Product Guide

McAfee ePolicy Orchestrator Cloud
COPYRIGHT
© 2017 McAfee LLC

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

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>7</td>
</tr>
<tr>
<td>About this guide</td>
<td>7</td>
</tr>
<tr>
<td>Audience</td>
<td>7</td>
</tr>
<tr>
<td>Conventions</td>
<td>7</td>
</tr>
<tr>
<td>Find product documentation</td>
<td>8</td>
</tr>
<tr>
<td><strong>1 Managing security with McAfee ePO Cloud</strong></td>
<td>9</td>
</tr>
<tr>
<td>Benefits of McAfee ePO Cloud</td>
<td>9</td>
</tr>
<tr>
<td>Differences between McAfee ePO and McAfee ePO Cloud</td>
<td>9</td>
</tr>
<tr>
<td>Sign up for a free trial</td>
<td>9</td>
</tr>
<tr>
<td>How McAfee ePO Cloud works</td>
<td>10</td>
</tr>
<tr>
<td><strong>2 Getting started with McAfee ePO Cloud</strong></td>
<td>13</td>
</tr>
<tr>
<td>Preparing for setup and installation</td>
<td>14</td>
</tr>
<tr>
<td>Activate your account</td>
<td>14</td>
</tr>
<tr>
<td>Log on to McAfee ePO Cloud</td>
<td>15</td>
</tr>
<tr>
<td>Reset a forgotten password</td>
<td>15</td>
</tr>
<tr>
<td>Choose an installation option</td>
<td>16</td>
</tr>
<tr>
<td>Install protection</td>
<td>16</td>
</tr>
<tr>
<td>Customize installation</td>
<td>16</td>
</tr>
<tr>
<td>Install protection on other computers</td>
<td>17</td>
</tr>
<tr>
<td>Confirm system management</td>
<td>18</td>
</tr>
<tr>
<td>Contact support</td>
<td>19</td>
</tr>
<tr>
<td>Provide feedback</td>
<td>19</td>
</tr>
<tr>
<td><strong>3 Manage your account</strong></td>
<td>21</td>
</tr>
<tr>
<td>Edit your user profile and change your password</td>
<td>21</td>
</tr>
<tr>
<td>Enable two-factor authentication</td>
<td>22</td>
</tr>
<tr>
<td>Secure your user session with two-factor authentication</td>
<td>23</td>
</tr>
<tr>
<td>View your subscription information</td>
<td>24</td>
</tr>
<tr>
<td>Transfer licenses from another account to your account</td>
<td>24</td>
</tr>
<tr>
<td>Personal settings categories</td>
<td>25</td>
</tr>
<tr>
<td>Manage user accounts</td>
<td>25</td>
</tr>
<tr>
<td><strong>4 Monitoring the health of your network</strong></td>
<td>27</td>
</tr>
<tr>
<td>Navigating the interface</td>
<td>27</td>
</tr>
<tr>
<td>Using the shortcut bar</td>
<td>27</td>
</tr>
<tr>
<td>Customizing the shortcut bar</td>
<td>29</td>
</tr>
<tr>
<td>Working with lists and tables</td>
<td>29</td>
</tr>
<tr>
<td>Filter a list</td>
<td>29</td>
</tr>
<tr>
<td>Search for specific list items</td>
<td>30</td>
</tr>
<tr>
<td>Clicking table row checkboxes</td>
<td>30</td>
</tr>
<tr>
<td>Selecting items in tree lists</td>
<td>31</td>
</tr>
<tr>
<td>Using dashboards and monitors</td>
<td>31</td>
</tr>
<tr>
<td>Specify the first-time dashboard</td>
<td>31</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing events</td>
<td>31</td>
</tr>
<tr>
<td>The Threat Event Log</td>
<td>32</td>
</tr>
<tr>
<td>Determine how events are forwarded</td>
<td>33</td>
</tr>
<tr>
<td>Server settings</td>
<td>34</td>
</tr>
<tr>
<td><strong>5 Generating queries and reports</strong></td>
<td>35</td>
</tr>
<tr>
<td>Introduction to queries</td>
<td>35</td>
</tr>
<tr>
<td>Run a query</td>
<td>36</td>
</tr>
<tr>
<td>Export query results to other formats</td>
<td>36</td>
</tr>
<tr>
<td>Custom queries</td>
<td>37</td>
</tr>
<tr>
<td>Query Builder</td>
<td>37</td>
</tr>
<tr>
<td>Manage custom queries</td>
<td>38</td>
</tr>
<tr>
<td>Introduction to reports</td>
<td>39</td>
</tr>
<tr>
<td>Run reports</td>
<td>39</td>
</tr>
<tr>
<td>View report output</td>
<td>39</td>
</tr>
<tr>
<td><strong>6 Setting up automatic responses</strong></td>
<td>41</td>
</tr>
<tr>
<td>Response planning</td>
<td>41</td>
</tr>
<tr>
<td>Create and edit Automatic Response rules</td>
<td>41</td>
</tr>
<tr>
<td>Define a rule</td>
<td>42</td>
</tr>
<tr>
<td>Set filters for the rule</td>
<td>42</td>
</tr>
<tr>
<td>Set Aggregation and grouping criteria for the rule</td>
<td>42</td>
</tr>
<tr>
<td>Configure the actions for an automatic response rule</td>
<td>43</td>
</tr>
<tr>
<td><strong>7 Organizing systems</strong></td>
<td>45</td>
</tr>
<tr>
<td>System Tree structure</td>
<td>45</td>
</tr>
<tr>
<td>My Organization group</td>
<td>45</td>
</tr>
<tr>
<td>The My Group subgroup</td>
<td>46</td>
</tr>
<tr>
<td>Lost and Found group</td>
<td>46</td>
</tr>
<tr>
<td>System Tree groups</td>
<td>46</td>
</tr>
<tr>
<td>Inheritance</td>
<td>47</td>
</tr>
<tr>
<td>Considerations when planning your System Tree</td>
<td>48</td>
</tr>
<tr>
<td>Environmental borders and their impact on system organization</td>
<td>48</td>
</tr>
<tr>
<td>Subnets and IP address ranges</td>
<td>48</td>
</tr>
<tr>
<td>Operating systems and software</td>
<td>48</td>
</tr>
<tr>
<td>Tags and systems with similar characteristics</td>
<td>49</td>
</tr>
<tr>
<td>Criteria-based sorting</td>
<td>49</td>
</tr>
<tr>
<td>IP address sorting criteria</td>
<td>50</td>
</tr>
<tr>
<td>Tag-based sorting criteria</td>
<td>50</td>
</tr>
<tr>
<td>Group order and sorting</td>
<td>50</td>
</tr>
<tr>
<td>Catch-all groups</td>
<td>50</td>
</tr>
<tr>
<td>How a system is added to the System Tree when sorted</td>
<td>51</td>
</tr>
<tr>
<td>Create and populate System Tree groups</td>
<td>52</td>
</tr>
<tr>
<td>Create groups manually</td>
<td>52</td>
</tr>
<tr>
<td>Add sorting criteria to groups</td>
<td>52</td>
</tr>
<tr>
<td>Enable or disable System Tree sorting on systems</td>
<td>53</td>
</tr>
<tr>
<td>Sort systems manually</td>
<td>53</td>
</tr>
<tr>
<td>Move systems within the System Tree</td>
<td>54</td>
</tr>
<tr>
<td>Remove a system from the System Tree</td>
<td>54</td>
</tr>
<tr>
<td><strong>8 Applying tags</strong></td>
<td>57</td>
</tr>
<tr>
<td>Create tags</td>
<td>57</td>
</tr>
<tr>
<td>Manage tags</td>
<td>58</td>
</tr>
<tr>
<td>Export and import tags</td>
<td>59</td>
</tr>
<tr>
<td>Create, delete, and modify tag subgroups</td>
<td>59</td>
</tr>
<tr>
<td>Exclude systems from automatic tagging</td>
<td>60</td>
</tr>
</tbody>
</table>
Apply tags to selected systems .................................................. 60
Clear tags from systems ................................................................. 61
Apply criteria-based tags to all matching systems ....................... 61

9 Assigning policies 63
About policies ............................................................................. 63
When policies are applied ......................................................... 63
How policies are applied .............................................................. 63
Policy ownership ......................................................................... 64
Policy assignment rules ............................................................... 64
Policy assignment rule priority .................................................... 65
User-based policy assignment ....................................................... 65
System-based policy assignment ................................................... 65
Create and manage policies ......................................................... 65
Create a policy from the Policy Catalog page ......................... 66
Manage an existing policy on the Policy Catalog page ............. 66
Enforcing product policies ............................................................ 67
Manage policy history ................................................................. 68
Compare policies .......................................................................... 69
Create and manage policy assignment rules .............................. 69
Create policy assignment rules ..................................................... 70
Manage policy assignment rules .................................................... 70
Export and import policy assignment rules ............................... 71
Manually assign policies .............................................................. 71
Assign policies to managed systems ........................................... 71
Copy and paste policy assignments ............................................. 73
View policy information ............................................................... 75
View groups and systems where a policy is assigned ............... 75
View policy settings ................................................................. 75
View assignments where policy enforcement is disabled .......... 76
View policies assigned to a group ............................................... 76
View policies assigned to a specific system ............................. 76
View policy inheritance for a group ............................................. 76
View and reset broken inheritance ............................................. 77

10 Deploying products 79
Benefits of product deployment projects ................................. 79
The Product Deployment page .................................................... 80
Viewing Product Deployment audit logs .................................... 81
View product deployment ............................................................ 81
Deploy products using a deployment project ............................... 82
Monitor and edit deployment projects ........................................... 83
Manage Agent Deployment URLs ................................................ 84
Uninstall product software from systems ................................. 85
The Audit Log ............................................................................. 86
View user actions ........................................................................ 86
Remove outdated actions from the Audit Log ....................... 87

11 Client tasks 89
How the Client Task Catalog works .......................................... 89
Updating tasks ............................................................................ 89
View assigned client task ............................................................. 90
Update managed systems regularly with a scheduled update task ........................................................................................................ 90
Manage client tasks ..................................................................... 91
Create client tasks ....................................................................... 91
Edit client tasks .......................................................................... 92
## Server and client tasks

### Client tasks
- How the Client Task Catalog works ........................................ 95
- Updating tasks ............................................................................. 95
- Manage client tasks ....................................................................... 97

### Server tasks
- View server tasks ........................................................................ 100
- Server task status .......................................................................... 100
- Remove outdated server tasks from the Server Task Log: best practice ........................................................................ 100
- Create a server task .......................................................................... 101
- Remove outdated log items automatically ........................................ 101
- Accepted Cron syntax when scheduling a server task .................... 102

## Index

92
93
93
95
95
95
97
100
100
100
101
101
102
103
Preface

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

Contents

- About this guide
- Find product documentation

About this guide

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

Audience

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

- Administrators — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

*Italic*  Title of a book, chapter, or topic; a new term; emphasis

*Bold*  Text that is emphasized

*Monospace*  Commands and other text that the user types; a code sample; a displayed message

*Narrow Bold*  Words from the product interface like options, menus, buttons, and dialog boxes

*Hypertext blue*  A link to a topic or to an external website

- **Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method

- **Tip:** Best practice information

- **Caution:** Important advice to protect your computer system, software installation, network, business, or data

- **Warning:** Critical advice to prevent bodily harm when using a hardware product
Find product documentation

On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

**Task**

1. Go to the ServicePortal at [https://support.mcafee.com](https://support.mcafee.com) and click the Knowledge Center tab.

2. In the Knowledge Base pane under Content Source, click Product Documentation.

3. Select a product and version, then click Search to display a list of documents.
Managing security with McAfee ePO Cloud

McAfee® ePolicy Orchestrator® Cloud (McAfee® ePO® Cloud) provides unified endpoint security management. It reduces incident response times, strengthens protection, and simplifies risk and security management with automation features and end-to-end network visibility.

