Contents

1 Product overview ................................................................. 13
   Overview ........................................................................... 13
   Key features ...................................................................... 13
   How it works ...................................................................... 14

2 Using the ePolicy Orchestrator interface ..................................... 17
   Log on and log off .............................................................. 17
   Navigating the interface ....................................................... 17
      Using the McAfee ePO navigation menu ......................... 17
      Customizing the shortcut bar ......................................... 18
      Personal settings categories .......................................... 18
      Server settings .................................................................. 18
   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
      Create a query group ....................................................... 39
      Run a query on a schedule ............................................. 39
   About reports ..................................................................... 40
   Report anonymization permissions .................................... 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
Enable Windows authentication in the McAfee ePO server ........................................... 90
Configure advanced Windows authentication ................................................................. 90
Windows authentication and authorization strategies ...................................................... 91
Locking out user accounts to protect your server ......................................................... 92
Restricting or allowing IP addresses to protect your server ........................................ 92
Managing password policy ......................................................................................... 93
Disable user account ................................................................................................. 93
Reset administrator password .................................................................................. 94
Create a custom logon message .................................................................................. 94
Restrict a user session to a single IP address ............................................................. 94
The Audit Log .............................................................................................................. 95
View user actions ....................................................................................................... 95
Remove outdated actions from the Audit Log ........................................................... 95
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 ........................................................................................................ 99
How users, groups, and permission sets fit together ................................................. 99
Add or edit permission set ......................................................................................... 101
Import or export permission set ................................................................................ 102
8 Software Catalog ...................................................................................................... 103
What's in the Software Catalog ................................................................................ 103
Check in, update, and remove software using the Software Catalog ....................... 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
   ePO Server Health ........................................ 131
   Manual server health checks ................................ 133
   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
   About policies .............................................. 137
   When policies are applied and enforced .................... 138
   How policies are assigned to systems ....................... 139
   Policy ownership .......................................... 139
   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 new policy ........................................ 142
   Enforcing product policies ................................. 142
   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 ........................ 144
   Compare policies ............................................ 145
   Change the owners of a policy .............................. 145
   Move and share policies between McAfee ePO servers .... 145
   Register servers for policy sharing ........................ 146
   Designate policies for sharing ............................. 146
   Schedule server tasks to share policies .................... 146
   Create and manage policy assignment rules ................. 147
   Create policy assignment rules ............................ 147
   Manage policy assignment rules ............................ 147
   Policy management users ................................... 148
   Create policy management permission sets .................. 149
   Create policy management users ............................ 150
   Configure approval settings for Policy Changes .......... 150
   Configure email notifications using Automatic Response .. 151
   Submit policy changes for review .......................... 151
   Cancel policy review ....................................... 151
   Review policy changes ...................................... 152
   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 ........................ 154
   Copy policy assignments from a group ...................... 155
   Copy policy assignments from a system ..................... 155
   Paste policy assignments to a group ....................... 155
   Paste policy assignments to a specific system ............. 155
View policy information ................................ 156
View groups and systems where a policy is assigned .................. 156
View policy settings ............................................. 156
View policy ownership ............................................. 157
View assignments where policy enforcement is disabled ................ 157
View policies assigned to a group .................................. 157
View policies assigned to a specific system ........................ 158
View policy inheritance for a group ................................ 158
View and reset broken inheritance .................................. 158
Create policy management queries ................................ 158

13 Server and client tasks ........................................ 161
Server tasks .................................................................. 161
View server tasks ....................................................... 161
Server task status ....................................................... 161
Create a server task .................................................... 161
Remove outdated server tasks from the Server Task Log: best practice ........... 162
Remove outdated log items automatically ................................ 163
Accepted Cron syntax when scheduling a server task .................... 163
Client tasks .................................................................. 164
How the Client Task Catalog works ................................ 165
Deployment tasks ....................................................... 166
Client task approvals ................................................... 168
Deploy products to managed systems .................................. 173
Updating tasks ......................................................... 175
Manage client tasks .................................................... 178

14 Setting up automatic responses .................................. 181
Using Automatic Responses ........................................... 182
Event thresholds ......................................................... 182
Default automatic response rules ..................................... 183
Response planning ...................................................... 183
Determine how events are forwarded .................................. 184
Determine which events are forwarded immediately ................. 184
Determine which events are forwarded to the server ................. 184
Configure Automatic Responses ...................................... 185
Assign permissions to notifications .................................... 185
Assign permissions to Automatic Responses ......................... 186
Manage SNMP servers ................................................. 187
Choose a notification interval .......................................... 188
Create and edit Automatic Response rule ............................... 189
Define a rule .............................................................. 189
Set filters for the rule .................................................. 189
Set Aggregation and grouping criteria for the rule .................. 189
Configure the actions for an automatic response rule ............... 190

15 Manage registered executables and external commands 205

16 Agent-server communication .................................... 207
How agent-server communication works ................................ 207
Estimating and adjusting the ASCI .................................... 207
Estimating the best ASCI: best practice ............................... 208
Configure the ASCI setting: best practice ............................... 208
Managing agent-server communication ................................ 209
Allow agent deployment credentials to be cached .................... 209
Change agent communication ports .................................... 209
17 Automating and optimizing McAfee ePO workflow ........................................... 211
  Best practice: Find systems with the same GUID ........................................... 211
  Best practices: Purging events automatically .............................................. 212
    Create a purge events server task best practice ........................................ 212
    Purge events by query ................................................................................. 213
  Best practice: Creating an automatic content pull and replication .................. 213
    Pull content automatically: best practice .................................................... 214
  Best practices: Filtering 1051 and 1059 events ............................................ 214
    Best practice: Filter 1051 and 1059 events ................................................ 215
  Best practice: Finding systems that need a new agent .................................... 215
    Create an Agent Version Summary query best practice ................................ 216
    Update the McAfee Agents with a product deployment project best practice .... 216
  Finding inactive systems: best practice ......................................................... 217
    Change the Inactive Agents query: best practice ....................................... 218
    Delete inactive systems: best practice ....................................................... 218
  Measuring malware events best practice ....................................................... 219
    Create a query that counts systems cleaned per week best practice .............. 219
  Finding malware events per subnet: best practice ......................................... 220
    Create a query to find malware events per subnet best practice ................... 220
  Create an automatic compliance query and report best practice ....................... 221
    Create a server task to run compliance queries best practice ....................... 221
    Create a report to include query output best practice .................................. 223
    Create a server task to run and deliver a report: best practice ..................... 223

18 Repositories ........................................................................................................ 225
  What repositories do ........................................................................................... 225
  Repository types and what they do ...................................................................... 226
  Repository branches and their purposes ........................................................... 228
  Using repositories .............................................................................................. 230
    Distributed repository types .......................................................................... 230
    Repository list files ......................................................................................... 234
    Best practice: Where to place repositories ................................................... 235
    Best practice: Global Updating restrictions ................................................... 235
  Setting up repositories for the first time ......................................................... 236
  Manage source and fallback sites best practice .............................................. 236
    Create source sites ......................................................................................... 236
    Switch source and fallback sites best practice .............................................. 237
    Edit source and fallback sites best practice ................................................ 238
    Delete source sites or disabling fallback sites best practice ......................... 238
  Verify access to the source site best practice .................................................. 238
    Configure proxy settings ................................................................................ 239
    Configure proxy settings for the McAfee Agent .......................................... 239
  Configure settings for global updates best practice ........................................ 240
  Configure agent policies to use a distributed repository best practice ............... 240
  Use SuperAgents as distributed repositories ................................................... 241
    Create SuperAgent distributed repositories ................................................. 241
    Replicate packages to SuperAgent repositories ............................................ 242
    Delete SuperAgent distributed repositories ................................................ 242
  Create and configure repositories on FTP or HTTP servers and UNC shares ....... 243
    Create a folder location .................................................................................. 243
    Add the distributed repository to McAfee ePO .............................................. 243
    Avoid replication of selected packages ........................................................ 245
    Disable replication of selected packages ....................................................... 245
    Enable folder sharing for UNC and HTTP repositories .................................. 246
    Edit distributed repositories .......................................................................... 246
    Delete distributed repositories ....................................................................... 246
Using UNC shares as distributed repositories ........................................ 246
Use local distributed repositories that are not managed ............................ 247
Work with the repository list files .................................................. 248
  Export the repository list SiteList.xml file .................................... 249
  Export the repository list for backup or use by other servers .............. 249
  Import distributed repositories from the repository list .................... 250
  Import source sites from the SiteMgr.xml file ............................... 250
Change credentials on multiple distributed repositories .......................... 250
Pulling tasks ............................................................................ 251
Replication tasks ....................................................................... 251
Repository selection .................................................................... 252

19  Agent Handlers ....................................................................... 253
How Agent Handlers work ............................................................ 253
Agent Handler details .................................................................. 254
  Best practice: Agent Handlers eliminate multiple McAfee ePO servers 257
Agent Handler functionality .......................................................... 257
  Providing scalability .................................................................. 257
  Failover protection with Agent Handlers best practice .................... 258
  Network topology and deployment considerations........................ 259
Best Practices: Agent Handler installation and configuration ..................... 261
  Deployment considerations ..................................................... 262
  Agent Handler configuration overview ..................................... 263
  Configure Agent Handlers list .................................................. 263
  Configure Agent Handlers groups and virtual groups .................... 263
  Configure Agent Handlers priority ......................................... 264
  Configure assignments for Agent Handlers ............................... 264
Best Practices: Adding an Agent Handler in the DMZ ......................... 265
  Configure hardware, operating system, and ports ....................... 265
  Install software and configure the Agent Handler ..................... 266
Connect an Agent Handler in the DMZ to a McAfee ePO server in a domain 268
Handler groups and priority .......................................................... 268
Assign McAfee agents to Agent Handlers ........................................ 269
Manage Agent Handler assignments ............................................... 270
Create Agent Handler groups ....................................................... 270
Manage Agent Handler groups ..................................................... 271
Move agents between handlers ...................................................... 271
  Group agents using Agent Handler assignments ....................... 272
  Group agents by assignment priority .................................... 272
  Group agents using the System Tree ...................................... 273
Frequently asked questions ............................................................... 273

20  Maintaining your McAfee ePO server and SQL databases ................. 275
Maintaining your McAfee ePO server ............................................... 275
  Best practices: Monitoring server performance .......................... 275
  Maintaining your SQL database .............................................. 278
  Best practices: Recommended tasks ........................................ 280
Managing SQL databases .............................................................. 287
  Best practice: Maintaining SQL databases ............................... 288
  Configure a Snapshot and restore the SQL database ....................... 288
  Use Microsoft SQL Server Management Studio to find McAfee ePO server information 289
  Common event format ............................................................ 290
Use a remote command to determine the Microsoft SQL database server and name 292

21  Reporting with queries .............................................................. 293
Reporting features ..................................................................... 293
1 Product overview

Contents
▶ Overview
▶ Key features
▶ How it works

Overview

The McAfee® ePolicy Orchestrator® (McAfee® ePO®) platform enables centralized policy management and enforcement for your endpoints and enterprise security products.

McAfee ePO monitors and manages your network, detecting threats and protecting endpoints against these threats.

By using McAfee ePO, you can perform many network and client tasks from a single console.
• Manage and enforce network and system security using policy assignments and client tasks.
• Monitor the health of your network.
• Collect data on events and alerts.
• Create reports using the query system builder, which displays configurable charts and tables of your network security data.
• Automate product deployments, patch installations, and security updates.

Key features

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, and schedule tasks.
• 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 information technology operations systems quickly remediate outstanding issues.

Large-scale deployments

• Architecture supports hundreds of thousands of devices on a single server, and complex and diverse environments.

• McAfee ePO supports 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 it works

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

What happens during an attack

 McAfee ePO components and processes 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 a Number of Threat Events dashboard and saves the history of the attack in the Threat Event Log.
McAfee ePO components

The architecture helps you successfully manage and protect your environment, regardless of size.

1 **McAfee ePO server**
   - 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 the security of your endpoint.

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 communication to the server for policy enforcement, product deployment and updates, and 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** — Hosts 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** — Provides various connections to resources stored on Distributed Repositories in your network. For example, HTTP, FTP, or UDP connections.

13 **Agent Handler in DMZ** — Supports specific port connections to Agent Handlers installed in the DMZ allowing you to connect through a firewall.
Using the ePolicy Orchestrator interface

Contents
- Log on and log off
- 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.

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.

A notification (bell) icon appears in the title bar, next to the user menu. Click the icon to view all notifications. Select a notification to navigate to the corresponding page.

A-colored dot appears over the icon to indicate the level of importance.
  • High—Red
  • Medium—Yellow
  • Low—Blue

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</td>
<td>Determines whether a warning message appears when you try to drag a query</td>
</tr>
<tr>
<td>Warning</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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>
</tbody>
</table>
| Agent Contact Method     | Specifies the priority of methods that McAfee ePO uses when it attempts to contact a McAfee Agent.  
To change the priority, select Agent Contact Method under Setting Categories, click Edit, then select the priority. Each contact method must have a different priority level. The methods to contact a McAfee Agent are:  
- Fully Qualified Domain Name  
- NetBIOS name  
- IP Address |
| Agent Deployment Credentials | Specifies whether users are allowed to cache agent deployment credentials. |
| Approvals                 | Allows you to choose whether or not, a user needs approvals to make policy changes and client task changes. |
| Certificate Based Authentication | Specifies whether Certificate Based Authentication is enabled, and the settings and configurations required for the Certificate Authority (CA) certificate being used. |
| Dashboards                | Specifies the default active dashboard that is assigned to new users’ accounts at the time of account creation, and the default refresh rate (5 minutes) for dashboard monitors. |
| Disaster Recovery         | Enables and sets the keystore encryption passphrase for Disaster Recovery. |
| Email Server              | Specifies the email server that McAfee ePO uses to send email messages. |
| Event Filtering           | Specifies which events the agent forwards. |
| Event Notifications       | Specifies how often McAfee ePO checks your notifications to see if any trigger Automatic Responses. |
| Global Updating           | Specifies whether and how global updating is enabled. |
| License Key               | Specifies the license key used to register this McAfee ePO software. |
| Logon Message             | Specifies whether a custom message is displayed when users log on to the McAfee ePO console, and the message content. |
| Policy and Task Retention | Specifies whether the policies and client task data is removed when you delete the product extension. |
| Ports                     | Specifies the ports used by the server when it communicates with agents and the database. |
| Printing and Exporting    | Specifies how information is exported to other formats, and the template for PDF exports. It also specifies the default location where the exported files are stored. |
| Product Compatibility List | Specifies whether the Product Compatibility List is automatically downloaded and whether it displays any incompatible product extensions. |
| Product Improvement Program | Specifies whether McAfee ePO can collect data proactively and periodically from the managed client systems. |
| Proxy Settings            | Specifies the type of proxy settings configured for your McAfee ePO server. |
| Scheduler Tasks           | Specifies the number of server tasks that run at the same time. |
| Security Keys             | Specifies and manages the agent-server secure communication keys and repository keys. |
### Table 2-1 Default server settings (continued)

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Catalog.</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>
<tr>
<td>Virtual MAC Vendors</td>
<td>Allows you to add virtual MAC vendor. You can also edit and delete existing vendors. For details, See Add Virtual MAC Vendor.</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.

### Add Virtual MAC Vendor

This feature allows you to add the duplicated MAC address to the McAfee ePO database and prevent it from matching the used MAC address to another system. Virtual machines are assigned a unique MAC (Media Access Control) address in a particular host system.

**Task**

1. Click Menu | Configuration | Server Settings.
2. In the Server Settings page, click Virtual MAC Vendors in the Setting Categories pane.
   - You see a list of vendors and their respective ID.
3. Click Edit.
4  In the **Add New Virtual MAC Vendor** area, enter a value in the **Vendor ID** field.
   The Vendor ID must consist of six characters. It can be numeric (0–9), alphabetical (A to Z), or alphanumeric (combination of numbers and alphabets). A Vendor ID cannot have special characters.

5  Enter the details in the **Vendor Name/Note** field.
   You can enter details such as the name of the organization, the reason to add the vendor, and you can also enter comments that you would like to add. This field does not accept these special characters:
   - { 
   - } 
   - > 
   - ?

6  Click **Add MAC Vendor** to add more vendors.

7  Click **Save**.
   The vendor name and ID are added to the list of vendors.

---

**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.

**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.
To select... | Action | Response
--- | --- | ---
Individual rows | Click checkbox for individual rows. | Selects each individual row independently.
Group of rows | Click one checkbox, then hold **Shift** while you click the last checkbox in the group. | Selects all rows between and including the first and last rows that you clicked.

---

**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>Available Columns</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>Selected Columns</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 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 McAfee ePO, can’t 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>
</table>
| Create a dashboard | To create a different view on your environment, create a new dashboard.  
  1. Click **Dashboard Actions | New**.  
  2. Type a name, select a dashboard visibility option, and click **OK**.  
  A new blank dashboard is displayed. You can add monitors to the new dashboard as needed. |
| Edit and assign permissions to a dashboard | 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.  
  1. Click **Dashboard Actions | Edit**.  
  2. Select a permission:  
    • **Private** — Do not share this dashboard  
    • **Public** — Share this dashboard with everyone  
    • **Shared** — Share this dashboard with the following permission sets  
      With this option, you must also choose one or more permission sets.  
  3. Click **OK** to change the dashboard.  
  It is possible to create a dashboard with more expansive permissions than one with 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 receive a message saying they do not have permission to use 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. |
### 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. McAfee ePO 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 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 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.
### 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.
   a. Select Menu | Configuration | Server Settings.
   b. From the Setting Categories list, select Dashboards.
   c. 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.

   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>
<tbody>
<tr>
<td>Add a monitor</td>
<td>1. Click <strong>Add Monitor</strong>. The Monitor Gallery appears at the top of the screen.&lt;br&gt;2. Select a monitor category from the View drop-down list.&lt;br&gt;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.&lt;br&gt;4. Configure the monitor as needed (each monitor has its own set of configuration options), then click <strong>OK</strong>.&lt;br&gt;5. After you have added monitors to this dashboard, click <strong>Save Changes</strong> to save the newly configured dashboard.&lt;br&gt;6. When you have completed your changes, click <strong>Close</strong>. 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.</td>
</tr>
<tr>
<td>Edit a monitor</td>
<td>Every monitor type supports different configuration options. For example, a query monitor allows the query, database, and refresh interval to be changed.&lt;br&gt;1. Choose a monitor to manage, click the arrow in its top-left corner, and select <strong>Edit Monitor</strong>. The monitor’s configuration dialog appears.&lt;br&gt;2. When you have completed modifying the monitor’s settings, click <strong>OK</strong>. If you decide to not make changes, click <strong>Cancel</strong>.&lt;br&gt;3. If you decide to save the resulting changes to the dashboard, click <strong>Save</strong>, otherwise click <strong>Discard</strong>.</td>
</tr>
<tr>
<td>Remove a monitor</td>
<td>1. Choose a monitor to remove, select the arrow in its top-left corner, and select <strong>Remove Monitor</strong>. The monitor’s configuration dialog appears.&lt;br&gt;2. When you are finished modifying the dashboard, click <strong>Save Changes</strong>. To revert the dashboard to its prior state, click <strong>Discard Changes</strong>.</td>
</tr>
</tbody>
</table>
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
Generating queries and reports

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 McAfee ePO 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 in 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
- Report anonymization permissions
- 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 various 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 allow 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 several charts and tables to display the data it retrieves. These charts and their drill-down tables are highly configurable.

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

Contents

- Manage custom queries
- Create a query group
- Run a query on a schedule

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. |
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 and controlling access. The list of groups you see in the McAfee ePO 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**.

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.

### 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.

### Report anonymization permissions

You can restrict or allow users to access anonymized data in the reports for Content Security Reporting by setting appropriate permissions.

Restrict access to sensitive data by masking the field with a numeric value. However, you can share the key file that contains the actual values of the masked data by setting permissions for the users.

Permission sets provide you with two options including:

- No Permissions
- Allow Anonymized Key file download

### 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:

- 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.
4. Click OK.
5. You can add, remove, rearrange elements, customize the header and footer, and change the page layout.
6. In the Runtime Parameters window, select the fields that you want to anonymize and set conditions applicable to the respective fields from the drop-down list.

> Report anonymization feature is applicable only for Content Security Reporting. This option is not available by default to all users.

7. Click Run to generate the report.
8. 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.

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.

4. 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.

5. 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**

1. Select **Menu** | **Reporting** | **Queries**. Select the **Report** tab.

2. Select a report and click **Actions** | **Edit**, then perform the required actions.
### Action

**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**.
   
   - If you want the logo to be text, select **Text** and enter the text in the edit box.
   - To upload a new logo, select **Image** then browse to and select the image on your computer and click **OK**.
   - To use a previously uploaded logo, select it.
   - Click **Save**.

4. Change the header and footer fields to match the wanted data, then click **OK**.

### 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.

### 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**.
**Task**

1. Open the Server Tasks page and click **New Task**.
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**, then click **Next**.
4. Select the report to run and the target language.
5. Optional and available only for Content Security Reporting: Select **Anonymize** to mask any sensitive information such as the IP address and User Name.
6. Optional and available only for Content Security Reporting: From the **Sub-Actions** drop-down list, select one of these:
   - **Email File** — only the report is sent to the email recipient.
   - **Export file and key (for anonymized reports)** — the report and the key file are saved to the specified location.
   - **Export to File** — only the report is saved to the specified location.
   - **Send email with file and key (for anonymized reports)** — the report and the key file are sent to the email recipient.
   
