Product Guide

McAfee Agent 5.0.0
For use with ePolicy Orchestrator Cloud Software
COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

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

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

LICENSE INFORMATION

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>5</td>
</tr>
<tr>
<td>About this guide</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>Conventions</td>
<td>5</td>
</tr>
<tr>
<td>Find product documentation</td>
<td>6</td>
</tr>
<tr>
<td><strong>Introducing McAfee Agent</strong></td>
<td></td>
</tr>
<tr>
<td>1 About the McAfee Agent</td>
<td>9</td>
</tr>
<tr>
<td>New features</td>
<td>9</td>
</tr>
<tr>
<td>McAfee Agent feature support</td>
<td>10</td>
</tr>
<tr>
<td><strong>Installing, upgrading, and removing the agent</strong></td>
<td></td>
</tr>
<tr>
<td>2 Installing McAfee Agent</td>
<td>15</td>
</tr>
<tr>
<td>System requirements</td>
<td>15</td>
</tr>
<tr>
<td>Supported languages</td>
<td>16</td>
</tr>
<tr>
<td>Deploying from McAfee ePO server</td>
<td>17</td>
</tr>
<tr>
<td>Deploying McAfee Agent using the McAfee Smart installer</td>
<td>18</td>
</tr>
<tr>
<td>Create customized McAfee Smart installer</td>
<td>19</td>
</tr>
<tr>
<td>Install McAfee Agent using customized McAfee Smart installer</td>
<td>19</td>
</tr>
<tr>
<td>Command-line options for installing URL-based McAfee Agent manually</td>
<td>20</td>
</tr>
<tr>
<td>Manage Agent Deployment URLs</td>
<td>22</td>
</tr>
<tr>
<td>Install McAfee Agent in Virtual Desktop Infrastructure mode</td>
<td>22</td>
</tr>
<tr>
<td>Processes used by McAfee Agent 5.0.0</td>
<td>23</td>
</tr>
<tr>
<td>3 Removing the McAfee Agent</td>
<td>25</td>
</tr>
<tr>
<td>Remove agents when deleting systems from the System Tree</td>
<td>25</td>
</tr>
<tr>
<td>Remove agents when deleting groups from the System Tree</td>
<td>25</td>
</tr>
<tr>
<td>Remove agents from systems in query results</td>
<td>26</td>
</tr>
<tr>
<td>Remove the agent from a Windows command prompt</td>
<td>26</td>
</tr>
<tr>
<td>Remove McAfee Agent from non-Windows operating systems</td>
<td>26</td>
</tr>
<tr>
<td><strong>Using McAfee Agent</strong></td>
<td></td>
</tr>
<tr>
<td>4 Configuring McAfee Agent policies</td>
<td>31</td>
</tr>
<tr>
<td>McAfee Agent policy settings</td>
<td>31</td>
</tr>
<tr>
<td>Configuring General policy</td>
<td>32</td>
</tr>
<tr>
<td>Priority event forwarding</td>
<td>33</td>
</tr>
<tr>
<td>Retrieve system properties</td>
<td>33</td>
</tr>
<tr>
<td>Configuring proxy settings for McAfee Agent</td>
<td>33</td>
</tr>
<tr>
<td>Configure proxy settings for the agent</td>
<td>34</td>
</tr>
<tr>
<td>5 Working with the agent from the McAfee ePO server</td>
<td>37</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How agent-server communication works</td>
<td>37</td>
</tr>
<tr>
<td>Agent-to-Server Communication Interval</td>
<td>37</td>
</tr>
<tr>
<td>Agent-server communication interruption handling</td>
<td>38</td>
</tr>
<tr>
<td>McAfee Agent relay capability</td>
<td>38</td>
</tr>
<tr>
<td>Communicating through a RelayServer</td>
<td>38</td>
</tr>
<tr>
<td>Enable relay capability</td>
<td>39</td>
</tr>
<tr>
<td>Disable relay capability</td>
<td>39</td>
</tr>
<tr>
<td>Peer-to-Peer communication</td>
<td>40</td>
</tr>
<tr>
<td>Downloading content update from peer agents</td>
<td>40</td>
</tr>
<tr>
<td>Best practices for using Peer-to-Peer communication</td>
<td>41</td>
</tr>
<tr>
<td>Enable Peer-to-Peer service</td>
<td>41</td>
</tr>
<tr>
<td>Collect McAfee Agent statistics</td>
<td>42</td>
</tr>
<tr>
<td>Change the agent user interface and event log language</td>
<td>42</td>
</tr>
<tr>
<td>Scheduling client tasks</td>
<td>43</td>
</tr>
<tr>
<td>Locate inactive agents</td>
<td>44</td>
</tr>
<tr>
<td>Windows system and product properties reported by the agent</td>
<td>44</td>
</tr>
<tr>
<td>View McAfee Agent and product properties</td>
<td>46</td>
</tr>
</tbody>
</table>

## 6 Running McAfee Agent tasks from the managed system

- Using the system tray icon                                             | 47   |
- What the system tray icon does                                         | 47   |
- Making the system tray icon visible                                   | 48   |
- Enabling user access to updating functionality                         | 48   |
- Updates from the managed system                                       | 49   |
- Run a manual update                                                    | 49   |
- Enforce policies                                                       | 49   |
- Update policies and tasks                                              | 50   |
- Send properties to the McAfee ePO server                               | 50   |
- Send events to the McAfee ePO server on-demand                         | 50   |
- View version numbers and settings                                      | 50   |
- McAfee Agent command-line options                                     | 51   |

## 7 McAfee Agent activity logs

- About the McAfee Agent activity logs                                  | 53   |
- View McAfee Agent activity log from the managed system                | 54   |

## A Frequently asked questions

- Index                                                                  | 57   |
Preface

This guide provides the information you need for all phases of product use, from installation to configuration to troubleshooting.

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.
- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.
- **Reviewers** — People who evaluate the product.

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**
  - Title of a book, chapter, or topic; a new term; emphasis.
- **Bold**
  - Text that is strongly emphasized.
- **User input, code, message**
  - Commands and other text that the user types; a code sample; a displayed message.
- **Interface text**
  - Words from the product interface like options, menus, buttons, and dialog boxes.
- **Hypertext blue**
  - A link to a topic or to an external website.
- **Note:** Additional information, like an alternate method of accessing an option.
- **Tip:** Suggestions and recommendations.
Find product documentation

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

**Task**

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

2. Enter a product name, select a version, then click **Search** to display a list of documents.
Introducing McAfee Agent

Get familiar with McAfee Agent and what it does after being installed on the client system.

Chapter 1  About the McAfee Agent
About the McAfee Agent

McAfee® Agent is the client-side component providing secure communication between McAfee® ePolicy Orchestrator® (McAfee ePO™) and managed products. It also serves as an updater for managed and unmanaged McAfee products.

In addition, McAfee Agent provides local services to the managed products and to products developed by McAfee Security Innovation Alliance partners.

Systems can be managed by McAfee ePO only if they have an agent installed. While running silently in the background, the McAfee Agent:

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

Contents

- New features
- McAfee Agent feature support

New features

McAfee Agent 5.0.0 architecture is single threaded and asynchronous based on services (messaging) architecture. In a messaging-based architecture the services communicate using a common language. This reduces the usage of system resources, such as number of threads, number of handles, memory, and CPU.