Contents

- Benefits of McAfee ePO Cloud
- Differences between McAfee ePO and McAfee ePO Cloud
- Sign up for a free trial
- How McAfee ePO Cloud works

Benefits of McAfee ePO Cloud

McAfee ePO Cloud is an extensible management platform for centralized policy management and enforcement of your security products and the systems where they are installed.

It also provides comprehensive reporting and product deployment, all through a single point of control.

Using McAfee ePO Cloud, you can manage security across endpoints, networks, and data while you identify, manage, and respond to security issues and threats.

Differences between McAfee ePO and McAfee ePO Cloud

We provide different platforms for managing the security of your network.

McAfee ePO is installed on a server in your network environment. It is intended for enterprises that already have an established infrastructure, including the necessary dedicated servers. It assumes that your organization can configure, maintain, and patch these servers. McAfee ePO features such as Automatic Response, Active Directory synchronization, and the Software Manager support in-house security administration.

McAfee ePO Cloud is a cloud-based instance of McAfee ePO. With McAfee ePO Cloud, you don't need to configure and maintain the servers where your security management software runs. Software management and other maintenance are taken care of by our administrators.

Sign up for a free trial

Sign up for a 60-day free trial of McAfee ePO Cloud.

After signing up for a trial account, you have full access to the products available in McAfee ePO Cloud for 60 days. This trial gives you an opportunity to evaluate McAfee ePO and its products in your environment.
Task
2. Enter your company information, billing address, and a primary contact.

Once you submit your details, you receive an email with the instructions about activating your trial account.

How McAfee ePO Cloud works

Your McAfee ePO Cloud environment includes these components:

- **McAfee ePO Cloud** — The center of your managed environment. McAfee ePO Cloud delivers security policies and tasks, controls updates, and processes events for all managed systems.

- **McAfee Agent** — A vehicle of information and enforcement between McAfee ePO Cloud and each managed system. The agent retrieves updates, implements tasks, enforces policies, and forwards events for each managed system. It uses a separate secure data channel to transfer data back to McAfee ePO Cloud.

- **McAfee Data Exchange Layer** — DXL provides bidirectional communication between systems on a network. DXL clients communicate throughout your environment, and help your security products track activity, risks, and threats in real time.

- **Security products** — Software like McAfee Endpoint Security, that protects your managed systems, and that you monitor and manage with McAfee ePO Cloud.

One function, besides security management, of McAfee product software and McAfee ePO Cloud is to stop malware attacks on managed systems and notify you when an attack occurs. This figure shows the components and processes used to stop an attack, notify you when the attack occurs, and record the incident.

These numbers correspond to the numbers in the figure.

1. Malware attacks a computer in your McAfee ePO Cloud managed network.
2. The McAfee product software, for example McAfee Endpoint Security, cleans or deletes the malware file.
3. The McAfee Agent notifies McAfee ePO Cloud of the attack.
4 McAfee ePO Cloud stores the attack information.

5 McAfee ePO Cloud displays the notification of the attack on the Number of Threat Events dashboard and saves the history of the attack in the Threat Event Log.
Getting started with McAfee ePO Cloud

McAfee ePO Cloud provides a centralized, cloud-based platform for remotely managing the security of your endpoints. You can use McAfee ePO Cloud to ensure that the software on your network is always up to date and your systems are protected. The tools you need to manage security for your network can be found by accessing the McAfee ePO Cloud web interface. This guide introduces you to McAfee ePO Cloud and describes how to use the web interface to complete the required setup tasks.

The setup process follows this basic outline:

1. As an administrator, you begin by requesting access to McAfee ePO Cloud. After you receive your welcome email, you can activate your account.

2. Next, log on to McAfee ePO Cloud. You are now ready to install software on the systems in your network.

3. As an administrator, you select the installation option and distribute an installation URL to each of the endpoints in your network.

4. Finally, each of the endpoints receives the installation URL, installs the product software, and communicates back to the McAfee ePO Cloud server. As an administrator, you can verify that each of these endpoints is now managed in the System Tree.

Contents

- Preparing for setup and installation
- Activate your account
- Log on to McAfee ePO Cloud
- Choose an installation option
- Install protection on other computers
Preparing for setup and installation

To begin, request access to McAfee ePO Cloud and wait to receive your welcome letter. You can also compile a list of the systems in your network. Make sure that you can access each endpoint remotely.

- **McAfee ePO Cloud welcome email** — provides your user name and an activation link.
- **List of systems in your organization** — allows you to begin managing your endpoints in McAfee ePO Cloud. This information is used when you distribute the installation instruction to each of your users.

After you receive this information, you are ready to activate your McAfee ePO Cloud account.

Activate your account

To use McAfee ePO Cloud, you need to activate your account. The activation link and activation code are included in your welcome letter. Remember that the link expires a week after you receive it.

**Task**

1. Open your welcome email and click the link:
   - Click Here to Begin
   - Accept Invitation
   - Activate Now

2. If prompted, click Use McAfee ePO Cloud to manage your network in the cloud.

3. Enter your email address.
   Your email address is also your user name in McAfee ePO Cloud

4. Enter your activation code.
   The code is included in your welcome email.

5. Enter a secure password and type it again as verification.

6. Click Activate or Accept.

Your user account is successfully activated and the McAfee ePO Cloud console opens to the **Getting Started** page. You are ready to begin managing your endpoints.

If you have already activated your account, you cannot activate it again. But, if you need a new welcome email or activation code:

Go to manage.mcafee.com. Click **Activate New User**. Click **Click Here**.

Check your inbox for the new welcome email and activation code.
Log on to McAfee ePO Cloud

To access McAfee ePO Cloud, enter your email address and password on the logon screen.

**Before you begin**
You must have the email address assigned to your account and your password.

**Task**
1. Navigate to the McAfee ePO Cloud logon page: manage.mcafee.com.
2. Type your account email address and password, select a language, then click Log On.

The first time you log on, McAfee ePO Cloud displays the Getting Started page. Subsequent logons display the first favorite in the Menu shortcut.

**Tasks**
- *Reset a forgotten password on page 15*
  If you have forgotten your password, you can reset it.

---

**Reset a forgotten password**

If you have forgotten your password, you can reset it.

**Before you begin**
Activate your McAfee ePO Cloud user account.

**Task**
1. Open the McAfee ePO Cloud logon page: manage.mcafee.com.
   - If you are already using McAfee ePO Cloud, log off.
2. Click Forgot Password to open the Forgot Password Recovery page.
3. Type your email address in the Email field, then click Submit.
   - McAfee sends you an email that allows you to reset your password on McAfee ePO Cloud.
4. Open the email and click Reset Password to create a new password.
   - The Forgot Password Recovery page opens in your browser.
5. Open the Forgot Password Recovery page: click the link in the verification email you received.
6. Type your email and the verification code
7. Choose a secure password, type it in the form, and re-enter it for verification. Use your organization's guidelines or McAfee best practices for choosing passwords.
8. Click Submit.

Your password is reset and you can log on to McAfee ePO Cloud.
Choose an installation option

To install the McAfee Agent and related product software on your endpoints, select an installation option and follow the instructions. When completed, you have an installation URL that you can distribute to your users. The Getting Started page includes these options:

- **Install Protection** — Click to complete the default installation on your endpoints.
- **Customize Installation** — Click to create a custom installation package.
- **Skip initial installation** — Click to skip the installation process and complete it later.

If you decide to wait, you can return to the installation options by selecting Menu | Software | Getting Started.

### Install protection

The easiest way to continue the installation process is to use the default products and policy settings.

If you are returning to the installation process, select Menu | Software | Getting Started.

**Task**

1. Click **Install Protection**.
   
   The page refreshes and states *You are now ready to install McAfee protection on your computers.*

2. Click **Install Protection on Other Computers**.
   
   To install on your local system, click **Install Protection on This Computer** and follow the steps.

   The Install Protection on Other Computers dialog box opens.

3. Copy the URL.

   You are now ready to email the URL to your users.

### Customize installation

Advanced users can proceed with the installation process by creating a customized list of products and policy settings. Your license agreement determines the options that appear in the Customize Software Installation table. This option is useful when installing Desktop Protection software, for example.

If you are returning to the installation process, select Menu | Software | Getting Started.

**Task**

1. Click **Customize Installation**.
   
   The Getting Started page refreshes and displays the Customize Software Installation table options.

2. In the **Group Name** field, type a group name for your custom installation.
3 In the **Platform** drop-down list, select an operating system.
   - Windows
   - Mac OSX
   - Linux

   The installation process automatically selects the correct software for the platform you choose.

4 In the **Software and Policies** area, select or deselect products as needed.

5 To customize policies for each product, click **McAfee Default Policies and Tasks** and select policies.

6 To automatically update product software, select **Auto Update**.

7 Click **Done**.

   The system processes your selections and refreshes, stating **You are now ready to install McAfee protection on your computers**.

8 Click **Install Protection on Other Computers**.

   To install on your local system, click **Install Protection on This Computer** and follow the steps.

   The **Install Protection on Other Computers** dialog box opens.

9 Copy the URL.

   You are now ready to email the URL to your users.

   **Customizing an installation for Desktop Protection**

   For example, if you select **Desktop Protection** software for your custom installation, configure these options:
   - Select the software products to install and, if needed, click **McAfee Default Policies and Tasks** to configure settings specific to that product. Only the latest version of the product software appears in the software list. There might be older versions available in the repository.
   - To automatically update your products with the latest versions, updates, patches, and content, select the **Auto Update** checkbox.

   During a new deployment, the McAfee Agent checks for new versions, hotfixes, and content packages for all products.

---

### Install protection on other computers

Send the installation URL to the endpoint users you want to manage in McAfee ePO Cloud. This is the list you created at the start of the process. When they receive the link, users can then click it to download and install McAfee Agent and other product software.

The installation URL has this format:

```
https://<epoServerName>.manage.mcafee.com:8443/ComputerMgmt/agentPackage.get?
token=<40-HexidecimalBytes>
```

If you forgot to copy the URL, select **Menu | Software | Getting Started**.
Task

1. Email the installation URL to the list of users you created.
2. Ask your users to click the URL and follow the installation steps for their operating system.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>When prompted, download the installer. Or, click <strong>Install</strong> to download it manually. Click <strong>Run</strong> to start the installation. A dialog box displays the progress of the installation. **The installation log, McAfeeSmartInstall_&lt;date&gt;_&lt;time&gt;.log, is saved in <code>&lt;LocalTempDir&gt;\McAfeeLogs</code>.</td>
</tr>
<tr>
<td>Mac OSX</td>
<td>When prompted, download the installer file, <code>McAfeeSmartInstall.app</code>. If you are using Mozilla Firefox, the customized URL downloads the <code>McAfeeSmartInstall.app.zip</code> file. Double-click the file to extract the <code>McAfeeSmartInstall.app</code> file. Double-click the <code>McAfeeSmartInstall.app</code> file to start the installation. A dialog box displays the progress of the installation. <strong>The installation log is saved in <code>/tmp</code>.</strong></td>
</tr>
<tr>
<td>Linux</td>
<td>Run the installer file, <code>./&lt;McAfeeSmartInstall.sh&gt;</code>, from the folder where it was downloaded. <strong>The installation log, McAfeeSmartInstall_&lt;date&gt;_&lt;time&gt;.log, is saved in the folder where you downloaded the installer.</strong></td>
</tr>
</tbody>
</table>

Your users now have McAfee Agent installed. They also have the product software and policies you selected.

Confirm system management

Verify that your users have installed the McAfee Agent, and that their systems have communicated with McAfee ePO Cloud, downloaded the product software, and are now managed.

Task

1. To confirm that the system users have installed the McAfee Agent, select **Menu** | **Systems** | **Systems**.
2. Using the list of email addresses that you used to send the installation URL, confirm that **Managed** appears in the Managed State column for each computer.
   