   The report is saved with the given name and the key file is saved with the report name followed by a numeric value.

   For example: if the name of the report is **Samplereport**, the key file is saved as **Samplereport1**. You can overwrite an existing report or increment it by selecting from the drop-down list. If you select **Increment**, the next report generated will be saved as **Samplereport2** and the key file will be saved as **Samplereport3**.
7. 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**.
8. 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.

- When 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.

If the report contains anonymized data, you see two entries. One to download the report and the other link allows you to download the key file that contains the mapped values to the masked fields. However, you need to have the correct set of permissions to be able to download the key file.

A PDF opens in your browser, and your browser behaves based on how you 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
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 and reinstall your McAfee ePO software.

To recover your McAfee ePO environment, you must have a backup of the data that is unique to your environment and a mechanism for restoring McAfee ePO using this backup. The data that makes your McAfee ePO environment unique consists of two things: the McAfee ePO database, and sections of the McAfee ePO server file system. For example, the extensions that you checked in and the configuration files that control McAfee ePO.

A McAfee ePO database backup containing a valid Disaster Recovery Snapshot allows you to restore:

- McAfee ePO to your current McAfee ePO server, which allows you to recover from. For example, a failed McAfee ePO software upgrade.
- McAfee ePO to new server hardware with the original server name and IP address. For example, in the case of catastrophic hardware failure.
- McAfee ePO server hardware with a new server name, which allows you to move your McAfee ePO server from one domain to another.

For security, the files stored in the Snapshot are encrypted using the Keystore Encryption Passphrase. Keep a record of this passphrase; you need it to decrypt the Disaster Recovery Snapshot records and McAfee can’t recover it.

**Important considerations**

For a successful disaster recovery, the database and the snapshot it contains must be in sync. For example, if you took a Disaster Recovery Snapshot a week ago, two days ago you checked in a new extension, and last night you backed up the McAfee ePO database without taking a new snapshot, the database and snapshot are not in sync and it is unlikely you will be able to successfully restore from that database. The Server Snapshot dashboard monitor can be used to tell you if your snapshot is up to date.

To prepare for disaster recovery, save the files to the Snapshot in the database, and then perform a full backup of the McAfee ePO database.

### Working with Snapshots

**Contents**

- Working with Snapshots
- Install McAfee ePO software on a restore server
- Change the server recovery passphrase

## Using Disaster Recovery Snapshots to restore your server

**Contents**

- Using Disaster Recovery Snapshots to restore your server
- How the Server Snapshot dashboard monitor works
- Save a snapshot from the McAfee ePO Dashboard
Save a snapshot using Web API commands

Using Disaster Recovery Snapshots to restore your server

The Disaster Recovery Snapshot Server task allows you to save your files in an encrypted format and save the Snapshot to the database.

Disaster Recovery Snapshot contents

The files are saved in an encrypted format in the database when the Disaster Recovery Snapshot Server task runs.

The extensions are processed one at a time. Extensions can specify additional files to be stored in the snapshot: when each extension is processed, the snapshot task asks each extension what other files are required, and if any are defined it stores them in the snapshot.

- Core McAfee ePO configuration files
  - <ePO Install path>\Server\Keystore\</ePO Install path>\Server\confl

- Installed extensions
  - <ePO Install path>\Server\extensions\installed\</ePO Install path>\Server\extensions\installed\n
The Disaster Recovery Snapshot records include the paths configured for your registered executables. The registered executable files are not stored in the Snapshot, and you must replace the executable files when you restore your McAfee ePO environment. After you restore the McAfee ePO environment, any registered executables with broken paths appear in 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 in red, but still fail because of dependency issues related to the registered executables.

Disaster Recovery Snapshot Server task

Use the Disaster Recovery Snapshot Server task to save the Snapshot to the database. The Snapshot is created when you install McAfee ePO. The task can be scheduled to run at a specific time, by default it’s configured to run every day at 2 a.m. You can also run the task manually from the McAfee ePO dashboard and the WebAPI interface.

When McAfee ePO is installed, the Disaster Recovery Snapshot Server task is enabled by default if the database is hosted on a full version of SQL Server. It’s disabled by default if the database is hosted on an SQL Express instance, due to the hard-coded database size limit enforced by SQL Express.

McAfee ePO only saves one Snapshot to the database at a time: each time the task runs, the current Snapshot information is removed, and the new Snapshot information takes its place.

How the Server Snapshot dashboard monitor works

The Server Snapshot monitor, found on your McAfee ePO dashboard, allows you to manage and monitor your Disaster Recovery Snapshot.

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

The Server Snapshot monitor allows you to:

- Manually start the Snapshot task by clicking Take Snapshot.
- View the Server Task Log entry for the last Snapshot task by clicking See details of last run. This page displays information and log messages about the most recent Snapshot saved.
- View the date and time the last Snapshot task ran.

The color and title of the Snapshot monitor tells you the status of your latest Snapshot.
• **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 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 change; for example, updated, removed, deleted, upgraded, or downgraded.
  - The Keystore folder changed.
  - The conf folder changed.
  - The Disaster Recovery passphrase changed in Server Settings.

**Save a snapshot from the McAfee ePO Dashboard**

Use the McAfee ePO 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**, then select **ePO Server Snapshot**.

2. Click **Take Snapshot** to start saving the Snapshot to the database.

   During the Snapshot process, the **Snapshot Monitor** title bar changes to indicate the status of the process. The time it takes for the Snapshot process to complete depends on several factors; for example, if the product extensions are checked in and the performance of the SQL Server.

3. (Optional) After the Snapshot process is finished, click **See details of current run** to open the **Server Task Log Details**.

**Save a snapshot using Web API commands**

Use Web API commands to save a snapshot for Disaster Recovery purposes.

**Before you begin**

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

These are the variables in the remote command:

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

Review the following before you begin this task:

- You are prompted for the administrator user name and password before the output appears.

- The default name for the Snapshot task is **Disaster Recovery Snapshot Server**.

- These commands are case sensitive; make sure to review them carefully for proper capitalization and syntax.

The Web API can also be scripted used Python. For detailed Web API use and examples, see the **McAfee ePolicy Orchestrator Web API Scripting Guide**.
**Task**

1. The task ID is required to run the Snapshot server task; use this command if you don't know the task ID:

   https://<server_name>[:<port>]/remote/scheduler.listAllServerTasks?output=terse

   Find the ID next to the Disaster Recovery Snapshot Server task. For example, ID: 2:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Disaster Recovery Snapshot Server</td>
<td>None</td>
</tr>
</tbody>
</table>

2. Run the Snapshot server task using the following command:

   https://<server_name>[:<port>]/remote/scheduler.runServerTask?taskId=2

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

   OK

   102

3. (Optional) 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://<server_name>[:<port>]/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:

      - 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 the task ID number 102 to display all task log messages:

      https://<server_name>[:<port>]/remote/tasklog.listMessages?taskLogId=102

---

**Install McAfee ePO software on a restore server**

You can restore the McAfee ePO software as a recovery installation where your Microsoft SQL Server already includes a McAfee ePO configuration from a previous installation.

To re-create the McAfee ePO server, reinstall the McAfee ePO software on a server and link it to the restored SQL database.

💡 Monitor the process because you might need to restart your system.
**Task**

1. When you select the existing SQL Server, gather this information and complete these steps before beginning your installation. These steps ensure that your McAfee ePO software can communicate with the database server:
   - Verify that the SQL Browser Service is running.
   - Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
   - Update the system that hosts your McAfee ePO server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.
   - Confirm the SQL backup file that you copied from the primary server was restored using the Microsoft SQL process.
   - Stop Agent Handler services on all systems, before restoring the McAfee ePO software.

2. If you have Agent Handlers configured, log on to the systems where the Agent Handlers are installed, then open the Windows Services panel. Stop the **McAfee Event Parser** and **McAfee Apache** services.

   See your Microsoft software product documentation for more information about using the Windows Services panel.

3. Using an account with local administrator permissions, log on to the Windows Server computer used as the restore McAfee ePO server.

4. Downloaded from the McAfee website, extract the files to a temporary location, right-click **Setup.exe**, and select **Run as Administrator**.

   The version you download must match the version being restored. If you try to run **Setup.exe** without first extracting the contents of the .zip file, the installation fails.

   The McAfee ePolicy Orchestrator - InstallShield Wizard starts.

5. Click **Restore ePO from an existing database snapshot** and **Next** to begin the restore installation process.

6. In the **Install additional software** step, any remaining prerequisites are listed. To install them, click **Next**.

7. In the **Destination Folder** step, click:
   - **Next** — Install your McAfee ePO software in the default location (C:\Program Files (x86)\McAfee\ePolicy Orchestrator).
   - **Change** — Specify a custom destination location for your McAfee ePO software. When the **Change Current Destination Folder** window opens, browse to the destination and create folders if needed. When finished, click **OK**.

8. In the **Database Information** step, select the Microsoft SQL Server name from the **Database Server** list. Specify which type of **Database Server Credentials** to use, then click **Next**.

   - **Windows authentication** — From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. Type the **User name** and **Password** of your restored SQL database.
   - **SQL authentication** — Type the **User name** and **Password** for your SQL Server. Make sure that credentials you provide represent an existing user on the SQL Server with appropriate rights.

   The **Domain** menu is grayed out when using SQL authentication.

   You might need to type the **SQL server TCP port** to use for communication between your McAfee ePO server and database server. The McAfee ePO installation tries to connect using the default ports, 1433 and 1434. If those ports fail, you are prompted to type an SQL Server TCP port.
9 In the HTTP Port Information step, review the default port assignments. Click Next to verify that the ports are not already in use on this system.

10 In the Administrator Information step, type the Username and Password you used for your previously existing server administrator account.

11 Type the Server recovery passphrase you saved during the initial installation of the previously existing McAfee ePO server, or changed in the Server Settings.

   The Server recovery passphrase decrypts the sensitive files stored in the Disaster Recovery Snapshot.

12 Accept the McAfee End User License Agreement and click OK.

13 From the Ready to install the Program dialog box, decide if you want to send anonymous usage information to McAfee, then click Install to begin installing the software.

14 When the installation is complete, click Finish to exit the InstallShield wizard.

15 If you restored McAfee ePO to a server with a different IP address or DNS name than your previously existing server, configure a way to allow your managed systems to connect to your new McAfee ePO server.

   Create a CNAME record in DNS that points requests from the old IP address, DNS name, or NetBIOS name of the previously existing McAfee ePO server to the new information for the restore McAfee ePO server.

16 If you stopped the Agent Handlers in step 1, log on to the systems where the Agent Handlers are installed, then open the Windows Services panel. Start the McAfee Event Parser and McAfee Apache services.

   Your McAfee ePO software is now restored. If needed, double-click the Launch ePolicy Orchestrator icon on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (https://<server_name>:<port>).

---

**Change the server recovery passphrase**

You can change the server recovery passphrase when you install McAfee ePO and link it to a SQL database restored with Disaster Recovery Snapshot records.

**Before you begin**

You must have administrator rights to change the server recovery passphrase.

Change the server recovery passphrase from the Server Settings page. You can also change the existing passphrase without knowing the previously configured passphrase. Once the passphrase is changed, the next Snapshot will be encrypted using the new passphrase, but the new passphrase is not applied to any Snapshot currently stored in the database.

   If you change the passphrase, we recommend that you run another Snapshot task as soon as possible, so that your database contains a snapshot encrypted with a known passphrase.

**Task**

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

2 From Server recovery passphrase, click Change passphrase, then type the new passphrase.
Using the System Tree and Tags

You can organize, group, and tag your managed systems using the System Tree and Tags features. The System Tree is a hierarchical structure that organizes the systems in your network into groups and subgroups.

Adding systems
You can add systems to your System Tree using these methods:
• Manually add systems to an existing group
• Import systems from a text file
• Active Directory synchronization

Organizing systems
You can organize your System Tree using these methods:
• Manual organization from the console (drag and drop)
• Automatic synchronization with your Active Directory or NT domain server
• Criteria-based sorting, using criteria applied to systems manually or automatically

What the System Tree controls
Your System Tree dictates these items:
• How your policies for different products are inherited
• How your client tasks are inherited
• Which groups your systems go into

If you are creating your System Tree for the first time, these are the primary options available for organizing your systems dynamically:
• Using Active Directory (AD) synchronization
• Dynamically sorting your systems

Although you can use AD synchronization with dynamic System Tree sorting, use only one method to avoid confusion and conflicts.

Contents
• Organizing systems with the System Tree
• Tags
Organizing systems with the System Tree

Contents
- Considerations when planning your System Tree
- System Tree groups
- Sorting your systems dynamically
- 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

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 parts 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**

Often, 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 win 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></td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</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></td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</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>

System Tree groups
System Tree groups represent a collection of systems. Deciding which systems to group depends on the unique needs of your network and business.
You can group systems based on any criteria that supports your needs:
Groups have these characteristics:

- Administrators or users can create and use them with the appropriate permissions.
- You can include both systems and other groups (subgroups).

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

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

The default System Tree structure includes these groups:

- **My Organization** — The root of your System Tree.
- **My Group** — The default subgroup added during the Getting Started initial software installation. This group name might have been changed during the initial software installation.
- **Lost and Found** — The catch-all subgroup for any systems that have not been or could not be added to other groups in your System Tree.

### My Organization group

The My Organization group, the root of your System Tree, contains all systems added to or detected on your network (manually or automatically).

Until you create your own structure, all systems are added by default to My Group. This group name might have been changed during the initial software installation.

The My Organization group has these characteristics:

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

### My Group subgroup

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

This group name might have been changed during the initial software installation.

When your network computers run the installation URL, they are grouped by default in My Group.

To rename the group, select **Menu | Systems | System Tree**, in the System Tree groups list click **My Group**, then click **System Tree Actions | Rename Group**.

### Lost and Found subgroup

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

Depending on the methods that you specify when creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost and Found group stores systems whose locations can't be determined.
The Lost and Found group has these characteristics:

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

If you delete systems from the System Tree, make sure that you select Remove McAfee Agent on next agent-server communication from all systems. If the McAfee Agent is not removed, deleted systems reappear in the Lost and Found group because the McAfee Agent still communicates with McAfee ePO.

**Group inheritance**

All child subgroups in the System Tree hierarchy inherit policies set at their parent groups. These inheritance rules simplify policy and task administration.

- Policies set at the My Organization level of the System Tree apply to all groups.
- Group policies apply to all subgroups or individual systems in that group.
- Inheritance is enabled by default for all groups and individual systems that you add to the System Tree. Default inheritance allows you to set policies and schedule client tasks in fewer places.
- To allow for customization, inheritance can be broken by applying a new policy at any location of the System Tree.
  
  You can lock policy assignments to preserve inheritance.

In this example, Windows users under the Server group for Los Angeles automatically inherit the Server group policies. Users under the Server group for San Francisco inherit a different set of policies.

<table>
<thead>
<tr>
<th>System Tree</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Organization</td>
<td>Top-level group</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>Child subgroup of My Organization</td>
</tr>
<tr>
<td></td>
<td>Desktop</td>
</tr>
<tr>
<td></td>
<td>Laptop</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>SQL</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
</tr>
<tr>
<td>San Francisco</td>
<td>Child subgroup of My Organization</td>
</tr>
<tr>
<td></td>
<td>Desktop</td>
</tr>
<tr>
<td></td>
<td>Laptop</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
<tr>
<td>Lost and Found</td>
<td>Child subgroup of My Organization</td>
</tr>
</tbody>
</table>
Sorting your systems dynamically

You can dynamically sort your systems into your McAfee ePO System Tree using a combination of system criteria and other elements.

Creating the basic groups

Sorting dynamically requires that you create some basic groups for your tree structure. For smaller organizations, your System Tree might not be complex and contain only a few groups. For larger organizations, we recommend that you create some groups similar to these sample designs:

• GEO — Geographic location
• NET — Network location
• BU — Business unit
• SBU — Subbusiness unit
• FUNC — Function of the system (web, SQL, app server)
• CHS — Chassis (server, workstation, laptop)

Selecting and ordering the basic groups

After you decide on the basic building blocks for groups in the System Tree, you must determine which building blocks to use and in which order based on these factors:

• Policy assignment — Do you have many custom product policies to assign to groups based on chassis or function? Do certain business units require their own custom product policy?
• Network topology — Do you have sensitive WANs in your organization that a content update might easily saturate? If you have only major locations, this is not a concern for your environment.
• Client task assignment — When you create a client task, such as an on-demand scan, do you need to do it at a group level, like a business unit, or system type, like a web server?
• Content distribution — Do you have an agent policy that specifies that certain groups must get their content from a specific repository?
• Operational controls — Do you need specific rights delegated to your McAfee ePO administrators that allow them to administer specific locations in the tree?
• Queries — Do you need many options when filtering your queries to return results from a specific group in the System Tree?

After you choose the basics for your tree structure, create a few sample System Tree models and look at the pros and cons of each design. There is no right way or wrong way to build your System Tree, just pluses and minuses depending on what you choose.

Here are a few of the most commonly used System Tree designs:

• GEO -> CHS -> FUNC
• NET -> CHS -> FUNC
• GEO -> BU -> FUNC

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 McAfee ePO. 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 McAfee ePO (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 McAfee ePO.
- 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 to not 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 McAfee ePO users from configuring sorting criteria on groups by mistake 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. 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. The server considers the sorting criteria of all top-level groups according to the sorting order on the **My Organization** group's **Group Details** tab. The system is placed in the first group with matching criteria or a catch-all group it considers.
   - Once sorted into a group, each of its subgroups is considered for matching criteria according to their sorting order on the **Group Details** tab.
   - Sorting continues until there is no subgroup with matching criteria for the system, and is placed in the last group found with matching criteria.

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

8. If such a second-level criteria-based group is not found, the criteria-based third-level groups of the second-level unrestricted groups are considered.

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

10. If the server cannot sort the system into any group, it is placed in the Lost 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>
</tbody>
</table>

   The status of the deployment task of the same version of the product or an older version of the same product is ignored.

   | Applied Policies | Displays the name of policies applied to this system and lists them alphabetically. |
   | Applied Client Tasks | Displays the name of client tasks assigned to this system and lists them alphabetically. |
   | Threat Events | Lists threat and other events, plus detailed information about those events, |
   | McAfee Agent | List configuration information about the McAfee Agent installed on the system. |

   Click More to display additional McAfee Agent configuration and status information.

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 needed 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 70
  Sorting criteria for System Tree groups can be based on IP address information or tags.

- Enable System Tree sorting on the server on page 71
  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 71
  The sorting status of a system determines whether it can be sorted into a criteria-based group.

- Sort systems manually on page 72
  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.
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.

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

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.
3 Next to **Synchronization type**, select Active Directory. The Active Directory synchronization options appear.
4 Select the type of Active Directory synchronization you want to occur between this group and the Active Directory container (and its subcontainers):
   - **Systems and container structure** — Select this option if you want this group to truly reflect the Active Directory structure. When synchronized, the System Tree structure under this group is 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.

1. Export your security keys from the old server.
2. Import the security keys in the new server.
3. Register the new McAfee ePO server to the old server.
4. Transfer your current systems to the new McAfee ePO server.
Confirm that you can view the systems in the new server’s System Tree.

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

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

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 77
  Export the 2048-bit and 1024-bit security keys.
- Import security keys to the new server on page 78
  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 79
  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 79
  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 80
  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

Contents
- Create tags
- Manage tags
- Create, delete, and change tag subgroups
- Exclude systems from automatic tagging
- Create a query to list systems based on tags
Create tags

Use tags to identify and sort systems. Create tags to run a task that is common for a particular domain, or systems with a specific configuration and assign a server task or client task to the systems with this tag to simplify the process.

Task
2. On the New Tag pane, enter a name.
3. Click + in the Criteria row or click Add below the Criteria row to open the Properties Catalog pane.
4. Click anywhere in the property row that you want to include.
5. Provide the specifications for the property on the New Tag pane to configure the criteria.
6. Expand Evaluation to 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.

These options are unavailable if criteria is 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.

7. Expand Restrictions and select Restrict usage to the below Permission Sets to restrict a tag to specific Permission Sets. Select the Permission Sets so that only those users belonging to these selected Permission Sets have access to this tag.

By default, Do not restrict by Permission Sets is selected.

After you save the tag, you can see this on the Restrictions (Permission Sets) column on the Tags pane.

8. Expand Usage to see the Policy Assignment rules, Client Task Assignments and Server Tasks that this tag is associated with.

9. 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 Group Tree pane on the Tag Catalog page.
Manage tags

Once tags are created, you can 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 the tag that you want to edit, then on the Tag Details pane, you can edit these settings:
      
      a. Select and configure the criteria.
      
      To apply the tag automatically, you must configure criteria for the tag.
      
      b. 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.
      
      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.
      
      c. Select **Restrict usage to the below Permission Sets** to restrict a tag to specific Permission Sets. Select the Permission Sets so that only those users belonging to these selected Permission Sets have access to this tag.
      
      d. Verify the information about this page, then click **Save**.
      
      This page displays the number of systems that receive this tag when evaluated against its criteria.

   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.

   ![Information icon]
   You are not limited to selecting one action for the query results. Click the + button to add additional actions. Be careful to place the actions in the order that you want them to occur. For example, you can apply the Server tag, then remove the Workstation tag. You can also add other subactions, such as assigning a policy to the systems.

8. Click Next.

9. Schedule the task, then click Next.

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

The task is added to the list on the Server Tasks page. If the task is enabled (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.