McAfee Agent 5.0.0 is the minimum required version for McAfee ePO Cloud 5.2.0 or later.

McAfee Agent 5.0.0 include these new features.

Manifest based policy

When using McAfee Agent 5.0.0 in combination with the McAfee ePO server 5.2.0, the Manifest-based policy feature will help improve the scalability of McAfee ePO platform. In a manifest-based policy, only the changed policy settings will be fetched by McAfee Agent from the McAfee ePO server. Because only the difference in the policy setting is downloaded, McAfee Agent doesn't use resources for comparing or merging the settings. Additionally, the McAfee ePO server will not have to compute the changed policies at each agent server communication. This helps saving network bandwidth every time a policy update is downloaded.
**Persistent connection**

When performing an agent-server communication (ASC), McAfee Agent keeps the communication channel with the McAfee ePO server active using Keep-Alive connection. This allows McAfee Agent to complete an ASC using a single TCP connection to send and receive multiple HTTP requests or responses.

Previous versions of McAfee ePO server required multiple TCP connections from McAfee Agent during a single ASC. This required more network bandwidth, whereas using Keep-Alive connection reduces the network bandwidth.

**Sensor services**

McAfee Agent 5.0.0 uses sensor services to track system events and take actions on the client system. There are two types of sensor services

- User sensors — Detects the logged on users on the client system using operating system APIs and apply the user-based policies accordingly.

- Network sensors — Detects the network connectivity status using operating system network APIs and determines if agent functionality such as pulling updates from the repository or communicating to McAfee ePO should be performed.

**Peer-to-Peer communication**

To retrieve updates and install products, McAfee Agent needs to communicate with the McAfee ePO server. These updates might be available with the agents in the same subnet. With Peer-to-Peer communication, McAfee Agent downloads these updates from the peer agents in the same subnet reducing bandwidth consumption between the McAfee ePO server and McAfee Agent.

See *Peer-to-Peer service* for details on configuring the feature.

---

### McAfee Agent feature support

The table lists the McAfee Agent features and its platform support.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows</th>
<th>Non-Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit Native</td>
<td>Partially</td>
<td>Linux only</td>
</tr>
<tr>
<td>Relay server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Peer-to-Peer</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy-enabled application service logging</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy-enabled debug logging</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable log rotation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>McAfee Agent upgrade from the McAfee ePO server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>McAfee Smart Installer</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Property collection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Most of the McAfee Agent services are in 64-bit. However, to support other managed products few McAfee Agent services or processes are retained in 32-bit.*
<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows</th>
<th>Non-Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy enforcement</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Task enforcement</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Product Update</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Product Deployment</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Event Forwarding</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv4, IPv6, and mixed mode compatibility</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Managed product Plugin Architecture support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Communication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CmdAgent</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Run Immediately scheduling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Run Once scheduling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Run missed task scheduling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System startup scheduling</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>At logon scheduling</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Automatic McAfee Agent uninstall from the McAfee ePO server</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cluster node property reporting</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>UNC repository updating</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>McAfee Agent status monitor</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>McTray application support</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Installing, upgrading, and removing the agent

Installing the agent on client systems is required for managing your security environment through ePolicy Orchestrator.

Chapter 2  Installing McAfee Agent
Chapter 3  Removing the McAfee Agent
Installing, upgrading, and removing the agent
You can create a customized McAfee Smart installer by selecting the required operating system and McAfee Agent version. Managed node users can install McAfee Agent with these customized McAfee Smart installer. You can install McAfee Agent on Windows and other supported platforms using the McAfee Smart installer.

Contents

- System requirements
- Deploying from McAfee ePO server
- Deploying McAfee Agent using the McAfee Smart installer
- Install McAfee Agent in Virtual Desktop Infrastructure mode
- Processes used by McAfee Agent 5.0.0

System requirements

Make sure your client systems meet these requirements before installing McAfee Agent.

System requirements

- Installed disk space — 50 MB (minimum), excluding log files
- Memory — 512 MB RAM (minimum)
- Processor speed — 1 GHz (minimum)

The list specifies the minimum system requirement for McAfee Agent. For information on system requirement for other McAfee products, refer to their respective McAfee product documentation.

Supported operating systems and processors

For information on supported operating systems, see KnowledgeBase article KB51573.

The agent supports all Data Execution Prevention modes in Windows operating systems.

Additional supported platforms

You can install the agent on the virtual guest operating systems using these virtualization environments.

- Windows 2008 Server Hyper-V
- ESX
- Citrix XenServer
- Citrix XenDesktop
Supported languages

McAfee Agent is translated into multiple languages and installs, by default in the locale of the operating system.

The Windows client systems support these languages:

<table>
<thead>
<tr>
<th>Language</th>
<th>Language code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazilian (Portuguese)</td>
<td>0416</td>
</tr>
<tr>
<td>Chinese (Simplified)</td>
<td>0804</td>
</tr>
<tr>
<td>Chinese (Traditional)</td>
<td>0404</td>
</tr>
<tr>
<td>Czech</td>
<td>0405</td>
</tr>
<tr>
<td>Danish</td>
<td>0406</td>
</tr>
<tr>
<td>Dutch</td>
<td>0413</td>
</tr>
<tr>
<td>English</td>
<td>0409</td>
</tr>
<tr>
<td>Finnish</td>
<td>040b</td>
</tr>
<tr>
<td>French</td>
<td>040c</td>
</tr>
<tr>
<td>German</td>
<td>0407</td>
</tr>
<tr>
<td>Italian</td>
<td>0410</td>
</tr>
<tr>
<td>Japanese</td>
<td>0411</td>
</tr>
<tr>
<td>Korean</td>
<td>0412</td>
</tr>
<tr>
<td>Norwegian</td>
<td>0414</td>
</tr>
<tr>
<td>Polish</td>
<td>0415</td>
</tr>
<tr>
<td>Portuguese</td>
<td>0416</td>
</tr>
<tr>
<td>Russian</td>
<td>0419</td>
</tr>
<tr>
<td>Spanish (Spain–Modern Sort)</td>
<td>0c0a</td>
</tr>
<tr>
<td>Spanish (Spain-Traditional Sort)</td>
<td>040a</td>
</tr>
<tr>
<td>Swedish</td>
<td>041d</td>
</tr>
<tr>
<td>Turkish</td>
<td>041f</td>
</tr>
</tbody>
</table>

Macintosh client systems support English, Japanese, French, German, and Spanish.

All other supported Non-Windows client systems support only English.

Using multiple languages in your environment

You might need to use more than one language in your environment. This requires additional steps to ensure that the appropriate character sets for your chosen languages are supported. McAfee recommends that you follow these suggestions to ensure that all characters for each language are properly displayed in the McAfee Agent monitor.

- Configure your Operating Systems to use Unicode support for McAfee Agent.
- Install the appropriate Operating System language packs on the systems that need to display language-specific characters.
Deploying from McAfee ePO server

Deploying from the McAfee ePO server allows you to install McAfee Agent on multiple client systems simultaneous.

- Systems must already be added to the System Tree.

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

- The user must have local administrator privileges on all target systems. Domain administrator rights are required on a system to access the default Admin$ shared folder. The McAfee ePO server service requires access to this shared folder to install McAfee Agent.

- The McAfee ePO server must be able to communicate with the target systems.

  Before beginning a large McAfee Agent deployment, ensure that the client systems are reachable from the McAfee ePO server. To test the connectivity between the McAfee ePO server and McAfee Agent, ping the client systems with either IP address or host name depending on how the client systems are identified in the McAfee ePO server.