   **If all computers don't appear, you might need to remind your users to install the McAfee Agent using the installation URL.**

McAfee ePO Cloud is now managing these systems in your network. You have successfully completed the getting started process.
Contact support

Contact support to get help with your McAfee ePO Cloud account.

Before you begin
Activate your McAfee ePO Cloud user account.

Task

1. Open the Support page:
   a. From the McAfee ePO Cloud console, select Menu | User Management | My Account.
      The My Account page opens in a new window.
   b. Click Support.

2. Use the information on the Support page to obtain help with your account.

3. Close the My Account page to return to the McAfee ePO Cloud console.

Provide feedback

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

Task

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

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

3. Click Send.

Thank you for taking the time to send your feedback. Although we can't guarantee a response, we appreciate your suggestions.
3

Manage your account

Manage basic McAfee ePO Cloud account settings.

Tasks

- **Edit your user profile and change your password on page 21**
  The Profile page shows your user and logon information. You can view your profile and change your email address, your password, or your account information.

- **Enable two-factor authentication on page 22**
  The Profile page allows you to enable two-factor authentication for additional security.

- **Secure your user session with two-factor authentication on page 23**
  Two-factor authentication adds another layer of security to your McAfee ePO Cloud session.

- **View your subscription information on page 24**
  View your active McAfee product subscriptions, utilization, and order history.

- **Transfer licenses from another account to your account on page 24**
  You can transfer the licenses from another account to your account. This allows you to manage all your licenses from one account.

- **Manage user accounts on page 25**
  User accounts allow you to control how users access and use the software.

Contents

- **Edit your user profile and change your password**
- **Enable two-factor authentication**
- **Secure your user session with two-factor authentication**
- **View your subscription information**
- **Transfer licenses from another account to your account**
- **Personal settings categories**
- **Manage user accounts**

---

**Edit your user profile and change your password**

The Profile page shows your user and logon information. You can view your profile and change your email address, your password, or your account information.

**Task**

1. Open the **My Profile** page.
   a. From the McAfee ePO Cloud console, select **Menu | Account Management | My Account**.
      The My Account page opens in a new window or tab.
   b. Click **My Profile**.
2 Click **Edit Profile** to change your profile, password, or the account you log on to.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Edit your profile             | To change your profile, click **Edit Profile**.  
1. Change the profile as needed.  
2. Click **Submit**.  
The changes appear on the Profile page. |
| Change your password          | To change your password, click **Edit Profile**.  
1. Click **Change Password**.  
2. Type your current password in the form. Choose a secure password, type it in the form, and enter it again for verification.  
   - Use your organization's guidelines or McAfee best practices for changing passwords.  
3. Click **Submit**. A confirmation window opens.  
4. Click **Done** to return to the Profile page. |
| Change the account you log on to | If you have access to multiple accounts, you can change the account specified in your user profile to log on to a different account.  
1. Click **Edit Profile**.  
2. From the **Default Sign In Account** drop-down list, select the account that you want to log on to.  
3. Click **Submit**. A confirmation window appears.  
The next time you log on, you are routed to McAfee ePO Cloud console for the specified account. |
| Enable two-factor authentication | Enable your account with two-factor authentication to use a combination of password and one-time password for logon.  
1. Click **Edit Profile**.  
2. Select **Log on** option to prompt the user for two-factor authentication while logging on.  
3. Click **Manage Delivery Options**, then set how the one-time password (OTP) is delivered to the user and test it.  
   - **Cell Phone** — Select the country and the mobile phone number, click **Verify**, enter the OTP that you receive in your mobile phone, then click **Verify**.  
   - **Email** — Click **Send a test OTP to this email address <your primary email>**, enter the OTP that you receive in your email address, then click **Verify**.  
Once your OTP is verified, click **Save**.  
4. Click **Submit**. |

3 Close the My Profile tab to return to the McAfee ePO Cloud console.

---

### Enable two-factor authentication

The Profile page allows you to enable two-factor authentication for additional security.
Task

1. Open the My Profile page.
   a. From the McAfee ePO Cloud console, select Menu | Account Management | My Account.
      The My Account page opens in a new window or tab.
   b. Click My Profile.

2. Click Edit Profile, then select Log on to prompt the user for two-factor authentication while logging on.

3. Click Manage Delivery Options, then set how the one-time password (OTP) is delivered to the user and test it.
   a. Cell Phone — Select the country and the mobile phone number, click Verify, enter the OTP that you receive in your mobile phone, then click Verify.
   b. Email — Click Send a test OTP to this email address <your primary email>, enter the OTP that you receive in your email address, then click Verify.

4. Once your OTP is verified, click Save and click Submit. Then click Done when the confirmation window opens to return to the Profile page.

5. Close the My Profile tab to return to the McAfee ePO Cloud console.

Secure your user session with two-factor authentication

Two-factor authentication adds another layer of security to your McAfee ePO Cloud session. The authentication factors include a combination of:

- A logon user name and password
- A one-time password (OTP) that is sent to your email or cell phone

Task

1. From the McAfee ePO Cloud console, open the My Account page: select Menu | My Account.

2. Enable two-factor authentication for either these profiles that you manage.

   a. For your own profile — Perform these steps:
      1. Click My Profile, then click Edit Profile.
      2. Select Log on to prompt for an OTP when you log on, then set how the OTP must be sent to you.
         a. Cell Phone — Select the country and the mobile phone number, click Verify, enter the OTP that you receive in your mobile phone, then click Verify.
         b. Email — Click Send a test OTP to this email address <your primary email>, enter the OTP that you receive in your email address, then click Verify.

      The OTP that you provide is verified.
   3. Click Save.
For any other user's profile — Perform these steps:

1. Click Users, select a user, then click Edit Profile.

   You can also select Menu | Account Management to open the Users page.

2. Select Log on to prompt for an OTP when the user logs on.
   By default, the OTP is sent to the user's email address. The user can change the OTP delivery option from the My Profile page in the user's logon.

3. Click Submit.

View your subscription information

View your active McAfee product subscriptions, utilization, and order history.

Before you begin
Activate your McAfee ePO Cloud user account.

Task

1. Open the Subscriptions page:
   a. From the McAfee ePO Cloud console, select Menu | Account Management | My Account.

      The My Account page opens in a new window or tab.
   b. Click Subscriptions.

      On the Subscriptions page, you can see your Active Subscriptions, Utilization Summary, and Order History.

2. Close the My Account window or tab to return to the McAfee ePO Cloud console.

Transfer licenses from another account to your account

You can transfer the licenses from another account to your account. This allows you to manage all your licenses from one account.

Before you begin
You need to get one of the following information from the owner of the other account:

- Grant number
- Log on credentials to the other account
**Task**

Once you raise the request to transfer the license, the other user needs to approve the transfer from the McAfee ePO Cloud license merger email. After the approval, you receive a confirmation email. Then you can view the licenses of the other user on your Subscription page and transfer them to your McAfee ePO Cloud account.

1. From the McAfee ePO Cloud console, open the Subscription page: select **Menu | My Account | Subscriptions**.
2. Click **Add licenses from another account**.
3. Enter the details of the other account.

<table>
<thead>
<tr>
<th>Using Grant number</th>
<th>Use log on credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter the email address and company name.</td>
<td>1. Select <strong>click here</strong> from the <strong>Note</strong>.</td>
</tr>
<tr>
<td>2. Enter the grant number.</td>
<td>2. Enter the credentials to the other account.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Personal settings categories**

Adjust personal settings to tailor your McAfee ePO Cloud experience. Your customizations affect only your user sessions.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Tree Warning</td>
<td>Determines whether a warning message appears when you try to drag systems or groups from one <strong>System Tree</strong> group to another.</td>
</tr>
<tr>
<td>Time Zone Preference</td>
<td>Sets the time zone used in the displayed Threat Event time.</td>
</tr>
<tr>
<td>User Session</td>
<td>Controls the length of time that your user session remains open after you stop interacting with the user interface.</td>
</tr>
</tbody>
</table>

**Option definitions**

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

**Manage user accounts**

User accounts allow you to control how users access and use the software.

**Before you begin**

You must have activated your user account.
**Owner users** (or owners) can create and add users. **Standard users** (or users) do not.

Consider the following when setting up accounts and users:

- Although there is only one owner for each account, an organization can have many accounts. For example, an organization might have separate accounts for different locations (Tokyo, Madrid), or for different groups in the organization (Accounting, Customer Service). Each account can have multiple standard users and users can be in multiple accounts.

- Owners can view their account and each user's account. Users can only view their account and cannot add or delete users.

- The **Delete** and **New User** buttons are available only to the owner. Owners can add or delete users, but cannot delete themselves as a user.

- When you delete a standard user, you remove only the link to the account for that user. The software maintains the user’s roles and relations to other accounts they might be a part of.

- Owners cannot change standard user roles and relations to other accounts.

**Task**

1. Open the Users page:
   - From the console, select **Menu | Account Management | My Account**.
     - The My Account page opens in a new window.
   - Click **Users**.

2. Perform one of these user actions:
   - **View user account** — Click the user's email address.
   - **Create user account** — Perform these steps:
     1. Click **New User**.
     2. Type the email address of the person you want to invite.
     3. Click **Invite**.
        - The software sends an invitation to the new user with instructions on how to activate themselves as a user and create a password. The invitation is valid for seven days.
   - **Delete user account** — Perform these steps:
     1. Click a user's email address. You can view their information.
     2. Click **Delete** and the Delete User Confirmation page appears.
     3. Click **Delete**.
        - The Users page appears with a confirmation message that the user has been deleted.

3. Close the My Account page to return to the console.
Monitoring the health of your network

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

Contents
- Navigating the interface
- Working with lists and tables
- Using dashboards and monitors
- Managing events
- Server settings

Navigating the interface

The McAfee ePO Cloud 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 Cloud, the main menu options like Dashboards, System Tree, and Policy Catalog include new options to select.

Using the shortcut bar

Use the McAfee ePO Cloud shortcut bar to navigate to the main menu and user menu.

The McAfee ePO Cloud shortcut bar, at the top of the interface, includes the menu items you use most often to manage your network security.
Main menu — Click to access menu items and functionality of McAfee ePO Cloud. Each section contains a list of primary feature pages associated with a unique icon. Select a category in the main menu to view and navigate to the primary pages that make up that feature.

Drag and drop menu items from the main menu into the shortcut bar for easy access in the future. Drag the menu items off the shortcut bar to delete.

This down-arrow indicates that more features are available in the shortcut bar.

User menu — Click to access:

• Help — Opens the McAfee Help Portal with links to the product documentation and user interface feature descriptions.

• Get Support — Allows you to:
  • Open Service Request — Opens the ServicePortal where you click the Service Requests tab to log on and create a service request.
  • Call Customer Service — Opens the Contact Us page for lists of contacts for support, sales, services, and partners.
  • Feedback — Opens the Provide Feedback page where you enter your information and send it to us.

• Log Off — Returns you to the McAfee ePO Cloud logon page and locks the user interface until you log on again.
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.

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

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

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

   ![This table row selection action does not work in the Audit Log table.]

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

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

Using dashboards and monitors
Dashboards help you keep constant watch on your environment.
Dashboards are collections of monitors. Monitors condense information about your environment into easily understood graphs and charts. Usually, related monitors are grouped on a specific dashboard. For example, the Threat Events dashboard contains four monitors that display information about threats to your network.
The McAfee ePO Cloud 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.
You can switch dashboards by selecting a different dashboard from the drop-down list.

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

**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. Select a dashboard.
3. Click **Save**.
The first time a user logs on, the dashboard you specified appears. Subsequent logons return the user to the page they were on when they logged off.

Managing events
You can specify which events McAfee ePO Cloud tracks.
Events are generated by the product software, and passed to the McAfee Agent. These events are uploaded either immediately or at the next agent-server communication. Events then appear on the Threat Events dashboard or in queries and reports you generate.
The event types you have depends on the software products that you are managing with McAfee ePO Cloud.
The Threat Event Log

Use the Threat Event Log to quickly view and sort through events in the database. You can purge the log only by age.