   ![Information icon]
   To limit the list to specific tags, type the tag name in the text box under Tags.

   ![Information icon]
   Only those tags to which you have permission are listed in the Apply Tag dialog box.
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. 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. Expand Systems on the Tag Details pane and select Apply tag now to systems that match the tag criteria.
   c. Click Save.

2. Select the tag or tag group from the Tags list.

3. Click Actions | Run Tag Criteria.
4  On the Run Tag Criteria window, 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.

5  Click OK.

The number of systems to which the tag is applied is displayed at the bottom of the page.

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

Contents

- User accounts
- Edit user accounts
- Creating McAfee ePO users with Active Directory
- Enable Windows authentication in the McAfee ePO server
- Configure advanced Windows authentication
- Windows authentication and authorization strategies
- Locking out user accounts to protect your server
- Restricting or allowing IP addresses to protect your server
- Managing password policy
- Disable user account
- Reset administrator password
- Create a custom logon message
- Restrict a user session to a single IP address
- The Audit Log
- Authenticating with certificates
- Permission sets

User accounts

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.

Authentication versus authorization

Authentication is the process of determining if a user is permitted to log on to McAfee ePO by verifying the user’s identity and matching the credentials supplied by the user to something the system trusts. For example, by providing the correct user name and password for an McAfee ePO user account, an Active Directory account, or a certificate.

Authorization is the process of determining what actions an authenticated user is permitted to perform in McAfee ePO. For example, adding new users or creating policies. Permissions and permission sets control what a user is authorized to perform in McAfee ePO.
Managing users

Before a user can access McAfee ePO, a user account must be created and assigned a permission set. McAfee ePO allows you to manually configure the user account. You can also configure McAfee ePO so that when a member of an Active Directory group tries to log on for the first time, a McAfee ePO account for that user is automatically created with a permission set assigned to it.

User Authentication Types

McAfee ePO supports three types of authentication.

- **ePO authentication** — The user name and password are stored in McAfee ePO and McAfee ePO authenticates the user.

- **Windows authentication** — The Windows domain and user name details are stored in McAfee ePO, and the user is authenticated by a Windows domain controller. By default McAfee ePO authenticates against the domain that the McAfee ePO server is a member of. Windows users who can't authenticate by the parent domain can enable the Windows Authentication feature and specify the details of the untrusted domains.

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

Edit user accounts

You can manage user access by adding, updating, or deleting user accounts on the User Management page.

**Task**


2. Select one of these actions.
   - Create user:
     1. Click New User, then type a user name.
     2. Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization, you might want to disable it.
     3. 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.

     Using McAfee ePO authentication allows the administrator to provide a one-time password. With a one-time password, the user is prompted to change the password when they log on the first time.

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

     5. Choose to make the user an administrator, or select the appropriate permission sets for the user.

   - Edit user:
     1. From the Users list, select the user you want to edit, then click Action | Edit, and the Edit User page appears.

     2. Edit the account as needed.

     3. Click Save.
Creating McAfee ePO users with Active Directory

McAfee ePO can simplify the process of managing users by automatically creating Windows authentication users based on their Active Directory group membership.

If Active Directory User Login is enabled when an unknown user tries to log on, McAfee ePO checks to see any permission sets mapped to Active Directory groups for which the user is a member. If there are, McAfee ePO creates a Windows authentication user and assigns the mapped permission sets to it.

To enable this feature, you must do the following:

• Active Directory User Login must be enabled
• At least one permission set must be mapped to the user’s Active Directory group
• A registered LDAP server must be configured for the domain, so that McAfee ePO can determine the user’s group membership

Active Directory User Login

You can enable the Active Directory User Login server setting from the Server Settings page, which allows user records to generate automatically 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.

Register an LDAP server

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.
Map a permission set to the Active Directory group
Assign at least one permission set to an Active Directory 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.

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

Consider these items when determining how permission sets are assigned:
• Permission sets can be assigned to multiple Active Directory groups.
• Permission sets can be dynamically assigned only to an entire Active Directory group. They can’t be assigned to just some users in a group.

If you want to assign special permissions to an individual user, create an Active Directory group that contains only that user.

Advanced Windows authentication
Users can authenticate with Windows credentials from the domain that the McAfee ePO server uses. They can also authenticate by using 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, enable and configure advanced Windows authentication.

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 McAfee ePO service.

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 advanced Windows authentication
There are many ways to use existing Windows account credentials in McAfee ePO.

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?

**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 tries 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.

---

**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 change if your overall network topology changes. Once servers are registered and Windows authentication is configured, you do not have to modify these settings often.

**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 in 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.

**Locking out user accounts to protect your server**

The option to **Lock Out User Accounts**, part of the **Logon Protection** feature, protects your McAfee ePO server by locking out user accounts after a specified number of failed attempts.

This feature is disabled by default and must be manually enabled by an administrator.

From **Server Settings**, you can enable the account lockout feature and edit these settings:

- Number of incorrect attempts before an account is locked
- Length of time until the lockout counter resets
- Length of time the account is locked

From **User Management | User**, you can reset your account before the specified wait period ends.

**Restricting or allowing IP addresses to protect your server**

The option to **Restrict IP Addresses**, part of the **Logon Protection** feature, protects your McAfee ePO server from invalid logon attempts by blocking source IP addresses or allowing only certain IP addresses. You can also monitor logon attempts and manage IP addresses, manually or automatically.

This feature is disabled by default and must be manually enabled by an administrator.

If McAfee ePO detects a malicious logon attempt from an IP address, that IP address is added to the IP Address Management table and blocked. Access to McAfee ePO is blocked until you unblock or delete the address from the table. The **Actions** option allows you to unblock an IP address by adding it, so logon from the address is allowed.

**Managing IP addresses**

You must enable automatic IP address restriction to manually add IP addresses.

From **Server Settings**, you can manage IP addresses in two ways:

- **Automatically** — When enabled, automatically blocks IP addresses after failed logon attempts (more than 10 tries within 60 seconds), and adds the address to the IP Address Management table.

- **Manually** — Allows you to add an IP address or range of addresses to the IP Address Management table. You can permanently block or allow access, regardless of logon attempts.

When adding a range of IP addresses, you might accidentally block your own IP address. If this occurs, access the McAfee ePO console directly from the hosted server and add or unblock the IP address so that it’s included in the **Allow List**. The server always has access because the localhost is never blocked.

**Monitoring logon attempts**

The Audit Log tracks the history of changes to or enforcement of any IP address. For example, you can see if an IP address is blocked, if logon attempts are made from a blocked IP address, and the start and completion time of an attempt.

From **Automatic Responses**, configure email notifications when the following occurs:
• Too many failed logons occur from an IP address.
• A blocked IP address attempts to log on.
• A system blocks an IP address.

Managing password policy

The Password Policy feature allows you to define the strength of a password. For example, an administrator can restrict the number of previously used passwords and limit the number of days before the password expires.

From Server Settings, you can define password criteria by editing these settings:

• Password Strength Criteria — Define the strength of a password and restrict the number of previously used passwords.
  • Minimum Password Length — configure the password length (7-30 characters).
  • Restrict usage of previously used passwords — configure the limit on password reuse (3-24 previous passwords).

When you enable password strength criteria, it automatically requires that passwords contain the following:

• One uppercase (A–Z)
• One lowercase (a–z)
• One numeric (0–9)
• One special character (#?!@$%^&*-)

The password requirements can't be customized. If an existing password doesn't match the criteria, you are prompted to change it during the next logon.

• Password Expiration Criteria — Enter the number of days before a password expires (30–365 days).

Disable user account

Disable a user account without permanently deleting it, retaining objects and policies that the user created. Use this feature when a user leaves an organization or if a user account is no longer in use.

This feature is only available to administrators.

If the user account is deleted, all policies and objects the user created are also deleted.

Task

1. Select Menu | User Management | Users, then select the user account you want to disable.
2. From the Actions menu, select Disable. You can also disable a user account from the Edit User page.
3. Click Save.

A user must re-enter their credentials to access the McAfee ePO console any time the IP address changes.
Reset administrator password

Reset the global administrator password if you have forgotten your credentials, or are locked out 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 ePO logon page opens.
2. Click **Restore Administrator Access**.
3. Under **Database credentials**, enter the current user name and password for the database.
4. Under **Administrator credentials**, enter the new password for the administrator account.
5. Click **Submit** to update the administrator account password.

After resetting the password, the global administrator user name is displayed in the confirmation message.

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.

Custom logon messages with HTML are now escaped by default to prevent Cross-site Scripting (XSS) issues. To include HTML markups and prevent formatting issues, go to the `<ePO_install_location>\Server\conf\orion` folder, open the `orion.properties` file, add `secure.login.custom.message=false`, and save the file and restart McAfee ePO services.

**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 McAfee ePO server 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.

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 in 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 McAfee ePO 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**.
Click **Save** to save all changes.

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:

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.
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.

**Add or edit permission set**

Control user access by creating and changing permission sets from the Permission Sets page. You can also copy and delete permission sets from the Permission Sets page.

**Task**

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

   • Add a permission set:
     1. Click New Permission Set.
     2. Type a unique name for the new permission set.
     3. To immediately assign specific users to this permission set, select their user names in the Users section.
     4. To map any Active Directory groups to this permission set, select the server from the Server Name list, then click Add.
     5. If you added any Active Directory servers that you want to remove, select them in the Active Directory list box, then click Remove.

   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.

   • Edit a permission set:
     1. Select a permission set to change.
     2. Type a unique name for the new permission set.
     3. To immediately assign specific users to this permission set, select their user names in the Users section.
     4. To map any Active Directory groups to this permission set, select the server from the Server Name list, then click Add.
     5. If you added any Active Directory servers that you want to remove, select them in the Active Directory list box, then click Remove.
Import or export permission set

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.

   - Export permission sets:
     1. Click Export All.

     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.

     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.

   - Import permission sets:
     1. Click Import.
     2. Click Browse to navigate to and select the XML file with the permission sets that you want to import.
     3. Choose whether to keep permission sets with the same name as an imported permission set by selecting the appropriate option. Click OK.

     If McAfee ePO cannot locate a valid permission set in the indicated file, an error message is displayed and the import process is stopped.

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

Contents

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

What's in the Software Catalog

The Software Catalog removes the need to access the McAfee Product Download website to retrieve new McAfee software and software updates.

You can use the Software Catalog to download:

- **Licensed software** — Software your organization has purchased from McAfee. The Status column provides a list of licensed software that is not currently installed on your server. The number displayed next to each category in the Status list indicates where updates are available. Select the number to view specific details about the updates. For example, the available version, checked in version, or component type.

- **Evaluation software** — 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** — Released software that has new updates. You can use the Software Catalog to check in new packages and extensions. Available software updates are listed in the Updates Available category.

- **Product documentation** — New and updated product documentation you can retrieve from the Software Catalog. Product Guides and Release Notes can also be downloaded from the Software Catalog.

DATs and Engines are not available from the Software Catalog.

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 Catalog interface

Use the Software Catalog to view and manipulate your new and existing software.
Check in, update, and remove software using the Software Catalog

From the Software Catalog, you can check in, update, and remove managed product components from your server. Both licensed and evaluation software can be accessed in the Software Catalog.

Software availability, and whether it is Licensed or Evaluation, depends on your license key. For more information, contact your administrator.

Task
1. Click Menu | Software | Software Catalog.
2. In the Software Catalog page Category 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.
   - **Evaluation** — Displays the Evaluation software installed or checked in to this server.
   - **Product categories** — Displays the licensed McAfee software installed or checked in to this server.
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.

Under **Check In**, review and accept the product details and End User License Agreement (EULA), select the Client Package Branch, then click **Check In** 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 Catalog
- 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.
Sometimes 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 Catalog 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 Catalog 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](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><code>setup.exe DISABLEPRODCOMPATUPDATE=1</code></td>
<td>Disables automatic downloading of the Product Compatibility List from the McAfee website.</td>
</tr>
<tr>
<td><code>setup.exe PRODCOMPATXML=&lt;full_filename_including_path&gt;</code></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

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.
   a. Select **Menu** | **Software** | **Master Repository**.
   b. Click **Check In Package**.

2. Select the package type, then browse to and select the package file.

3. Click **Next**.

4. Confirm or configure the following:
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the branch. If there are requirements in your environment to test new packages before deploying them throughout the production environment, 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 choose move the content manually from the Evaluation branch into the Current branch of the repository.

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.
5. Depending on the on-demand scan output, one of these scenarios occurs:
   - a. 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.
   - b. 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.

**DAT file validation overview**

![Figure 9-1 Automatic DAT file testing steps](image)

**Figure 9-1 Automatic DAT file testing steps**
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.

8 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.

1. Use the Software Catalog to automatically review and update McAfee software and software components.
2. 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.
3. The Product Deployment feature offers a simplified workflow and increased functionality to deploy products to your McAfee ePO managed systems.
4. Create client tasks to manually assign and schedule product deployments to groups or individual managed system.
5. 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. 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.

5. From the **Actions** list, select **Install** or **Uninstall**.

6. 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.

7. Under **Select the systems**, click **Select Individual Systems** or **Select by Tag or Group**.
   - **Select Individual Systems** — Results in a fixed deployment
   - **Select by Tag or Group** — Results in a continuous deployment

   The System Selection dialog box allows you to select systems 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.

   The **Total** field displays the number of systems, groups, or tags selected for the deployment.

8. To automatically update your products, select from these **Auto Update** options.
   - **Automatically deploy latest version of the products**
   - **Allow end users to postpone this deployment (Windows only)**
   - **Maximum number of postponements allowed**
   - **Option to postpone expires after**
   - **Display this text**

   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.
9 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.

10 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**
   - **Resume**
   - **Delete**
   - **Stop**
   - **Duplicate**
   - **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.

   Selecting a package type determines what initiates a global update (not what is updated during the global update process). Agents receive a list of updated packages during the global update process. The agents use this list to install only updates that are needed. For example, agents only update packages that have changed since the last update and not all packages if they have not changed.

5. When finished, click **Save**.
   
   Once enabled, global updating initiates an update the next time you check in any of the selected packages or move them to another branch.

   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>Package</td>
<td>Specifies which package to deploy or uninstall. To add or remove packages, click + and -.</td>
</tr>
<tr>
<td>Branch</td>
<td>Specifies which branch the package is stored in.</td>
</tr>
<tr>
<td></td>
<td>• Current — Used when you want the package available to managed systems in your production environment.</td>
</tr>
<tr>
<td></td>
<td>• Evaluation — 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>• Previous — 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>Language</td>
<td>Specifies which interface language to use for the deployment.</td>
</tr>
<tr>
<td></td>
<td>![Note](Neutral allows the multiple language package to query the operating system and install the correct language.)</td>
</tr>
<tr>
<td>Command line</td>
<td>Specifies command-line installation options.</td>
</tr>
<tr>
<td></td>
<td>![Note](See the product documentation for information about command-line options for the product you are installing.)</td>
</tr>
</tbody>
</table>

### Table 10-4 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the systems</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Click Select Systems, then select the systems to receive the new deployment using these tabs.</td>
</tr>
<tr>
<td></td>
<td>![Note](The type of deployment you select, fixed, or continuous, determines which tabs appear.)</td>
</tr>
<tr>
<td></td>
<td>• Systems Tree tab — (Fixed) Selects and displays systems. Used with continuous deployment, selects System Tree groups.</td>
</tr>
<tr>
<td></td>
<td>• Selected Systems tab — (Fixed) Selects individual or System Tree groups of systems.</td>
</tr>
<tr>
<td></td>
<td>• Queries tab — (Fixed) Select the output from preconfigured query output systems tables.</td>
</tr>
<tr>
<td></td>
<td>• Tags tab — (Continuous) Selects systems configured with specific tags.</td>
</tr>
<tr>
<td></td>
<td>Click Allow end users to postpone this deployment as needed.</td>
</tr>
<tr>
<td></td>
<td>Enter number for Maximum number of postponements allowed.</td>
</tr>
<tr>
<td></td>
<td>Enter number of seconds for Option to postpone expires after.</td>
</tr>
<tr>
<td></td>
<td>Select Display this text, 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>Select a start time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• Run Immediately — Starts the deployment immediately.</td>
</tr>
<tr>
<td></td>
<td>• Once — Starts the deployment using specified settings.</td>
</tr>
<tr>
<td></td>
<td>• Start date — Specifies the date to start this task.</td>
</tr>
<tr>
<td></td>
<td>• Start Time — Specifies the time to start this task.</td>
</tr>
<tr>
<td></td>
<td>• Coordinated Universal Time (UTC) — Specifies whether the task schedule runs according to the local time on the managed system or UTC.</td>
</tr>
<tr>
<td></td>
<td>• Enable randomization — Specifies that this task runs randomly in 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 70%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning — More than 70%</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</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>JVM CPU Check</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</td>
<td>Verifies the memory load of the ePO Application Server JVM.</td>
<td>Free memory is...</td>
</tr>
<tr>
<td>JVM Memory Check</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</td>
<td>Verifies the waiting queue load for data channel messages.</td>
<td>Waiting count is...</td>
</tr>
<tr>
<td>Check</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</td>
<td>Tasks are in a waiting state for more than an hour?</td>
</tr>
<tr>
<td></td>
<td>an hour at the time of the check.</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.
### 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.
Enforcing policies

A policy is a collection of settings that you create and configure, then enforce.

McAfee ePO organizes its policies by product, then by categories in each product. For example, McAfee Agent 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. The Policy Catalog page displays only policies for products that the user has 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, you might want to change the default response time that managed systems communicate back to the McAfee ePO server.

Contents

- About policies
- Policy assignment rules
- Create and manage policies
- Move and share policies between McAfee ePO servers
- Create and manage policy assignment rules
- Policy management users
- Assign policies to managed systems
- Copy and paste policy assignments
- View policy information

About policies

A policy is a collection of settings that you create and configure, then enforce.

McAfee ePO organizes its policies by product, then by categories for 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 from the Products pane and the corresponding categories appear on the right pane. Expand the category to see the list of policies. 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, you might want to 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 amount of time defined in 2 settings. ASCI defines how often the agent communicates with the server. Policy enforcement interval 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 might change the ASCI using the agent wake-up client task.

If you want to change the settings of a default policy, you need to duplicate the policy and rename it. Make the required changes and reassign the policy to the managed systems. The next time an agent-server communication occurs, the new policy is applied to these systems.

Enforcing policies
The timing of policy enforcement depends on the configuration of the policies. Enforcement can happen:

- **Instantly**
  
  Example: On-Access Scan policy occurs when you start any application.

- **At agent-server communication or policy enforcement intervals**
  
  Example: 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**:
  
  Example: On-demand scan policy, by default, runs every day at midnight 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 (default is 60 minutes). You can adjust this interval on the General tab as well.

When you want an on-demand scan to run every day at midnight, you configure the settings so that:

1. The Policy Based on-demand scan Client Task runs at 12 a.m.
2. The client task starts the full on-demand scan on the managed systems.
3. Using the configured settings in the policy, the scan runs 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 inheritance or assignment.

**Inheritance** — When a system or group of systems takes its policy settings and client tasks from its parent group. Enabled by default.

**Assignment** — When an administrator assigns a policy to a system or group of systems. You can define a policy once for a specific need, then apply it to multiple locations.

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.

> The inherited policy might be a different policy than the source policy.

**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 remove 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**

The user that creates a policy is the assigned owner of that policy. You must have the correct permissions to edit a policy you don't own.

You can't use a policy owned by a different user, but you can 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 assignments rules reduce the overhead of managing numerous policies and help maintain more generic policies across your System Tree.

This level of granularity in policy assignments limits the instances of broken inheritance in the System Tree. Policy assignments can be based on 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 the members of the IT department 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 how you manage and maintain your policy assignments. 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 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.

Policy assignment rule priority on multi-slot policies

Multi-slot policies allow administrators to send more than 1 policy of a particular policy type to the client system. For example, an administrator can assign more than 1 Firewall rules policy which are merged and enforced on the client system.

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. Multi-slot policies assigned using policy assignment rules override policies assigned in the System Tree. Also, user-based policies take priority over system-based policies. Consider the following scenario where:

**Scenario: Using multi-slot policies to control Internet access**

Your System Tree includes a group named "Engineering" that consists of systems tagged with "IsServer" or "IsLaptop." 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 allow 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**

Rules that consist of multi-slot policies are applied to assigned systems without regard to priority. Because of this, you might need to prevent policy setting aggregation. You can do this 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**

With user-based policy assignment rules, you can create user-specific policy assignments. These assignments are enforced at the target system when a user logs on.

On a managed system, the agent keeps a record of the users who log on to the network. The policy assignments you create for each user are pushed down to the system they log on to, and are cached during each agent-server communication. The McAfee ePO server applies the policies that you assigned to each user.

To use user-based policy assignments, you must register and configure a registered LDAP server for use with your McAfee ePO server.

**System-based policy assignment**

With system-based assignments, you can assign policies based on System Tree location or tags. System-based policies are assigned based on selection criteria you define with 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 build 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 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

Contents

- Create a new policy
- Enforcing product policies
- Enforce policies for a product in a System Tree group
- Enforce policies for a product on a system
- Managing policy history
- Manage policy history
- Edit policy history permission sets
- Compare policies
- Change the owners of a policy

Create a new policy

Custom policies that you can create from 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.
   a. Select Menu | Policy | Policy Catalog.
   b. Select the product in the left pane to display the corresponding categories in the right pane.
   c. Click New Policy.
2. Select a category from the drop-down list.
3. Select the policy you want to duplicate from the Create a policy based on this existing policy drop-down list.
4. Type a name for the new policy.
5. Enter a note that might be useful to track the changes for this policy, then click OK.
6. Click the name of the new policy to open the Policy Details pane.
7. Click the edit icon to edit the policy settings as needed.
8. Click Save.