    The ability to successfully use ping commands from the McAfee ePO server to managed systems is not required for the McAfee Agent to communicate with the server. It is, however, a useful test to determine if you can deploy McAfee Agent to those client systems from the McAfee ePO server.

- The Admin$ share folder on Windows target systems must be accessible from the McAfee ePO server. Verify that this is true on a sample of target systems. This test also validates your administrator credentials, because you cannot access remote Admin$ shares without administrator rights.

  From the McAfee ePO server, click Windows Start | Run, then type the path to the target system's Admin$ share, specifying system name or IP address. For example, type \\<System Name>\Admin$.

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

- Enable SSH on the Linux and Macintosh client systems before installing McAfee Agent from McAfee ePO.

  Comment out the following line in the /etc/sudoers file on a Red Hat operating system.

    Default requiretty

  Remove the comment from the following line /etc/ssh/sshd_config file

    PermitRootLogin Yes

  You must have root permissions to install McAfee Agent on non-Windows system.

- Network access must be enabled on Windows XP Home and Windows 7 Home client systems.

  Deploy the McAfee Agent from the McAfee ePO server or install a custom McAfee Agent installation package on systems running Windows XP Home.

- File and Print sharing must be enabled.

- Server services should be enabled.
Remote registry services should be enabled.

User Account Control must be temporarily disabled on client systems to push McAfee Agent from the McAfee ePO server.

The push deployment feature can install to many systems simultaneously. You can only install a single version of McAfee Agent on a client system. To install multiple McAfee Agent versions, you must configure multiple Product Deployment tasks.

## Deploying McAfee Agent using the McAfee Smart installer

The McAfee Smart installer is a customized URL-based installer that can be created using the McAfee ePO server.

You can create a customized McAfee Smart installer by selecting the required operating system and McAfee Agent version using the McAfee ePO server.

Clicking the McAfee Smart installer prompts you to save or run the executable file. The managed node users with administrator rights can run the executable file and install McAfee Agent on their system. Running the executable on the client system extracts the McAfee ePO server details and McAfee Agent unique token.

Once the executable is extracted, the client system tries to discover peer-to-peer servers in its broadcast domain to download the McAfee Agent installation and configuration files. On receiving the request, McAfee Agent that is configured as peer-to-peer server responds to the request and serves the content. See Peer-to-Peer communication section for more details.

If the client system is unable to find peer-to-peer servers in its broadcast domain, it tries to connect to the McAfee ePO server to download the configuration files. If the connection succeeds, the client system downloads and installs McAfee Agent.

If the installer is unable to connect to the McAfee ePO server directly, it uses the proxy server setting configured on the client system to download and install McAfee Agent. The installer uses the proxy server settings configured in the Internet Explorer for Windows client systems and System Preferences for Macintosh client systems.

- Download using proxy server is supported only on Windows and Macintosh client systems.
- You must provide the proxy server credentials if your client system requires authentication to connect to the proxy server.

If the client system fails to connect to the McAfee ePO server directly or using the proxy server, it broadcasts a message to discover an McAfee Agent with relay capability in its network. The RelayServer responds to the message and establishes connection with the client system. See McAfee Agent relay capability section for more details.

If McAfee Agent package download fails due to network connectivity problems, McAfee Agent resumes downloading the remaining installation files from the point it stopped when the McAfee Smart installer is run next time.
Create customized McAfee Smart installer

Use the New Systems page to create the McAfee Smart installer. The McAfee Smart installer can then be distributed to the user for downloading and installing the agent on the managed node.

**Before you begin**

- Ensure that the McAfee Agent extension is installed and the software package is checked in to the McAfee ePO server.
- To apply policies and install other McAfee products, create a group of managed nodes in the System Tree and assign policies and client tasks to them.

For option definitions, click ? or Help in the interface.

**Task**

1. Click **Menu | Systems | System Tree**, then in the **System Tree Actions** menu click **New Systems**.
   
   Alternatively, you can click **Menu | Systems | Agent Deployment tab**, then select **Actions | Create Agent Deployment Url**.

2. Select **Create url for client-side agent download** to create a URL from McAfee Agent installer.

3. Select the appropriate operating system and McAfee Agent version.

4. Click **OK**. A customized URL is displayed on the Agent Deployment URL page.

Install McAfee Agent using customized McAfee Smart installer

Managed node users can install McAfee Agent with the customized McAfee Smart installer created using the McAfee ePO server. You can install McAfee Agent on Windows and other supported platforms using the McAfee Smart installer.

**Before you begin**

You must have administrator rights to install McAfee Agent on the managed node.

Running the executable on the client system extracts the McAfee ePO server details from the coninfo .xml file. The client system tries to connect to the McAfee ePO server to download the installation and configuration files.

For option definitions, click ? or Help in the interface.

**Task**

1. Click the URL or copy and paste it into a browser.
   
   When entering the URL into a browser, make sure to enter the entire URL without spaces.

2. Perform one of these depending on the operating system.
## Operating system

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Steps to install</th>
</tr>
</thead>
</table>
| Windows          | 1. When prompted, download the installer. Alternatively, click **Install** to download and install McAfee Agent.  
2. In the **File Download** dialog box, click **Run**.  
You can also **Save** the file to local drive for later installation.  
3. Click **Run** to confirm installation. A dialog box appears displaying the progress of the installation.  
   The installation log **McAfeeSmartInstall_<date>_<time>.log** is saved in `<LocaltempDir>\McAfeeLogs`.  
Any time during the installation, click **Cancel** to stop installation. |
| Macintosh        | 1. When prompted, download the installer. The customized URL downloads the McAfeeSmartInstall.app file.  
   If you are using Mozilla Firefox, the customized URL downloads the McAfeeSmartInstall.app.zip file. Double-click the file to extract the McAfeeSmartInstall.app file.  
   2. Double-click the McAfeeSmartInstall.app file to confirm installation. A dialog box appears displaying the progress of the installation.  
   The installation log is saved in `/tmp`.  
   Click **Cancel** to stop McAfee Agent download. |
| Other supported non-Windows operating systems | • Run McAfee Agent installer from the folder where it is downloaded.  
   `<McAfeeSmartInstall.sh>` |

### Command-line options for installing URL-based McAfee Agent manually

By manually installing the URL-based McAfee Agent on Windows and other supported operating systems, you can override default installation parameters.

