip file. Change the name of the file if needed, then click Save.

5. On the target McAfee ePO server where you want to load the Master Repository key pair, select Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.
On the Edit Security Keys page:

a. Next to Import and back up keys, click Import.

b. Next to Select file, browse to and select the master key pair file you saved, then click Next.

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

7. From the list, select the file you imported in the previous steps, then click Make Master. This setting changes the existing master key pair to the new key pair you imported.

8. Click Save to complete the process.

Agent-server secure communication (ASSC) keys

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

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

Manage ASSC keys

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

Task

1. Select Menu | Configuration | Server Settings, select Security Keys, then click Edit.

2. Select one of these actions.
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate and use new ASSC key pairs</td>
<td>1. Next to the Agent-server secure communication keys list, click New Key. In the dialog box, type the name of the security key.</td>
</tr>
<tr>
<td></td>
<td>2. If you want existing agents to use the new key, select the key in the list, then click Make Master. Agents begin using the new key after the next McAfee Agent update task is complete.</td>
</tr>
<tr>
<td></td>
<td>Make sure that there is an Agent Key Updater package for each version of the McAfee Agent managed by McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>In large installations, only generate and use new master key pairs when you have specific reason to do so. We recommend performing this procedure in phases so that you can more closely monitor progress.</td>
</tr>
<tr>
<td></td>
<td>3. 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.</td>
</tr>
<tr>
<td></td>
<td>4. Back up all keys.</td>
</tr>
<tr>
<td>Export ASSC keys</td>
<td>Export ASSC keys from one McAfee ePO server to a different McAfee ePO server, to allow agents to access the new McAfee ePO server.</td>
</tr>
<tr>
<td></td>
<td>1. In the Agent-server secure communication keys list, select a key, then click Export.</td>
</tr>
<tr>
<td></td>
<td>2. Click OK. Your browser prompts you to download the sr&lt;ServerName&gt;.zip file to the specified location.</td>
</tr>
<tr>
<td></td>
<td>If you specified a default location for all browser downloads, this file might be automatically saved to that location.</td>
</tr>
<tr>
<td>Import ASSC keys</td>
<td>Import ASSC keys that were exported from a different McAfee ePO server, allowing agents from that server to access this McAfee ePO server.</td>
</tr>
<tr>
<td></td>
<td>1. Click Import.</td>
</tr>
<tr>
<td></td>
<td>2. Browse to and select the key from the location where you saved it (by default, on the desktop), then click Open.</td>
</tr>
<tr>
<td></td>
<td>3. Click Next and review the information about the Import Keys page.</td>
</tr>
<tr>
<td></td>
<td>4. Click Save.</td>
</tr>
</tbody>
</table>
### Designate an ASSC key pair as the master

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Change which key pair is specified as the master. Specify a master key pair after importing or generating a new key pair. | 1. From the Agent-server secure communication keys list, select a key, then click **Make Master**.  
2. Create an update task for the agents to run immediately, so that agents update after the next agent-server communication. Make sure that the Agent Key Updater package is checked in to the McAfee ePO Master Repository. Agents begin using the new key pair after the next update task for the McAfee Agent is complete. At any time, you can see which agents are using any of the ASSC key pairs in the list.  
3. Back up all keys. |

### Delete ASSC keys

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Do not delete any keys that are being used by any agents. If you do, those agents cannot communicate with the McAfee ePO server. | 1. From the Agent-server secure communication keys list, select the key that you want to remove, then click **Delete**.  
2. Click **OK** to delete the key pair from this server. |

### View systems that use an ASSC key pair

You can view the systems whose agents use a specific agent-server secure communication key pair in the Agent-server secure communication keys list.

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

#### Task

1. Select Menu | Configuration | Server Settings, select **Security Keys** from the Setting Categories list, then click **Edit**.
2. In the Agent-server secure communication keys list, select a key, then click **View Agents**.

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

### Use the same ASSC key pair for all servers and agents

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

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

#### Task

1. Create an agent update task.
2. Export the keys chosen from the selected McAfee ePO server.
3. Import the exported keys to all other servers.
4. Designate the imported key as the master on all servers.
5. Perform two agent wake-up calls.
6 When all agents are using the new keys, delete any unused keys.

7 Back up all keys.

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

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

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

**Task**

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

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

**Back up and restore keys**

Periodically back up all security keys, and always create a backup before changing the key management settings.

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

**Task**

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

2 From the Edit Security Keys page, select one of these actions.
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Back up all security   | 1 Click **Back Up All** near the bottom of the page.  
| keys.                  | The Backup Keystore dialog box appears.  
|                        | 2 You can optionally enter a password to encrypt the Keystore .zip file or click **OK** to save the files as unencrypted text.  
|                        | 3 From the File Download dialog box, click **Save** to create a .zip file of all security keys.  
|                        | The Save As dialog box appears.  
|                        | 4 Browse to a secure network location to store the .zip file, then click **Save**.                                                    |
| Restore security       | 1 Click **Restore All** near the bottom of the page.  
| keys.                  | The Restore Security Keys page appears.  
|                        | 2 Browse to the .zip file containing the security keys, select it, and click **Next**.  
|                        | The Restore Security Keys wizard opens to the Summary page.  
|                        | 3 Browse to the keys you want to replace your existing key with, then click **Next**.  
|                        | 4 Click **Restore**.  
|                        | The Edit Security Keys page reappears.  
|                        | 5 Browse to a secure network location to store the .zip file, then click **Save**.                                                    |
| Restore security       | 1 Click **Restore All** near the bottom of the page.  
| keys from a backup     | The Restore Security Keys page appears.  
| file.                  | 2 Browse to the .zip file containing the security keys, select it, and click **Next**.  
|                        | The Restore Security Keys wizard opens to the Summary page.  
|                        | 3 Browse to and select the backup .zip file, then click **Next**.  
|                        | 4 Click **Restore All** at the bottom of the page.  
|                        | The Restore Security Keys wizard opens.  
|                        | 5 Browse to and select the backup .zip file, then click **Next**.  
|                        | 6 Verify that the keys in this file are the ones you want to overwrite your existing keys, then click **Restore All**.    |
The McAfee Product Improvement Program helps improve McAfee products. It collects data proactively and periodically from the client systems managed by the McAfee ePO server.