The policy is added to the list on the Policy Catalog page.

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:
Enforcing policies

Create and manage policies

- 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.

**Important consideration:** 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

The systems in a group, by default, inherit policies for a product from their parent group. Now, you can enforce changes to this default policy assignment on a product by using policy enforcement feature. You can also choose to lock policy inheritance to prevent any user from making changes to this assignment inadvertently.

**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**.
5. Choose whether to lock policy inheritance to prevent breaking enforcement for groups and systems that inherit this policy.
6. Click **Save**.

Now, you have enforced new policy settings on the selected product and locked the inheritance.

### Enforce policies for a product on a system

The systems in a group, by default, inherit policies from their parent group. Now, you can enforce changes to this default policy assignment on a single managed system by using policy enforcement feature.

**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 | Agent | Edit Policies on a Single System** to open the **Policy Assignment** page.
3. Select a product, then click **Enforcing** next to **Enforcement status**.
4. Select **Break inheritance and assign the policy and settings below**.
5. Next to **Enforcement status**, select **Enforcing** or **Not enforcing**.
6. Click **Save**.

Now, the policy changes are enforced to the target system.
Managing policy history
When you change a policy, 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 provides a record of your changes.

If you have policy users configured to create and edit policies, the Status column options depend on user permissions. For example:

- McAfee ePO administrators have full control of all policy history functions.
- Policy administrators can approve or reject 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. You can also revert to a previous version of a policy if you feel the changes are not required anymore.

Before you begin
You must have appropriate permissions to revert to a previous policy version.

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.
   - 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 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
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 have provided the required permissions to revert existing policies for the selected product to their previous versions.

Compare policies
Compare and 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 | Policy Comparison, then select a product, category, and Show settings from the lists.
2. From the Policy 1 and Policy 2 column lists, select the policies to compare in the Compare policies row.
   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. Expand the category to see all the policies for that category.
2. Click the policy you want, then click the owner of the policy on the Policy Details pane.
3. Select the owners of the policy from the list, then click Save.

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 146**
  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

Contents

- Create policy assignment rules
- Manage 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

You can assign different permission sets to different policy users, so that they can create and modify specific product policies. Some users can approve or deny changes from policies submitted by other users.

Policies can be managed by users with different permissions. As an administrator, you can create users with hierarchical levels of policy permissions. For example, you can create these policy users:

- **Policy administrator** — Approves policies created and modified by other users.
- **Policy user** — Duplicates and creates policies that they submit to the policy administrator for approval before they are used.

Overview of creating policy users

1. In Permission Sets, create different permission sets for the policy administrator and policy user.

2. In User Management, create policy administrator and policy user, then manually assign them the different permission sets.

Policy user capabilities

- Duplicate, modify, or create policies and submit them to the policy administrator for approval
- Monitor the approval status by the policy administrator

Policy administrator capabilities

- All functions of the policy user
- Approve or reject changes
Table 12-1 Comparing capabilities of a policy user vs. policy administrator

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Policy user</th>
<th>Policy administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate, modify, or create policies and submit them for approval</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Monitor the approval status</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Approve or reject policies</td>
<td></td>
<td>×</td>
</tr>
</tbody>
</table>

Create policy management permission sets

As an administrator, you can create permission sets for different policy user levels. The Permission Sets allow some policy users not only to create and modify policies, but also to approve or reject policies created by other users.

**Before you begin**

You must have administrator rights to change Permission Sets.

To 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 to approve or reject those changes.

- Policy User permission set — The policy user can create and modify specific product policies, but the policy changes must be approved before the policy is saved.
- Policy Administrator permission set — The policy administrator can create and modify specific product policies, and approve or reject the changes created by policy users and other administrators.

**Task**

1. Select **Menu | User Management | Permission Sets**, then click **New Permission Sets**.

2. To create the policy administrator permission set, type the name, for example, `policyAdminPS`, then click **Save**.

3. Select the new permission set, scroll down to the Policy Management row, then click **Edit**.

4. Select **Can approve or decline the policy changes submitted by other users**, then click **Save**.
   
   This option allows the policy administrator to approve or reject policy changes for other users who don't have administrator approval.

5. Scroll down to a row, for example, the Endpoint Security Common, and click **Edit**.

6. Select **View and change policy and task settings** and click **Save**.
   
   This option allows the policy administrator to make changes to Endpoint Security Common policies.

7. Configure the edit permissions for different parameters as needed.

8. To create the policy user permission set, click **Actions | Duplicate**.
   
   a. Type a name for the policy user permission set, for example, `policyUserPS` and click **OK**.
   
   b. From the Permission Sets list, click the policyUserPS permission set.

   c. Scroll down to the Policy Management row and click **Edit**.

   d. Select **No Permissions** for Policy Approval setting , then click **Save**.
      
      This setting forces the users assigned with this permission set to request approval from the administrator before they can save a new or changed policy.
You have created two permission sets; one to assign to a policy user and one to assign to a policy administrator.

**Create policy management users**

You can create different policy user levels with different permission sets that allow users to create and modify policies, and an administrator user to approve or reject policy changes.

**Before you begin**

You must have administrator rights to create users.

**Task**

1. Open the User Management page: select **Menu | User Management | Users**.
2. Click **New User**.
3. Type a user name. For example, `policyUser` or `policyAdmin`.
4. Select **Enable** for the logon status of this account.
5. Select the authentication method for the new user.
   - McAfee ePO authentication
   - Windows authentication
   - Certificate-based authentication

   The McAfee ePO authentication password is for one-time use only and must be changed during the next logon.

6. Provide the required credentials or browse to select the certificate.
7. (Optional) Provide the user’s full name, email address, phone number, and a description.
8. Select the policy user permission set you created, then click **Save**.

The new user or administrator appears in the Users list of the User Management page.

You have two policy users: a policy user who can change policies and a policy administrator who can approve or reject those changes.

**Configure approval settings for Policy Changes**

You can choose whether policy users and administrators need approval to make policy changes. This prevents users from making inadvertent changes to any product policies.

**Before you begin**

You must have administrator rights.

**Task**

1. Select **Menu | Configuration | Server Settings**.
2. Click **Approvals** on the Setting Categories pane.
3 Click Edit.
   a Select Users need approval for policy changes if policy users have to seek approval to make changes.
   b Select Administrators and Approvers need approval for policy changes if the administrators and approvers also need to seek approval to make changes.

   If you change these settings when a policy or task is submitted for review, it is rejected automatically.

**Configure email notifications using Automatic Response**

You can set up an automatic response to receive email notifications when a policy is submitted for approval, or when a policy submitted for approval is approved or rejected.

**Before you begin**
Your email server must be configured and registered.

**Task**

1 Select Menu | Automation | Automatic Responses.

2 Click New Response.

3 Enter a name for the new response and provide a description about this automatic response.

4 Select ePO Approval Events in the Event group drop-down list.

5 Select Policy Approval in the Event type drop-down list.

6 Click Next to set filters to define when to trigger an email notification.

7 Click Next to set aggregation.

8 Click Next and select Send emails in the Actions drop-down list.

   You receive a warning message stating that the email server is not configured if you have not registered and configured your email server.

9 Enter details for the email to be triggered as an automatic response and click Next.

10 Verify the settings of the automatic response on the Summary tab and click Save.

Now, you receive an automatic email notification when a policy is submitted for approval and if the policy is approved or rejected.

**Submit policy changes for review**

All users, including administrators and policy approvers, can create and change policies; but they might need to submit the policy for review by the administrator, or users with approval permissions, or a policy administrator.

**Before you begin**
Server Settings and user permission sets must be configured to allow users to submit policies for approval.
Task

1. Create and maintain policies.

   Policy users only have access to policies and settings configured by the administrator in their assigned permission set.

2. To save the policy and send it to the administrator, click Submit for Review.

3. Check the policy approval status using one of these methods:
   - Select Menu | Policy | Policy History.
   - Select Pending Approvals | Policy Details | History.

4. Use the Product, Category, and Name filters to select Policy History entries to check.

   The Status column displays one of these entries:
   - Review in progress — Has not been reviewed
   - Rejected — Has been rejected and not saved
   - Approved — Has been approved and saved

   The notification icon notifies if an action has been taken on the policy submitted for review.

Cancel policy review

If you are the user making changes and submitting a policy for review, you can withdraw the policy from review.

Before you begin

You must be the user who submitted the policy changes for review.

Task

1. Select Menu | Policy | Policy Catalog.

2. Select Pending Approvals from the Products pane.

3. Select the policy for which you want to cancel review.


5. Click Cancel on the pop-up dialog box that appears to confirm cancellation of review.

   The policy changes that were submitted for review are cancelled. The policy is removed from the Pending Approvals list.

Review policy changes

As a policy administrator, you need to periodically approve or reject policies submitted by non-admin users. You receive notifications when a non-admin user submits a policy for approval.

Before you begin

The Server Settings and user permission sets must be configured to allow users to submit policies for approval.
Task

1. To change the status of the policy submitted for review, select Menu | Policy | Policy Catalog.

2. Select Pending Approvals from the Products pane and select the policy you want to review.

3. View all proposed changes on the Policy Details pane.

4. Click Approve or Reject.

   A pop-up dialog box appears to confirm your decision. You can enter comments (optional) in the Comments text box.

   If you approve the changes, the policy is saved; otherwise the policy changes are 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 system that inherits 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**

**Contents**
- Copy policy assignments from a group
- Copy policy assignments from a system
- Paste policy assignments to a group
- Paste policy assignments to a specific 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.

   > 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.
   
   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

Contents

- View groups and systems where a policy is assigned
- View policy settings
- View policy ownership
- View assignments where policy enforcement is disabled
- View policies assigned to a group
- View policies assigned to a specific system
- View policy inheritance for a group
- View and reset broken inheritance
- Create policy management queries

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 Assignments
   The Assigned Policies tab opens on the System Tree page.

2. Click the link next to Enforcement status, which indicates the number of assignments where enforcement is disabled, if any. The Enforcement for <policy name> page appears.

3. Select Enforcing for the Enforcement Status to enforce a policy for the selected product.

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 error 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.
   a. Select **Menu | Automation | Server Tasks**.
   b. 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 "LW", which means the last weekday of the month.
- The pound character "#" identifies the "Nth" day of the month. For example, using "6#3" in the Day of Week field is the third Friday of every month, "2#1" is the first Monday, and "4#5" is the fifth Wednesday.
  - If the month does not have a fifth Wednesday, the task does not run.

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.

1. The client task starts when you run the Smart Installer URL on a system.
2. 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.
3. Once the software is installed, it is run periodically using other client task requests sent from McAfee ePO to protect your systems.
4. 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.

5. 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</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>(SDAT.exe) files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File type: SDAT.exe</td>
<td></td>
<td></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>File type: Extra.DAT</td>
<td></td>
<td></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>File type: zip</td>
<td></td>
<td></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>
<tr>
<td>File type: zip</td>
<td></td>
<td></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.

Client task approvals

Contents
- Create client task users
- Create client task permission sets
- Configure approval settings for Task changes
- Submit task changes for review
- Cancel or update a client task review
- Review client task changes
- Configure email notifications using Automatic Response
Create client task users

You can create different task user levels with different permission sets that allow users to create and modify tasks, and allows an administrator to approve or decline task changes.

Before you begin
You must have administrator rights to create users.

Task
1. Open the User Management page: select **Menu | User Management | Users**.
2. Click **New User**.
3. Type a user name. For example, `taskUser` or `taskAdmin`.
4. Select **Enable** for the logon status of this account.
5. 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.
   - The McAfee ePO authentication password is for one-time use only and must be changed during the next logon.
6. (Optional) Provide the user’s full name, email address, phone number, and a description.
7. Select the task user permission set you created, then click **Save**.

The new user or administrator appears in the Users list of the User Management page.

You have two task users. A task user who can change tasks and a task administrator who can approve or decline those changes.

Create client task permission sets

As an administrator, you can create permission sets for different user levels. Based on the permission sets users can either create and modify client tasks, or approve or reject tasks created by other users.

Before you begin
You must have administrator rights to change permission sets.

To manage task creation, you can create permission sets for users who can create and modify specific tasks. For example, you can create permission sets that allow one user to change tasks and another user permission to approve or reject those changes.

- **Task User permission set** — The task user can create and modify specific product tasks, but the changes must be approved before the task is saved.
- **Task Administrator permission set** — The task administrator can create and modify specific tasks, and approve or reject the changes made by task users, and other administrators.

Task
1. Select **Menu | User Management | Permission Sets**, then click **New Permission Sets**.
2. To create the task administrator permission set, type the name, for example, `taskAdminPS`, then click **Save**.
   a. Select the `taskAdminPS` permission set, scroll down to the Client Task Management row, then click **Edit**.
   b. Select **Can approve or decline the task changes submitted by other users**, and click **Save**.

   This allows the task administrator to respond to others’ task changes without administrator approval.
c Scroll down to a parameter that you want to edit, for example, the Endpoint Security Common, and click Edit.

d Select View and change policy and task settings and click Save.

This allows the task administrator user to make task changes to Endpoint Security Common tasks.

e Configure the edit permissions for different parameters as needed.

3 To duplicate the task administrator permission set and create the policy user permission set, click Actions | Duplicate.

a Type the name of the task user permission set, for example, taskUserPS and click OK.

A duplicate task administrator permission set is created.

b From the Permission Sets list, click the taskUserPS permission set.

c Scroll down to the Client Task Management row and click Edit.

d Select No Permissions for Task Approval, and click Save.

This setting forces the users assigned with this permission set to request approval from the administrator before they can save a new or changed policy.

Now, you have created two permission sets; one to assign to a task user and another one to assign to a task administrator.

**Configure approval settings for Task changes**

You can choose whether a user needs approval to make client task changes.

**Before you begin**

You must have administrator rights.

**Task**

1 Select Menu | Configuration | Server Settings.

2 Click Approvals on the Setting Categories pane.

3 Click Edit.

a Select Users need approval for client task changes if task users have to seek approval to make changes.

b Select Administrators and Approvers need approval for client task changes if the administrators and approvers also need to seek approval to make changes.

If you change these settings when a client task is submitted for review, it is rejected automatically.

**Submit task changes for review**

All users, including administrators and approvers, can create and change tasks. However, if configured by the administrator, it must be reviewed by the administrator or a user with approval permissions. Only tasks that are approved are available for task assignment.

**Before you begin**

The Server Settings and user permission sets must be configured to allow users to submit client tasks for approval.
Task
1 Create client tasks.
   Users only have access to tasks that are configured by the administrator in their assigned permission set.

2 To save the task, click Submit for Review.

3 A pop-up dialog box appears to confirm your submission and you must enter comments about the changes (existing task) or the purpose (new task).
   This sends the task to the administrator to approve or reject.

4 To check the approval status, select Menu | Client Task Catalog.
   a Select Pending Approvals in the Client Task Types pane.
   b Click the task in the Pending Approvals pane.
   The latest 10 actions on the task are displayed on the Task Details pane.
   c Click View Full Task History to see the status of the task on the Comment History page.
   d Use the Product, Category, and Name filters to select Task History entries to check.
   e The Status column displays one of these entries:
      • Submit for review — Has not been reviewed
      • Rejected — Has been rejected and not saved
      • Approved — Has been approved and saved
   The notification icon indicates if an action was taken on the task submitted for review. If you have configured an automatic response, you also receive an email notification.

Cancel or update a client task review
You can update or cancel a task that you have submitted for review.

   You must be the user who submitted the client task for review.

Task
1 Select Menu | Client Task Catalog.

2 Select Pending Approvals from the Client Task Types pane.

3 Select the task review that you want to cancel or update and submit again.

4 Click Cancel Review on the Task Details pane or click Update Review to edit the task and submit again for approval. Alternately, you can click Review on the Pending Approvals pane and click Cancel Review or Update Review.

5 Enter comments and click OK on the pop-up dialog box that appears.
   This action deletes the task if it is a new task that was not saved earlier.
Review client task changes
As an administrator or approver, you need to periodically approve or reject requests submitted by users and other administrators or approvers. You receive notifications when a user submits a task for approval.

Before you begin
Server Settings and user permission sets must be configured to allow users to submit tasks for approval.

Task
1. To change the status of the task submitted for review, select Menu | Client Task Catalog.
2. Select Pending Approvals from the Client Task Types pane and select the task you want to review.
3. View all proposed changes on the Task Details pane.
4. Click Approve or Reject. When prompted to confirm your decision, enter your comments in the text box and click OK. Alternately, you can click Review on the Pending Approvals pane to open the task and click Approve or Reject on this page.

If you approve the changes, the task is saved; otherwise the task is sent back to the submitter.

Configure email notifications using Automatic Response
You can set up an automatic response to receive email notifications when a task is submitted for approval, or when a task submitted for approval is approved or rejected.

Before you begin
Your email server must be configured and registered in Server Settings to complete this task.

Task
1. Select Menu | Automation | Automatic Responses.
2. Click New Response.
   a. Enter a name for the new response and provide a description.
   b. Select ePO Approval Events in the Event group drop-down list.
   c. Select Task Approval in the Event type drop-down list.
3. Click Next to set filters to define when to trigger an email notification.
4. Click Next to set aggregation.
5. Click Next and select Send emails in the Actions drop-down list.

   You receive a warning message that the email server is not configured if you have not registered and configured your email server.

6. Enter details for the email to be triggered as an automatic response and click Next.
7. Verify the settings of the automatic response on the Summary tab and click Save.

You have set up an automatic response that triggers an email notification when a task is approved, rejected, or submitted for approval.
Deploy products to managed systems

Contents

- Configure a deployment task for groups of managed systems
- Configure a deployment task to install products on a managed system

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.

13 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

14 Review the summary, then click Save.

At every scheduled run, the deployment task installs the latest sensor package to systems that meet the specified criteria.

**Configure a deployment task to install products on a managed system**

Deploy products to a single system using a product deployment task. Create a product deployment client task for a single system when that system requires:

- A product installed that other systems within the same group do not require.
- A different schedule than other systems in the group. For example, if a system is located in a different time zone than its peers.

### 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.

9 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.

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

Once you select the criteria, the number of systems that fall into that criteria is displayed on top of the page. For example, if you create a tag for a domain group and apply this tag to 5 systems in a group, the page displays "5 systems are affected" in red colored font.

10 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

11 Review the summary, then click Save.

The task is added to the list of client tasks for the groups and systems 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.
   - 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

Contents
- Create client tasks
- Edit client tasks
- Compare client tasks
- View client tasks assigned to a specific system

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.
- Run system commands.
- Execute server tasks.
- Send an email message.
- Run external commands.
- 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 an email message to multiple recipients.
- Run external commands.
- 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 failed</td>
<td>Distributed repository update or replication failed</td>
<td>Any update or replication fails.</td>
</tr>
</tbody>
</table>
| Malware detected | Any events from any unknown products | These criteria are met:  
  - The number of events is at least 1,000 in an hour.  
  - The number of selected distinct values is 500.  
  - At most, once every 2 hours.  
  The email includes the source system IP address, threat names, product information, and other parameters. |
| Master Repository update or replication failed | Master Repository update or replication failed | Any update or replication fails. |
| Noncompliant computer detected | Noncompliant Computer Detected events | Any event is received from the Generate Compliance Event server task. |

**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 184
  Determine whether events are forwarded immediately or only during agent-server communication.

• Determine which events are forwarded to the server on page 184
  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 McAfee Agent on the Products pane and expand General category.
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>
<tr>
<td>Edit a registered executable</td>
<td>1. Find the registered executable to edit in the Registered Executable page, then click Edit.</td>
</tr>
<tr>
<td></td>
<td>2. Change the information as needed and click Save.</td>
</tr>
<tr>
<td>Duplicate a registered executable</td>
<td>1. Find the registered executable to duplicate in the Registered Executable page, then click Duplicate.</td>
</tr>
<tr>
<td></td>
<td>2. Type a name for the registered executable, then click OK.</td>
</tr>
<tr>
<td></td>
<td>The duplicated registered executable appears in the Registered Executables list.</td>
</tr>
<tr>
<td>Delete a registered executable</td>
<td>1. Find the registered executable to delete in the Registered Executable page, then click Delete.</td>
</tr>
<tr>
<td></td>
<td>2. When prompted, click OK.</td>
</tr>
<tr>
<td></td>
<td>The deleted registered executable no longer appears in the Registered Executables list.</td>
</tr>
</tbody>
</table>

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.

Automatic response rules do not have a dependency order.