You can choose which columns are displayed in the sortable table. You can choose from various event data to use as columns.

Depending on which products you are managing, you can also take certain actions on the events. Actions are available in the Actions menu at the bottom of the page.

Common event format

Most managed products now use a common event format. The fields of this format can be used as columns in the Threat Event Log. These 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 Cloud 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.

**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 on page 33**
  Use the Server Settings page to determine which events are forwarded to the server.
- **Determine which events are forwarded immediately on page 33**
  Determine whether events are forwarded immediately or only during agent-server communication.

**Determine which events are forwarded**

Use the Server Settings page to determine which events are forwarded to the server.

> The default interval for processing event notifications is one minute. As a result, there might be a delay before events are processed. You can change the default interval in the Event Notifications server settings (Menu | Configuration | Server Settings).

**Task**

1. Select **Menu | Configuration | Server Settings**, select **Event Filtering**, then click **Edit**.
2. Select the events, then click **Save**.

These settings take effect for each managed system after its next agent-server communication.

**Determine which events are forwarded immediately**

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

If the currently applied policy is not set for immediate uploading of events, either edit the currently applied policy or create a McAfee Agent policy. This setting is configured on the Threat Event Log page.
Task

1. Select **Menu | Policy | Policy Catalog**, then select **Product** as McAfee Agent and **Category** as **General**.

2. Click an existing agent policy.

3. On the **Events** tab, select **Enable priority event forwarding**.

4. Select the event severity.
   
   Events of the selected severity (and greater) are forwarded immediately to the server.

5. To regulate traffic, type an **Interval between uploads** (in minutes).

6. To regulate traffic size, type the **Maximum number of events per upload**.

7. Click **Save**.

Server settings

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

Here are descriptions of the default categories.

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

**Table 4-1  Default server settings**

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>Specifies the default active dashboard that is assigned to new users’ accounts at the time of account creation, and the default refresh rate (5 minutes) for dashboard monitors.</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Specifies the Directory Services server DNS name, URL, and Configuration Services URL.</td>
</tr>
<tr>
<td>Event Filtering</td>
<td>Specifies which events the agent forwards.</td>
</tr>
<tr>
<td>Printing and Exporting</td>
<td>Specifies how information is exported to other formats, and the template for PDF exports. It also specifies the default location where the exported files are stored.</td>
</tr>
<tr>
<td>System Details</td>
<td>Specifies which queries and systems properties are displayed in the System Details page for your managed systems.</td>
</tr>
</tbody>
</table>
Generating queries and reports

McAfee ePO Cloud comes with its own querying and reporting capabilities. In addition to the querying and reporting systems, you can use these logs to gather information about activities on your McAfee ePO Cloud server and your network:

- Audit Log
- Server Task Log
- Threat Event Log

Contents
- Introduction to queries
- Run a query
- Export query results to other formats
- Custom queries
- Introduction to reports
- Run reports
- View report output

Introduction to queries

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

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.

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.
Run a query

Run a query when you want specific information about your network environment or McAfee ePO Cloud.

Task

1. Select Menu | Reporting | Queries & Reports, then select a query from the Queries list.
2. Click Actions | Run. When the query results appear, you can drill down into the report and act on items as needed.
3. Click Close when finished.

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) Include a cover page with this text and enter the needed text.
Specify the recipients and body text for the query email.

Click Export.

The files are emailed as attachments to the recipients.

Custom queries

Some products allow you to create custom queries. You can use the features of the Query Builder to manage and run your own queries.

Query Builder

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

Table 5-1  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.
Generating queries and reports

Custom queries

Query results displayed in a table are actionable. For example, if the table is populated with systems, you can deploy agents on those systems directly from the table.

**Filters**
Specify criteria by selecting properties and operators to limit the data retrieved by the query.

**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>
<tbody>
<tr>
<td>Create custom query</td>
<td>1. Click <strong>New Query</strong>, and the Query Builder appears.</td>
</tr>
<tr>
<td></td>
<td>2. On the Result Type page, select the <strong>Feature Group</strong> and <strong>Result Type</strong> for this query, then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Select the type of chart or table to display the primary results of the query, then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Boolean Pie Chart</strong>, configure the criteria to include in the query before proceeding.</td>
</tr>
<tr>
<td></td>
<td>4. Select the columns to be included in the query, then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you selected <strong>Table</strong> on the Chart page, the columns you select here are the columns of that table. Otherwise, these columns make up the query details table.</td>
</tr>
<tr>
<td></td>
<td>5. Select properties to narrow the search results, then click <strong>Run</strong>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property.</td>
</tr>
<tr>
<td></td>
<td>• If the query didn't return the expected results, click <strong>Edit Query</strong> to go back to the Query Builder and edit the details of this query.</td>
</tr>
<tr>
<td></td>
<td>• If you don't want to save the query, click <strong>Close</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If you want to use this query again, click <strong>Save</strong> and continue to the next step.</td>
</tr>
<tr>
<td></td>
<td>6. Select a query group.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>The new query appears in the Queries list.</td>
</tr>
</tbody>
</table>

| 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.                                                                |
# Introduction to 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.

---

## Run reports

Reports must be run before examining their results.

Reports can be run from these locations within McAfee ePO Cloud:

- The report listing
- Within a server task

These instructions assume that you are running reports from within the report listing.

### Task

1. Select **Menu | Reporting | Queries & Reports**, then select the **Report** tab.

2. Select a report from the report list, then click **Actions | Run**.

   When the report is complete, the resulting PDF is sent to your browser. It is displayed or downloaded according to your browser settings.

   Some reports take a while to complete. It is possible to have more than one report running simultaneously, but you cannot initiate more than one report at a time through the interface. When the report is complete, the software updates the **Last Run Result** column in the report list with a link to the PDF containing those results.

---

## View report output

View the last run version of every report.

Every time a report runs, the results are stored on the server and displayed in the report list.

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

1. Select **Menu | Reporting | Queries & Reports**.

2. Select the **Report** tab

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

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

Take immediate action against threats and outbreaks by automatically starting McAfee ePO Cloud processes when events occur.

McAfee ePO Cloud 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:
• Run system commands.
• Send an email message.

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.

Contents
▶ Response planning
▶ Create and edit Automatic Response rules

Response planning

Before creating automatic response rules, think about the actions you want the McAfee ePO Cloud 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.

Create and edit Automatic Response rules

Define when and how to respond to an event. Automatic Response rules do not have a dependency order.
Tasks

- **Define a rule on page 42**
  When creating a rule, include information that other users might need to understand the purpose or effect of the rule.

- **Set filters for the rule on page 42**
  To limit the events that can trigger the response, set the filters for the response rule on the Filters page of the Response Builder.

- **Set Aggregation and grouping criteria for the rule on page 42**
  Define when events trigger a rule on the Aggregation page of the Response Builder.

- **Configure the actions for an automatic response rule on page 43**
  Configure the responses triggered by the rule on the Actions page of the Response Builder.

**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. Select the **Event group** and **Event type** that trigger this response.

4. Next to **Status**, select **Enabled** or **Disabled**. The default is Enabled.

5. 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.
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 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, type the email address for the recipient. To add multiple recipients, separate email addresses with 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.

2 On the Summary page, verify the information, then click Save.

The new rule appears in the Responses list.

Information: Automatic response rules do not have a dependency order.
Setting up automatic responses
Create and edit Automatic Response rules
Organizing systems

Use McAfee ePO Cloud to automate and customize your systems' organization. The structure you put in place affects how security policies are inherited and enforced throughout your environment. The System Tree is the graphical representation of this structure. You can organize your System Tree using these methods:

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

## Contents

- **System Tree structure**
- **Considerations when planning your System Tree**
- **Criteria-based sorting**
- **Create and populate System Tree groups**
- **Move systems within the System Tree**
- **Remove a system from the System Tree**

### System Tree structure

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

#### 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.
The 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.

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

When your network computers run the installation URL, they are assigned by default to the subgroup My Group of the System Tree.

Task

1. Select Menu | Systems | System Tree, in the System Tree.

2. Click Delete Group or Rename Group to change the My Group subgroup.

If you delete systems from the System Tree, make sure that you select the option Remove agent from all systems. If the McAfee Agent is not removed, deleted systems reappear in the Lost and Found group because the McAfee Agent continues to communicate to McAfee ePO Cloud. Also, unless you select Remove agent installed products from all systems, the product software remains installed on the systems deleted from the System Tree.

Lost and Found group
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 within it.
• It always appears last in the System Tree list and is not alphabetized among its peers.
• 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 Cloud.

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:
• Machine-type (for example, laptops, servers, or desktops)
• Geography (for example, North America or Europe)
• Department boundaries (for example, Finance or Marketing)

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.

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.

### Inheritance

Inheritance is a property that simplifies policy and task administration. Because of inheritance, child subgroups in the System Tree hierarchy inherit policies set at their parent groups.

For example:

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

This table is an example of a System Tree hierarchy.

<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>Desktop</td>
<td>Child subgroup of Los Angeles</td>
</tr>
<tr>
<td>Laptop</td>
<td>Child subgroup of Los Angeles</td>
</tr>
<tr>
<td>Server</td>
<td>Child subgroup of Los Angeles</td>
</tr>
<tr>
<td>Windows</td>
<td>Child subgroup of Server</td>
</tr>
<tr>
<td>SQL</td>
<td>Child subgroup of Server</td>
</tr>
<tr>
<td>Linux</td>
<td>Child subgroup of Server</td>
</tr>
<tr>
<td>San Francisco</td>
<td>Child subgroup of My Organization</td>
</tr>
<tr>
<td>Desktop</td>
<td>Child subgroup of San Francisco</td>
</tr>
<tr>
<td>Laptop</td>
<td>Child subgroup of San Francisco</td>
</tr>
<tr>
<td>Server</td>
<td>Child subgroup of San Francisco</td>
</tr>
<tr>
<td>Lost and Found</td>
<td>Child subgroup of My Organization</td>
</tr>
</tbody>
</table>

In this example, all policies assigned to the Los Angeles | Server group are inherited by the Windows, SQL, and Linux child subgroups.

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.
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. Because every network is different and requires different policies, and possibly different management, McAfee recommends planning your System Tree before moving the systems from the default group where they were created.

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

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.

Political borders

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

Functional borders

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

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

Subnets and IP address ranges

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

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

Best practice: Consider using sorting criteria based on IP address information to automate System Tree creation and maintenance. Set IP address subnet masks or IP address range criteria for applicable groups within the System Tree. These filters automatically populate locations with the appropriate systems.

Operating systems and software

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

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

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

<table>
<thead>
<tr>
<th>Location</th>
<th>Chassis type</th>
<th>Platform</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Los Angeles</td>
<td>Desktop</td>
<td>Windows</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td>Laptop</td>
<td>Macintosh</td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td></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>

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 McAfee ePO Cloud 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 McAfee ePO Cloud
For sorting to take place, it must be enabled on McAfee ePO Cloud 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.

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 Cloud, 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 when you have 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.

Subgroups of groups with criteria that doesn't match are not considered. A group must have matching criteria or have no criteria for its subgroups to be considered for a system.
9 This process continues down through the System Tree until a system is sorted into a group.

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

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

Create and populate System Tree groups

Create System Tree groups and populate the groups with systems.

You can populate groups by dragging selected systems to any group in the System Tree. Drag and drop to move groups and subgroups within the System Tree.

There is no single way to organize a System Tree, and because every network is different, your System Tree organization can be as unique as your network layout. You can use more than one method of organization.

Tasks

- **Create groups manually on page 52**
  Create System Tree subgroups. Groups are automatically populated as the systems in your network communicate with McAfee ePO Cloud.

- **Add sorting criteria to groups on page 52**
  Sorting criteria for System Tree groups can be based on IP address information or tags.