**Task**

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

- Run the following command on the client system with any of these parameters:
  ```
  <McAfeeSmartInstall.exe>
  ```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d &quot;Data path&quot;</td>
<td>Overrides the path of McAfee Agent data files. The default location is: &lt;Documents and Settings&gt;\All Users\Application Data\McAfee\Agent. If the operating system does not have a Documents and Settings folder, the default location is C:\ProgramData\ McAfee\Agent. Example: McAfeeSmartInstall.exe -d D:\McAfeeAgent\Data</td>
</tr>
<tr>
<td>-i &quot;Install path&quot;</td>
<td>Overrides the default folder where installation files are saved. You can use Windows system variables, such as &lt;SYSTEM_DRIVE&gt;. If not specified, the default location is: &lt;DRIVE&gt;:\Program Files\McAfee\Agent. Example: McAfeeSmartInstall.exe -i D:\McAfeeAgent</td>
</tr>
<tr>
<td>-g</td>
<td>Generates the debug log McAfeeSmartInstall_&lt;date&gt;_&lt;time&gt;.log. • On Windows client system, the log file is saved in &lt;Documents and Settings&gt;&lt;User&gt;\Local\Temp\McAfeeLogs. • On Macintosh client system, the log file is saved in /tmp. • On other Non-Windows client system, the log file is saved in installation folder.</td>
</tr>
<tr>
<td>-a &quot;Proxy address&quot; -p &quot;Proxy port&quot;</td>
<td>Specifies the proxy server address and the port number. If the proxy server details are not provided, the installer uses the default browser proxy server setting.</td>
</tr>
<tr>
<td>-k</td>
<td>Switches off the peer and certificate verification of the https server from where the installer downloads the configuration file.</td>
</tr>
<tr>
<td>-u &quot;Proxy user name&quot; -w &quot;Proxy password&quot;</td>
<td>Specifies the user name and password for the authenticated proxy server.</td>
</tr>
<tr>
<td>-f</td>
<td>Forces McAfee Agent installation</td>
</tr>
<tr>
<td>-s</td>
<td>Installs McAfee Agent in silent mode</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-v</td>
<td>Installs McAfee Agent in the VDI mode.</td>
</tr>
<tr>
<td>?</td>
<td>Displays the help for command-line options.</td>
</tr>
<tr>
<td></td>
<td>This command-line parameter is not supported on Macintosh operating systems.</td>
</tr>
</tbody>
</table>

All the parameters are optional. If you don't specify a parameter, the installer uses the default value.

**Manage Agent Deployment URLs**

You can create, delete, enable, disable, or view agent deployment URLs using the ePolicy Orchestrator server.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Systems** | **System Tree** | **Agent Deployment**. The Agent Deployment pages appears.
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 allowing you to select the columns that will be displayed in the Agent Deployment page.</td>
</tr>
<tr>
<td>Create Agent Deployment Url</td>
<td>Opens Agent Deployment URL page allowing you to create 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>Enables or disables the client system users from deploying the agent using the URL.</td>
</tr>
<tr>
<td>Export Table</td>
<td>Displays the Export page allowing you to 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>

**Install McAfee Agent in Virtual Desktop Infrastructure mode**

If a new McAfee Agent identifier is created every time a virtual image or a system is started, it results in duplication of GUID. Installing McAfee Agent in Virtual Desktop Infrastructure (VDI) mode can avoid duplication of GUID.

Installing McAfee Agent in the VDI mode deprovisions the virtual image or the system every time its shut down. This enables the McAfee ePO server to save the deprovisioned McAfee Agent in its database. Once deprovisioned in the database, McAfee Agent will not be displayed in the McAfee ePO server console.

**Task**

For option definitions, click ? or Help in the interface.

1. Click **Menu** | **Systems** | **System Tree**, then from the **System Tree Actions** drop-down menu, select **New Systems**.
2. Type a name for the URL.
3. Select a **Agent version**.
When prompted, select the file to be downloaded. Right click and save the file.

Copy McAfee Agent installer on the virtual image and run the following command to install McAfee Agent in VDI mode:

```
McAfeeSmartInstaller.exe -v
```

McAfee Agent will start the ASC and enforce all the policies and tasks as configured on the McAfee ePO server.

To verify if McAfee Agent was installed in VDI mode, click **Menu | Systems | System Tree**, then select the system. The **System Information** page displays the properties of the client system reported by McAfee Agent. The value of the system property **Vdi** should be **Yes**.

### Processes used by McAfee Agent 5.0.0

The table lists the processes used by McAfee Agent 5.0.0.

<table>
<thead>
<tr>
<th><strong>Windows Processes/Applications</strong></th>
<th><strong>Non-Windows Processes</strong></th>
<th><strong>Service name</strong></th>
<th><strong>Service display name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>masvc.exe</td>
<td>masvc</td>
<td>Masvc</td>
<td>McAfee Agent Service</td>
<td>Performs functions such as property collection, policy enforcement, scheduling of tasks, agent server communication, and trigger update session</td>
</tr>
<tr>
<td>macmnsvc.exe</td>
<td>macmnsvc</td>
<td>Macmnsvc</td>
<td>McAfee Agent Common Services</td>
<td>Hosts multiple McAfee Agent services such as Peer-to-Peer server, Wake-up, and RelayServer</td>
</tr>
<tr>
<td>maccompatsvc.exe</td>
<td>maccompatsvc</td>
<td>McAfeeFramework</td>
<td>McAfee Agent Backwards Compatibility Service</td>
<td>This executable is the compatibility service for the McAfee Agent Service. McAfee Agent service starts this service and communicates to the various managed product plugins.</td>
</tr>
<tr>
<td>cmdagent.exe</td>
<td>cmdagent</td>
<td>N/A</td>
<td>N/A</td>
<td>This is a command line program that invokes McAfee Agent. To know more about switches available with this command, use <code>cmdagent.exe /?</code></td>
</tr>
<tr>
<td>FrmInst.exe</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>MA installation program To know more about switches available with this command, use <code>FrmInst.exe /?</code></td>
</tr>
<tr>
<td>Windows Processes/Applications</td>
<td>Non-Windows Processes</td>
<td>Service name</td>
<td>Service display name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
<td>--------------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>maconfig.exe</td>
<td>maconfig</td>
<td>N/A</td>
<td>N/A</td>
<td>This is a command line program used to configure different options of McAfee Agent. To know more about switches available with this command, use <code>maconfig -help</code>.</td>
</tr>
<tr>
<td>McScanCheck.exe</td>
<td>McScanCheck</td>
<td>N/A</td>
<td>N/A</td>
<td>Command line program used by McScript_InUse.exe to perform DAT or engine updates.</td>
</tr>
<tr>
<td>McScript_InUse.exe</td>
<td>Mue_InUse</td>
<td>N/A</td>
<td>N/A</td>
<td>Runs scripts for updating DAT files, Engines, Service Packs, or any other component checked into a repository. This process loads when update task is started.</td>
</tr>
<tr>
<td>UpdaterUI.exe</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>Provides user interface for updates. They also control the McAfee Agent icon in the System tray and are loaded via the Run key in the Windows registry.</td>
</tr>
<tr>
<td>McTray.exe</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>System tray icon management tool. It runs under the same user session and is started by UpdaterUI.exe.</td>
</tr>
</tbody>
</table>
Removing the McAfee Agent

After deleting McAfee Agent, the system is deleted from the System Tree and McAfee Agent is removed during the next agent-server communication.

If managed products still reside on systems after attempting to remove McAfee Agent, it continues to run unmanaged in updater mode to maintain those managed products.

Contents

- Remove agents when deleting systems from the System Tree
- Remove agents when deleting groups from the System Tree
- Remove agents from systems in query results
- Remove the agent from a Windows command prompt
- Remove McAfee Agent from non-Windows operating systems

Remove agents when deleting systems from the System Tree

You can remove McAfee Agent from a Windows system by deleting it from the System Tree.
For option definitions, click ? or Help in the interface.

Task

1. Click Menu | Systems | System Tree, then select the group with the systems you want to delete.
2. Select the systems from the list, then click Actions | Directory Management | Delete.
3. Select Remove agent on next agent-to-server communication, then click OK.

Remove agents when deleting groups from the System Tree

You can remove McAfee Agent from a group of Windows system when you delete that group from the System Tree.