**Table D-1 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Allow McAfee to collect anonymous diagnostic and usage data | • **Yes** — Allows the data collection.  
• **No** — Stops the data collection. |
Create a temporary administrator account when you are locked out of the system and no other administrator accounts are available.

**Before you begin**
- You must be able to log on to your server directly and access McAfee ePO using the localhost address.
- You must have the current database credentials for McAfee ePO.

**Task**
1. From your server, open a browser to localhost:8080.
   The McAfee Foundation Services logon page opens.
2. Click **Restore Administrator Access**.
   The **Restore Administrator Access** page opens.
3. Under **Database credentials**, enter the current user name and password.
   - **Database user name**: — the current user name for the database.
   - **Database password**: — the current password for the database.
4. Under **Administrator credentials**, enter the user name and password for the new temporary administrator account.
   - **User name**: — the user name for the new account.
   - **Password**: — the password for the new account.
   - **Confirm password**: — re-enter the password for the new account to verify it.
5. Click **Submit**.
   The system creates the new temporary account.

You can now access McAfee ePO using the new administrator account. Use the account to restore access for your administrator users. After they have access, delete the temporary administrator account.
Ports overview

Follow these guidelines when customizing the ports used by the McAfee ePO server.

Contents

- Change console-to-application server communication port
- Change agent-server communication port
- Ports required for communicating through a firewall

Change console-to-application server communication port

If the McAfee ePO console-to-application server communication port is in use by another application, follow these steps to specify a different port.

Before you begin

- Back up your registry and understand the restore process. For more information, see the Microsoft documentation.
- Make sure that you run only .reg files that are not confirmed to be genuine registry import files.

Task

1. Stop the McAfee ePO services:
   a. Close all McAfee ePO consoles.
   b. Click Start | Run, type services.msc, then click OK.
   c. Right-click each of these services and select Stop:
      • McAfee ePolicy Orchestrator Application Server
      • McAfee ePolicy Orchestrator Event Parser
      • McAfee ePolicy Orchestrator Server

2. In the registry editor, select this key:
   \[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall \{53B73DFD-AFBE-4715-88A1-777FE404B6AF\}]
3 In the right pane, double-click TomcatSecurePort.SQL and change the value data to reflect the required port number (default is 8443).

4 Open a text editor and paste this line into a blank document:

```
UPDATE EPOServerInfo SET rmdSecureHttpPort = 8443
```

Change 8443 to the new port number.

5 Name the file TomcatSecurePort.sql and save it to a temporary location on the SQL Server.

6 Use Microsoft SQL Server Management Studio to install the TomcatSecurePort.SQL file that you created.
   a Click Start | All Programs | Microsoft SQL Server Management Studio.
   b On the Connect to Server dialog box, click Connect.
   c Expand Databases, then select ePO database.
   d From the toolbar, select New Query.
   e Click File | Open | File..., then browse to the TomcatSecurePort.sql file.
   f Select the file, click Open | Execute.

7 In Windows Explorer, browse to this directory:
   \Program Files (x86)\McAfee\ePolicy Orchestrator Cloud\Server\conf\

8 In Notepad, open Server.xml and replace all entries for port 8443 with the new port number.

9 Click Start | Run, type services.msc, then click OK.

10 Right-click each of these services and select Start:
   • McAfee ePolicy Orchestrator Application Server
   • McAfee ePolicy Orchestrator Event Parser
   • McAfee ePolicy Orchestrator Server

---

**Change agent-server communication port**

Follow these steps to change the agent-server communication port.

**Before you begin**

- This topic contains information about opening or modifying the registry. This information is for network and system administrators only. Registry modifications are irreversible and can cause system failure if done incorrectly.
- We strongly recommend that you back up your registry and understand the restore process. For more information, see the Microsoft documentation.
- Make sure that you run only .REG files that are confirmed to be genuine registry import files.

Modifying the agent-server communication port requires five steps and one optional step if you are using remote Agent Handlers.

1 Stop the McAfee ePO services
2 Modify the port value in the registry
3 Modify the value in the McAfee ePO database
4 Modify the port value in the McAfee ePO configuration files
5 Restart the McAfee ePO services
6 (Optional) Modify settings on remote Agent Handlers

Task

1 Stop the McAfee ePO services:
   a Close all McAfee ePO consoles.
   b Click Start | Run, type services.msc, then click OK.
   c Right-click each of these services and select Stop:
      • McAfee ePolicy Orchestrator Application Server
      • McAfee ePolicy Orchestrator Event Parser
      • McAfee ePolicy Orchestrator Server

2 Modify the port value in the registry:
   a Click Start | Run, type regedit, then click OK.
   b Navigate to the key that corresponds to McAfee ePO:
      [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall \{ 53B73DFD-AFBE-4715-88A1-777FE404B6AF}]
   c Modify the string value AgentPort to reflect the appropriate port, then close the registry editor. The default value for this port is 80.

3 Modify the value in the McAfee ePO database:
   a Open a text editor, and add these lines to the blank document:
      ```
      UPDATE EPOServerInfo
      ServerHTTPPort=80
      ```
   b Save the file as DefaultAgentPort.SQL in a temporary location on the SQL Server.
   c Click Start | All Programs | Microsoft SQL Server Management Studio to use Microsoft SQL Server Management Studio to install the DefaultAgentPort.sql file.
   d On the Connect to Server dialog box, click Connect.
   e Expand Databases, then select ePO database.
   f From the toolbar, select New Query.
   g Click File | Open | File, browse to and select the DefaultAgent.SQL file, then click Open | Execute.
   h Paste this line into a blank document:
      ```
      UPDATE EPOServerInfo SET ServerHTTPPort =80
      ```
      Change 80 to the new port number.
   i Name the file DefaultAgentPort.SQL and save it to a temporary location on the SQL Server.
j Use Microsoft SQL Server Management Studio to install the DefaultAgentPort.SQL file.
   • Click Start | All Programs | Microsoft SQL Server Management Studio.
   • On the Connect to Server dialog box, click Connect.
   • Expand Databases, then select ePO database.
   • From the toolbar, select New Query.
   • Click File | Open | File, browse to and select the DefaultAgentPort.SQL file, then click Open | Execute.