- **Enable or disable System Tree sorting on systems on page 53**
  The sorting status of a system determines whether it can be sorted into a criteria-based group.

- **Sort systems manually on page 53**
  Sort selected systems into groups with criteria-based sorting enabled.

Create groups manually

Create System Tree subgroups. Groups are automatically populated as the systems in your network communicate with McAfee ePO Cloud.

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.

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.

   ![Information](image)

   Although you can configure multiple sorting criteria for the group, a system only has to match a single criterion to be placed in this group.

4. Configure the criteria. Options include:
   - **IP addresses** — Use this text box to define an IP address range or subnet mask as sorting criteria. Any system whose address falls within it is sorted into this group.
   - **Tags** — Click **Add Tags** and perform these steps in the **Add Tags** dialog box.
     1. Click the tag name, or names, to add and sort the systems in this parent group.
     2. Click **OK**.

   ![Information](image)

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

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

**See also**

- *IP address sorting criteria* on page 50
- *Tag-based sorting criteria* on page 50

**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.

   ![Information](image)

   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.

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.

See also

Lost and Found group on page 46

Remove a system from the System Tree

If a system user leaves your company or gets a new computer, you can delete their managed system using the System Tree.

You also can delete systems from the System Tree by deleting the System Tree group that includes the systems.

If you don't select Remove McAfee Agent on next agent-server communication from all systems, the systems reappear in the System Tree at the next agent-server communication to McAfee ePO Cloud.
Task

1. Select Menu | Systems | System Tree, click the Systems tab, and click the group with the systems you want to remove.

2. In the System Name column, select the systems you want to remove and click Actions | Directory Management | Delete.

3. Select Remove McAfee Agent on next agent-server communication from all systems.

4. To remove the security software from the system, select Remove McAfee Agent-installed software.

5. Click OK.

The system is removed from the System Tree at the next agent-server communication.
Organizing systems
Remove a system from the System Tree
Applying tags

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

Tags can use criteria that is evaluated against every system:
• Automatically at agent-server communication.
• When the Run Tag Criteria action is taken.
• Manually on selected systems, regardless of criteria, with the Apply Tag action.

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

Contents
- Create tags
- Manage tags
- Export and import tags
- Create, delete, and modify tag subgroups
- Exclude systems from automatic tagging
- Apply tags to selected systems
- Clear tags from systems
- Apply criteria-based tags to all matching systems

Create tags

Use the New Tag Builder to create tags quickly.

Task

2. On the Description page, enter a name and meaningful description, then click Next. The Criteria page appears.
3. Select and configure the criteria, then click Next. The Evaluation page appears.

To apply the tag automatically, configure criteria for the tag.
4. Select whether systems are evaluated against the tag's criteria only when the Run Tag Criteria action is taken, or also at each agent-server communication, then click Next. The Preview page appears.

   These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and have not been excluded from the tag.

5. Verify the information on this page, then click Save.

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

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

---

Manage tags

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

**Task**

1. Select Menu | Systems | Tag Catalog.

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

   - **Edit tag** — Click Actions | Edit, then from the Edit Tag Builder:
     - The number of affected systems is listed at the top of the page.
     - a. On the Description page, type a name and meaningful description, then click Next.
     - b. Select and configure the criteria, then click Next.
     - These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and have not been excluded from the tag.
     - c. Select whether systems are evaluated against the tag's criteria only when the Run Tag Criteria action is taken, or also at each agent-server communication, then click Next.

   - d. Verify the information about this page, then click Save.

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

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

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

4. **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.
Export and import tags

Once tags are created, you can save and import them using Export and Import.

**Task**

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

2. Perform one of these tasks:
   - **Export your Tags** — From the top of the page, click **Export**.
     1. From the Tag Catalog page, click the file link or right-click and select **Save link as** to download the file.
     2. From the Save as dialog box, save the **Tags.xml** file to a local system.
   - **Import your Tags** — From the top of the page, click **Import**.
     1. From the Import Tags dialog box, click **Choose File** and navigate to the **Tags.xml** file saved on a local system.
     2. From the Open dialog box, navigate to the **Tags.xml** file and click **Open**.
     3. From the Importing page, select the tags that you want to import, then click **OK**.

**Create, delete, and modify tag subgroups**

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

**Task**

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

2. From the **Tag Catalog** page, select one of these actions.
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a tag subgroup</td>
<td>1 In the <strong>Tag Tree</strong>, select the tag group (or parent tag group) where you want to create the tag subgroup.</td>
</tr>
<tr>
<td></td>
<td><img src="my_tags.png" alt="My Tags is the default top-level tag added during McAfee ePO Cloud installation." /></td>
</tr>
<tr>
<td></td>
<td>2 Click <strong>New Subgroup</strong> to see the <strong>New Subgroup</strong> dialog box.</td>
</tr>
<tr>
<td></td>
<td>3 In the <strong>Name</strong> field, enter a descriptive name for the new tag subgroup.</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>OK</strong> to create the tag subgroup.</td>
</tr>
<tr>
<td>Rename a tag subgroup</td>
<td>1 In the <strong>Tag Tree</strong>, select the tag subgroup that you want to rename.</td>
</tr>
<tr>
<td></td>
<td>2 Click **Tag Tree Actions</td>
</tr>
<tr>
<td></td>
<td>3 In the <strong>Name</strong> field, enter the new name for the tag subgroup.</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>OK</strong> and the tag subgroup is renamed.</td>
</tr>
<tr>
<td>Delete a tag subgroup</td>
<td>1 In the <strong>Tag Tree</strong>, select the tag subgroup that you want to delete.</td>
</tr>
<tr>
<td></td>
<td>2 Click **Actions</td>
</tr>
<tr>
<td></td>
<td>3 If you are sure you want to delete the tag subgroup, click <strong>OK</strong> and the tag subgroup is removed.</td>
</tr>
</tbody>
</table>

### 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.

### Apply tags to selected systems

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

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

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

4. 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**.
   a. 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.]

   b. Remove all tags — Select **Clear All**.
4. Verify that the tags have been removed:
   a. Select **Menu** | **Systems** | **Tag Catalog**, then select a tag or tag group in the list of tags.
   b. Next to **Systems with tag** in the details pane, click the link for the number of systems tagged manually. The **Systems with Tag Applied Manually** page appears.
   c. Verify that the systems are not included in the list.

**Apply criteria-based tags to all matching systems**

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

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

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

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

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

Policies ensure that product features are configured correctly on managed systems.

Contents

- About policies
- Policy assignment rules
- Create and manage policies
- Create and manage policy assignment rules
- Manually assign policies
- View policy information

About policies

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

Policies are organized by product, then by categories within each product. For example, the McAfee Agent product includes categories for General, Repository, and Troubleshooting.

To see policies in a specific policy category, select Menu | Policy | Policy Catalog, then select a product and category from the drop-down lists.

Each category includes a default policy, McAfee Default. You can’t delete, edit, export, or rename this policy, but you can copy it and edit the copy.

When policies are applied

Policies are applied to systems according to the agent-server communication and policy enforcement intervals.

When 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.

After policy settings are in effect on the managed system, the McAfee Agent continues to enforce policy settings according to the policy enforcement interval. By default, the policy enforcement occurs every 60 minutes. You can adjust this interval on the General tab as well.

How policies are applied

Policies are applied to any system by one of two methods: inheritance or assignment.

You can assign any policy in the Policy Catalog to any group or system. Assignment allows you to define policy settings once for a specific need, then apply the policy to multiple locations.

Inheritance determines whether the policy settings and client tasks for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree.
Assignment locking
You can lock the assignment of a policy on any group or system. Assignment locking prevents other users from inadvertently replacing a policy. Assignment locking is inherited with the policy settings.

Assignment locking is valuable when you want to assign a certain policy at the top of the System Tree and make sure that no other users move it.

Assignment locking does not prevent the policy owner from changing policy settings. Therefore, if you intend to lock a policy assignment, make sure that you are the owner of the policy.

See also
Assign a policy to a System Tree group on page 72
Assign a policy to a managed system on page 72
Assign a policy to systems in a System Tree group on page 73
Copy policy assignments from a group on page 73
Copy policy assignments from a system on page 73
Paste policy assignments to a group on page 74
Paste policy assignments to a specific system on page 74

Policy ownership
Each policy is assigned an owner — the user who created it. You must have the correct permissions to edit a policy you don’t own.

If you want to use a policy owned by a different user, we recommend that you duplicate the policy, then use the duplicate. Duplicating policies prevents unexpected policy changes from affecting your network. If you assign a policy that you don’t own, and the owner modifies the policy, all systems that were assigned the policy receive the modifications.

You can specify multiple users as owners of a single policy.

Policy assignment rules
Policy assignments rules reduce the overhead of managing numerous policies for individual users or systems that meet specific criteria, while maintaining more generic policies across your System Tree.

This level of granularity in policy assignments limits the instances of broken inheritance in the System Tree to accommodate the policy settings that particular users or systems require. Policy assignments can be based on either user specific or system-specific criteria:

• User-based policies — Policies that include at least one user-specific criteria. For example, you can create a policy assignment rule that is enforced for all users in your engineering group. You can then create another policy assignment rule for members of your IT department. This rule allows them to log on to any computer in the engineering network with the access rights to troubleshoot problems on a specific system in that network. User-based policies can also include system-based criteria.

• System-based policies — Policies that include only system-based criteria. For example, you can create a policy assignment rule that is enforced for all servers on your network based on the tags you have applied, or all systems in a specific location in your System Tree. System-based policies cannot include user-based criteria.
Policy assignment rule priority

Policy assignment rules can be prioritized to simplify maintenance of policy assignment management. When you set priority to a rule, it is enforced before other assignments with a lower priority.

In some cases, the outcome can be that some rule settings are overridden. For example, consider a system that is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included systems unrestricted access to Internet content. Rule B has priority level 2, and heavily restricts the same system's access to Internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the system has unrestricted access to Internet content.

User-based policy assignment

User-based policy assignment rules give you the ability to create user-specific policy assignments. These assignments are enforced at the target system when a user logs on.

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 Cloud server applies the policies that you assigned to each user.

System-based policy assignment

System-based assignments allow you to assign policies based on System Tree location or tags. System-based policies are assigned based on selection criteria you define using the Policy Assignment Builder.

All policy assignment rules require that System Tree location is specified. Tag-based policy assignments are useful when you want all systems of a particular type to have the same security policy, regardless of their System Tree location.

Create and manage policies

McAfee ePO Cloud provides a number tools to manage policies, including the Policy Catalog, Policy History, and Policy Comparison.

Tasks

- Create a policy from the Policy Catalog page on page 66
  Custom policies created using the Policy Catalog are not assigned to any groups or systems. You can create policies before or after a product is deployed.
- Manage an existing policy on the Policy Catalog page on page 66
  Edit, duplicate, rename, or delete a policy.
- Enforcing product policies on page 67
  Policy enforcement is enabled by default, and is inherited in the System Tree, but you can manually enable or disable enforcement on specified systems.
- Manage policy history on page 68
  You can view and compare policy history entries, or revert to a previous version of a policy.
- Compare policies on page 69
  Policy Comparison can help you identify differences between similar policies.
Create a policy from the Policy Catalog page

Custom policies created using the Policy Catalog are not assigned to any groups or systems. You can create policies before or after a product is deployed.

**Task**

1. Open the **New Policy** dialog box.
   a. Select **Menu | Policy | Policy Catalog**.
   b. Select the product and category from the drop-down lists.
      
      All created policies for the selected category appear in the **Details** pane.
   c. Click **New Policy**.

2. Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.

3. Type a name for the new policy and click **OK**.
   The policy appears in the Policy Catalog.

4. Click the name of the new policy.
   The Policy Settings Builder opens.

5. Edit the policy settings as needed.

6. Click **Save**.

**Manage an existing policy on the Policy Catalog page**

Edit, duplicate, rename, or delete a policy.