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

For option definitions, click ? or Help in the interface.

Task

1. Click Menu | Systems | System Tree, then select a group to be deleted.
2. At the bottom of the System Tree panel, click System Tree Actions | Delete Group.
3. Select Remove agent from all systems, then click OK.
Remove agents from systems in query results

You can remove McAfee Agent from Windows systems listed in the results of a query (for example, the Agent Versions Summary query).

For option definitions, click ? or Help in the interface.

Task

1. Run a query, then from the results page, select the systems to be deleted.
2. Select Directory Management from the drop-down menu, then select Delete from the submenu.
3. Select Remove agent on next agent-to-server communication, then click OK.

Remove the agent from a Windows command prompt

The agent can be removed from a Windows system by running the agent installation program, FrmInst.exe, from the command line.

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

Task

1. Open a command prompt on the target system.
2. Run the agent installation program, FrmInst.exe, from the command line with the /REMOVE=AGENT option.

Remove McAfee Agent from non-Windows operating systems

Removing the agent from non-Windows operating systems must be done manually.

The task involves:

- Removing McAfee Agent from the system.
- Removing the system names from the McAfee ePO System Tree.
**Task**

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

1. Open a terminal window on the client system.

2. Run the command appropriate for your operating system, providing root credentials when requested.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Linux            | rpm -e MFEcma  
rpm -e MFErt  |
|                  | Run the commands in the listed order. |
| Ubuntu           | dpkg --remove MFEcma  
dpkg --remove MFErt  |
|                  | Run the commands in the listed order. |
| Macintosh        | /Library/McAfee/agent/uninstall.sh |

3. On the McAfee ePO server, click **Menu | Systems | System Tree**, then select the systems where you uninstalled McAfee Agent.

4. From the **Actions** drop-down menu, select **Directory Management**, then select **Delete** from the submenu.
Removing the McAfee Agent
Remove McAfee Agent from non-Windows operating systems
Using McAfee Agent

McAfee Agent can be updated and centrally managed from McAfee ePO through application and enforcement of policies and scheduled tasks. The log files record the events and actions on the managed systems.

Chapter 4 Configuring McAfee Agent policies
Chapter 5 Working with the agent from the McAfee ePO server
Chapter 6 Running McAfee Agent tasks from the managed system
Chapter 7 McAfee Agent activity logs
# Configuring McAfee Agent policies

McAfee Agent policy settings determine its performance and behavior in your environment.

## Contents
- McAfee Agent policy settings
- Configuring General policy
- Configuring proxy settings for McAfee Agent

## McAfee Agent policy settings

McAfee Agent provides configuration pages for setting policy options that are organized into these categories: **General**, **Repository**, and **Troubleshooting**.

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

When using McAfee Agent 5.0.0 with McAfee ePO 5.2.0, only the difference in the policy settings is downloaded from the server.

### General policy

Settings available for **General** policy is divided into following tabs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>- Policy enforcement interval</td>
</tr>
<tr>
<td></td>
<td>- Use of system tray icon in Windows environments</td>
</tr>
<tr>
<td></td>
<td>- Whether to accept connections only from the McAfee ePO server</td>
</tr>
<tr>
<td></td>
<td>- Yielding of the CPU to other processes in Windows environments</td>
</tr>
<tr>
<td></td>
<td>- Rebooting options after product deployment in Windows environments</td>
</tr>
<tr>
<td></td>
<td>- Agent-server communication</td>
</tr>
<tr>
<td></td>
<td>- Retrieving all system and product properties</td>
</tr>
<tr>
<td></td>
<td>- Restricting McAfee Agent processes, services, and registry keys modif.</td>
</tr>
<tr>
<td>SuperAgent</td>
<td>- Enabling RelayServer on McAfee Agent</td>
</tr>
<tr>
<td></td>
<td>- Enabling discovery of relay serves</td>
</tr>
</tbody>
</table>
**Configuring McAfee Agent policies**

Configuring General policy

You can configure policy enforcement interval, wake-up call support, reboot options, use of system tray icon, event forwarding on a priority basis, and system properties retrieval using **General policy**.

**Tasks**

- **Retrieve system properties on page 33**
  You can use McAfee Agent to retrieve system properties from managed systems.

---

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
</table>
| Events | - Enabling/disabling Priority event forwarding  
- Level of priority events forwarded  
- Interval between event uploads  
- Maximum number of events per upload |
| Logging | - Enabling/disabling application logging  
- Setting the log file size limit and roll over count  
- Level of logging detail |
| Updates | - Custom update log file location  
- Specifying post-update options  
- Downgrading DAT files  
- Selecting repository branches |
| Peer-to-Peer | - Enable peer-to-peer communication on McAfee Agent  
- Enable McAfee Agent to serve updates to peer agents  
- Specify the repository path  
- Specify the disk space for the updates on the peer-to-peer server  
- Specify the time interval to purge the files from the peer-to-peer server memory |

**Repository policies**

Proxy server settings can be configured using the **Repository** policy.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>Proxy configuration</td>
</tr>
</tbody>
</table>

**Troubleshooting policies**

Settings available for **Troubleshooting** policies are contained within a single tab.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>McAfee Agent user interface and log language</td>
</tr>
</tbody>
</table>
**Priority event forwarding**

You can configure McAfee Agent to forward events on a priority basis if they are equal to or greater than a specified severity.

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

Specific event severities are determined by the product that generates the events. You can enable priority uploading of events on the Events tab of the McAfee Agent policy pages.

The table lists the events generated by McAfee Agent with IDs and severity.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2401</td>
<td>Common update success</td>
<td>3</td>
</tr>
<tr>
<td>2402</td>
<td>Common update fail</td>
<td>4</td>
</tr>
<tr>
<td>2411</td>
<td>Deployment success</td>
<td>3</td>
</tr>
<tr>
<td>2412</td>
<td>Deployment fail</td>
<td>4</td>
</tr>
<tr>
<td>2413</td>
<td>McAfee Agent uninstall attempt</td>
<td>3</td>
</tr>
<tr>
<td>2422</td>
<td>Policy enforce fail</td>
<td>3</td>
</tr>
<tr>
<td>2427</td>
<td>Props collect fail</td>
<td>3</td>
</tr>
</tbody>
</table>

**Retrieve system properties**

You can use McAfee Agent to retrieve system properties from managed systems.

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

- McAfee Agent policy that specifies whether to retrieve a full set of information about installed programs, or only a minimal set as defined by the McAfee products.

**Task**

1. Click Menu | Policy | Policy Catalog.
2. Select McAfee Agent in the Product drop-down list and General in the Category drop-down list.
3. Click a policy name to update it.
4. Deselect Retrieve all system and product properties (recommended). If unchecked retrieve only a subset of properties. to send system properties and minimal product properties.
   
   This is selected by default.
5. Click Save.

**Configuring proxy settings for McAfee Agent**

To access the McAfee update sites, McAfee Agent must be able to access the Internet. Use McAfee Agent policy settings to configure proxy server settings for managed systems.

The Proxy tab of the McAfee Agent policy pages includes these settings:
Do not use a proxy (default setting)

You can select one of these depending on the product.

- **Use Internet Explorer proxy settings (For Windows)** — This setting allows McAfee Agent in a Windows environment to use the proxy server and credential information currently configured for Internet Explorer. There are several methods to configure Internet Explorer for use with proxies. For information, see Internet Explorer Help.