4 Modify the port value in the McAfee ePO configuration files:
   a Navigate to C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\....
   b Using a text editor, open Server.ini and change the value for HTTPPort=80 to reflect the new number, then save the file.
   c Using a text editor, open Siteinfo.ini and change the value for HTTPPort=80 to reflect the new number, then save the file.
   d Navigate to C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\.... open httpd.conf, then change these lines to reflect the new port number:

   ```
   Listen 80
   ServerName<YourServerName>: 80
   If using VirtualHosts, change:
   NameVirtualHost *:80
   <VirtualHost *:80>
   ```
   e Save the file and exit the text editor.

5 Restart the McAfee ePO services:
   a Click Start | Run, type services.msc, then click OK.
   b Right-click each of these services and select Start:
      • McAfee ePolicy Orchestrator Application Server
      • McAfee ePolicy Orchestrator Event Parser
      • McAfee ePolicy Orchestrator Server

6 (Optional) Modify settings on remote Agent Handlers:
   a Make sure that all McAfee ePO consoles are closed, then click Start | Run, type services.msc and click OK.
   b Right-click each of these services and select Start:
      • McAfee ePolicy Orchestrator Event Parser
      • McAfee ePolicy Orchestrator Server

   This server might be listed as MCAFEEAPACHESRV if the server wasn’t restarted since the Agent Handler was installed.
c. Navigate to `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\...`, using a text editor open `httpd.conf`, then change these lines to reflect the new port number:

```plaintext
Listen 80
ServerName<YourServerName>: 80
```

If using VirtualHosts, change:

```plaintext
NameVirtualHost *:80
<VirtualHost *:80>
```

d. Save the file and exit the text editor.

e. Click **Start** | **Run**, type `services.msc`, then click **OK**.

f. Right-click each of these services and select **Start**.
   - McAfee ePolicy Orchestrator Event Parser
   - McAfee ePolicy Orchestrator Server

   This server might be listed as `MCAFEEAPACHESRV` if the server has not been restarted since the Agent Handler was installed.

If you previously deployed agents to clients, reinstall the agent on all clients using the `/forceinstall` switch to overwrite the existing `Sitelist.xml` file. For more information about specific McAfee Agent versions that allow the `/forceinstall` switch to work successfully, see McAfee KnowledgeBase article [KB60555](#).

---

**Ports required for communicating through a firewall**

Use these ports to configure a firewall to allow traffic to and from your McAfee ePO server.

**Relevant terms**

- **Bidirectional** — The remote or local system can initiate the connection.
- **Inbound** — The remote system initiates the connection.
- **Outbound** — The local system initiates the connection.
### Table F-1 McAfee ePO server

<table>
<thead>
<tr>
<th>Port</th>
<th>Default</th>
<th>Description</th>
<th>Traffic direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent-server communication port</td>
<td>80</td>
<td>TCP port opened by the McAfee ePO server service to receive requests from agents.</td>
<td>Bidirectional between the Agent Handler and the McAfee ePO server and inbound from McAfee Agent to Agent Handlers and McAfee ePO server.</td>
</tr>
</tbody>
</table>
| Agent communicating over SSL (4.5 and later agents only) | 443     | By default, 4.5 agents must communicate over SSL (443 by default). This port is also used for the Remote Agent Handler to communicate with the McAfee ePO Master Repository. | Inbound connection to the McAfee ePO server from agents or Agent Handlers to the Master Repository. Inbound connection:  
  • Agent to McAfee ePO  
  • Agent Handler to Master Repository  
  • McAfee ePO to Master Repository  
  • Agent to Agent Handler |
| Agent wake-up communication port          | 8081    | TCP port opened by agents to receive agent wake-up requests from the McAfee ePO server. TCP port opened to replicate repository content to a SuperAgent repository. | Outbound connection from the McAfee ePO server and Agent Handler to the McAfee Agent.                |
| SuperAgent repository port                |         |                                                                                                                                                    |                                                                                                      |
| Agent broadcast communication port        | 8082    | UDP port opened by SuperAgent to forward messages from the McAfee ePO server and Agent Handler.                                                        | Outbound connection from the SuperAgent to other agents.                                             |
| Console-to-application server communication port | 8443  | HTTPS port opened by the McAfee ePO Application Server service to allow web browser console access.                                                    | Inbound connection to the McAfee ePO server from the McAfee ePO console.                             |
| Client-to-server authenticated communication port | 8444  | Used by the Agent Handler to communicate with the McAfee ePO server to get required information (for example, LDAP servers).                         | Outbound connection from remote Agent Handlers to the McAfee ePO server.                             |
| SQL Server TCP port                      | 1433    | TCP port used to communicate with the SQL Server. This port is specified or determined automatically during the setup process.                        | Outbound connection from the McAfee ePO server and Agent Handler to the SQL Server.                   |
| SQL Server UDP port                      | 1434    | UDP port used to request the TCP port that the SQL instance hosting the McAfee ePO database is using.                                                | Outbound connection from the McAfee ePO server and Agent Handler to the SQL Server.                   |
| Default LDAP server port                 | 389     | LDAP connection to look up computers, users, groups, and Organizational Units for User-Based Policies.                                                | Outbound connection from the McAfee ePO server and Agent Handler to an LDAP server.                   |
| Default SSL LDAP server port             | 636     | User-Based Policies use the LDAP connection to look up users, groups, and Organizational Units.                                                        | Outbound connection from the McAfee ePO server and Agent Handler to an LDAP server.                   |
Traffic quick reference

Use this port and traffic direction information to configure a firewall to allow traffic to and from your McAfee ePO server.

Relevant terms

- **Bidirectional** — A local or remote system can initiate the connection.
- **Inbound** — A remote system can initiate the connection.
- **Outbound** — A local system can initiate the connection.