**Task**

1. To select an existing policy, select **Menu | Policy | Policy Catalog**, then select the product and category from the drop-down lists.
   All created policies for the selected category appear in the details pane.

2. Select one of these actions.
### Action

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit policy settings</td>
<td>1 Locate the policy, then click the policy name.</td>
</tr>
<tr>
<td></td>
<td>2 Edit the settings as needed, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>To record policy revisions, type a comment in the text field next to <strong>Duplicate</strong>, in the footer of the Policy Catalog page.</td>
</tr>
<tr>
<td></td>
<td>The number of affected systems is listed at the top of the page.</td>
</tr>
</tbody>
</table>

#### Duplicate a policy

<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Locate the policy, then click <strong>Duplicate</strong> in that policy's row.</td>
</tr>
<tr>
<td>The Duplicate Existing Policy dialog box appears.</td>
</tr>
<tr>
<td>2 Type the name of the new policy in the field, then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>The new policy appears on the Policy Catalog page.</td>
</tr>
<tr>
<td>3 Click the new policy in the list.</td>
</tr>
<tr>
<td>4 Edit the settings as needed, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td>To record policy revisions, type a comment in the text field next to <strong>Duplicate</strong>, in the footer of the Policy Catalog page.</td>
</tr>
<tr>
<td>The new policy appears in the details pane.</td>
</tr>
</tbody>
</table>

#### Rename a policy

<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Locate the policy, then click <strong>Rename</strong> in a policy row.</td>
</tr>
<tr>
<td>The Rename Policy dialog box appears.</td>
</tr>
<tr>
<td>2 Type a new name for the existing policy, then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>The renamed policy appears in the details pane.</td>
</tr>
</tbody>
</table>

#### Delete a policy

<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Locate the policy, then click <strong>Delete</strong> in the policy row.</td>
</tr>
<tr>
<td>2 Click <strong>OK</strong> when prompted.</td>
</tr>
<tr>
<td>The deleted policy is removed from the details pane.</td>
</tr>
</tbody>
</table>

### Enforcing product policies

Policy enforcement is enabled by default, and is inherited in the System Tree, but you can manually enable or disable enforcement on specified systems.

You can manage policy enforcement from these locations:

- **Assigned Policies tab of the System Tree** — Choose whether to enforce policies for products or components on the selected group.
- **Policy Catalog page** — View policy assignments and enforcement. You can also lock policy enforcement to prevent changes below the locked node.

If policy enforcement is turned off, systems in the specified group don't receive updated site lists during an agent-server communication. As a result, managed systems in the group might not function as expected.

### Tasks

- **Enforce policies for a product in a System Tree group** on page 67
  Enable or disable policy enforcement in a group.

- **Enforce policies for a product on a system** on page 68
  Enable or disable policy enforcement on a managed system.

### Enforce policies for a product in a System Tree group

Enable or disable policy enforcement in a group.
Assigning policies
Create and manage policies

Task

1. Select **Menu | Systems | System Tree**, click **Assigned Policies** tab, then select a group in the **System Tree**.
2. Select the product you want, then click the link next to **Enforcement Status**.
3. To change the enforcement status, select **Break inheritance and assign the policy and settings below**.
4. Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.
5. Choose whether to lock policy inheritance.
   - Locking inheritance for policy enforcement prevents breaking enforcement for groups and systems that inherit this policy.
6. Click **Save**.

**Enforce policies for a product on a system**
Enable or disable policy enforcement on a managed system.

Task

1. Select **Menu | Systems | System Tree**, click **Systems** tab, then select the group under **System Tree** where the system belongs.
   - The list of systems belonging to this group appears in the details pane.
2. Select a system, then click **Actions | Modify Policies on a Single System**.
   - The **Policy Assignment** page appears.
3. Select a **Product**, then click **Enforcing** next to **Enforcement status**.
   - The Enforcement page appears.
4. If you want to change the enforcement status you must first select **Break inheritance and assign the policy and settings below**.
5. Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.
6. Click **Save**.

**Manage policy history**
You can view and compare policy history entries, or revert to a previous version of a policy.

Task

1. To view the Policy History, select **Menu | Policy | Policy History**.
   - No Policy History entries appear for McAfee Default policies. You might need to use the page filter to select a created or duplicated McAfee Default policy.
2. Use the **Product, Category, and Name** filters to select Policy History entries.
3 To manage a policy or Policy History entry, click Actions, then select an action.

- **Choose Columns** — Opens a dialog box that allows you to select which columns to display.
- **Compare Policy** — Opens the Policy Comparison page where you can compare two selected policies.
  The current version of a policy has the latest date. To compare the current revision of a policy and a previous policy revision, select the latest revision and a previous revision to compare.
- **Export Table** — Opens the Export page where you can specify the package and format of Policy History entry files to export, then email the file.
- **Revert Policy** — Reverts the policy to the selected policy version.
  You can select only one target policy.
  When you revert a policy, you are prompted to add a comment to the Policy History entry.

**See also**
*Manage an existing policy on the Policy Catalog page on page 66*

**Compare policies**
Policy Comparison can help you identify differences between similar policies.

Many of the values and variables included on the Policy Comparison page are specific to each product. For option definitions not included in the table, see the documentation for the product that provides the policy you want to compare.

**Task**

1 Select Menu | Policy Comparison, then select a product, category, and Show settings from the lists.

![Best practice: Change the Show setting from All Policy Settings to Policy Differences or Policy Matches to reduce the data displayed.]

These settings populate the policies to compare in the Policy 1 and Policy 2 lists.

2 Select the policies to compare in the Compare policies row from the Policy 1 and Policy 2 column lists.

The top two rows of the table display the number of settings that are different and identical.

3 Click Print to open a printer friendly view of the comparison.

---

## Create and manage policy assignment rules

Configure policy assignment rules to simplify policy management.

**Tasks**

- **Create policy assignment rules on page 70**
  Creating policy assignment rules allows you to enforce policies for users or systems based on configured rule criteria.

- **Manage policy assignment rules on page 70**
  Perform common management tasks when working with policy assignment rules.
Create policy assignment rules
Creating policy assignment rules allows you to enforce policies for users or systems based on configured rule criteria.

Task

1. Open the Policy Assignment Builder.
   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 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


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:
     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.
Export and import policy assignment rules
To back up and restore policy assignment rules, you can use export and import.

Task

2. Select one of these actions:
   • Export policy assignment rules — Perform these steps:
     1. Select Actions | Export.
     2. From the Export page, click the link to open the file, or right-click a link to download and save the policy assignment rule .xml file to a local system.
   • Import policy assignment rules — Perform these steps:
     1. Select Actions | Import.
     2. From the Actions Import page, click Choose File, navigate to the .xml file, then click OK.
     3. From the Importing page, select the policy assignment rule .xml file that you want to import, then click OK.

Policy assignment rule files that conflict with identically named existing files appear red. Importing files indicating a conflict overwrite the existing identically named file.

Manually assign policies
You can assign or copy and paste policies to specific systems in the System Tree. These methods override policy inheritance, so they're helpful for applying policies on systems that require special privileges or settings.

Tasks

• Assign policies to managed systems on page 71
  Assign policies to a group or to specific systems in the System Tree. You can assign policies before or after a product is deployed.
• Copy and paste policy assignments on page 73
  Copy and paste policy assignments to easily share multiple assignments between groups and systems from different portions of the System Tree.

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 72
  Assign a policy to a specific group of the System Tree.
• Assign a policy to a managed system on page 72
  Assign a policy to a specific managed system.
• Assign a policy to systems in a System Tree group on page 73
  Assign a policy to multiple managed systems within a group.
Assigning policies
Manually assign policies

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.

See also
How policies are applied on page 63

Assign a policy to a managed system
Assign a policy to a specific managed system.

Task

1. Select Menu | Systems | System Tree, click Systems tab, then select a group under System Tree.
   All systems within this group (but not its subgroups) appear in the details pane.

2. Select a system, then click Actions | Agent | Modify Policies on a Single System.
   The Policy Assignment page for that system appears.

3. Select a product.
   The categories of selected product are listed with the system's assigned policy.

4. Locate the policy category you want, then click Edit Assignments.

5. If the policy is inherited, next to Inherited from, select Break inheritance and assign the policy and settings below.

6. Select the policy from the Assigned policy drop-down list.
   From this location, you can also edit settings of the selected policy, or create a policy.

7. Choose whether to lock policy inheritance.
   Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

8. Click Save.

See also
How policies are applied on page 63
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.

See also
How policies are applied on page 63

Copy and paste policy assignments
Copy and paste policy assignments to easily share multiple assignments between groups and systems from different portions of the System Tree.

Tasks
- Copy policy assignments from a group on page 73
  You can use Copy Assignments to copy policy assignments from a group in the System Tree.
- Copy policy assignments from a system on page 73
  You can use Copy Assignments to copy policy assignments from a specific system.
- Paste policy assignments to a group on page 74
  You can paste policy assignments to a group after you copy them from a group or system.
- Paste policy assignments to a specific system on page 74
  Paste policy assignments to a specific system after copy the policy assignments from a group or system.

Copy policy assignments from a group
You can use Copy Assignments to copy policy assignments from a group in the System Tree.

Task

1. Select Menu | Systems | System Tree, click Assigned Policies tab, then select a group in the System Tree.
2. Click Actions | Copy Assignments.
3. Select the products or features where you want to copy policy assignments, then click OK.

Copy policy assignments from a system
You can use Copy Assignments to copy policy assignments from a specific system.

Task

1. Select Menu | Systems | System Tree, click Systems tab, then select a group in the System Tree. The systems belonging to the selected group appear in the details pane.
2  Select a system, then click Actions | Agent | Modify Policies on a Single System.

3  Click Actions | Copy Assignments, select the products or features where you want to copy policy assignments, then click OK.

**See also**

*How policies are applied on page 63*

**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.

   ![Info](image)
   
   When pasting policy assignments, the Enforce Policies and Tasks policy appears in the list. This policy controls the enforcement status of other policies.

3  Select the policy categories you want to replace with the copied policies, then click OK.

**See also**

*How policies are applied on page 63*

**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.

   ![Info](image)
   
   When pasting policy assignments, the Enforce Policies and Tasks policy appears in the list. This policy controls the enforcement status of other policies.

4  Confirm the replacement of assignments.

**See also**

*How policies are applied on page 63*
View policy information

View detailed information about your policies, including policy owners, assignments, and inheritance.

Tasks

• View groups and systems where a policy is assigned on page 75
  View the Policy Catalog Assignment page to see the group, or system that inherits the policy.

• View policy settings on page 75
  View details for a policy assigned to a product category or system.

• View assignments where policy enforcement is disabled on page 76
  View assignments where policy enforcement, per policy category, is disabled.

• View policies assigned to a group on page 76
  View the policies assigned to a System Tree group, sorted by product.

• View policies assigned to a specific system on page 76
  View a list of all policies assigned to a system from one central location, the System Tree.

• View policy inheritance for a group on page 76
  View the policy inheritance of a specific group.

• View and reset broken inheritance on page 77
  Identify the groups and systems where policy inheritance is broken.

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 assignments where policy enforcement is disabled
View assignments where policy enforcement, per policy category, is disabled. Normally you want policy enforcement enabled. Use this task to find any policies that are not being enforced and change their configuration.

Task
1 Select Menu | Policy | Policy Catalog, then select a product and category. All created policies for the selected category appear in the details pane.
2 Click the link next to Product enforcement status, which indicates the number of assignments where enforcement is disabled, if any.
The Enforcement for <policy name> page appears.
3 Go to System Tree | Assigned Policies page to change the enforcement policy of the listed policy.

View policies assigned to a group
View the policies assigned to a System Tree group, sorted by product. For example, if you have different policies assigned to servers and workstation groups, use this task to confirm the policies are set correctly.

Task
1 Select Menu | Systems | System Tree, click Assigned Policies tab, then select a group in the System Tree.
All assigned policies, organized by product, appear in the details pane.
2 Click any policy link to view its settings.