## 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>
<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.
### 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>

- 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></td>
<td>• Server — Applies the tag on all managed servers.</td>
</tr>
<tr>
<td></td>
<td>• Workstation — 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></td>
<td>• Product — The product selected.</td>
</tr>
<tr>
<td></td>
<td>• Category — The category selected.</td>
</tr>
<tr>
<td></td>
<td>• Policy — 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></td>
<td>• Server — Managed server tags.</td>
</tr>
<tr>
<td></td>
<td>• Workstation — Managed workstation tags.</td>
</tr>
<tr>
<td></td>
<td>• Clear all — 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><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>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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>• <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 <strong>Master Repository</strong>.</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 &lt;system_drive&gt;\McAfee\Common Framework) 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>Exclude Tag</td>
<td>Runs the system command to exclude server and workstation tags.</td>
</tr>
<tr>
<td>Move Systems</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>Resort Systems</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>
</table>
| **Run Client Task Now**       | Runs the system command to run a client task using the following:  
  • **Abort after** — Specifies the number of minutes before canceling the task.  
  • **Connect Using** — Specifies the handler to use for the task.  
  • **Number of attempts** — Specifies the number of attempts before canceling the task.  
  • **Product** — The product selected.  
  • **Randomization** — Specifies the randomization intervals, in minutes, to mitigate the bandwidth impact.  
  • **Retry interval** — Specifies the number of seconds between attempts to run the task.  
  • **Stop Task on the Client After** — Specifies the number of minutes before the attempt to run the task is canceled.  
  • **Task** — Select the task from the list.  
  • **Task Type** — Select the task type from the list. |
| **Sensor Blacklist Management** | Runs the system command to add or remove sensors from the blacklist.  
| **Set User Properties**       | Runs the system command to set the description.  
| **Transfer Systems**          | Runs the system command to transfer systems between McAfee ePO servers.  
| **Wake Up Agents**            | Runs the system command to wake up agents using the following:  
  • **Abort after** — Specifies the number of minutes or hours before canceling the wake-up attempt.  
  • **Force complete policy and task update** — Forces policy and task updates during the agent wake-up.  
  • **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.  
  • **Number of attempts** — Specifies the number of attempts before canceling the agent wake-up.  
  • **Randomization** — Specifies the randomization intervals, in minutes, to mitigate the bandwidth impact.  
  • **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.  
  • **Wake up Agent using** — Specifies the Agent Handler to use based on the following selection:  
    • Using the last connected Agent Handler  
    • Using all Agent Handlers  
  • **Wake-up call type** — Specifies the call type as either:  
    • **Agent Wake-Up Call**  
    • **SuperAgent Wake-Up Call** |
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.</td>
</tr>
<tr>
<td>Body</td>
<td>Enter the text that appears in the event email.</td>
</tr>
</tbody>
</table>

Using the Insert variable lists, you can insert variables in the email with descriptions of the event.

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.</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>• Trigger this response for every event — The response occurs every time the event occurs.</td>
</tr>
<tr>
<td></td>
<td>• Trigger this response if multiple events occur within — 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>• When the number of distinct values for an event property is at least a certain value — 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>• When the number of events is at least — 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>• Do not group aggregated events — Aggregated events are not grouped according to any specific criteria.</td>
</tr>
<tr>
<td></td>
<td>• Group aggregated events by — 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 actions</td>
<td>New Response</td>
<td>Opens the Response Builder where you can create a response.</td>
</tr>
<tr>
<td></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 options</td>
<td>Show Filter/Hide Filter</td>
<td>Shows or hides the filter options used to filter the displayed responses.</td>
</tr>
</tbody>
</table>
### Table 14-8 Option definitions (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Preset**     | Filter the displayed responses. The McAfee products that you have installed determine the selections in this list. These filters are included by default: | • **All** — Displays all responses.  
• **ePO Notification Events** — Displays only those responses for McAfee ePO notification events. |
| **Quick Find** | To filter the displayed responses to the search results, enter a search term. Click **Apply** to perform the search.                                                                                                                |
| **Clear**      | Removes all filter settings.                                                                                                                                            |
| **Show selected rows** | Select to restrict the displayed list of responses to only selected responses.                                                                                                           |
| **Actions column** | **View** | Opens the Response details page where you can review the details of the selected response.                                                                                       |
| **Edit**       | Opens the Response Builder where you can edit the response.                                                                                                               |
| **Duplicate**  | Creates a copy of the selected response.                                                                                                                                     |
| **Choose Columns** | **Actions** | Opens the Select the Columns to Display page where you can select the columns of data to display on the Automatic Responses page.                                                                 |
| **Delete**     | Deletes the selected response.                                                                                                                                              |
| **Disable Responses** | Disables the selected responses.                                                                                                                                               |
| **Duplicate**  | Creates a copy of the selected response.                                                                                                                                     |
| **Edit**       | Opens the Response Builder where you can edit the response.                                                                                                               |
| **Enable Responses** | Enables the selected responses.                                                                                                                                               |
| **Export Responses** | Downloads the selected response as an .xml file.                                                                                                                              |
| **Export Table** | Opens the Export page where you can specify the format and details about how to download your responses.                                                                    |
| **View**       | Opens the Response details page where you can review the details of the selected response.                                                                                     |
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><strong>Description</strong></td>
<td>Allows you to type a description of this response.</td>
</tr>
<tr>
<td><strong>Event</strong></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><strong>McAfee ePO Notification Events</strong></td>
<td>Specifies the available McAfee ePO notification event types, including:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client</strong> — Events that occur on managed systems. For example, &quot;Product update succeeded.&quot;</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server</strong> — Events that occur on the McAfee ePO server. For example, &quot;Repository pull failed.&quot;</td>
</tr>
<tr>
<td></td>
<td>• <strong>Threat</strong> — Events that indicate a possible threat are detected. For example, &quot;Virus detected.&quot;</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Allows you to select the language of response from the list.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Allows you to type a name for the response. Spaces, underscores, and special characters are allowed.</td>
</tr>
<tr>
<td><strong>Status</strong></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 McAfee ePO 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><strong>Authentication</strong></td>
<td>Specifies the credentials required to authenticate to the email server.</td>
</tr>
<tr>
<td><strong>From address</strong></td>
<td>Specifies the email address that appears in the From text box in email messages that are sent from the McAfee ePO server.</td>
</tr>
<tr>
<td><strong>SMTP server name</strong></td>
<td>Specifies the IP address or name of the SMTP server.</td>
</tr>
<tr>
<td><strong>SMTP server port</strong></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>
<tr>
<td><strong>The server accepts</strong></td>
<td>Specifies, globally, events accepted by the McAfee ePO server. Options include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Events from any source</strong> — All events sent by any agent are processed by the McAfee ePO server. The default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Events that were generated by the sending agent</strong> — The McAfee ePO server processes only those events sent by the source agent.</td>
</tr>
</tbody>
</table>
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 14-12 Option definitions

<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 McAfee ePO response server settings.

Table 14-13 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Specifies how often you want McAfee ePO to check for new notifications.</td>
</tr>
<tr>
<td>Startup Delay</td>
<td>Specifies how long McAfee ePO 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 14-14 Option definitions

<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 14-15 Option definitions

<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 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>
Setting up automatic responses
Client events page
15 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. |
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
- 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

Estimating and adjusting the ASCI

Contents

- Estimating the best ASCI: best practice
- Configure the ASCI setting: best practice
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.
4. Click Save.
   If you send a policy change or add a client task immediately, you can execute an agent wake-up call.
Managing agent-server communication

Contents

- Allow agent deployment credentials to be cached
- Change agent communication ports

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>
</tbody>
</table>
### Table 16-1 Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Installation path</strong></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><strong>Installation options</strong></td>
<td>• <strong>Install only on systems that do not have an agent managed by this McAfee ePO server</strong> — 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>• <strong>Suppress agent installation user interface</strong> — Hides the installation of the agent from the end user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force installation over existing version</strong> — 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 <strong>Install only on systems that do not have an agent managed by this McAfee ePO server</strong>.</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 function 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.

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.

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.

Typing the current agent number means that the query finds only versions “earlier than” that 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.

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
   • Threat Target Host Name
   • Threat Target IPv4 Address

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.](image)

   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 221**
  
  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 223**
  
  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 223**
  
  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.
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
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.

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 master or 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.

![Diagram of source sites and repositories delivering packages to systems](image-url)
**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 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*.

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.

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.

**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.

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 236**
  Create a source site from Server Settings.
- **Switch source and fallback sites best practice on page 237**
  Use Server Settings to change source and fallback sites.
- **Edit source and fallback sites best practice on page 238**
  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 238**
  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.
   - 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 239**
  To update your repositories, configure proxy settings to pull DATs.

- **Configure proxy settings for the McAfee Agent on page 239**
  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.

   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.
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 241**
  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 242**
  Select which repository-specific packages are replicated to distributed repositories.

- **Delete SuperAgent distributed repositories on page 242**
  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 webservice.

5 Click **Save**.

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

The next time the agent calls 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 243
  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 243
  Add an entry to the repository list and specify the folder the new distributed repository uses.

• Avoid replication of selected packages on page 245
  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 245
  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 246
  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 246
  Edit a distributed repository configuration, authentication, and package selection options as needed.

• Delete distributed repositories on page 246
  Delete HTTP, FTP, or UNC 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.
   - 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.

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

9 Review the Summary page, then click Save to add the repository. The McAfee ePO software adds the new distributed repository to its database.

Avoid replication of selected packages

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

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.

**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.

**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 the account used to access the UNC share is secure.

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

  ![](image)

  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.
   c. On the Repositories tab, click Add.
   d. Type a name in the Repository Name text field.
      
      The name does not have to be the name of the system hosting the repository.
   e. Under Retrieve Files From, select the type of repository.
   f. Under Configuration, type the location of the repository using appropriate syntax for the repository type.
   g. Type a port number or keep the default port.
   h. Configure authentication credentials as needed.
   i. Click OK to add the new distributed repository to the list.
   j. Select the new repository in the list.
      
      The type Local indicates it is not managed by the McAfee ePO software. When an unmanaged repository is selected in the Repository list, the Edit and Delete buttons are enabled.
   k. Click Save.

Any system where this policy is applied receives the new policy at the next agent-server communication.

Work with the repository list files

You can export the repository list files.

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

- **Export the repository list SiteList.xml file on page 249**
  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 249**
  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.

- **Export distributed repositories from the repository list on page 250**
  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 250**
  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**

It is not recommended to import distributed repositories from another server unless the server is inactive and you want to use the existing repositories.

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 control which distributed repositories agents use for updating by enabling or disabling distributed repositories in the agent policy settings. It is recommended not to 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.

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.

- **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.

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](image)
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.

Network topology and deployment considerations

Contents

- Using Agent Handlers behind a DMZ, firewall, or in NAT networks: best practices
- Roaming with Agent Handlers
- Repository cache and how it works
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 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

This table lists all ports used by the McAfee ePO server and the other network components.

<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>
</tbody>
</table>

This Agent Handler connection requires access to both the SQL database and the McAfee ePO server. Some firewall rules are necessary for this configuration.

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 (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Direction</th>
<th>Connection</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<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.

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.
This diagram shows how Agent Handlers cache product update content if the configured remote repository is unavailable to remote systems.

![Diagram showing Agent Handler repository caching]

**Best Practices: Agent Handler installation and configuration**

You can configure mid-range servers, located in 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.

⚠️ When 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.

**Configure Agent Handlers list**

Use the Handlers List to see a list of your Agent Handlers and their detailed information,

**Task**

1. Select **Menu | Configuration | Agent Handlers.**
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.

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:

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 — Agent Handler to the McAfee ePO server
   - Port 8444 — Agent Handler to the McAfee ePO server
   - Port 443 — Bidirectional
5. 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 — Agent Handler to SQL database server
   - Port 1434 UDP — Agent Handler to SQL database server
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 — Bidirectional
   - Port 8082 UDP — Bidirectional

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.
To start the Agent Handler configuration on the McAfee ePO server, select **Menu | Configuration | Agent Handlers**.

To open the Agent Handler Assignment page, select **New Assignment**.

Configure these settings:

- **Type an Assignment Name.** For example, **NAT Systems Assignment**.
- **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.
- **Next to Handler Priority, click Use custom handler list and Add Handlers**.
- **From the list, select the Agent Handler to handle these selected systems.** Disregard the warning that appears.
- **Click Save.**

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:

- **Move the Agent Handler to the top of the priority list by moving the Agent Handler names.**
- **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.

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.

Confirm that the Agent Handler in the DMZ is managing the systems behind the DMZ:

- 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.
- 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.
   You must use SQL authentication to connect to the database. If Agent Handler cannot use domain account and McAfee ePO uses the domain account for SQL connection, you need to manually deselect the option to use McAfee ePO database configuration and provide non-domain SQL credentials with appropriate roles to access 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
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.
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 <strong>Delete</strong> in the selected assignment row.</td>
</tr>
<tr>
<td>Edit a handler assignment</td>
<td>Click <strong>Edit</strong> for the selected assignment. The Agent Handler Assignment page opens, where you can specify:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Assignment name</strong> — The unique name that identifies this handler assignment.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Agent criteria</strong> — The systems that are included in this assignment. You can add and remove System Tree groups, or modify the list of systems in the text box.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Handler priority</strong> — Choose whether to use all Agent Handlers or a custom handler list. Agents randomly select which handler to communicate with when <strong>Use all Agent Handlers</strong> is selected.</td>
</tr>
<tr>
<td>Export handler assignments</td>
<td>Click <strong>Export</strong>. The Download Agent Handler Assignments page opens, where you can view or download the AgentHandlerAssignments.xml file.</td>
</tr>
<tr>
<td>Import handler assignments</td>
<td>Click <strong>Import</strong>. The Import Agent Handler Assignments dialog box opens, where you can browse to a previously downloaded AgentHandlerAssignments.xml file.</td>
</tr>
<tr>
<td>Edit the priority of handler assignments</td>
<td>Click <strong>Edit Priority</strong>. The Agent Handler Assignment</td>
</tr>
<tr>
<td>View the summary of 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 272
  Create Agent Handler assignments to group McAfee Agents together.
• Group agents by assignment priority on page 272
  Group agents together and assign them to an Agent Handler that is using assignment priority.
• Group agents using the System Tree on page 273
  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.

   - 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**.
     - 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.

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

5. Click **Save**.

**Group agents by assignment priority**

Group agents together and assign them to an Agent Handler that is using assignment priority. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers. This list defines the order in which agents attempt to communicate using a particular Agent Handler.

- When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.
Task

1. Select **Menu | Configuration | Agent Handlers.**
   - 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.**

3. As needed, modify the priority or hierarchy of the assignments by clicking **Actions | Edit Priority.**
   - Moving one assignment to a priority lower than another assignment creates a hierarchy where the lower assignment is actually part of the higher assignment.

4. To change the priority of an assignment, which is shown in the **Priority** column on the left, do one of the following:
   - Use drag and drop — Use the drag-and-drop handle to drag the assignment row up or down to another position in the Priority column.
   - Click **Move to Top** — In **Quick Actions**, click **Move to Top** to automatically move the selected assignment to the top priority.

5. 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.

**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).

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-server Operating System versions have severe (~10) limits set on the number of incoming network connections.</td>
</tr>
</tbody>
</table>
Maintaining your McAfee ePO server and SQL databases

Contents
- Maintaining your McAfee ePO server
- Managing SQL databases
- Use a remote command to determine the Microsoft SQL database server and name

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.

**Task**

1. To find the 32-bit version of the Windows Performance Monitor, use Windows Explorer and navigate to C:\Windows\SysWOW64, then find and double-click perfmon.exe.
2. To confirm that you opened the 32-bit version of Performance Monitor, click Monitoring Tools | Performance Monitor, Add Counters, then click the + sign to open the Add Counters dialog box.
3. To find the McAfee ePO server counters, scroll down the list of counters, find ePolicy Orchestrator Server, and expand the list.

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**

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**
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:

- [Configure the Performance Monitor Display](http://technet.microsoft.com/en-us/library/cc722300.aspx)

### 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**.

   ![In the Services Manager list, find McAfee ePolicy Orchestrator 5.10.0 Event Parser and confirm it is Started.]

   b. In the Services Manager list, find **McAfee ePolicy Orchestrator 5.10.0 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`

   ![Open this log file and check for errors: eventparser_<servername>.log]

   b. Open this log file and check for errors:

   `eventparser_<servername>.log`
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:
   - Application Server
   - Event Parser
   - 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), 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 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.

**Learn more**

Select **Menu | Automation | Server Tasks** to run the **ePO Database Index Maintenance** server task.

For details about creating your maintenance task, see KB67184.

To learn more about database fragmentation and how to determine the fragmentation of your database, use the DBCC command found here: [https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-showcontig-transact-sql](https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-showcontig-transact-sql).

**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.

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>`
   - **Enter information to log on to the server** — Type the SQL database credentials.
   - **Select the database on the server** — Type the database name.
5. 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:

- Once you learn the processes, they don't take too long to perform.
- They are repeatable, manageable, and effective practices.
- They are based on input from McAfee experts and IT managers.
**Recommended daily tasks: 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.

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>Daily threat tasks</td>
<td></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>Examine product-specific reports, such as VirusScan Enterprise, Endpoint Security, Access Protection, or McAfee Host IPS, for threat events</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). |
<p>| Review the McAfee® Global Threat Intelligence™ (McAfee 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                                     |                                                                                                                                             |
| 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 and 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. |</p>
<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 update. 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>Review the inactive agents log to determine which systems are not reporting to McAfee ePO.</td>
<td>In Server Tasks, run the Inactive Agent Cleanup Task. This task identifies systems that have not connected to the McAfee ePO server for a specific number of days, weeks, or months. 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.</td>
</tr>
<tr>
<td>Ensure that Active Directory or NT Synchronization is working.</td>
<td>Active Directory or NT Domain synchronization pulls in a list of new systems and containers that McAfee ePO must manage. If they are used, confirm that the Sync task can be configured to run at least once a day and is working.</td>
</tr>
<tr>
<td>Confirm that a Memory Process Scan occurs at least daily.</td>
<td>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.</td>
</tr>
<tr>
<td>Check Rogue System Detection</td>
<td>Rogue System Detection tells you which devices are attached to the network. It reports unmanaged systems, so they can be quickly found and removed from the network.</td>
</tr>
<tr>
<td>Daily SQL database tasks</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

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 updates on the McAfee website or from the Software Catalog.</td>
<td>McAfee periodically releases updates and hotfixes, as well as DATs and Engine updates. Check the McAfee website and McAfee ePO Software Catalog frequently for new updates to check in to the McAfee ePO console for local environment testing. You can also use the Software Catalog to download and check in these updates.</td>
</tr>
<tr>
<td></td>
<td>DAT and Engine files are not updated with the Software Catalog.</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></td>
<td>Incremental replication tasks only copy new or non-existent files and can't fix any corrupt files.</td>
</tr>
<tr>
<td>Run Distributed Repository Status.</td>
<td>Select Menu</td>
</tr>
<tr>
<td>Schedule an On-Demand Scan of all systems in your environment.</td>
<td>Schedule an on-demand scan of all systems in your environment that runs during off-hours.</td>
</tr>
<tr>
<td></td>
<td>See these documents for additional information:</td>
</tr>
<tr>
<td></td>
<td>• Best practices for on-demand scans in McAfee Endpoint Security and VirusScan Enterprise, See KB74059.</td>
</tr>
<tr>
<td></td>
<td>• How to create a McAfee ePO report for the event: 1203 (On-Demand Scan Completed), see KB69428.</td>
</tr>
<tr>
<td></td>
<td>• For details about configuring on-demand scans, see the McAfee Endpoint Security product documentation.</td>
</tr>
<tr>
<td><strong>Weekly SQL database tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Back up the McAfee ePO SQL database.</td>
<td>Use the Microsoft SQL Enterprise Manager to back up the McAfee ePO database. Verify that the back-up was successful after it has completed.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See these documents for additional information:</td>
</tr>
<tr>
<td></td>
<td>• How to back up and restore the McAfee ePO database using SQL Server Management Studio, see KB52126</td>
</tr>
<tr>
<td></td>
<td>• McAfee ePO server backup and disaster recovery procedure, KB66616</td>
</tr>
</tbody>
</table>
Table 20-2  Recommended McAfee ePO weekly tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Weekly Windows Server operating system tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Remove inactive systems from Active Directory.</td>
<td>Active Directory pulls in a list of new systems and containers that McAfee ePO must manage. Confirm that the synchronization task is configured to run at least once a day and is working.</td>
</tr>
<tr>
<td></td>
<td>If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection.</td>
</tr>
</tbody>
</table>

**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.

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>Run your McAfee ePO SQL database Maintenance Plan</td>
</tr>
<tr>
<td>Remove and update duplicate GUIDs</td>
<td>Confirm the Microsoft Operating System and other vendor patch levels on the McAfee ePO server are current</td>
</tr>
<tr>
<td>Review Audit Logs</td>
<td></td>
</tr>
<tr>
<td>Validate ePolicy Orchestrator Administrator and Reviewer IDs</td>
<td></td>
</tr>
</tbody>
</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 *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove and update duplicate GUIDs.</td>
<td>Run the Duplicate Agent GUID server tasks to find and fix any duplicate GUIDs in your environment. Also, run these server tasks:</td>
</tr>
<tr>
<td></td>
<td>• Duplicate Agent GUID - clear Error Count</td>
</tr>
<tr>
<td></td>
<td>• Duplicate Agent GUID - remove systems with potentially duplicated GUIDs</td>
</tr>
<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>
<tr>
<td>SQL database tasks</td>
<td>Run your McAfee ePO SQL database Maintenance Plan. See Recommended maintenance plan for McAfee ePO database using SQL Server Management Studio, KB67184.</td>
</tr>
<tr>
<td>Monthly Windows Server operating system tasks</td>
<td>Confirm that the Microsoft Operating System and other vendor update levels on the McAfee ePO server are current. Review and implement all Microsoft updates to eliminate vulnerabilities and mitigate risk.</td>
</tr>
<tr>
<td></td>
<td>Other vendor updates might also be released and need updating to reduce vulnerabilities in the environment.</td>
</tr>
</tbody>
</table>

### 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>
</tbody>
</table>
**Task** | **Description**
---|---
Review product exclusions (for example, VirusScan Enterprise) and includes/excludes (for example, Access Protection rules) periodically to validate relevancy. | 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.