When this setting is selected, the fields for specifying user authentication for HTTP and FTP proxies become available, as well as the option **Allow user to configure proxy settings**. By selecting this option, the administrator grants permission to the user of a managed product to access additional update repositories that are configured behind the proxy server.

- **System Preferences settings (For Mac OSX)** — This setting allows McAfee Agent in a Macintosh environment to use the proxy server and credential information currently configured in its System Preferences.

- **Manually configure the proxy settings** — When this setting is selected, the fields for specifying user authentication for HTTP and FTP proxies and exceptions become available. This selection also allows the administrator to specify the HTTP and FTP locations using DNS name, IPv4 address, or IPv6 address.

### Configure proxy settings for the agent

You might need to configure proxy settings if an agent is having trouble accessing the Internet. For option definitions, click ? or Help in the interface.

**Task**

1. Click Menu | Policy | Policy Catalog, then from the Product drop-down menu, select McAfee Agent, and from the Category drop-down menu, select Repository.

2. From the list of policies, click any policy listed on this page other than McAfee Default.

3. Click Proxy.

4. Select your preferred option:

   - Select **Do not use a proxy** if your agent does not require a proxy to access the Internet. This is the default selection.

   - Select **Use Internet Explorer proxy settings (For Windows)** or **System Preferences settings (For Mac OSX)** depending on the operating system and if appropriate, select **Allow user to configure proxy settings**.

5. Select **Manually configure the proxy settings** if you need a proxy other than Internet Explorer, and configure the following settings:

   a. Select a form for the address of the source HTTP or FTP location where the agent is to pull updates.
      - DNS Name
      - IPv4
      - IPv6

   b. Type the DNS name or IP address and Port numbers of the HTTP and/or FTP source. If appropriate, select **Use these settings for all proxy types**.

   c. Select **Specify exceptions** to designate systems that do not require access to the proxy.
d Select Use HTTP proxy authentication and/or Use FTP proxy authentication, then provide a user name and credentials.

e Click Save.
Configuring McAfee Agent policies
Configuring proxy settings for McAfee Agent
Working with the agent from the McAfee ePO server

The McAfee ePO interface includes pages where agent tasks and policies can be configured, and where system properties, agent properties, and other McAfee product information can be viewed.

Contents

- How agent-server communication works
- McAfee Agent relay capability
- Peer-to-Peer communication
- Collect McAfee Agent statistics
- Change the agent user interface and event log language
- Scheduling client tasks
- Locate inactive agents
- Windows system and product properties reported by the agent

How agent-server communication works

McAfee Agent communicates with the McAfee ePO server periodically to send events and, ensure all settings are up-to-date. These communications are referred to as *agent-server communication*. During each agent-server communication, McAfee Agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the McAfee Agent. McAfee Agent enforces the new policies locally on the managed system and applies any tasks.

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

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

**Agent-to-Server Communication Interval**

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

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

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

• Enforces policies.

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

• How many systems are managed by the McAfee ePO server

• If your organization has stringent threat response requirements.

• If the network or physical location of clients is highly distributed

• If there is inadequate available bandwidth

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

**Agent-server communication interruption handling**

Interruption handling resolves issues that prevent a system from connecting with a McAfee ePO server. Communication interruptions can happen for many of reasons, and the Agent-Server connection algorithm is designed to reattempt communication if its first attempt fails.

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

• IP address

• Fully qualified domain name

• NetBIOS name

---

**McAfee Agent relay capability**

If your network configuration blocks communication between the McAfee Agent and the McAfee ePO server, McAfee Agent can't receive content updates, policies, or send events. Relay capability can be enabled on McAfee Agent that have direct connectivity to the McAfee ePO server to bridge communication between the client systems and the McAfee ePO server. You can configure more than one McAfee Agent as a RelayServer to maintain network load balance.

**Communicating through a RelayServer**

Enabling relay capability in your network converts a McAfee Agent to a RelayServer. A McAfee Agent with relay capability can access the McAfee ePO server or RelayServer listed in SiteList.xml. When a McAfee Agent fails to connect to the McAfee ePO server, it broadcasts a message to discover any McAfee Agent with relay capability in its network. Each RelayServer responds to the message and the McAfee Agent establishes a connection with the first RelayServer to respond.

Later, if a McAfee Agent fails to connect to the McAfee ePO server, it tries to connect to the RelayServer that first responded to the discovery message. McAfee Agent discovers each RelayServer in the network at every agent-server communication, and caches the details of the first five unique servers that responded to the discovery message. If the current RelayServer fails to connect with the McAfee ePO server or doesn't have the required content update, McAfee Agent connects to the next RelayServer available in its cache. Enable the policy option Enable Relay Communication to allow the client system to discover the relay servers.
When McAfee Agent uses relay to communicate with the McAfee ePO server, the connections are established on two parts; first between McAfee Agent and the RelayServer and, second between RelayServer and the McAfee ePO server. These connections are maintained till the duration of the communication.

**Enable relay capability**

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

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

For option definitions, click ? or Help in the interface.

**Task**

1. Click **Menu** | **Systems** | **System Tree** | **Systems**, then select a group under System Tree. All the systems within this group appear in the details pane.

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

3. From the product drop-down list, select **McAfee Agent**. The policy categories under McAfee Agent are listed with the system’s assigned policy.

4. If the policy is inherited, select **Break inheritance and assign the policy and settings below**.

5. From the **Assigned policy** drop-down list, select a **General** policy.

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

6. Select whether to lock policy inheritance to prevent any systems that inherit this policy from having another one assigned in its place.

7. On the SuperAgent tab, select these options as appropriate
   - Select **Enable Relay Communication** to allow agents to discover relay servers in the network.
   - Select **Enable RelayServer** to enable relay capability on an agent.

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

8. Click **Save**.

**Disable relay capability**

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

For option definitions, click ? or Help in the interface.
Task
1 Click **Menu | Systems | System Tree | Systems**, then select a group under the **System Tree**. All the systems within this group appear in the details pane.

2 Select the system on which the relay capability was enabled, then click **Actions | Agent | Modify Policies on a Single System**. The **Policy Assignment** page for that system appears.

3 From the product drop-down list, select **McAfee Agent**. The policy categories under **McAfee Agent** are listed with the system’s assigned policy.

4 From the **Assigned policy** drop-down list, select the **General** policy enforced on the client system and disable the policy.

5 On the **SuperAgent** tab, deselect these options as appropriate
   - Deselect **Enable Relay Communication** to stop agents from discovering the **RelayServers** in the network.
   - Deselect **Enable RelayServer** to disable the relay capability on McAfee Agent.

6 Click **Save**.

---

**Peer-to-Peer communication**

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

**Downloading content update from peer agents**

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

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

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

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

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

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

The peer-to-peer communication uses port 8082 to discover peer servers and port 8081 to serve peer agents with updates.
Best practices for using Peer-to-Peer communication

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

- We recommend that you enable peer-to-peer servers on PCs or virtual systems. Enabling peer-to-peer server on laptops or other mobile devices is not recommended.

- We recommend that you disable peer-to-peer servers on the systems that have poor network connectivity or are connected using VPN.

- When deploying McAfee Agent or managed products, or updating the products on large number of systems, we recommend that you enable peer-to-peer server on all systems. This limits the network traffic within the local subnet during the deployment or update.

- Peer-to-Peer communication is enabled by default. If your organization restricts peer-to-peer communication, disable the Peer-to-Peer policy.