Table G-1  Agent Handler

<table>
<thead>
<tr>
<th>Default port</th>
<th>Protocol</th>
<th>Traffic direction on McAfee ePO server</th>
<th>Traffic direction on Agent Handler</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Bidirectional connection to and from McAfee ePO server.</td>
<td>Bidirectional connection to and from Agent Handler.</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>Outbound connection from McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Inbound connection to McAfee ePO server.</td>
<td>Inbound connection to the Agent Handler.</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>Outbound connection from McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>Outbound connection from McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
<tr>
<td>1434</td>
<td>UDP</td>
<td>Outbound connection from McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
<tr>
<td>8081</td>
<td>TCP</td>
<td>Outbound connection from McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>Inbound connection to McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
<tr>
<td>8444</td>
<td>TCP</td>
<td>Inbound connection to McAfee ePO server.</td>
<td>Outbound connection from Agent Handler.</td>
</tr>
</tbody>
</table>

Table G-2  McAfee Agent

<table>
<thead>
<tr>
<th>Default port</th>
<th>Protocol</th>
<th>Traffic direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Outbound connection to McAfee ePO server and Agent Handler.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Outbound connection to the McAfee ePO server and Agent Handler.</td>
</tr>
</tbody>
</table>
### Table G-2  McAfee Agent (continued)

<table>
<thead>
<tr>
<th>Default port</th>
<th>Protocol</th>
<th>Traffic direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>8081</td>
<td>TCP</td>
<td>Inbound connection from the McAfee ePO server and Agent Handler.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Tip:</strong> If the agent is a SuperAgent repository, the inbound connection is from other agents.</td>
</tr>
<tr>
<td>8082</td>
<td>UDP</td>
<td>Inbound connection to agents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Tip:</strong> Inbound and outbound connection is from or to a SuperAgent.</td>
</tr>
</tbody>
</table>

### Table G-3  SQL Server

<table>
<thead>
<tr>
<th>Default port</th>
<th>Protocol</th>
<th>Traffic direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>TCP</td>
<td>Inbound connection from McAfee ePO server and Agent Handler.</td>
</tr>
<tr>
<td>1434</td>
<td>UDP</td>
<td>Inbound connection from McAfee ePO server and Agent Handler.</td>
</tr>
</tbody>
</table>
A

access requirements for System Tree 61
accounts
  user 89
actions
  Apply Tag 86
  Check IP Integrity 67
  Run Tag Criteria 83
  Sort Now 74
  Test Sort 74
  used with Product Deployment 124
Active Directory
  applying permission sets 91
  configuring Windows authorization 93
  containers, mapping to System Tree groups 74
  implementation strategies 91
  systems only synchronization 65
Active Directory synchronization
  borders and 62
  deleting systems 63, 64
  duplicate entry handling 63
  Synchronize Now action 63
  systems and structure 64
  tasks 63
  to System Tree structure 74
  types 64
adding comments to issues 353
administrators
  about 100
  contacted automatically to stop DAT release 118
  contacted automatically with compliance report 220
  permission needed for Disaster Recovery 50
  permissions 100
  recommended monthly task to review IDs 294
  source sites, configuring 238
agent
  configuring policies to use repositories 242
  configuring proxy settings for 241
  deployment credentials 205
  first call to server 67
  grouping 278
  grouping by assignment rules 278
  GUID and System Tree location 67
  maintenance 203
agent (continued)
  traffic direction and ports 379
agent communication port 205
Agent Handlers
  about 257
  assigning agents 276
  assignment priority 279
  assignments 269
  authentication modes 257
  behind a DMZ 263
  component in McAfee ePO 14
  configure priority 269
  configure virtual groups 268
  deployment 266
  eliminates multiple McAfee ePO servers 261
  enable and disable from Handlers List 268
  failover protection 262
  frequently asked questions 280
  hardware, software, and port requirements 270
  how they work 257
  LDAP access 347
  managing assignments 277
  moving agents between 278
  multiple 257
  ports used to communicate through firewall 377
  priority in sitelist file 275
  software installation 271
  traffic direction and ports 379
  user interface 266
  virtual settings 268
  why use them 259
Agent Status Monitor, to collect and send properties 336
agent-server communication
  interval reduced with LDAP mirroring 347
  managing 204
  secure communication keys (ASSC) 364
  System Tree sorting 66
agent-server communication interval
  adjusting 203
  change default 204
Agent-server communication interval
  change setting 137
agent-server communication port, change 374
Agent-server secure communication
about 14
Agent-server secure communication (ASSC)
about 361
using different key pairs for servers 367
using one key pair 366
viewing systems that use a key pair 366
working with keys 364
Agent-server secure communication keys
export and import keys 80
with Transfer Systems 78
Agents
and SuperAgent repositories 230
assignment to Agent Handlers 269
finding inactive agents 215
finding older versions 212
updating using Product Deployment 213
AIA, See Authority Information Access
Apache server 228
API, reports
run with the web API 319
run with web API 319
using API ID number example report 327
using API table objects, commands, and arguments example report 330
using API XML data example report 328
using parsed query export data to create web URL queries 325
using S-Expressions in web URL queries 322
using the McAfee command framework 320
using the web URL Help 320
Applied Policies, creating queries 159
Apply Tag action 83
ASSC
agent-server secure communication 14
ASSC keys, See agent-server secure communication keys
Assign client tasks 165
assigning issues 353
assignment rules
agents and handlers 278
Audit Log
about 94
deleting old entries 95
purge automatically 208
recommended monthly task 294
used with Product Deployment 124
viewing user actions 95
Authentication
certificate-based 96
certification authority 96
authentication, certificate-based 96
authentication, configuring for Windows 89
Authority Information Access, defined 96
authorization strategies 91
Automatic responses (continued)
actions 186
certification authority 96
Automatic responses (continued)
actions 186
certification authority 96
Automatic responses (continued)
actions 186
certification authority 96
components
Disaster Recovery 50
repositories, about 224
configuration
agent-server communication interval 204
automatic updates of DAT and product files 210
client event summary queries 311
custom queries 308
disabling 1051 and 1059 events 211
event purging 208
event purging with a query 209
Global Updating limitations 237
queries with tables 315
system list on tag groups 85
threat event summary queries 313
console
McAfee ePO 14
contacts
responses and 186
CPUs
needed for node count 234
over-utilized 283, 285
creating issues 352
credentials
changing, on distributed repositories 253
distributing 253
modifying database registrations 344
criteria-based tags
applying 87, 88
sorting 72
CRL, See certificate revocation list
Cron syntax used with server tasks 163
Current branch
checking in update packages 111
defined 226
custom logon messages 93
D
dashboard monitors
configuring 29
moving and resizing 30
dashboards 348
configuring for exported reports 46
configuring monitors 29
create Snapshot 55
first-time 28
granting permissions to 26
import and export 27
introduction 25
managing 26
McAfee 25
moving and resizing monitors 30
private 25
public 25
server settings 28, 30
DAT file updating
  checking in manually 111
  considerations for creating tasks 171
  daily task 172
  deployment 168
  from source sites 238
  in master repository 226
  scheduling a task 172