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

Validate that you have the required software, such as the latest version of the McAfee Agent. | 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.

Remove any unsupported software or software for products you aren't using from the master and distributed repositories. | 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.

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. | 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.

Remove server tasks that are no longer used. | 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.

Remove Automated Responses that are no longer relevant. | Automated responses are configured to alert individuals, particularly system administrators; when malware event threats, client treats, or compliance issues must be resolved.

Delete shell systems using a McAfee ePO server task. | 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.

Monitor database size | 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.

---

**Managing SQL databases**

**Contents**
- **Best practice: Maintaining SQL databases**
- **Configure a Snapshot and restore the SQL database**
- **Use Microsoft SQL Server Management Studio to find McAfee ePO server information**
- **Common event format**
Best practice: Maintaining SQL databases

Your McAfee ePO databases require regular maintenance to promote optimal performance and to protect your data.

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.

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 288**
  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 289**
  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.
   - **LastKnownTCP/IP** — 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.

• **User Name** — Threat source user name or email address.

**View and purge the Threat Event Log**
You should periodically view and purge your threat events.

**Task**

1. Select **Menu** | **Reporting** | **Threat Event Log**.

2. Select one of these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Threat Event Log.</strong></td>
<td>1. Click any of the column titles to sort the events. You can also select <strong>Actions</strong></td>
</tr>
<tr>
<td></td>
<td>2. From the Available Columns list, select different table columns that meet your needs, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Select events in the table, then click <strong>Actions</strong> and select <strong>Show Related Systems</strong> to see the details of the systems that sent the selected events.</td>
</tr>
<tr>
<td><strong>Purge Threat Events.</strong></td>
<td>1. Select <strong>Actions</strong></td>
</tr>
<tr>
<td></td>
<td>2. In the Purge dialog box, next to <strong>Purge records older than</strong>, type a number and select a time unit.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>. Records older than the specified age are deleted permanently.</td>
</tr>
</tbody>
</table>

**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**.
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
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 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 are done, 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**.
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 [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.](image)

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.
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.

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:
   a Create a query that shows all events you are questioning, then use the information in this section to analyze these threat events.
   b Determine if anyone is looking at these excessive events in the first place.
   c If events are not being analyzed, change your policy to stop the event forwarding.
   d If the event is important, make sure that you are monitoring the number of events.

   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.
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.
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

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.

https://<localHost>:8443/remote/core.executeQuery?queryId=34&:output=terse

<table>
<thead>
<tr>
<th>count</th>
<th>Completion Time (Week)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4/27/19 - 5/3/19</td>
</tr>
<tr>
<td>2</td>
<td>5/4/19 - 5/10/19</td>
</tr>
<tr>
<td>6</td>
<td>5/11/19 - 5/17/19</td>
</tr>
<tr>
<td>1</td>
<td>5/18/19 - 5/24/19</td>
</tr>
</tbody>
</table>

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 "[...]"
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.

- `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.

```
Table 21-1  Web URL core.executeQuery Help

<table>
<thead>
<tr>
<th>Command</th>
<th>Arguments</th>
<th>Parameters</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>core.executeQuery</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></td>
<td>[database=&lt;&gt;]</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>core.executeQuery</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></td>
<td>[select=&lt;&gt;]</td>
<td>—</td>
<td>The SQUID select clause of the query; if blank, all columns are returned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[where=&lt;&gt;]</td>
<td>—</td>
<td>The SQUID where clause of the query; if blank, all rows are returned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[order=&lt;&gt;]</td>
<td>—</td>
<td>The SQUID order-by clause of the query; if blank, database order is returned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[group=&lt;&gt;]</td>
<td>—</td>
<td>The SQUID group-by clause of the query; if blank, no grouping is performed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[database=&lt;&gt;]</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></td>
<td>[depth=&lt;&gt;]</td>
<td>—</td>
<td>The SQUID depth to fetch sub-results. (default: 5).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[joinTables=&lt;&gt;]</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>
```
This diagram shows the basic requirements for a fully qualified S-Expression query.

Figure 21-1  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.

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.

```plaintext
https://<localHost>:8443/remote/core.listTables?table=<tableName>
```

This example confirms you can sort the `EPOBranchNode` table `NodeName` column data. In the `NodeName` row, `True` is listed in the `Order ?` column.

```plaintext
https://<localHost>:8443/remote/core.listTables?table=EPOBranchNode
```

This command displays this Help.

<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>
</tbody>
</table>
This Order command is used to sort the McAfee ePO branch nodes, or System Tree Group Names, in descending order.

https://<localHost>:8443//remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOLeafNode.NodeName EPOLeafNode.Tags
EPOBranchNode.NodeName)&order=(order desc EPOBranchNode.NodeName)

This is the command output.

```
OK: System Name Tags Group Name
------------------ ------------------ --------------
DP-2K12R2S-SRVR Server SuperAgents
DP-2K8ER2EPO510 Server Servers
DP-W7PIP-1 Workstation NAT Systems
DP-W7PIP-2 Workstation NAT Systems
DP-W7PIP-3 Workstation NAT Systems
DP-EN-W7E1XP-2 Workstation Lost&Found
DP-2K8AGTHDLR Server, test Agent handlers
```

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.

https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOBranchNode.NodeName (count))&group=(group EPOBranchNode.NodeName)

This is the command output.

```
OK: Group Name count
--------------------- ----- 
Agent handlers 1
Lost&Found 1
NAT Systems 3
Servers 1
SuperAgents 1
```

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.

```
OK: System Name Tags Group Name
------------------ ------------------ --------------
DP-2K8ER2EPO510 Server Servers
DP-2K8AGTHDLR Server, test Agent handlers
```
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.


This is the command output displaying the top 3 names in the list.

OK:

<table>
<thead>
<tr>
<th>System Name</th>
<th>Tags</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-2K8ER2EPO510</td>
<td>Server</td>
<td>Servers</td>
</tr>
<tr>
<td>DP-2K12R2S-SRVR</td>
<td>Server</td>
<td>SuperAgents</td>
</tr>
<tr>
<td>DP-EN-W7E1XP-2</td>
<td></td>
<td>Lost&amp;Found</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.


This is the command output with 4 common attributes.

OK:

<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,</td>
<td>Workstation</td>
</tr>
<tr>
<td>DP-W7PIP-2</td>
<td>7,</td>
<td>Workstation</td>
</tr>
<tr>
<td>DP-W7PIP-3</td>
<td>7,</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.

```
<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.enginever64%3AEPOProdPropsView_VIRUSCAN.datver %3AEPOLeafNode.LastUpdate&amp;orion.table.order.by=EPOComputerProperties.ComputerName %3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComputerProperties.Description %3AEPOLeafNode.Tags%3AEPOProdPropsView_VIRUSCAN.productversion %3AEPOProdPropsView_VIRUSCAN.hotfix%3AEPOProdPropsView_VIRUSCAN.servicepack %3AEPOProdPropsView_VIRUSCAN.enginever %3AEPOProdPropsView_VIRUSCAN.datver %3AEPOLeafNode.LastUpdate&amp;orion.table.order=az</table-uri>
    <condition-uri>query:condition?orion.condition.sexp=%28+where+%28+version_ge +EPOProdPropsView_VIRUSCAN.productversion+%28+%28+%28+%28+%228%22+%29+%29+%29+%29</condition-uri>
    <summary-uri>query:summary?pie.slice.title=EPOProdPropsView_VIRUSCAN.datver&amp;pie.count.title=EPOLeafNode&amp;orion.query.type=pie.pie&amp;orion.sum.query=true&amp;orion.sum.group.by=EPOProdPropsView_VIRUSCAN.datver&amp;orion.sum.order=desc&amp;orion.show.other=true&amp;orion.sum.aggregation=count&amp;orion.sum.aggregation.showTotal=true</summary-uri>
  </query>
</list>
```

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;</td>
</tr>
<tr>
<td>&quot;+&quot;</td>
<td>space &quot; &quot;</td>
</tr>
<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;</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.

**Exported query**

```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>
      psView_VIRUSCAN.enginever%3AEPOProdPropsView_VIRUSCAN.enginever6%3A
      EPOProdPropsView_VIRUSCAN.datver%3AEPOLeafNode.LastUpdate&amp;amp;
      orion.table.order.by=EPOComputerProperties.ComputerName% 
      orion.table.order=az&amp;amp;orion.condition=query:condition?orion.condition.sexp=%28+where+%28+version_ge+
      orion.table.order=az&amp;amp;orion.condition.query:condition?orion.condition.sexp=%28+where+%28+version_ge+
      sum.query=true&amp;amp;orion.sum.group.by=EPOProdPropsView_VIRUSCAN.datver&amp;amp;orion.sum.
      order=desc&amp;amp;orion.show.other=true&amp;amp;orion.sum.aggregation=count&amp;amp;orion.sum.aggregation.showTotal=true</table-uri>
  </query>
</list>
```

**Web URL query**

```xml
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&amp;
select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)&amp;
:output=terse&amp;
order=(order(desc EPOLeafNode.NodeName))
```

Figure 21-2  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><code>&lt;target&gt;...&lt;/target&gt;</code></td>
<td><code>target=</code>...</td>
<td>Lists the table parsed in the query.</td>
</tr>
<tr>
<td>2</td>
<td><code>sexp=</code>...</td>
<td><code>select=</code>(select...</td>
<td>Lists the S-Expressions command objects, their parameters, and joint tables.</td>
</tr>
<tr>
<td>3</td>
<td><code>order=</code>...</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:

```xml
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.

```xml
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.

```
OK:
System Name     DAT Version (VirusScan Enterprise)
--------------- ----------------------------------
DP-W7PIP-3      7465.0000
DP-W7PIP-2      7429.0000
DP-W7PIP-1      7437.0000
DP-EN-W7E1XP-2  7465.0000
DP-2K8ER2EPO510 7465.0000
DP-2K8AGTHDLR   7437.0000
DP-2K12R2S-SRVR
```

**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&amp;orion.table.order.by=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&amp;orion.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&amp;pie.count.title=EPOLeafNode&amp;orion.query.type=pie.pie&amp;orion.sum.query=true&amp;orion.sum.group.by=EPOProdPropsView_VIRUSCAN.datver&amp;orion.sum.order=desc&amp;orion.show.other=true&amp;orion.sum.aggregation=count&amp;orion.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.

```
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.

```
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.

```
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.

```
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.

```
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.

```plaintext
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.

<table>
<thead>
<tr>
<th>System Name</th>
<th>DAT Version (VirusScan Enterprise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-2K12R2S-SRVR</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>DP-EN-W7E1XP-2</td>
<td>7429.0000</td>
</tr>
<tr>
<td>DP-W7PIP-2</td>
<td>7437.0000</td>
</tr>
<tr>
<td>DP-W7PIP-1</td>
<td>7437.0000</td>
</tr>
<tr>
<td>DP-2K8AGTSDLR</td>
<td>7437.0000</td>
</tr>
<tr>
<td>DP-2K8ER2EPOS10</td>
<td>7465.0000</td>
</tr>
<tr>
<td>DP-W7TP-3</td>
<td>7465.0000</td>
</tr>
</tbody>
</table>

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
- When the agent was last updated
- 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.
   ```plaintext
   https://<localHost>:8443/remote/core.listTables?:output=terse
   ```

2. Using your text editor, type this web URL template command.
   ```plaintext
   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.
   ```plaintext
   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
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):
7 Finally, to show the output as a table, add the command `:output=terse&` after the first ampersand and rerun the command.