View policies assigned to a specific system
View a list of all policies assigned to a system from one central location, the System Tree. For example, if you have different policies assigned to specific systems, use this task to confirm the policies are set correctly.

Task
1 Select Menu | Systems | System Tree, click the Systems tab, then select a group in the System Tree.
All systems belonging to the group appear in the details pane.
2 Click the name of a system to drill into the System Information page, then click the Applied Policies tab.

View policy inheritance for a group
View the policy inheritance of a specific group. For example, if you have policy inheritance configured for different groups, use this task to confirm the policy inheritance is set correctly.
Task

1. Select Menu | Systems | System Tree.

2. Click Assigned Policies tab.

   All assigned policies, organized by product, appear in the details pane.

The policy row, under Inherit from, displays the name of the group from which the policy is inherited.

**View and reset broken inheritance**

Identify the groups and systems where policy inheritance is broken.

For example, if you have policies with broken inheritance configured for some groups, use this task to confirm the policies are set correctly.

Task

1. Select Menu | Systems | System Tree, then click Assigned Policies tab.

   All assigned policies, organized by product, appear in the details pane. The policy row, under Broken Inheritance, displays the number of groups and systems where this policy's inheritance is broken.

   ![Note](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.
Deploying products

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

Contents

- Benefits of product deployment projects
- The Product Deployment page
- Viewing Product Deployment audit logs
- View product deployment
- Deploy products using a deployment project
- Monitor and edit deployment projects
- Manage Agent Deployment URLs
- Uninstall product software from systems
- The Audit Log

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 allow you 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 Product Deployment page

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

The page is separated into two main areas. The second area is separated into five smaller areas.

![Product Deployment page](image)

**Figure 10-1  Product Deployment page**

The main areas are:

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

   An exclamation point icon, ![exclamation point](image), indicates that either deployment is an uninstallation in progress or that a package that the deployment uses has been moved, deleted, or expired.

2. **Deployment details** — Lists the details of the selected deployment and includes the following areas.
Status monitor — Displays the progress and status depending on the type of deployment and its status:

- Continuous deployments display a calendar if the deployment is pending, or a bar chart during the deployment.
- Fixed deployments display a calendar if the deployment is pending, a bar chart if Current is selected, or a histogram if Duration is selected.

You can use Action to change a deployment.

Details — Allows you to view deployment configuration details, status, and if needed, click View Task Details to open the Edit Deployment page.

System name — Displays a filterable list of target systems receiving the deployment. The systems are displayed according to the deployment type and whether the systems were selected individually, as tags, as System Tree groups, or query output tables. Clicking System Actions displays the filtered list of systems in a dialog box with more detail and allows you to perform actions on the systems, such as update.

Status — Displays a three-section bar indicating the progress of the deployment and its status.

Tags — Displays tags associated with the row of systems.

### Viewing Product Deployment audit logs

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

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 Cloud 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.

**Task**

1 Select Menu | Software | Product Deployment.

2 Select New Deployment to start a new project.

3 Type a name and description for this deployment. This name appears on the Product Deployment page after you save the deployment.

4 Choose the type of deployment:
   - **Continuous** — Uses your System Tree groups or tags to configure the systems receiving the deployment. This feature allows these systems to change over time as they are added or removed from the groups or tags.
   - **Fixed** — Uses a fixed (defined) set of systems to receive the deployment. System selection is done using your System Tree or the output of Managed Systems Queries.

5 To automatically update your products, make sure that the Auto Update checkbox is selected. If the checkbox is deselected, products are still updated with the latest patches, hotfixes, and content packages, but major and minor releases are ignored.

   During a new deployment, the McAfee Agent checks for new updates, hotfixes, and content packages of all installed products on the client. See the McAfee Agent documentation for details.

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

7 From the Actions list, select Install or Uninstall.

8 In the Command line text field, specify any command-line installation options. For information about command-line options, see the product documentation for the software you're deploying.

9 Under Select the systems, click Select Systems.
The System Selection dialog box is a filter that allows you to select groups in your System Tree using these tabs:

- **System Tree** — Select System Tree groups or subgroups and their associated systems.
- **Tags** — Select tag groups or tag subgroups and their associated systems.
- **Selected Systems** — Displays the total selections you made in each tab, creating the target systems for your deployment.

For example, if your System Tree contains Group A, which includes both servers and workstations, you can target the entire group. You can also target only the servers or only the workstations (if they are tagged correctly), or a subset of either system type in Group A.

If needed, configure the following:

- Allow end users to postpone this deployment (Windows only)
- Maximum number of postponements allowed
- Option to postpone expires after
- Display this text

10 Under **Select a start time** select a schedule for your deployment:

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

11 Click **Save** at the top of the page. The Product Deployment page opens with your new project added to the list of deployments.

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

---

**Monitor and edit deployment projects**

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

**Task**

1. Select **Menu | Software | Product Deployment**.
2. Filter the list of deployment projects using the following:
   - **Type** — Filters the deployments that appear by All, Continuous, or Fixed.
   - **Status** — Filters the deployments that appear by All, Finished, In Progress, Pending, Running, or Stopped.
3. From the list on the left side of the page, click a deployment to display its details on the right side of the page.

   If a package in this deployment expires, the deployment is invalid. If you mouse-over the deployment, you see this message: "Package(s) in this deployment have been moved, deleted, or expired."
4 Use the progress section of the details display to view:
   • Calendar displaying the start date for pending continuous and fixed deployments.
   • Histogram displaying systems and the time to completion for fixed deployments.
   • Status bar displaying system deployment and uninstallation progress.

      Under the status bar, Task Status lists Successful, Failed, and Pending for the number of target systems in parentheses.

5 Click Action and one of these actions to modify a deployment:
   • Edit
   • Delete
   • Duplicate
   • Mark Finished
   • Resume
   • Stop
   • Uninstall

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.

Manage Agent Deployment URLs

You can create, delete, enable, disable, or view Agent Deployment URLs using the McAfee ePO Cloud server.
Task

1. Select Menu | Systems | System Tree, then click the Agent Deployment tab.
2. Click Actions, then select the required option.

<table>
<thead>
<tr>
<th>Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Columns</td>
<td>Opens the Choose Columns page where you select the columns to display in the Agent Deployment page.</td>
</tr>
<tr>
<td>Create Agent Deployment URL</td>
<td>Opens the Agent Deployment URL page where you to create a new URL for Agent Deployment.</td>
</tr>
<tr>
<td>Delete Agent Deployment URL</td>
<td>Deletes the selected Agent Deployment URL.</td>
</tr>
<tr>
<td>Enable/Disable Agent Deployment URL</td>
<td>Controls whether the client system users can deploy the agent using the URL.</td>
</tr>
<tr>
<td>Export Table</td>
<td>Displays the Export page where you choose the way the table is exported.</td>
</tr>
<tr>
<td>View Agent Deployment URL</td>
<td>Displays the Agent Deployment URL.</td>
</tr>
</tbody>
</table>

Uninstall product software from systems

You can uninstall all product software from managed systems in a group using the existing product deployment task.

Before you begin

You must know the group name of the systems where the product software is installed to use the uninstall feature in Product Deployment.

If there are any systems you don’t want to uninstall the product software from, move them to a different group before starting this process.

This product software uninstallation process uses the Product Deployment task created during your initial software installation. When the uninstallation task is complete, all systems in the System Tree group specified at installation have all product software removed. You can use this process when you are done evaluating products.

You can’t use this process to choose which products are installed or removed. To install a subset of products on a group of systems, create a different product deployment task or installation URL to do so.

Task

1. To open the Product Deployment page, select Menu | Software | Product Deployment.
2. In the product deployment list, select the deployment task that you used to initially create the installation URL. That task is the product deployment task used to uninstall the product software from that group of systems.

To find the correct task to use, look for the product deployment name with the group name or URL name appended to "Initial Deployment <GroupName>." For example, "Initial Deployment My Group."
With the product deployment task selected, in the Actions list, select **Uninstall**.

The uninstallation task starts with the status displayed in a progress bar.

The configured product software is removed from all systems in the selected System Tree group. When the uninstallation is finished, **Uninstall Successful** appears with the number of updated systems shown in parentheses.

To delete the product deployment task, select it from the product deployment list and select **Delete** from the Actions list.

Delete the associated System Tree group.

1. Open the System Tree: select **Menu | Systems | System Tree**.

2. Click **System Tree Actions | Delete Group**.

3. Select **Remove McAfee Agent on next agent-server communication from all systems**, then click **OK**.

The group is removed from the System Tree, and all associated systems are removed from McAfee ePO Cloud management. You can reuse the group name later.

After the products are uninstalled and the systems removed from McAfee ePO Cloud management, you can create a product deployment task or installation URL. For example, you might configure a different product deployment task to install a subset of products on the systems in the group.

### The Audit Log

Use the Audit Log to maintain and access a record of all McAfee ePO Cloud user actions. The Audit Log entries are displayed in a sortable table. For added flexibility, you can also filter the log so that it displays only failed actions, or only entries that are in a certain age.

The Audit Log displays these columns:

- **Action** — The name of the action the McAfee ePO Cloud user tried.
- **Completion Time** — The time the action finished.
- **Details** — More information about the action.
- **Priority** — Importance of the action.
- **Start Time** — The time the action was initiated.
- **Success** — Whether the action was successfully completed.
- **UserName** — User name of the logged-on user account that was used to take the action.

### View user actions

The Audit Log displays past user actions. Use the Audit Log to track access to your McAfee ePO Cloud 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.**
Client tasks

Create and schedule client tasks to automate how you manage systems in your network. Client tasks are commonly used for these activities.

- Product functionality
- Upgrades and updates

For information about which client tasks are available and what they can help you do, see the documentation for your managed products.

Contents
- How the Client Task Catalog works
- Updating tasks
- Manage client tasks

How the Client Task Catalog works

Use the Client Task Catalog to create client task objects you can reuse to help manage systems in your network. The Client Tasks Catalog applies the concept of logical objects to McAfee ePO Cloud 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.

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.

Updating tasks

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.

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.

- 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 Cloud 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. 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**.

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

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

11 Review the summary, then click **Save**.

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

---

**Manage client tasks**

Create and maintain client tasks.

**Tasks**

- **Create client tasks on page 91**
  Use client tasks to automatically perform product updates. The process is similar for all client tasks.

- **Edit client tasks on page 92**
  You can edit any previously configured client task settings or schedule information.

- **Delete client tasks on page 92**
  You can delete any previously configured client tasks.

- **Compare client tasks on page 93**
  The Client Task Comparison tool determines which client task settings are different and which are the same.

- **View client tasks assigned to a specific system on page 93**
  View a list of all client tasks assigned to a system from one central location, the System Tree.

**Create client tasks**

Use client tasks to automatically perform product updates. The process is similar for all client tasks. In some cases, you must create a new client task assignment to associate a client task to a System Tree group.
**Task**

1. Open the New Task dialog box.
   a. Select **Menu** | **Policy** | **Client Task Catalog**.
   b. Under Client Task Types, select a product, then click **New Task**.

2. Select a task type from the list, then click **OK** to open the Client Task Builder.

3. Enter a name for the task, add a description, then configure the settings specific to the task type you are creating.
   
   The configuration options depend on the task type selected.

4. Review the task settings, then click **Save**.

   The task is added to the list of client tasks for the selected client task type.

**Edit client tasks**

You can edit any previously configured client task settings or schedule information.

**Task**

1. Select **Menu** | **Policy** | **Client Task Catalog**.

2. Select the **Client Task Type** from the navigation tree on the left.

   The available client tasks appear in the window on the right.

3. Click the client task name to open the Client Task Catalog dialog box.

4. Edit the task settings as needed, then click **Save**.

   The managed systems receive the changes you configured the next time the agents communicate with the server.

**Delete client tasks**

You can delete any previously configured client tasks.