DAT files
  automate DAT file testing 113, 115
  average size 302
  creating a compliance query 218
  deleting from repository 110
  deploying to repositories 233
  evaluating 173
  overview of automatic testing process 111
  pull server task 113
  replicating and repositories 305
  repository branches 110
  test before deployment 115
  update with Global Updating 237
  updating automatically 209
  using repositories 228

Data Migration Tool, used for product compatibility check 105

Data Rollup server task 316

database servers
  editing registrations 344
  registering 343
  removing 344
  traffic direction and ports 379
  using 343

databases
  back up and restore process 298
  backup weekly tasks 292
  component in McAfee ePO 14
  determining server and name 297
  Disaster Recovery 50
  maintaining 286
  multi-server querying 315
  overview of back up 52
  overview of recovery 53
  purge events automatically 208
  queries and retrieving data 35
  reindex 286
  restoring the SQL 297
  scheduling Snapshot 297
  script to add virtual MAC vendor ID value 338
  server clusters for disaster recovery 59
  spares on physical sites 59
  test connection 287

deleting issues 353

deployment
  Agent Handler considerations 266
  calculating repository bandwidth 302
  checking in packages manually 109

)(continued)
  global updating 128
  installing products 169, 170
  package security 166
  products and updates 168
  supported packages 166
  tasks 166
  tasks, for managed systems 168
  to repositories 233
  view 124
  view assigned client task 171
detection definition files
  DAT files 228

Directory (See System Tree) 74
disaster recovery
  using cold and hot spares 59
  using server clusters 59
  using the Disaster Recovery feature 58

Disaster Recovery
  components 50
  configuring snapshots 297
  information needed for 299
  Keystore encryption passphrase 50
  overview 52
  server settings 57
  server task 297
  Snapshot 49
  what it is 49
distributed repositories
  about 224
  adding to ePolicy Orchestrator 246
  automatically pull and copy DAT updates from McAfee 113
  changing credentials on 253
  configuring agent policies ePO 14
  creating and configuring 245
  creating in SuperAgents 231
  deleting 249
  deleting SuperAgent repositories 244
  different types 228
  editing existing 248
  enabling folder sharing 248
  folder, creating 246
  how agents select 254
  limited bandwidth and 224
  part of weekly tasks 292
  replicated with an automatic content pull 209
  replicating packages to SuperAgent repositories 244
  SuperAgent, tasks 243
  unmanaged, copying content to 250

DNS
  used to find the ePolicy Orchestrator server 59, 270
  domain synchronization 62
  duplicate entries in the System Tree 75
duplicate GUID
recommended monthly task 294
run server task 207

e
editing database server registrations 344
ingo to nowed issues 353
enforcement, See policy enforcement
engine updating
checking in manually 111
deployment packages 168
from source sites 238
in master repository 226
scheduling a task 172
engines
deleting from repository 110
repository branches 110
ePolicy Orchestrator
disable server as repository 234
disaster recovery 58
event processing 285
multiple server alternative 261
Performance Monitor 284
remote console connection 57
server best practices 288
server clusters for disaster recovery 59
spares on physical sites 59
traffic direction and ports 379
Evaluation branch
defined 226
using for new DATs and engine 173
event log, purging 301
events
1051 and 1059 filtering 210
aggregation 178
automatic purge 208
causing ePolicy Orchestrator performance problems 283
causing performance problems 285
compliance events 317
creating client event summary queries 311
creating custom queries 308
creating queries 315
determining which are forwarded 180
enabling folder sharing 248
export
dashboards 348
exporting
dashboards 348
permissions 348
policy assignments 348
queries 348
repositories 348
responses 348
systems 348
tags 348
tasks 348
exporting systems 71
event log, purging 301
events (continued)
thresholds 178
throttling 178
executables, managing 183, 201
export
formats 35
exporting
dashboards 27
permission sets 101
policies 348
exporting and importing
client task objects 348
dashboards 348
permissions 348
policy assignments 348
queries 348
repositories 348
responses 348
systems 348
tags 348
tasks 348
exporting systems 71
extension files, installing 109
F
failback to your original server 53
failover protection using Agent Handlers 262
failover sites
about 224
configuring 238
deleting 240
edit existing 240
switching to source 240
features, McAfee ePO 13
filters
creating 22
custom 22
list 21
overview 21
query results 36
setting for response rules 185
used with Policy Assignment Rules 148
used with Product Deployment 126
firewall
ports used to communicate through to server 377
fragmentation in the database 286
frequently asked questions about Agent Handlers 280
FTP repositories 228
creating and configuring 245
dediting 248
enabling folder sharing 248
G

geographic borders, advantages of 62

global unique identifier (GUID) 67

global updating

- contents 242
- enabling 128
- process description 127
- requirements 127

Global Updating, about 237

groups

- Agent Handlers 266
- catch-all 67
- configuring criteria for sorting 72
- controlling access 100
- creating manually 70
- criteria-based 67
- importing NT domains 75
- moving systems manually 78
- of SuperAgents 230
- operating systems and 63
- pasting policy assignments to 156
- policy enforcement for a product 143
- sorting criteria 72
- sorting, automated 63
- updating manually with NT domains 77
- using IP address to define 62
- viewing policy assignment 158

GTI, See McAfee Global Threat Intelligence

GUIDs

- finding duplicates 207

H

handler assignment

- editing priority 279
- managing 277

handler groups

- about 275
- creating 277
- deleting 278
- editing settings 278

handlers

- creating groups 277
- grouping agents 280
- moving agents between 278
- priority 275