Confirm that your example command looks similar to the following.

```sql
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.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Agent Version (deprecated)</th>
<th>Last Communication</th>
<th>ProdProps.productFamily (VirusScan Enterprise)</th>
<th>Product Version (VirusScan Enterprise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DP-2K8ER2EPO510</td>
<td>4.8.0.887</td>
<td>6/13/14 10:21:50 AM FDT</td>
<td>VIRUSCAN</td>
<td>8.8.0.1266</td>
</tr>
<tr>
<td>DP-EN-W7E1XF-2</td>
<td>null</td>
<td>null</td>
<td>VIRUSCAN</td>
<td></td>
</tr>
<tr>
<td>DP-W7PIP-1</td>
<td>4.8.0.887</td>
<td>6/13/14 10:37:20 AM FDT</td>
<td>VIRUSCAN</td>
<td>8.8.0.1266</td>
</tr>
<tr>
<td>DP-W7PIP-2</td>
<td>4.8.0.887</td>
<td>6/13/14 10:36:56 AM FDT</td>
<td>VIRUSCAN</td>
<td>8.8.0.1266</td>
</tr>
<tr>
<td>DP-W7PIP-3</td>
<td>4.8.0.887</td>
<td>6/13/14 10:37:00 AM FDT</td>
<td>VIRUSCAN</td>
<td>8.8.0.1266</td>
</tr>
<tr>
<td>DP-2K8AGTHDLR</td>
<td>4.8.0.887</td>
<td>6/13/14 10:25:10 AM FDT</td>
<td>VIRUSCAN</td>
<td>8.8.0.1266</td>
</tr>
</tbody>
</table>
Troubleshooting for systems that connect over a VPN

Systems in the System Tree are typically identified with their unique MAC address. But, when systems connect over a VPN they can become associated with the MAC address of the VPN server instead. This can create problems when multiple systems are all connecting through the same VPN. To resolve this, McAfee recommends using the Client GUID to uniquely identify systems that use a VPN.

How systems are associated with a MAC address

The following diagram shows how two systems can be associated with the same MAC address in McAfee ePO.

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.

As a result, Client A is deleted from the System Tree because both clients are associated with the same MAC address.
Preventing MAC address conflicts by using the client GUID instead

To resolve this issue, McAfee recommends using client GUIDs instead of MAC addresses to uniquely identify systems.

First, find the Organizationally Unique Identifier (OUI) of the VPN server. The OUI is the first six digits of the MAC address.

Add the VPN server OUI to the virtual MAC vendor values. This change allows McAfee ePO to identify the VPN server and begin using the client GUID as the unique identifier for systems that connect through it.

Contents

- Add Virtual MAC Vendor
- Use the System Tree to find the MAC address of the VPN
- Create a report to find the MAC address of the VPN

Add Virtual MAC Vendor

This feature allows you to add the duplicated MAC address to the McAfee ePO database and prevent it from matching the used MAC address to another system. Virtual machines are assigned a unique MAC (Media Access Control) address in a particular host system.

Task

1. Click Menu | Configuration | Server Settings.
2. In the Server Settings page, click Virtual MAC Vendors in the Setting Categories pane.
   You see a list of vendors and their respective ID.
3. Click Edit.
4. In the Add New Virtual MAC Vendor area, enter a value in the Vendor ID field.
   The Vendor ID must consist of six characters. It can be numeric (0–9), alphabetical (A to Z), or alphanumeric (combination of numbers and alphabets). A Vendor ID cannot have special characters.
5. Enter the details in the Vendor Name/Note field.
   You can enter details such as the name of the organization, the reason to add the vendor, and you can also enter comments that you would like to add. This field does not accept these special characters:
   • {  
   • }  
   • ;  
   • <  
   • >  
   • ?
6. Click Add MAC Vendor to add more vendors.
7. Click Save.

The vendor name and ID are added to the list of vendors.

You can also edit or delete existing Vendors.
Use the System Tree to find the MAC address of the VPN

To prevent MAC address duplication when systems connect through a VPN, first determine the MAC address of the VPN server. The primary way to learn the MAC address is to access one of the systems that connects through the VPN.

Before you begin
Ensure that you have a remote connection to systems connecting to McAfee ePO through a VPN server.

Task
1. Remotely connect to a system that uses the VPN.
2. Click the McAfee Agent icon to open the McAfee Agent Status Monitor.
   If you don't see the McAfee Agent icon, you can run the application from a command line:
   1. From the command prompt, change directories to this default folder:
      C:\Program Files\McAfee\Common Framework\
   2. Type:
      CmdAgent.exe /s
      The McAfee Agent Status Monitor opens.
3. Click Collect and Send Props.
   This process collects system properties and sends the information to the McAfee ePO server.
4. From the McAfee ePO console, select Menu | Systems | System Tree.
5. Locate the system and double-click the system name.
6. Click the System Properties tab, then click Customize on the right of the display.
7. From the Properties list, find MAC Address, click Move to Top, and click Save.
   The MAC address appears at the top of the list.
8. Make note of the first six digits of the system MAC address. This is the OUI value.
   Use the OUI value in the SQL Server Management Studio to update the virtual MAC vendor ID.

Create a report to find the MAC address of the VPN

To prevent MAC address duplication when systems connect through a VPN, first determine the MAC address of the VPN server. An alternative way to learn the MAC address is to create a report and identify the systems that share an address.

Task
1. Select Menu | Reporting | Queries & Reports.
2. Click New Query to display the Result Type tab, configure these settings:
   • In the Feature Group list, select System Management.
   • In Result Types pane, select Systems.
3 Click Next.

4 From the Chart tab, configure these settings:
   • In the Summary list, select Single Group Summary Table.
   • In the Labels list, under Computer Properties, select MAC Address.

5 Click Next.

6 In the Columns tab, from the Available Columns list under Computer Properties, select MAC Address, then click Next.

7 In the Filter tab, configure these settings:
   • In the Available Properties list, expand 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.

8 Click Run.

9 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. Make note of the first six digits of the system MAC address, which is the OUI of the VPN server.

Use the OUI value in the SQL Server Management Studio to update the virtual MAC vendor ID.
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
- SNMP servers
- Additional, remote, database servers
- Syslog 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 KB87731.

**TLS 1.0 is disabled by default for communication to external servers, such as SQL Server. For more information about TLS support, see KB90222.**

**Contents**

- Register McAfee ePO servers
- Using database servers
- Register SNMP servers
- What is a syslog server?
- 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>database McAfee 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</td>
</tr>
<tr>
<td></td>
<td>instance, by providing the Instance name.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the SQL browser service is running before connecting to a</td>
</tr>
<tr>
<td></td>
<td>specific SQL instance using its instance name. Specify the port number if</td>
</tr>
<tr>
<td></td>
<td>the SQL browser service is not running.</td>
</tr>
<tr>
<td></td>
<td>Select the Default SQL server instance and type the port number to</td>
</tr>
<tr>
<td></td>
<td>connect to the SQL server instance.</td>
</tr>
<tr>
<td>SSL communication with</td>
<td>Specifies whether McAfee ePO uses SSL (Secure Socket Layer) communication</td>
</tr>
<tr>
<td>database server</td>
<td>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>
<tr>
<td></td>
<td>If you register a server with a different McAfee ePO version, this</td>
</tr>
<tr>
<td></td>
<td>information-only warning appears: Warning Version mismatch!</td>
</tr>
</tbody>
</table>
### 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**.
3 Choose a **Database type** from the drop-down list of registered types. Indicate if you want this database type to be as the default.

If there is already a default database assigned for this database type, it is indicated in the **Current Default database for database type** row.

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

5 Enter the connection specifics and 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.

What is a syslog server?

Syslog is a protocol used by network devices to send event messages to a logging server – known as a syslog server. Event log forwarding consolidates all event logs in a central location such as a syslog server. Consolidation reduces the hassle of logging into every server to check logs individually.

Syslog server must be SSL enabled. McAfee ePO server syslog client supports SyslogNG RFC 5424 + 5425 only which requires TCP, and Transport Layer Security (TLS). There is no support for UDP or unencrypted TCP syslog receivers.

How does event log forwarding work?

The McAfee Agent sends events to the Agent Handler. You need to store these events in a server. Use McAfee ePO to configure syslog server and forward events to the syslog server or store the events on the SQL database server.

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. To know how to create a syslog server, see KB87927
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. This log file includes any syslog server errors that might occur.

See also

Determine which events are forwarded to the server on page 184

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.

McAfee ePO only supports Microsoft Active Directory to synchronize and import systems into the System Tree, apply policies on those systems, and apply user-based policies based on LDAP users and groups. No other LDAP server types are supported.

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=realmdc=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.

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.
3 Shows the LDAP server user information mirrored to the McAfee ePO database.

4 Shows an Agent Handler behind the DMZ accessing the mirrored LDAP server information in the McAfee ePO database.

**Default process**

**Mirrored process**

**Figure A-1 Default and LDAP mirrored connection processes**

**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.
Issues

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

1. Open the Issues page: select **Menu | Automation | Issues**.
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**

1. Open the Issues page: select \[Menu \| Automation \| Issues.\]
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 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></td>
</tr>
<tr>
<td></td>
<td></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>
</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.
Disaster Recovery example scenarios

Contents

- Perform failover of your small and medium-sized McAfee ePO server (example)
- Perform failover of your enterprise McAfee ePO server (example)
- Small and medium-sized McAfee ePO network configuration and components (example)
- Enterprise McAfee ePO network configuration and components (example)
- How McAfee Agent responds to a restored McAfee ePO server

Perform failover of your small and medium-sized McAfee ePO server (example)

This example task shows how to use the Disaster Recovery Snapshot in the SQL database for recovery if the primary McAfee ePO server fails.

Before you begin

- If the McAfee ePO server is damaged, you must restore the SQL database from the backup before performing the failover process.
- See the Small and medium-sized McAfee ePO Disaster Recovery network configuration graphic to reference names and connections described in these steps.

Task

1. From the primary McAfee ePO server, stop these services:
   a. Click Start | Run, type services.msc, and click OK.
   b. Right-click each of the following services and select Stop:
      - McAfee ePolicy Orchestrator Application Server
      - McAfee ePolicy Orchestrator Event Parser
      - McAfee ePolicy Orchestrator Server
   c. Double-click each of the following services and change the Startup type to Disabled:
      - McAfee ePolicy Orchestrator Application Server
      - McAfee ePolicy Orchestrator Event Parser
      - McAfee ePolicy Orchestrator Server

2. (Optional) If you have remote Agent Handlers, use Windows Services on all Agent Handlers, and stop the Event Parser and Apache services. This step is only required if the primary Agent Handlers aren't used in failover situations.
3 On the restore server, install McAfee ePO using the same version as the Snapshot:
   a When prompted, click **Restore ePO from an existing database Snapshot**.
   b Point to the McAfee ePO database on SQL-DC1 or SQL-DC2 using a Windows or Active Directory account with local administrator permissions on the McAfee ePO server.
   c Use the same drive and directory location used for the McAfee ePO software on the EPO-DC1.
   d Point McAfee ePO to the SQL-DC1 or SQL-DC2, the physical node hosting the McAfee ePO database.
   e Use Windows Active Directory or Server Administration account credentials to access to the McAfee ePO database.
   f Confirm the port information is correct.
   g Provide the McAfee ePO administrator account and password.
   h Provide the Keystore Password. Recovery takes about 15 minutes, depending on the performance of the McAfee ePO server and SQL Server.

4 On the DNS server, change the CNAME record in epo.customer.net to point to the restore McAfee ePO server.

5 (Optional) If you have remote Agent Handlers, change their configuration to use epo.customer.net and to find the restore McAfee ePO server based on the CNAME.

6 Complete the McAfee ePO software installation process using the documented steps until your new McAfee ePO server is up and running.

7 Confirm your managed systems and remote Agent Handlers (if used) can connect to the restore McAfee ePO server.

---

**Perform failover of your enterprise McAfee ePO server (example)**

This example task shows how to use the Disaster Recovery Snapshot for recovery if the primary McAfee ePO server fails.

### Before you begin
- If the McAfee ePO server is damaged, you must restore the SQL database from the backup before performing the failover process.
- You must have a Snapshot and backup of the database on your SQL Server.

### Task
1 From the EPO-DC1 McAfee ePO server, stop these services:
   a Click **Start | Run**, type `services.msc`, and click **OK**.
   b Right-click each of the following services and select **Stop**:
      - McAfee ePolicy Orchestrator Application Server
      - McAfee ePolicy Orchestrator Event Parser
      - McAfee ePolicy Orchestrator Server
Double-click each of the following services and change the **Startup type** to **Disabled**:

- McAfee ePolicy Orchestrator Application Server
- McAfee ePolicy Orchestrator Event Parser
- McAfee ePolicy Orchestrator Server

2. Using Windows Services on all Agent Handlers, stop the Event Parser and Apache services. Make sure the Agent Handlers in DC1 aren't active.

3. On the SQL Server "Virtual-SQL-name," disable **Always On Group**.

4. On the DNS server, identify the physical node hosting the McAfee ePO SQL database. The recovery installation must point to the physical SQL Server (SQL-DC1 or SQL-DC2) during recovery installation, and then change the name to "Virtual-SQL-name" after recovery installation.

5. On the restore server, McAfee ePO Server-DC2, confirm McAfee ePO isn't installed. Delete McAfee ePO if it is installed.

6. On the restore server, follow the steps to install McAfee ePO:
   a. When prompted, click **Restore ePO from an existing database Snapshot**.
   b. Point to the McAfee ePO database on SQL-DC1 or SQL-DC2 using a Windows or Active Directory account with local administrator permissions on the McAfee ePO server.
   c. Use the same drive and directory location used for the McAfee ePO software on EPO-DC1.
   d. Point McAfee ePO to the SQL-DC1 or SQL-DC2, the physical node hosting the McAfee ePO database.
   e. Use Windows Active Directory or Server Administration account credentials to access to the McAfee ePO database.
   f. Confirm the port information is correct. For detailed port requirements, see **Port configuration from failed to restored McAfee ePO server**.
   g. Provide the McAfee ePO administrator account and password.
   h. Provide the Keystore Password. Recovery takes about 15 minutes, depending on the performance of the McAfee ePO server and SQL Server.
   i. Install McAfee ePO hotfixes in sequential order.

7. Change the CNAME record in the DNS for epo.customer.net to point to EPO-DC2 in DC2.

8. On the SQL Server "Virtual-SQL-name," enable **Always On Group**.

9. Reconfigure McAfee ePO to use the shared SQL resource "Virtual-SQL-name."

10. Browse to **https://epo.customer.net:8443/core/config** and change the host name of the SQL Server to "Virtual-SQL-name."

11. Make sure McAfee ePO is uninstalled on EPO-DC1.

   Follow these steps when reverting McAfee ePO back from DC2 to DC1.
Small and medium-sized McAfee ePO network configuration and components (example)

This is an example of a simple McAfee ePO network and how it recovers after a McAfee ePO server failure.

Create a Snapshot of your current McAfee ePO server and make sure the server task is finished before starting the restore process.

1 McAfee ePO server
   a  Primary McAfee ePO server — Used for day-to-day activities. The McAfee ePO snapshots of the SQL database are completed automatically or initiated manually just after updates occur.

       By default, server tasks automate snapshots every night.

   b  Restore McAfee ePO server — This server is running with only the SQL database installed. This is where you copy the Disaster Recovery snapshot and SQL database backups from the primary McAfee ePO server.

       After a primary McAfee ePO server failure, reinstall the McAfee ePO software using the restore option during the McAfee ePO setup process.

2 Shared resource — The DNS server configured with an availability name (for example, epo.customer.net) uses CNAME to point to the primary McAfee ePO server, and is configured to point to the restore McAfee ePO server after a failure.
3 SQL database servers

a Primary SQL database — Used for day-to-day activities. Use either a Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line process to copy the Disaster Recovery Snapshots and database backups daily to the Restore SQL database.

b Restore SQL database — Used for running and receiving the Disaster Recovery Snapshots and database backups daily from the Primary SQL database.

4 McAfee ePO console — Depending on the DNS server configuration, the console is connected to either the primary or restore McAfee ePO server. The console is used to manage systems, run the SQL backups, and install the McAfee ePO software.

![Diagram of McAfee ePO network configuration and components]

* McAfee ePO and SQL Database can reside on one server

Figure C-1 Small and medium-sized business McAfee ePO Disaster Recovery network configuration

Enterprise McAfee ePO network configuration and components (example)

This is an example of a complex McAfee ePO network and how it recovers after a McAfee ePO server failure. You must create a Snapshot of your current McAfee ePO server before a failover occurs. Make sure the server task is finished before starting the restore process.

1 McAfee ePO server

a McAfee ePO server-DC1 — This is the primary McAfee ePO server used for day-to-day activities. The McAfee ePO snapshots of the SQL database are completed automatically or initiated manually just after updates occur.

> By default, server tasks automate snapshots every night.
b McAfee ePO server-DC2 is installed and running in DC2 — This is the Cold Standby or recovery McAfee ePO server.

2 Shared resources
a A McAfee ePO shared resource name configured using DNS (for example, epo.customer.net) uses CNAME to point to the active McAfee ePO server, and is configured to point to McAfee ePO Server-DC1 or McAfee ePO Server-DC2.

b SQL database configured with Always on Availability Groups — The SQL Server is reachable by a virtual name of SQL Availability Group. For example, Virtual-SQL-name. The Snapshots of the SQL database are completed daily and sent to the SQL databases SQL-DC1 and SQL-DC2.

3 SQL database servers — Use SQL replication or SQL Log Shipping to copy the McAfee ePO database from the primary site SQL-DC1 to the secondary site's SQL Server SQL-DC2 in real time.

4 Agent Handlers — Agent Handler Groups and Agent Handlers in the DMZ are configured in DC1 and DC2 to use the SQL resource "Virtual-SQL-name."
   • Active-Passive Data Center strategy — Configure all Agent Handlers in DC2 to passive while DC1 is active, and make sure that all Agent Handlers in DC2 aren't running. This is only needed if the date center strategy for Agent Handlers is active-passive. The Agent Handler servers can be in "cold" standby and only turned on when a failover from DC1 to DC2 is initiated. If the Agent Handler servers are running, make sure the two Agent Handler services are stopped and disabled. The DC2 Agent Handlers listed in the Agent Handler Assignment still need to be listed as enabled, so the McAfee Agent is aware of their existence and starts looking for them if all DC1 Agent Handlers are unavailable.
   • Active-Active Data Center strategy — All services, except the McAfee ePO server must be installed and running in both data centers. With this strategy, Agent Handlers are available and running in both data centers. You must have a good network connection between the two data centers because there's heavy traffic between the Agent Handler in one data center and the SQL Server available in the other data center.

5 McAfee ESM or forensic tools — These tools can use the second SQL database to relieve the active SQL Server. These tools often only require read-only access to the McAfee ePO database, SQL-DC2, to monitor events in the database.
### Table C-1  Example DNS configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>epo.customer.net</td>
<td>CNAME</td>
<td>EPO-DC1 or EPO-DC2</td>
</tr>
<tr>
<td>EPO-DC1</td>
<td>A</td>
<td>10.1.1.100</td>
</tr>
<tr>
<td>EPO-DC2</td>
<td>A</td>
<td>10.2.2.200</td>
</tr>
</tbody>
</table>

### How McAfee Agent responds to a restored McAfee ePO server

Changes made to a restored McAfee ePO server cause minimum impact to an existing McAfee Agent. McAfee Agent communication doesn't change because the Agent Handler IP addresses and FQDN didn't change.

By default, the McAfee Agent tries connecting to the McAfee ePO server in this order, depending on the Agent Handler configuration:

1. IP address of the Agent Handler and McAfee ePO server.
2. FQDN of the Agent Handler and McAfee ePO server.
3. NetBIOS name the Agent Handler and McAfee ePO server.
If you change any of these items, make sure the McAfee Agent has a way to locate the server. For example, using the CNAME record, change the existing DNS record so it directs to the new IP address. After the McAfee Agent successfully connects to the McAfee ePO server, it downloads an updated Sitelist.xml with the current information.
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:

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

To create and self-sign a certificate to use with your McAfee ePO server, use OpenSSL for Windows software. There are many tools you can use to create a self-sign a certificate. This task describes the process using OpenSSL.

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 (ox10001)
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 pass phase 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,CCE327868DS10D1882
   4Ev9bqetekbo60Wy0cFh6o8gUbc0TDnn/cdppSeykvQBAsEhFfcF+uHLort8Kks
   b39DAqczf65kMoob19m57X/PZ+7dcTH7yXN8skfoqED7/7VZxktAEhA1Vw+wj
   ...
   ...
   im2DEkLWq3kI+6Mde0MnQFa99SnH2JzvAd6F6lBUNULLPDe3wvaGeMJ68lfAF9C3
   4+iDiT5RiF3piLpCOK+0L1Dp0g5FC723ZiDrrDuwghE5dyD1oRKLw==
   -----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]: AU
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]: 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-----
MIIDTCCAQgAwIBAgIJAJe1ldIh0GDA0GCSqGSIb3DQEBAwIBCgAwIBAgIhI8XqQXQqQXQgI
VQ5EQwJUZzEPMA0GA1UECFMGTF09OMRIwEAYDVQQHEwICRUFWRVJUT04x

The self-signed certificate is generated and stored in the path C:\ssl\certs. The self-signed certificate looks similar to the following example.

-----BEGIN CERTIFICATE-----
MIIDTCCAQgAwIBAgIJAJe1ldIh0GDA0GCSqGSIb3DQEBAwIBCgAwIBAgIhI8XqQXQqQXQgI
VQ5EQwJUZzEPMA0GA1UECFMGTF09OMRIwEAYDVQQHEwICRUFWRVJUT04x

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.
5 Browse to the server certificate file, then click Open.
   In this example, browse to \C:\ssl\certs\ and select ca.cer.

6 If needed, type the PKCS12 certificate password.

7 If needed, type the certificate alias name.

8 Browse to the private key file, then click Open.
   In this example, browse to \C:\ssl\keys\ and select ca.key.

9 If needed, type the private key password, then click Save.

10 Restart McAfee ePO for the change to take effect.

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:

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.

   Make sure that the distribution percentage is as close to 100% as possible before you continue. Otherwise, any pending systems will not receive the newly generated certificates and will be unable to communicate with the McAfee ePO after the certificates are activated. You can stay in this state for as long as is necessary to achieve sufficient saturation.

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 any separate Agent Handlers).
   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.

  ![Warning]

  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

Contents

- Use one Master Repository key pair for all servers
- Use Master Repository keys in multi-server environments

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.
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. 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.
6 On the Edit Security Keys page:
   a Next to Import and back up keys, click Import.
   b Next to Select file, browse to and select the master key pair file you saved, then click Next.
   c If the summary information appears correct, click Save. The new master key pair appears in the list next to Agent-server secure communication keys.
7 From the list, select the file you imported in the previous steps, then click Make Master. This 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 <strong>Agent-server secure communication keys</strong> list, click <strong>New Key</strong>. 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 <strong>Make Master</strong>. 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><strong>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.</strong></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 <strong>Agent-server secure communication keys</strong> list, select a key, then click <strong>Export</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>OK</strong>. Your browser prompts you to download the <strong>sr&lt;ServerName&gt;.zip</strong> file to the specified location.</td>
</tr>
<tr>
<td></td>
<td><strong>If you specified a default location for all browser downloads, this file might be automatically saved to that location.</strong></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 <strong>Import</strong>.</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 <strong>Open</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Next</strong> and review the information about the Import Keys page.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
### Designate an ASSC key pair as the master

**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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Back up all keys.</td>
</tr>
</tbody>
</table>

#### Delete ASSC keys

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.
When all agents are using the new keys, delete any unused keys.

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>
<tbody>
<tr>
<td><strong>Back up all security keys.</strong></td>
<td>1 Click <strong>Back Up All</strong> near the bottom of the page. The Backup Keystore dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>2 You can optionally enter a password to encrypt the Keystore .zip file or click <strong>OK</strong> to save the files as unencrypted text.</td>
</tr>
<tr>
<td></td>
<td>3 From the File Download dialog box, click <strong>Save</strong> to create a .zip file of all security keys. The Save As dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>4 Browse to a secure network location to store the .zip file, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Restore security keys.</strong></td>
</tr>
<tr>
<td></td>
<td>1 Click <strong>Restore All</strong> near the bottom of the page. The Restore Security Keys page appears.</td>
</tr>
<tr>
<td></td>
<td>2 Browse to the .zip file containing the security keys, select it, and click <strong>Next</strong>. The Restore Security Keys wizard opens to the Summary page.</td>
</tr>
<tr>
<td></td>
<td>3 Browse to the keys you want to replace your existing key with, then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>Restore</strong>. The Edit Security Keys page reappears.</td>
</tr>
<tr>
<td></td>
<td>5 Browse to a secure network location to store the .zip file, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Restore security keys from a backup file.</strong></td>
</tr>
<tr>
<td></td>
<td>1 Click <strong>Restore All</strong> near the bottom of the page. The Restore Security Keys page appears.</td>
</tr>
<tr>
<td></td>
<td>2 Browse to the .zip file containing the security keys, select it, and click <strong>Next</strong>. The Restore Security Keys wizard opens to the Summary page.</td>
</tr>
<tr>
<td></td>
<td>3 Browse to and select the backup .zip file, then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>Restore All</strong> at the bottom of the page. The Restore Security Keys wizard opens.</td>
</tr>
<tr>
<td></td>
<td>5 Browse to and select the backup .zip file, then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>6 Verify that the keys in this file are the ones you want to overwrite your existing keys, then click <strong>Restore All</strong>.</td>
</tr>
</tbody>
</table>
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 E-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. |
Ports overview

Contents
- Change console-to-application server communication port
- Change agent-server communication port
- Ports required for communicating through a firewall
- Port configuration from failed to restored McAfee ePO server

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:

```sql
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\McAfee ePO\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              | 443     | By default, 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. |
Port configuration from failed to restored McAfee ePO server

Use these port configurations when restoring a failed McAfee ePO server.

<table>
<thead>
<tr>
<th>Number</th>
<th>Ports</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SQL 1433 (SSL)</td>
<td>Agent Handler group to virtual SQL name</td>
</tr>
<tr>
<td>2</td>
<td>80, 443, 8443, 8444</td>
<td>Agent Handler group to McAfee ePO virtual name</td>
</tr>
<tr>
<td>3</td>
<td>8443</td>
<td>McAfee ePO virtual name to McAfee ePO console</td>
</tr>
<tr>
<td>4</td>
<td>Read only access to secondary replica</td>
<td>ESM to SQL-DC2</td>
</tr>
</tbody>
</table>
Ports overview
Port configuration from failed to restored McAfee ePO 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>
<thead>
<tr>
<th>Table G-1 Agent Handler</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default port</td>
</tr>
<tr>
<td>80</td>
</tr>
<tr>
<td>389</td>
</tr>
<tr>
<td>443</td>
</tr>
<tr>
<td>636</td>
</tr>
<tr>
<td>1433</td>
</tr>
<tr>
<td>1434</td>
</tr>
<tr>
<td>8081</td>
</tr>
<tr>
<td>8443</td>
</tr>
<tr>
<td>8444</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table G-2 McAfee Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default port</td>
</tr>
<tr>
<td>80</td>
</tr>
<tr>
<td>443</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>Note:</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>Note:</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>
Index

A
access requirements for System Tree 56
accounts
user 87
actions
Apply Tag 84
Check IP Integrity 65
Run Tag Criteria 81
Sort Now 72
Test Sort 72
used with Product Deployment 124
Active Directory
applying permission sets 91
containers, mapping to System Tree groups 72
implementation strategies 91
systems only synchronization 63
Active Directory synchronization
borders and 57
deleting systems 61, 62
duplicate entry handling 61
Synchronize Now action 61
systems and structure 62
tasks 61
to System Tree structure 72
types 62
adding comments to issues 333
administrators
about 99
contacted automatically to stop DAT release 118
contacted automatically with compliance report 223
permission needed for Disaster Recovery 50
permissions 99
recommended monthly task to review IDs 285
source sites, configuring 236
Administrators
creating groups 58
agent
configuring policies to use repositories 240
configuring proxy settings for 239
deployment credentials 209
first call to server 65
grouping 271
grouping by assignment rules 272
GUID and System Tree location 65
agent (continued)
maintenance 207
traffic direction and ports 367
agent communication port 209
Agent Handlers
about 253
assigning agents 269
assignment priority 272
assignments 264
authentication modes 253
behind a DMZ 260
component in McAfee ePO 14
configure priority 264
configure virtual groups 263
deployment 262
eliminates multiple McAfee ePO servers 257
enable and disable from Handlers List 263
failover protection 258
frequently asked questions 273
hardware, software, and port requirements 265
how they work 253
LDAP access 327
managing assignments 270
moving agents between 271
multiple 253
ports used to communicate through firewall 363
priority in sitelist file 268
software installation 266
traffic direction and ports 367
user interface 263
virtual settings 263
why use them 255
Agent Status Monitor, to collect and send properties 319
agent-server communication
interval reduced with LDAP mirroring 327
secure communication keys (ASSC) 352
System Tree sorting 64
agent-server communication interval
adjusting 208
change default 208
Agent-server communication interval
change setting 137
agent-server communication port, change 360
agent-server secure communication
   about 14
agent-server secure communication (ASSC)
   about 349
   using different key pairs for servers 355
   using one key pair 354
   viewing systems that use a key pair 354
   working with keys 352
agent-server secure communication keys
   export and import keys 77
   with Transfer Systems 76
agents
   and SuperAgent repositories 232
   assignment to Agent Handlers 264
   finding inactive agents 218
   finding older versions 216
   updating using Product Deployment 216
AIA, See Authority Information Access
Apache server 230
API, reports
   run with the web API 302
   run with web API 302
   using API ID number example report 310
   using API table objects, commands, and arguments example report 313
   using API XML data example report 311
   using parsed query export data to create web URL queries 308
   using S-Expressions in web URL queries 311
   using the McAfee command framework 302
   using the web URL Help 303
Applied Policies, creating queries 158
Apply Tag action 81
ASSC
   agent-server secure communication 14
ASSC keys, See agent-server secure communication keys
assign client tasks 165
assigning issues 333
assignment rules
   agents and handlers 272
Audit Log
   about 95
   deleting old entries 95
   purge automatically 212
   recommended monthly task 285
   used with Product Deployment 124
   viewing user actions 95
authentication
   certificate-based 96
   configuring for Windows 90
   authentication, certificate-based 96
   authentication, configuring for Windows 89
Authority Information Access, defined 96
authorization strategies 91
automatic responses (continued)
   actions 190
   component in McAfee ePO 14
   configuring 190
   interaction with System Tree 80
   notification intervals 188
   planning 183
   rule defaults 183
   rules 183
   setup 181
   used to automate DAT file testing 118
automation
   copy files from Evaluation branch to Current 114
   create compliance query and report 221
   pull and copy DAT updates from McAfee 113
   pulling content into repositories 214
   purge events server task 212
B
back up and restore process for SQL database 289
backups
database 278
bandwidth
   calculation for repository updates 235
   considerations for event forwarding 184
   considerations for pull tasks 251
   distributed repositories and 226
   replication tasks and 251
best practice
   duplicating policies before assigning 139
   policy assignment locking 139
best practices
   importing Active Directory containers 72
   product deployment 166
   System Tree creation 67
branches
   Change Branch action 177
   Current 111
   deleting DAT and engine packages 110
   Evaluation 177
   manually moving packages between 110
   Previous 109
   types of, and repositories 228
Broken Inheritance
   creating queries 158
C
CA, See certification authority
catch-all groups 65
certificate authentication
   convert PVK to PEM file 347
   creating a self-signed certificate 343
   signed by third-party certificate authority 343
configuration (continued)
  client event summary queries 296
  custom queries 294
  disabling 1051 and 1059 events 215
  event purging 212
  event purging with a query 213
  Global Updating limitations 235
  queries with tables 298
  system list on tag groups 83
  threat event summary queries 296