- We recommend that you configure the Max disk quota always greater than the size of sum of commonly used application and updates (For example, if the DAT file size is 150MB and the average product update size is 100MB, the peer-to-peer disk quota should be more than 250MB).

Enable Peer-to-Peer service

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

Peer to peer service is enabled by default.

Task

For option definitions, click ? or Help in the interface.

1. Click Menu | Systems | System Tree | Systems, then select a group under System Tree. All the systems within this group appear in the details pane.

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

3. From the product drop-down list, select McAfee Agent. The policy categories under McAfee Agent are listed with the system's assigned policy.

4. If the policy is inherited, select Break inheritance and assign the policy and settings below.

5. From the Assigned policy drop-down list, select a General policy.

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

6. Select whether to lock policy inheritance to prevent any systems that inherit this policy from having another one assigned in its place.

7. On the Peer-to-Peer tab, select these options as appropriate
   - Select Enable Peer-to-Peer Communication to allow McAfee Agent to discover and use Peer-to-Peer servers in the network.
   - Select Enable Peer-to-Peer Serving to enable McAfee Agent to serve content to peer agents.

8. Click Save.
Collect McAfee Agent statistics

Run the McAfee Agent Statistics client task on the managed nodes to collect RelayServer statistics and network bandwidth saved by Peer-to-Peer communication.

For option definitions, click ? or Help in the interface.

Task

1. Click Menu | Systems | System Tree | Systems, then select a group under the System Tree. All systems within this group appear in the details pane.

2. Select a system, then click Actions | Agent | Modify Tasks on a Single System. The client tasks assigned for that system appear.

3. Click Actions | New Client Task Assignment.

4. From the product list, select McAfee Agent, then select McAfee Agent Statistics as the Task Type.

5. Click Create New task. The new client task page appears.

6. Select the required option, then click Save.

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

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

Change the agent user interface and event log language

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

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

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

Task

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog.

2. Select McAfee Agent from the Product drop-down list, and Troubleshooting in the Category drop-down list.

3. Click the name of a policy to modify, or duplicate an existing policy.

   The McAfee Default policy can’t be modified.

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

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

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

**Scheduling client tasks**

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

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

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

- **Daily** — Specifies that the task runs every day, at a specific time, on a recurring basis between two times of the day, or a combination of both.

- **Weekly** — Specifies that the task runs on a weekly basis. Such a task can be scheduled to run on a specific weekday, all weekdays, weekends, or a combination of them. You can schedule such a task to run at a specific time of the selected days, or on a recurring basis between two times of the selected days.

- **Monthly** — Specifies that the task runs on a monthly basis. Such a task can be scheduled to run on one or more specific days of each month at a specific time.

- **Once** — Starts the task on the time and date you specify.

- **At System Startup** — Starts the task the next time you start the server.

- **At logon** — Starts the task the next time you log on to the server.

- **Run immediately** — Starts the task immediately.

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

Additionally you can:

- Configure the start and end date on which the client task is available or unavailable to run at the scheduled intervals.

- Specify the time at which the task should begin.

- Specify whether to run the task only once at the Start time, or to continue running until a later time. You can also specify the interval at which the task runs during this interval.

- Specify whether the task should run at the local time on the managed system or Coordinated Universal Time (UTC).

- Configure how the task should behave and the action that should be taken if the task runs too long, or whether the task should run if it was missed.

See ePolicy Orchestrator product documentation for details on assigning and scheduling a client task.
**Locate inactive agents**

An inactive McAfee Agent is one that has not communicated with the McAfee ePO server within a user-specified time period.

Some agents might become disabled or be uninstalled by users. In other cases, the system hosting the McAfee Agent might have been removed from the network. McAfee recommends performing regular weekly searches for systems with these inactive agents.

**Task**

For option definitions, click ? or Help in the interface.

1. Click **Menu | Reporting | Queries & Reports**.
2. In the **Groups** list, select the **Agent Management** shared group.
3. Click **Run** in the **Inactive Agents** row to run the query.

The default configuration for this query finds systems that have not communicated with the McAfee ePO server in the last month. You can specify hours, days, weeks, quarters, or years.

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication.

---

**Windows system and product properties reported by the agent**

The McAfee Agent reports system properties to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

**System properties**

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

Each McAfee product designates the properties it reports to ePolicy Orchestrator and, of those, which are included in a set of minimal properties. This list shows the kinds of product data that are reported to ePolicy Orchestrator by the McAfee software installed on your system. If you find errors in the reported values, review the details of your products before concluding that they are incorrectly reported.
View McAfee Agent and product properties
A common troubleshooting task is to verify that the policy changes you made match the properties retrieved from a system.
For option definitions, click ? or Help in the interface.

Task
1. Click Menu | Systems | System Tree.
2. On the Systems tab, click the row corresponding to the system you want to examine.

Information about the system's properties, installed products, and agent appears. The top of the System Information page contains Summary, Properties, and Threat Events windows. It also displays System Properties, Products, Threat Events, and McAfee Agent tabs.
Running McAfee Agent tasks from the managed system

If you can access the managed system where McAfee Agent is installed, you can view and manage some its features.

McAfee Agent interface is available on the managed Windows system only if you selected Show McAfee system tray icon on the General tab of the McAfee Agent policy pages. To enable the Update Security... task for end users, you must have also selected Allow end users to update security from the McAfee System tray menu.

Contents

- Using the system tray icon
- Updates from the managed system
- Run a manual update
- Enforce policies
- Update policies and tasks
- Send properties to the McAfee ePO server
- Send events to the McAfee ePO server on-demand
- View version numbers and settings
- McAfee Agent command-line options

Using the system tray icon

The system tray icon provides a collection point for actions that can be performed on a client system. Every McAfee point-product provides actions and information to the system tray icon.

What the system tray icon does

The system tray icon resides in the Windows system tray on the client system and provides a user-interface entry point to products installed on that system.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Security</td>
<td>Triggers immediate updating of all installed McAfee software products. This includes application of patches and hotfixes, as well as DAT and signature updates.</td>
</tr>
<tr>
<td></td>
<td>This feature is available only if enabled in the agent policy.</td>
</tr>
<tr>
<td>Quick Settings</td>
<td>Links to certain product menu items that are frequently used.</td>
</tr>
<tr>
<td>Manage Features</td>
<td>Displays links to the administrative console of managed products.</td>
</tr>
<tr>
<td>Scan Computer for</td>
<td>Launches McAfee programs, such as VirusScan Enterprise, that scan systems on-demand and detect malicious software.</td>
</tr>
<tr>
<td>Option</td>
<td>Function</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View Security Status</td>
<td>Displays the current system status of managed McAfee products, including current events.</td>
</tr>
<tr>
<td>McAfee Agent Status Monitor</td>
<td>Triggers the Agent Status Monitor, which:</td>
</tr>
<tr>
<td></td>
<td>• Displays information on the collection and transmission of properties.</td>
</tr>
<tr>
<td></td>
<td>• Sends events.</td>
</tr>
<tr>
<td></td>
<td>• Enforces policies.</td>
</tr>
<tr>
<td></td>
<td>• Collect and send properties.</td>
</tr>
<tr>
<td></td>
<td>• Checks for new policies and tasks.</td>
</tr>
<tr>
<td>About...</td>
<td>Displays system and product information, including the agent, the McAfee ePO server or Agent Handler with which McAfee Agent communicates, and the software products being managed.</td>
</tr>
<tr>
<td>Agent status</td>
<td>Displays if the system managed or unmanaged. If it is a managed system, displays if these features are enabled.</td>
</tr>
<tr>
<td></td>
<td>• Peer-to-Peer</td>
</tr>
<tr>
<td></td>
<td>• Relay capability</td>
</tr>
</tbody>
</table>

**Making the system tray icon visible**

You can hide the system tray icon to restrict the use of McAfee Agent and other managed products. For option definitions, click `?` or `Help` in the interface.