Handlers List, enable, and disable Agent Handlers 268

hardware

- used for repositories 234

HTTP repositories

- about 229
- creating and configuring 245
- editing 248
- enabling folder sharing 248

I

IIS

- Microsoft IIS server 228

importing

- basics 349
- dashboards 27
- permission sets 101

inactive agent

- finding 214
- query 215
- removed as part of weekly tasks 292

inheritance

- and policy settings 139
- broken, resetting 159
- viewing for policies 159

installation

- Agent Handler software 271
- use Disaster Recovery after installation 58

interface

- main menu 18
- navigation 18
- shortcut bar 18

Internet Explorer

- configuring proxy settings 241

intervals

- between notifications 184

IP address

- as grouping criteria 62
- range, as sorting criteria 72
- restricting user sessions to a single 93
- sorting and checking overlap 67
- sorting criteria 69, 72
- subnet mask, as sorting criteria 72

issues

- about 351
- adding comments 353
- assigning 353
- creating 352
- creating automatically from responses 352
- deleting 353
- editing 353
- managing 351
- removing outdated 352
- viewing 351
- viewing details 353

K

keys, See security keys

Keystore encryption passphrase

- Disaster Recovery 50
- setting 57

L

LAN connections and geographical borders 62
language packages, See agent
lazy caching, SuperAgent configuration 230
LDAP servers
  authentication strategies 91
  McAfee ePO component 14
  mirroring overview 347
  registering 346
lists
  filtering 21
  searching 22
lists, working with 21
load balancing Agent Handlers 262
local distributed repositories 250
log on and log off 17
logon messages 93

M
main menu
  navigating in the interface 18
maintenance
  periodic tasks 295
  recommended daily 289
Maintenance Plan, See database maintaining
making comments and suggestions 17
malware events
  count systems cleaned per week 216
  create query to find malware events per subnet 217
  measuring 216
  per subnet 217
  send Automatic Response 118
managed systems
  deployment tasks for 169
  global updating and 224
  installing products on 170
  policy management on 137
  rollup querying 315
  sorting, criteria-based 65
  tasks for 169
  viewing policy assignment 158
Master Repository
  about 224
  checking in packages manually 111
  communicating with source sites 240
  configuring proxy settings 241
  default 234
  key pair for unsigned content 362
  on ePolicy Orchestrator 228
  part of product deployment 121
  security keys in multi-server environments 363
  updating with pull tasks 253
  using replication tasks 254
McAfee Agent Status Monitor, to collect and send properties 336
McAfee Agents
  agents 14
McAfee Endpoint Security
  restriction for Global Updating 237
McAfee ePO
  components 14
  console 14
  differences from McAfee ePO Cloud 13
  functions 14
  how it works 14
  key features 13
  server 14
McAfee ePO Cloud
  differences from McAfee ePO 13
McAfee Global Threat Intelligence suggested daily task 289
McAfee recommendations
  create a Rollup Data server task 316
  deploy agents when importing large domains 75
  evaluate borders for organization 62
  phased rollout for Product Deployment 166
  schedule replication tasks 254
  System Tree planning 61
  use global updating 127
  use IP addresses for sorting 62
  use tag-based sorting criteria 63
menu, See main menu
menu-based navigation 18
message
  custom logon 93
Microsoft
  Windows Reliability and Performance Monitor 283
  Windows Task Manager 283
Microsoft IIS server 228
Microsoft SQL database
database 14
Microsoft Windows Resource Kit 71
monitors
  configuring 29
  default refresh interval 30
  Disaster Recovery Snapshot status 50
  using 25
  multiple McAfee ePO servers
    policy sharing 147

N
navigation
  main menu 18
  menu-based 18
  shortcut bar 18
NETDOM.EXE utility, creating a text file 71
network bandwidth, See System Tree organization
New Group wizard, creating new groups 39
node counts
  and repositories 230
  repository hardware 234
notification interval 184
notification rules, importing .MIB files 183
notifications
assigning permissions 181
event forwarding 180
how they work 82
recipients 82
registered executables, managing 183, 201
SNMP servers 344
NT domains
importing to manually created groups 75
synchronization 65, 75
updating synchronized groups 77

O
OAS, See on-access scan
OCSP, See Online Certificate Status Protocol
ODS, See on-demand scan
on-access scan, recommended daily task 289
on-demand scan
recommended daily task 289
recommended weekly task 292
schedule for the test group 117
used to automate DAT file testing 116
Online Certificate Status Protocol, another method to check a certificate's authenticity 96
operating systems
Agent Handlers 270
for repositories 228
grouping 63
legacy systems (Windows 95, Windows 98) 63
OUI, See Organizationally Unique Identifier

P
packages
checking in manually 109
configuring deployment task 170
managing 109
moving between branches in repository 110
part of product deployment 121
security for 166
passwords
log on and log off 17
patches
copying and pasting 155, 156
deleting and editing 153
locking 139
Policy Catalog 139
systems, assigning to 154
viewing 157, 158
policy assignment
about 140
and multi-slot policies 140
creating 147
deleting and editing 148
editing priority 148
priority 140
rule criteria 140
system-based 140
system-based policies 141
user-based 140
user-based policies 141
viewing summary 148

permission sets 348 (continued)
managing 101
mapping to Active Directory groups 89
System Tree 61
permissions
administrator 100
assigning for notifications 181
assigning for responses 182
for queries 34
to dashboards 26
personal settings, categories 19
policies 348
about 137
broken inheritance, resetting 159
categories 137
changing the owner 146
comparing 145
controlling on Policy Catalog page 142
create SuperAgent policy 231
creating SuperAgent 230
disabling the Master Repository 236
disabling a DAT test group 115
disabling a DAT test group 115
disabling Master Repository 236
edit policy history permission sets 145
importing and exporting 137
inheritance 139
manage policies using policy history entries 144
McAfee Agent policy for a DAT test group 115
ownership 140, 158
set the ASCI 204
settings, viewing 157
viewing 137, 156
working with Policy Catalog 142
policy assignment rules
about 140
and multi-slot policies 140
creating 147
deleting and editing 148
defining priority 148
priority 140
rule criteria 140
system-based 140
system-based policies 141
user-based 140
user-based policies 141
viewing summary 148