console
  McAfee ePO 14

contacts
  responses and 190

CPUs
  over-utilized 275, 276

creating issues 332

credentials
  caching deployment 209
  changing, on distributed repositories 250
  modifying database registrations 324

criteria-based tags
  applying 85, 86
  sorting 70

CRL, See certificate revocation list

Cron syntax used with server tasks 163

Current branch
  checking in update packages 111
  defined 228

custom logon messages 94

D

dashboard monitors
  configuring 29
  moving and resizing 30

dashboards 329
  configuring for exported reports 47
  configuring monitors 29
  create Snapshot 51
  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 175
  daily task 176
  deployment 168
  from source sites 236

certificates
  authenticating with 96
  CA 96
  client 96
  replacing 96
  revoking client 98
  server 96

certification authority 96

Change Branch action 177

charts (See queries) 36

Check IP Integrity action 65

client certificates 96

client events
  create custom queries 298
  creating summary queries 296
  purge automatically 212

client tasks
  about 164, 165
  assignment 165
  compared with product deployment projects 123
  comparing 178
  creating 178
  editing settings for 178
  part of product deployment 121
  view 176
  viewing assignment on a specific system 179

clients
  converting to SuperAgents 232
  disappear from System Tree 317

compare client tasks 178

compare policies 145

compliance
  automate query and report processes 221
  create server task to run compliance queries 221
  creating a query for 300
  generating events 300
  report part of daily tasks 281
  reports 223
  running task to deliver report 223

components
  Disaster Recovery 50
  repositories, about 226

configuration
  agent-server communication interval 208
  automatic updates of DAT and product files 214
DAT file updating (continued)
in master repository 228
scheduling a task 176
DAT files
automate DAT file testing 113, 115
creating a compliance query 221
deleting from repository 110
deploying to repositories 235
evaluating 177
overview of automatic testing process 111
pull server task 113
repository branches 110
test before deployment 115
update with Global Updating 235
updating automatically 213
using repositories 230
Data Migration Tool, used for product compatibility check 105
Data Rollup server task 299
database servers
editing registrations 324
registering 323
removing 324
traffic direction and ports 367
using 323
databases
back up and restore process 289
backup weekly tasks 284
component in McAfee ePO 14
determining server and name 292
Disaster Recovery 50
maintaining 278
multi-server querying 299
purge events automatically 212
queries and retrieving data 35
reindex 278
restoring the SQL 288
scheduling Snapshot 288
test connection 279
deleting issues 333
deployment
Agent Handler considerations 262
checking in packages manually 109
global updating 128
installing products 173, 174
package security 166
products and updates 168
supported packages 166
tasks 166
to repositories 235
view 124
view assigned client task 176
detection definition files
DAT files 230
Directory (See System Tree) 72
Disaster Recovery
components 50
configuring snapshots 288
information needed for 289
Keystore encryption passphrase 50
server settings 54
server task 288
Snapshot 49
what it is 49
Disaster Recovery Snapshot
used during software restore 52
distributed repositories
about 226
adding to ePolicy Orchestrator 243
automatically pull and copy DAT updates from McAfee 113
changing credentials on 250
component in McAfee ePO 14
configuring agent policies 240
creating and configuring 243
creating in SuperAgents 233
deleting 246
deleting SuperAgent repositories 242
different types 230
ingoing existing 246
enabling folder sharing 246
folder, creating 243
how agents select 252
limited bandwidth and 226
part of weekly tasks 284
replicated with an automatic content pull 213
replicating packages to SuperAgent repositories 242
SuperAgent, tasks 241
unmanaged, copying content to 247
DNS
used to find the ePolicy Orchestrator server 265
domain synchronization 57
duplicate entries in the System Tree 73
duplicate GUID
recommended monthly task 285
run server task 211
E
editing database server registrations 324
editing issues 333
enforcement, See policy enforcement
global updating
checking in manually 111
deployment packages 168
from source sites 236
in master repository 228
scheduling a task 176
global updating
checking in manually 111
deployment packages 168
from source sites 236
in master repository 228
scheduling a task 176
engines
deleting from repository 110
repository branches 110
extension files, installing 109

F
failover protection using Agent Handlers 258
fallback sites
about 226
configuring 236
deleting 238
eedit existing 238
switching to source 237
features, McAfee ePO 13
filters
creating 21
custom 21
list 21
overview 21
query results 36
setting for response rules 189
used with Policy Assignment Rules 147
used with Product Deployment 126
firewall
ports used to communicate through to server 363
fragmentation in the database 278
frequently asked questions about Agent Handlers 273
FTP repositories 230
creating and configuring 243
dediting 246
enable folder sharing 246
G
geographic borders, advantages of 57
global unique identifier (GUID) 65
global updating
contents 240
enabling 128
process description 127
requirements 127
Global Updating, about 235
groups
Agent Handlers 263
catch-all 65
configuring criteria for sorting 70
controlling access 99
creating manually 68
criteria-based 65
defined 58
importing NT domains 73
in the System Tree 61
moving systems manually 76
My Group 59
of SuperAgents 232
operating systems and 58
pastin policy assignments to 155
policies, inheritance of 60
groups (continued)
  policy enforcement for a product 143
  sorting criteria 70
  sorting, automated 58
  updating manually with NT domains 75
  using IP address to define 57
  viewing policy assignment 157
GTI, See McAfee Global Threat Intelligence
GUIDs
  finding duplicates 211

H
handler assignment
  editing priority 272
  managing 270
handler groups
  about 268
  creating 270
  deleting 271
  editing settings 271
handlers
  creating groups 270
  grouping agents 273
  moving agents between 271
  priority 268
Handlers List, enable, and disable Agent Handlers 263
HTTP repositories
  about 231
  creating and configuring 243
  editing 246
  enabling folder sharing 246

I
IIS
  Microsoft IIS server 230
importing
  basics 330
  dashboards 27
  permission sets 101
inactive agent
  finding 217
  query 218
  removed as part of weekly tasks 284
inheritance
  and policy settings 139
  broken, resetting 158
  defined 60
  viewing for policies 158
installation
  Agent Handler software 266
interface
  main menu 17
  navigation 17
  shortcut bar 17
Internet Explorer
  configuring proxy settings 239
  intervals
    between notifications 188
IP address
  as grouping criteria 57
  range, as sorting criteria 70
  restricting user sessions to a single 94
  sorting and checking overlap 65
  sorting criteria 67, 70
  subnet mask, as sorting criteria 70
  used to sort the System Tree 61
issues
  adding comments 333
  assigning 333
  creating 332
  creating automatically from responses 332
  deleting 333
  editing 333
  managing 331
  removing outdated 332
  viewing 331
  viewing details 333

K
keys, See security keys
Keystore encryption passphrase
  Disaster Recovery 50
  setting 54

L
LAN connections and geographical borders 57
language packages, See agent
lazy caching, SuperAgent configuration 232
LDAP servers
  authentication strategies 91
  McAfee ePO component 14
  mirroring overview 327
  registering 326
lists
  filtering 21
  searching 22
lists, working with 21
load balancing Agent Handlers 258
local distributed repositories 247
log on and log off 17
logon messages 94
Lost and Found group 59

M
main menu
  navigating in the interface 17, 18
maintenance
  periodic tasks 286
maintenance (continued)
recommended daily 281
Maintenance Plan, See database maintaining malware events
count systems cleaned per week 219
create query to find malware events per subnet 220
measuring 219
per subnet 220
send Automatic Response 118
managed systems
deployment tasks for 173
global updating and 226
installing products on 174
policy management on 137
rollup querying 299
sorting, criteria-based 63
tasks for 173
viewing policy assignment 158
Master Repository
about 226
checking in packages manually 111
communicating with source sites 238
configuring proxy settings 239
key pair for unsigned content 350
on ePolicy Orchestrator 230
part of product deployment 121
security keys in multi-server environments 351
updating with pull tasks 251
using replication tasks 251
McAfee Agent
agents 14
McAfee Agent Status Monitor, to collect and send properties 319
McAfee Endpoint Security
restriction for Global Updating 235
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 281
McAfee recommendations
create a Rollup Data server task 299
deploy agents when importing large domains 73
evaluate borders for organization 57
phased rollout for Product Deployment 166
schedule replication tasks 251
System Tree planning 56
use global updating 127
use IP addresses for sorting 57
use tag-based sorting criteria 58
menu, See main menu
menu-based navigation 17
message
custom logon 94
Microsoft
Windows Reliability and Performance Monitor 275
Windows Task Manager 275
Microsoft IIS server 230
Microsoft SQL database
database 14
Microsoft Windows Resource Kit 69
monitors
configuring 29
default refresh interval 30
Disaster Recovery Snapshot status 50
using 25
multiple McAfee ePO servers
policy sharing 146
My Group 59
My Organization group of System Tree 59
N
navigation
main menu 17
menu-based 17
shortcut bar 18
NETDOM.EXE utility, creating a text file 69
network bandwidth, See System Tree organization
New Group wizard, creating new groups 39
node counts
and repositories 232
notification interval 188
notification rules, importing .MIB files 187
notifications
assigning permissions 185
event forwarding 184
how they work 80
recipients 80
registered executables, managing 187, 205
SNMP servers 324
NT domains
importing to manually created groups 73
synchronization 63, 73
updating synchronized groups 75
O
OAS, See on-access scan
OCSP, See Online Certificate Status Protocol
ODS, See on-demand scan
on-access scan, recommended daily task 281
on-demand scan
recommended daily task 281
recommended weekly task 284
schedule for the test group 117
on-demand scan (continued)  
used to automate DAT file testing 116  

Online Certificate Status Protocol, another method to check a certificate's authenticity 96  

operating systems  
Agent Handlers 265  
for repositories 230  
grouping 58  
legacy systems (Windows 95, Windows 98) 58  

P  
packages  
checking in manually 109  
configuring deployment task 174  
moving between branches in repository 110  
part of product deployment 121  
security for 166  
passwords  
log on and log off 17  
patches  
deployment packages for products and updates 166  
using repositories 230  
Performance Monitor  
finding performance problems 276  
using 276  
permission sets 329  
applying to Active Directory groups 91  
assigning to reports 47  
example 99  
interaction with users and groups 99  
managing 101  
mapping to Active Directory groups 89  
System Tree 56  
permissions  
administrator 99  
assigning for notifications 185  
assigning for responses 186  
for queries 34  
to dashboards 26  
personal settings, categories 18  
policies 329 (continued)  
McAfee Agent policy for a DAT test group 115  
ownership 139, 157  
set the ASCI 208  
settings, viewing 156  
viewing 137  
policy assignment  
copying and pasting 155  
disabled enforcement, viewing 157  
group, assigning to 153  
locking 139  
Policy Catalog 139  
systems, assigning to 154  
viewing 156–158  
policy assignment rules  
about 140  
and multi-slot policies 140  
creating 147  
deleting and editing 147  
editing priority 147  
priority 140  
rule criteria 140  
system-based 140  
system-based policies 141  
user-based 140  
user-based policies 141  
viewing summary 147  
Policy Catalog  
manage policies using policy history entries 144  
manage policy history permissions 144  
page, viewing 137  
policy enforcement  
enabling and disabling 142  
viewing assignments where disabled 157  
when policies are enforced 137  
policy management  
assigning policies 137  
creating queries 158  
using groups 58  
policy sharing  
designating 146  
multiple McAfee ePO servers 146  
using registered server 146  
using server tasks 146  
ports  
agent communication 209  
console-to-application server 359  
used and traffic direction 367  
used for Agent Handlers 265  
used to communicate through firewall to server 363  
used with Agent Handler behind DMZ 260  
Previous branch  
defined 228  
moving DAT and engine packages to 110  
saving package versions 109
replication (continued)
- disabling of selected packages 245
replication tasks
- full vs. incremental 251
- updating master repository 251
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 47
- configuring text elements 43
- creating 33, 41
- creating custom queries 294
- 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 319
- viewing output 46
reports, using API
- created using S-Expressions in web URL queries 304
- example created with ID number 310
- example created with table objects, commands, and arguments 313
- example created with XML data 311
- parsing query with web URL queries 308
- running 302
- using the McAfee command framework 302
- using the web URL Help 303
reports, using user interface
- creating 293
- creating custom queries 294
- include query output 223
repositories 329 (continued)
- master, configuring proxy settings for 239
- pull content automatically 214
- replication and selection of 252
- security keys 349, 351
- source site 226
- SuperAgent 232
- types of 226
- UNC 246
- UNC shares 231
- unmanaged, copying content to 247
- update with Global Updating 235
- used to automate DAT file testing 115
- what they do 225
repository list files
- about 234
- adding distributed repository to 243
- exporting to 249
- importing from 250
- priority of Agent Handlers 268
- SiteList.xml, uses for 234
- working with 248
Response Builder 190
response rules
- Description page 189
- setting filters for 189
- setting thresholds 189
responses 329
- actions 190
- assigning permissions 186
- configuring 187, 190, 205
- configuring to automatically create issues 332
- contacts for 190
- event forwarding 184
- rules 183
- SNMP servers 187
responses, automatic
- about 181
restore
- ePolicy Orchestrator software 52
- restore process 52
rules
- configuring contacts for responses 190
- defaults for automatic responses 183
- setting up for notifications, SNMP servers 187
Run Tag Criteria action 81
S
scaling McAfee ePO
- using Agent Handlers 255, 257
- using repositories 225, 257
scheduling
- applying criteria-based tags 86
- automatic updates of DAT and product files 214
- Disaster Recovery Snapshot 288
scheduling (continued)
  event purging 212, 213
  purging the event log 291
  server task for policy sharing 146
  server tasks with Cron syntax 163

security certificate
  creating a self-signed certificate 343

security keys
  agent-server secure communication (ASSC) 349, 352
  ASSC, working with 352
  for content from other repositories 350
  general 349
  master keys in multi-server environments 351
  private and public 350
  using one master key 350

selected packages
  avoid replication of 245
  disabling replication of 245

server certificates
  migrate certificates to hash algorithm 347

server settings
  agent deployment credentials 209
  certificate-based authentication 96–98
  dashboards 28, 30
  Disaster Recovery 54
  email server 183
  event filtering 184
  event notifications 184
  example setting 20
  global updating 128, 240
  Internet Explorer 239
  logon message 94
  notifications 188
  overview 18
  ports 209
  printing and exporting 47
  Product Compatibility List 106
  proxy settings 239
  security keys 350–352, 354, 355
  source sites 236–238, 250
  System Tree sorting 71
  User Session 94

Server Settings 20, 318
Server Task Builder 86
Server Task Log
  removing outdated tasks 162
  Status column 161
  viewing server tasks 161

server tasks
  about 161
  creating 162
  Data Rollup 299
  Disaster Recovery 288
  pull DAT files 113
  purge the logs 212

server tasks (continued)
  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 61
  viewing 161

servers
  back up and restore process 289
  database 323
  Disaster Recovery 50, 289
  finding performance problems 275, 276
  hardware upgrade using Disaster Recovery 49
  master repository key pair 350
  recommended best practices 280
  registering additional servers 321
  registering LDAP servers 326
  settings and controlling behavior 18
  SNMP, and responses 187
  supported server types 321
  traffic direction and ports 367
  transferring systems 79
  types you can register 321

shortcut bar
  customizing 18

sitelist files 268

sites
  deleting source or fallback 238
  editing existing 238
  fallback 226, 236
  switching source and fallback 237

Snapshot 52
  create from Dashboard 51
  create from Web API 51
  Dashboard monitor 50
  part of Disaster Recovery 49
  scheduling defaults 288

snapshots
  configuring 288

SNMP servers
  registering 324
  responses 187

Software Catalog 103
  about 103
  checking in extensions 104
  checking in packages 104
  contents 103
  evaluation software 104
  licensed software 104
  part of weekly tasks 284
  product compatibility 105
  recommended weekly task 284
Software Catalog 103 (continued)
removing extensions 104
removing packages 104

Sort Now action 63
sorting criteria
configuring 70
for groups 70
groups, automated 58
IP address 65, 70
sorting systems into groups 63
tag 70
tag-based 58, 65

source sites
about 226
configuring 236
creating 236
deleting 238
editing existing 238
fallback 226
importing from SiteMgr.xml 250
product updates and 226
switching to fallback 237
update packages and 168

SQL database
back up and restore process 289
databases 14
Disaster Recovery 50
maintaining 288
ports used to communicate through firewall 363
restoring the database 288
scheduling Snapshot 288

SQL Server
determining database server and name 292
SQL servers, See databases
SQL Servers
backup file 52
Status Monitor, to collect and send properties 319
subgroups
and policy management 73
criteria-based 65

subnets, as grouping criteria 57
SuperAgent repositories
creating 241
deleting 242
global updating requirements 127
replicating packages to 242
tasks 241
SuperAgent systems
assign SuperAgent policy to SuperAgent group 233

SuperAgents (continued)
ports used to communicate through firewall 363
synchronization
Active Directory and 63
defaults 65
deploying agents automatically 62
excluding Active Directory containers 62
NT domains 63
preventing duplicate entries 63
scheduling 75
Synchronize Now action 61
systems and structures 62
systems only, with Active Directory 63

syslog server
registering 325

System Tree
access requirements 56
assigning policies to a group 153
clients disappear 319
configuring SuperAgent group 232
create group for DAT file testing 115
create SuperAgents group 233
creation, automated 57
criteria-based sorting 63
defined 58
deleting inactive systems 218
deleting systems from 58
grouping agents 273
inherence 60
Lost and Found group 59
My Group 59
My Organization level 59
permission sets 56
populating groups 67
system information details 66

System Tree organization
add systems to groups 68
borders in your network 57
creating groups 67
duplicate entries 73
importing Active Directory containers 72
importing systems and groups 70
mapping groups to Active Directory containers 72
moving systems to groups manually 76
network bandwidth 57
operating systems 58
planning considerations 56
selecting multiple items 23
using subgroups 73

System Tree sorting
default settings 65
enabling 71
IP address 65
ordering subgroups 65
server and system settings 64
System Tree sorting (continued)
tag-based criteria 65
System Tree synchronization
scheduling 75
to Active Directory structure 72
system-based policies
about 141
criteria 141
systems 329
assigning policies to 154
exporting from the Systems Tree 69
pasting policy assignments to 155
policy enforcement for a product 143
sorting into groups 72
viewing detailed information 66
viewing policy assignment 158

T
table row, select checkboxes 22
tables, working with 21
Tag Builder wizard 81
Tag Catalog 81
tag-based sorting criteria 58, 65
tags 329
applying 85, 86
create, delete, and change subgroups 82
creating with Tag Builder wizard 81
criteria-based 63
criteria-based sorting 70edit, delete, and move 82
excluding systems from automatic tagging 83
group sorting criteria 58
manual application of 84
policy assignment based on 141
tags, subgroups
create, delete, and change 82
selecting multiple items 23
tasks 329
automatically pull and copy DAT updates from McAfee 113
copying files from Evaluation branch into Current 114
find inactive agents 217
Inactive Agents task 218
periodic 286
pull content automatically 214
purge events 285
purge events automatically 212
purge events with a query 213
recommended daily 281
recommended monthly 285
recommended weekly 284
running compliance queries 221
scheduling on-demand scan of test group 117
to run and deliver a report 223
Test Sort action 63

Threat Event Log
common event format 290
viewing and purging 291
ticketing server 14
Ticketing with McAfee ePO 334
tools, third party
use Windows Explorer to check ePolicy Orchestrator events 277
Windows Performance Monitor 276
troubleshooting
client certificate authentication 99
finding inactive systems 217
product deployment 166
SQL database connectivity 279
VPN system connection problem 317

U
UBP, See user-based policies
UNC share repositories 231
creating and configuring 243
editing 246
enabling folder sharing 246
using recommendations 246
Universal Naming Convention, See UNC share repositories
unmanaged repositories 230
updates
checking in manually 109
client tasks 175
considerations for creating tasks 175
DAT files and products automatically 213
deployment packages 168
package signing and security 166
packages and dependencies 166
scheduling an update task 176
source sites and 226
updating
automatically, with global updating 128
DATs and Engine 168
deployment tasks 166
global, process 127
process description 168
user accounts 87
user actions
removing outdated 95
viewing 95
user menu, navigating in the interface 17
user-based policies 327
about 141
criteria 141
users
about 87
permission sets and 99
restricting to a single IP address 94
utilities
   NETDOM.EXE, creating a text file 69

V
viewing issue details 333
Virtual MAC Vendors 20, 318
virtual machines
   used for automatic DAT file testing 115
VPN
   server OUI 319
   system connection problem 317

VPN connections and geographical borders 57

W
WAN connections and geographical borders 57
Windows
   authentication, configuring 89, 90
Windows authentication
   enabling 90
   strategies 91
Windows Reliability and Performance Monitor 275, 276
Windows Task Manager 275