**Task**

1. Select **Menu** | **Policy** | **Client Task Catalog** to open the Client Task Catalog dialog box.

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. From the **Actions** column, click **Delete** next to the client task.

4. Click **OK**.
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.
Client tasks
Manage client tasks
Use server and client tasks to automate McAfee ePO Cloud and managed system processes. McAfee ePO Cloud includes preconfigured server tasks and actions. Most of the additional software products you manage with McAfee ePO Cloud also add preconfigured server and client tasks.

**Contents**
- **Client tasks**
- **Server tasks**

## Client tasks

Create and schedule client tasks to automate how you manage systems in your network. Client tasks are commonly used for these activities.

- Product functionality
- Upgrades and updates

For information about which client tasks are available and what they can help you do, see the documentation for your managed products.

### 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 Cloud 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.

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.

### Updating tasks

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.
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.

• 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 Cloud 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. 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.

   To limit the list to specific tags, type the tag name in the text box under Tags.
10. On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.
11. Review the summary, then click Save.

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

Manage client tasks
Create and maintain client tasks.
Tasks

• **Create client tasks on page 91**
  Use client tasks to automatically perform product updates. The process is similar for all client tasks.

• **Edit client tasks on page 92**
  You can edit any previously configured client task settings or schedule information.

• **Delete client tasks on page 92**
  You can delete any previously configured client tasks.

• **Compare client tasks on page 93**
  The Client Task Comparison tool determines which client task settings are different and which are the same.

• **View client tasks assigned to a specific system on page 93**
  View a list of all client tasks assigned to a system from one central location, the System Tree.

Create client tasks

Use client tasks to automatically perform product updates. The process is similar for all client tasks.

In some cases, you must create a new client task assignment to associate a client task to a System Tree group.

**Task**

1. Open the New Task dialog box.
   a. Select **Menu | Policy | Client Task Catalog**.
   b. Under Client Task Types, select a product, then click **New Task**.

2. Select a task type from the list, then click **OK** to open the Client Task Builder.

3. Enter a name for the task, add a description, then configure the settings specific to the task type you are creating.
   
   The configuration options depend on the task type selected.

4. Review the task settings, then click **Save**.

   The task is added to the list of client tasks for the selected client task type.

Edit client tasks

You can edit any previously configured client task settings or schedule information.

**Task**

1. Select **Menu | Policy | Client Task Catalog**.

2. Select the **Client Task Type** from the navigation tree on the left.

   The available client tasks appear in the window on the right.

3. Click the client task name to open the Client Task Catalog dialog box.

4. Edit the task settings as needed, then click **Save**.

   The managed systems receive the changes you configured the next time the agents communicate with the server.
Delete client tasks
You can delete any previously configured client tasks.

Task

1. Select **Menu | Policy | Client Task Catalog** to open the **Client Task Catalog** dialog box.

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. From the **Actions** column, click **Delete** next to the client task.

4. Click **OK**.

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.

Server tasks
Server tasks are configurable actions that run on McAfee ePO Cloud at scheduled times or intervals. Leverage server tasks to automate repetitive tasks. McAfee ePO Cloud includes preconfigured server tasks and actions. Most of the additional software products you manage with McAfee ePO Cloud also add preconfigured server tasks.
View server tasks
The Server Task Log provides the status of your server tasks and displays any errors that might have occurred.

Task

1. Open the Server Task Log: select \textit{Menu} \textbar \textit{Automation} \textbar \textit{Server Task Log}.
2. Sort and filter the table to focus on relevant entries.
   - To change which columns are displayed, click \textit{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.

See also
\textit{Server task status} on page 100

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>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>

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 \textit{Menu} \textbar \textit{Automation} \textbar \textit{Server Task Log}.
2. Click \textit{Purge}.
3. In the Purge dialog box, enter a number, then select a time unit.
4. Click \textit{OK}.

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

- Create a server task to automatically remove outdated items.
Create a server task
Create server tasks to schedule various actions to run on a specified schedule.
If you want McAfee ePO Cloud 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.

See also
Accepted Cron syntax when scheduling a server task on page 102

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.

See also
Accepted Cron syntax when scheduling a server task on page 102

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 "1W", 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.
Index

A
about this guide 7
actions
Apply Tag 60
Check IP Integrity 50
Run Tag Criteria 57
Sort Now 53
Test Sort 53
used with Product Deployment 82
activate
users 14
administrators
change password 21
edit profile 21
view profile 21
agent
first call to server 51
GUID and System Tree location 51
Apply Tag action 57
Audit Log
about 86
deleting old entries 87
used with Product Deployment 81
viewing user actions 86
automatic responses
actions 43
configuring 43
planning 41
setup 41

B
best practices
duplicating policies before assigning 63
policy assignment locking 63
System Tree creation 52
borders, See System Tree organization

C
catch-all groups 50
charts (See queries) 37
Check IP Integrity action 50
client tasks (continued)
   comparing 93, 99
   creating 91, 98
   deleting 92, 99
   editing settings for 92, 98
   view 90, 96
   viewing assignment on a specific system 93, 99
   working with 91, 97
compare client tasks 93, 99
compare policies 69
contact support 19
criteria-based tags
   applying 61
   sorting 52
Cron syntax used with server tasks 102

dashboards
   first-time 31
   McAfee 31
   private 31
   public 31
   server settings 31
DAT file updating
   considerations for creating tasks 89, 95
daily task 90, 96
deployment
   installation URL 17
   view 81
   view assigned client task 90, 96
documentation
   audience for this guide 7
   product-specific, finding 8
typographical conventions and icons 7
domain synchronization 48

E
effect, See policy enforcement
engine updating
   scheduling a task 90, 96
Index

L
LAN connections and geographical borders 48
language packages. See agent License transfer 24
lists
filtering 29
searching 30
lists, working with 29
log on and log off 15
Lost and Found group 46

M
main menu
navigating in the interface 27, 29
making comments and suggestions 19
managed state 18
managed systems
policy management on 63
sorting, criteria-based 49
viewing policy assignment 76
McAfee ePO
differences from McAfee ePO Cloud 9
McAfee ePO Cloud
about 9
differences from McAfee ePO 9
how it works 10
McAfee recommendations
duplicate policies before assignment 63
evaluate borders for organization 48
System Tree planning 48
use IP addresses for sorting 48
use tag-based sorting criteria 49
McAfee ServicePortal, accessing 8
menu, See main menu
menu-based navigation 27
Merge licenses 24
monitors
using 31
My Group 46
My Organization group of System Tree 45

N
navigation
main menu 27
menu-based 27
shortcut bar 29
network bandwidth, See System Tree organization
notifications
event forwarding 33

O
one-time password
used with two-factor authentication 22
operating systems
  grouping 48
  legacy systems (Windows 95, Windows 98) 48
OTP, See one-time password

P
passwords
  change 21
  create 14
  reset 15
  Server Settings 25
personal settings, categories 25
policies
  about 63
  assigning and managing 71
  broken inheritance, resetting 77
  categories 63
  comparing 69
  controlling on Policy Catalog page 66
  group inheritance, viewing 76
  how they are applied to systems 63
  importing and exporting 63
  inheritance 63
  manage policies using policy history entries 68
  managing, on Policy Catalog page 66
  ownership 64
  settings, viewing 75
  viewing 63, 75
  working with Policy Catalog 65
policy assignment
  copying and pasting 73, 74
  disabled enforcement, viewing 76
  group, assigning to 72
  locking 63
  Policy Catalog 63
  systems, assigning to 72, 73
  viewing 75, 76
policy assignment rules
  about 64, 65
  and multi-slot policies 65
  creating 70
  deleting and editing 70
  editing priority 70
  importing and exporting 71
  priority 65
  rule criteria 64
  system-based 64
  system-based policies 65
  user-based 64
  user-based policies 65
  viewing summary 70
Policy Catalog
  manage policies using policy history entries 68
  page, viewing 63
  working with 65
policy enforcement
  enabling and disabling 67
  viewing assignments where disabled 76
  when policies are enforced 63
policy management
  assigning policies 63
  using groups 46
  working with client tasks 91, 97
product deployment
  about monitoring and changing 80
  creating 82
  methods 79
  monitoring and modifying 83
  projects 79
  uninstalling software 85
  view 81
  view assigned client task 90, 96
profile
  change password 21
  enable two-factor authentication 22
  view and edit 21
  providing feedback 19
Q
queries
  actions on results 35
  chart types 37
  custom, managing 38
  export formats 35
  exporting to other formats 36
  filters 37
  results as tables 37
  run existing 36
  using results to exclude tags on systems 60
Query Builder
  about 37
  creating custom queries 38
  result types 37
Quick Find 30
R
reports
  about 39
  actions 39
  running 39
  viewing output 39
Response Builder 43
response rules
  creating and editing 41
  Description page 42
  setting filters for 42
  setting thresholds 42
responses
  actions 43
responses
  configuring 43
  event forwarding 33
responses, automatic
  about 41
Run Tag Criteria action 57

S
  scheduling
    server tasks with Cron syntax 102
server settings
  dashboards 31
  event notifications 33
  overview 34
Server Task Log
  removing outdated tasks 100
  Status column 100
  viewing server tasks 100
server tasks
  about 99
  creating 101
  removing outdated 100
  removing outdated log items 101
  scheduling with Cron syntax 102
  status of 100
  viewing 100
servers
  settings and controlling behavior 34
ServicePortal, finding product documentation 8
shortcut bar
  customizing 29
  using 27
Sort Now action 49
sorting criteria
  configuring 52
  for groups 52
  groups, automated 49
  IP address 50, 52
  sorting systems into groups 49
  tag 52
  tag-based 49, 50
SQL servers, See databases
subgroups
  criteria-based 51
subnets, as grouping criteria 48
subscription, view information 24
synchronization
  defaults 51
System Tree
  assigning policies to a group 72
  creation, automated 48
  criteria-based sorting 49
  defined 46
  deleting systems from 46
  inheritance 47
  (continued)
  Lost and Found group 46
  My Group 46
  My Organization level 45
  organization 45
  populating groups 52
  removing systems 54
  structure 45
System Tree organization
  borders in your network 48
  creating groups 52
  moving systems to groups manually 54
  network bandwidth 48
  operating systems 48
  planning considerations 48
  selecting multiple items 31
System Tree sorting
  default settings 51
  enabling 53
  IP address 50
  ordering subgroups 50
  tag-based criteria 50
system-based policies
  about 65
  criteria 65
systems
  assigning policies to 72, 73
  managed state 18
  pasting policy assignments to 74
  policy enforcement for a product 68
  sorting into groups 53
  viewing policy assignment 76
T
  table row, select checkboxes 30
  tables, working with 29
Tag Builder wizard 57
Tag Catalog 57
tag-based sorting criteria 49, 50
tags
  applying 61
  create, delete, and modify subgroups 59
  creating with Tag Builder wizard 57
  criteria-based 49
  criteria-based sorting 52
  edit, delete, and move 58
  excluding systems from automatic tagging 60
  export and import 59
  group sorting criteria 49
  manual application of 60
  policy assignment based on 65
  tags, subgroups
  create, delete, and modify 59
  selecting multiple items 31
technical support, finding product information 8
Test Sort action 49
Threat Event Log
common event format 32
time zone, personal 25
two-factor authentication
edit yours or a user’s profiles 23
enable in profile 22

U
updates
client tasks 89, 95
considerations for creating tasks 89, 95
scheduling an update task 90, 96
user accounts
activate 14
change default 21
change password 21
contact support 19
edit profile 21
log on 15
manage 25
password 14
reset password 15
user accounts (continued)
view profile 21
view subscription information 24
user actions
removing outdated 87
viewing 86
user menu, navigating in the interface 27
user-based policies
about 65
criteria 65
user, time zone 25
users
activate 14
contact support 19
log on 15
reset password 15
view subscription information 24

V
VPN connections and geographical borders 48

W
WAN connections and geographical borders 48