Index

388 McAfee ePolicy Orchestrator 5.9.0 Product Guide
queries, using user interface (continued)
  event summary overview 311
  find Agent Version Summary 212
  Inactive Agents 215
  malware events 216
  threat event summary 313
  to count systems cleaned per week 216
  to display compliance 218
  to find malware events per subnet 217
  use report input 220
  used to purge events 209
  using tables 315

Query Builder
  about 36
  creating custom queries 33, 37
  result types 36

Quick Find 22

R
RAM
repository servers 234
registered servers
  adding SNMP servers 344
  enabling policy sharing 146
  LDAP servers, adding 346
  registering 341
  supported 341
  syslog 345
registering database servers 343
remote commands
  determining SQL database server and server name 297
remote console connection 57
removing database server registrations 344
  replication
    avoiding for selected packages 247
    disabling of selected packages 248
replication tasks
  full vs. incremental 254
  updating master repository 254
Report Builder, creating custom reports 33
  report elements
    configuring charts 44
    configuring images 42
    configuring tables 43
    configuring text 43
reports
  about 40
  adding elements 42
  adding to a group 47
  configuring chart elements 44
  configuring image elements 42
  configuring table elements 43
  configuring template and location for 46
  configuring text elements 43
  creating 33, 41

reports (continued)
  creating custom queries 308
  editing existing 41
  exported query results 35
  running with a server task 45
  scheduling 45
  structure and page size 40
  to find VPN server MAC address 337
  viewing output 46
reports, using API
  created using S-Expressions in web URL queries 322
  example created with ID number 327
  example created with table objects, commands, and arguments 330
  example created with XML data 328
  parsing query with web URL queries 325
  running 319
  using the McAfee command framework 320
  using the web URL Help 320
reports, using user interface
  creating 307
  creating custom queries 308
  include query output 220
repositories 348
  about 233
  automatically pull and copy DAT updates from McAfee 113
  bandwidth recommendations 303
  branches 110, 173, 226
  calculating bandwidth use 233
  calculating update bandwidth 302
  concept 223
  creating SuperAgent repository 243
  DAT file replication 305
  determine how many and location 233, 234
  disabling the Master Repository 243
  FTP servers 228
  global updating 237
  HTTP servers 229
  importing from repository list files 252
  master, configuring proxy settings for 241
  pull content automatically 210
  replication and selection of 254
  security keys 361, 363
  source site 224
  SuperAgent 230
  types of 224
  UNC 249
  UNC shares 229
  unmanaged, copying content to 250
  update with Global Updating 237
  used to automate DAT file testing 115
  what they do 223
repository list files
  about 233
  adding distributed repository to 246
repository list files (continued)
  exporting to 251, 252
  importing from 252
  priority of Agent Handlers 275
  SiteList.xml, uses for 233
  working with 251
Response Builder 186
response rules
  Description page 185
  setting filters for 185
  setting thresholds 185
responses 348
  actions 186
  assigning permissions 182
  configuring 183, 186, 201
  configuring to automatically create issues 352
  contacts for 186
  event forwarding 180
  rules 179
  SNMP servers 183
responses, automatic
  about 177
rules
  configuring contacts for responses 186
  defaults for automatic responses 179
  setting up for notifications, SNMP servers 183
Run Tag Criteria action 83
S
scaling McAfee ePO
  using Agent Handlers 259, 261
  using repositories 223, 261
scheduling
  applying criteria-based tags 88
  automatic updates of DAT and product files 210
  Disaster Recovery Snapshot 297
  event purging 208, 209
  purging the event log 301
  server task for policy sharing 147
  server tasks with Cron syntax 163
security certificate
  creating a self-signed certificate 355
security keys
  agent-server secure communication (ASSC) 361, 364
  ASSC, working with 364
  for content from other repositories 362
  general 361
  managing 362
  master keys in multi-server environments 363
  private and public 362
  using one master key 362
selected packages
  avoid replication of 247
  disabling replication of 248
server certificates
  migrate certificates to hash algorithm 359
  path to files 52
server clusters for disaster recovery 59
server settings
  agent deployment credentials 205
  certificate-based authentication 96–98
  dashboards 28, 30
  Disaster Recovery 57
  email server 179
  event filtering 180
  event notifications 180
  example setting 21
  global updating 128, 242
  Internet Explorer 241
  logon message 93
  notifications 184
  overview 19
  ports 205
  printing and exporting 46
  Product Compatibility List 106
  proxy settings 241
  security keys 362–364, 366, 367
  source sites 239, 240, 252
  System Tree sorting 73
  User Session 93
Server Task Builder 88
Server Task Log
  removing outdated tasks 162
  Status column 161
  viewing server tasks 161
server tasks
  about 161
  creating 162
  Data Rollup 316
  Disaster Recovery 297
  pull DAT files 113
  purge the logs 208
  query with a sub-action 39
  removing outdated 162
  removing outdated log items 163
  running reports 45
  scheduling a query 39
  scheduling with Cron syntax 163
  status of 161
  Synchronize Domain/AD 63
  viewing 161
servers
  back up and restore process 298
  database 343
  disabling the Master Repository 236
  disaster recovery 58
  Disaster Recovery 50, 299
  finding performance problems 283, 285
  hardware upgrade using Disaster Recovery 49

servers (continued)
  master repository key pair 362
  overview of back up 52
  overview of recovery 53
  recommended best practices 288
  registering additional servers 341
  registering LDAP servers 346
  settings and controlling behavior 19
  SNMP, and responses 183
  supported server types 341
  traffic direction and ports 379
  transferring systems 82
  types you can register 341
shortcut bar
  customizing 18
sitelist files 275
sites
  deleting source or fallback 240
  editing existing 240
  fallback 224, 238
  switching source and fallback 240
Snapshot
  create from Dashboard 55
  create from Web API 55
  creating 54
  Dashboard monitor 50
  overview 52
  part of Disaster Recovery 49
  records saved to database 52
  scheduling defaults 297
  Server Task Log Details 54
snapshot, with Disaster Recovery feature 58
snapshots
  configuring 297
SNMP servers
  registering 344
  responses 183
software manager 103
  about 103
  contents 103
  product compatibility 105
Software Manager
  checking in extensions 104
  checking in packages 104
  evaluation software 104
  licensed software 104
  part of weekly tasks 292
  recommended weekly task 292
  removing extensions 104
  removing packages 104
Sort Now action 65
sorting criteria (continued)
  IP address 67, 72
  sorting systems into groups 65
  tag 72
  tag-based 63, 67
source sites
  about 224
  configuring 238
  creating 239
  deleting 240
  editing existing 240
  fallback 224
  importing from SiteMgr.xml 252
  product updates and 224
  switching to fallback 240
  update packages and 168
SQL database
  back up and restore process 298
  databases 14
  Disaster Recovery 50
  maintaining 296
  managing 296
  overview of back up 52
  overview of recovery 53
  ports used to communicate through firewall 377
  restoring the database 297
  scheduling Snapshot 297
SQL replication, required with spare database 59
SQL Server
  determining database server and name 297
SQL Server Management Studio
  add virtual VPN server MAC vendor ID value 338
  Disaster Recovery 58
SQL servers, See databases
Status Monitor, to collect and send properties 336
subgroups
  and policy management 75
  criteria-based 67
subnets, as grouping criteria 62
SuperAgent repositories
  creating 243
  deleting 244
  global updating requirements 127
  replicating packages to 244
  tasks 243
SuperAgent systems
  assign SuperAgent policy to SuperAgent group 232
SuperAgents
  configuring 230
  convert client systems into SuperAgents 232
  create group in System Tree 232
  create policy 231
  lazy caching 230
  ports used to communicate through firewall 377
  sharing hardware 234
synchronization
  - Active Directory and 65
    - defaults 67
    - deploying agents automatically 64
    - excluding Active Directory containers 64
    - NT domains 65
    - preventing duplicate entries 65
    - scheduling 77
    - Synchronize Now action 63
    - systems and structures 64
    - systems only, with Active Directory 65
  - syslog server
    - registering 345
  - System Tree
    - access requirements 61
    - assigning policies to a group 153
    - clients disappear 336
    - configuring SuperAgent group 230
    - create group for DAT file testing 115
    - create SuperAgents group 232
    - creation, automated 62
    - criteria-based sorting 65
    - deleting inactive systems 215
    - grouping agents 280
    - organization 61
    - permission sets 61
    - populating groups 69
    - system information details 68
  - System Tree organization
    - add systems to groups 70
    - borders in your network 62
    - creating groups 69
    - duplicate entries 75
    - importing Active Directory containers 74
    - importing systems and groups 72
    - mapping groups to Active Directory containers 74
    - moving systems to groups manually 78
    - network bandwidth 62
    - operating systems 63
    - planning considerations 61
    - selecting multiple items 23
    - using subgroups 75
  - System Tree sorting
    - default settings 67
    - enabling 73
    - IP address 67
    - ordering subgroups 67
    - server and system settings 66
    - tag-based criteria 67
  - System Tree synchronization
    - scheduling 77
    - to Active Directory structure 74
  - system-based policies
    - about 141
    - criteria 141

  - systems 348
    - assigning policies to 154
    - exporting from the Systems Tree 71
    - pasting policy assignments to 156
    - policy enforcement for a product 143
    - sorting into groups 74
    - viewing detailed information 68
    - viewing policy assignment 158

  T
  - table row, select checkboxes 22
  - tables, working with 21
  - Tag Builder wizard 83
  - Tag Catalog 83
  - tag-based sorting criteria 63, 67
  - tags 348
    - applying 87, 88
    - create, delete, and change subgroups 84
    - creating with Tag Builder wizard 83
    - criteria-based 65
    - criteria-based sorting 72
    - edit, delete, and move 83
    - excluding systems from automatic tagging 85
    - group sorting criteria 63
    - manual application of 86
    - policy assignment based on 141
  - tags, subgroups
    - create, delete, and change 84
    - selecting multiple items 23
  - tasks 348
    - automatically pull and copy DAT updates from McAfee 113
    - copying files from Evaluation branch into Current 114
    - find inactive agents 214
    - Inactive Agents task 215
    - periodic 295
    - pull content automatically 210
    - purge events 294
    - purge events automatically 208
    - purge events with a query 209
    - recommended daily 289
    - recommended monthly 294
    - recommended weekly 292
    - running compliance queries 218
    - scheduling on-demand scan of test group 117
    - to run and deliver a report 220
  - Test Sort action 65
  - Threat Event Log
    - common event format 299
    - viewing and purging 300
  - ticketing server 14
  - Ticketing with McAfee ePO 354
  - tools, third party
    - Windows Performance Monitor 284
tools, third-party
  use Windows Explorer to check ePolicy Orchestrator events 285
troubleshooting
  client certificate authentication 99
  finding inactive systems 214
  product deployment 166
  SQL database connectivity 287
  VPN system connection problem 335

U
UBP, See user-based policies
UNC share repositories 229
  creating and configuring 245
  editing 248
  enabling folder sharing 248
  using
    recommendations 249
Universal Naming Convention, See UNC share repositories
unmanaged repositories 228
updates
  calculating required bandwidth 302
  checking in manually 109
  client tasks 171
  considerations for creating tasks 171
  DAT files and products automatically 209
  deployment packages 168
  package signing and security 166
  packages and dependencies 166
  scheduling an update task 172
  source sites and 224
updating
  automatically, with global updating 128
  DATs and Engine 168
  deployment tasks 166
  global, process 127
  process description 168
user accounts 89
user actions
  removing outdated 95
user actions (continued)
  viewing 95
user menu, navigating in the interface 18
user-based policies 347
  about 141
  criteria 141
users
  about 89
  permission sets and 100
  restricting to a single IP address 93
utilities
  NETDOM.EXE, creating a text file 71

V
viewing issue details 353
virtual machines
  used for automatic DAT file testing 115
VirusScan Enterprise
  on-demand scan as part of suggested weekly tasks 292
VPN
  server OUI 337
  system connection problem 335, 336
  VPN connections and geographical borders 62

W
WAN connections and geographical borders 62
Windows
  authentication, configuring 89, 92
  Authorization, configuring 93
Windows authentication
  enabling 91
  strategies 91
Windows Reliability and Performance Monitor 283, 285
Windows Task Manager 283