**Task**

1. Click `Menu | Systems | System Tree.`
2. On the `Assigned Policies` tab, select `McAfee Agent` in the `Product` drop-down list.
3. Click the name of a policy that is in the `General` category.
4. Select `Show the McAfee system tray icon` (Windows only).
5. To allow users to update security on-demand, select `Allow end users to update security from the McAfee system tray menu`.
6. When selected, users who are running McAfee Agent can choose `Update Security` from the McAfee system tray icon to update all products for which an update package is present in the repository.
7. When you have completed your changes to the default configuration, click `Save`.

**Enabling user access to updating functionality**

You can enable users to update security settings on demand. This functionality is disabled by default. For option definitions, click `?` or `Help` in the interface.

**Task**

1. Click `Menu | Systems | System Tree.`
2. On the `Assigned Policies` tab, select `McAfee Agent` in the `Product` drop-down list.
3. Click the name of a policy that is in the `General` category.
4. Select Allow end users to run update security from the McAfee system tray menu.

5. When you have completed your changes to the default configuration, click Save.

---

**Updates from the managed system**

Security updates from a Windows managed system are possible, but the functionality is disabled by default to control when updates occur. If you want to allow Windows users to update all McAfee products on their managed systems, you must enable this functionality. The icon cannot be used to update applications selectively. The user can update all the items in the repository, or none of them.

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

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

---

**Run a manual update**

Updates can be run manually from a client system.

**Task**

- On the managed system, right-click the McAfee system tray icon and select **Update Security**.

McAfee Agent performs an update from the repository defined in the policy.

> **Important:** McAfee Agent pulls any updates available as defined by the policy. It does not use the configuration of any scheduled update tasks that might have selective updating enabled.

---

**Enforce policies**

The agent can enforce all configured policies on the managed system on demand.

**Task**

1. On the managed system, right-click the McAfee system tray icon, then select **McAfee Agent | McAfee Agent Status Monitor**.

2. Click **Enforce Policies**.

The policy enforcement activity is displayed in the **McAfee Agent Status Monitor**.
Update policies and tasks
You can manually trigger the agent to communicate with the server to update policy and tasks settings before the next agent-server communication.

Task
1. On the managed system, right-click the McAfee system tray icon, then select McAfee Agent | McAfee Agent Status Monitor.
2. Click Check New Policies.

The policy-checking activity is displayed in the McAfee Agent Monitor.

Send properties to the McAfee ePO server
The agent can manually send properties to the McAfee ePO server from the managed system if required before the next agent-server communication.

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

Agent policy controls whether full or minimal properties are sent.

Send events to the McAfee ePO server on-demand
You can force the agent to send events to the server on-demand from the managed system, instead of waiting for the next agent-server communication.

There is only one event that’s sent immediately, and that is when you uninstall the agent. All other events are queued and sent as soon as possible.

Task
1. On the managed system, right-click the McAfee system tray icon, then select McAfee Agent Status Monitor.
2. Click Send Events.

A record of the sending-events activity is added to the list of activities in the McAfee Agent Monitor.

This action sends all events to ePolicy Orchestrator regardless of severity.

View version numbers and settings
Information about McAfee Agent settings can be found on the managed system.

This is useful for troubleshooting when installing new McAfee Agent versions, or to confirm that the installed McAfee Agent is the same version as the one displayed in the properties on the server.
Each installed managed product provides information to the About dialog. McAfee Agent provides these information:

- McAfee Agent version number
- McAfee Agent Status
- SuperAgent status (Peer-to-Peer and RelayServer)
- Date and time of Last security update check
- Date and time of Last agent-server communication
- Agent-server communication interval
- Policy Enforcement Interval
- McAfee Agent GUID
- McAfee ePO server or Agent Handler DNS Name
- McAfee ePO server or Agent Handler IP Address
- McAfee ePO server or Agent Handler Port Number

**Task**

1. On the managed system, right-click the McAfee system tray icon.
2. Select About to view information about McAfee Agent.

---

**McAfee Agent command-line options**

Use the Command Agent tool to perform selected McAfee Agent tasks from the managed system.

Different Command Agent tools are available for Windows and non-Windows operating systems.

- **Windows** — `cmdagent.exe`
- **Non-Windows** — `cmdagent`

The Command Agent tool is installed on the managed system at the time of McAfee Agent installation. Perform this task locally on managed systems. It must be run within an Administrator command prompt.

The Command Agent tool file is located in the McAfee Agent installation folder. By default, this location is:

- **Windows** — `<Program Files>\McAfee\Agent`
- **Linux** — `/opt/McAfee/Agent`
- **Macintosh** — `/Library/McAfee/Agent`

- Using multiple switches per command can launch multiple concurrent Agent-to-Server communications and can cause policy errors. For example, `CmdAgent.exe /p /e /c`. Make sure you use only one switch per command.
- These switches are case-sensitive.

**Command-line options**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/c</td>
<td>Checks for new policies. McAfee Agent contacts the McAfee ePO server for new or updated policies, then enforces them immediately upon receipt.</td>
</tr>
<tr>
<td>/e</td>
<td>Prompts McAfee Agent to enforce policies locally.</td>
</tr>
</tbody>
</table>
### McAfee Agent command-line options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/p</td>
<td>Sends properties to the McAfee ePO server.</td>
</tr>
<tr>
<td>/s</td>
<td>Displays the McAfee Agent monitor on Windows client systems.</td>
</tr>
<tr>
<td>/f</td>
<td>Forwards events from client systems to the McAfee ePO server.</td>
</tr>
<tr>
<td>/i</td>
<td>McAfee Agent information</td>
</tr>
<tr>
<td>/h</td>
<td>Lists all the switches with their description</td>
</tr>
</tbody>
</table>

You can use McAfee Agent Return Codes with installation and removal scripts to allow the script to proceed to the next step or stop depending on the code returned. There are two possible return codes:

- **0** — Success  
- **-1** — Failure

For a code -1, either the parameter is invalid or it failed to open one of the global events for the framework service. Ensure that the service is running, the user has administrator rights, and you are using a valid command line.
The McAfee Agent activity log files are useful for determining agent status or for troubleshooting. McAfee Agent has two types of logs; Application logs and Remote logs. Application logs record the installer activities and agent activities such as policy enforcement and agent-server communication. Remote logs enable you to record and view McAfee Agent activities on the McAfee ePO server.

### About the McAfee Agent activity logs

You can configure General policy to enable agent activity logging on the managed systems and the McAfee ePO server.

Configuring the Application Logging options on the Logging policy tab allows McAfee Agent to record its activities in Agent log files and installation related activities in Install log files.

The table lists the Agent and Windows install log files

<table>
<thead>
<tr>
<th>Agent logs</th>
<th>Windows install logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>masvc_&lt;hostname&gt;.log</td>
<td>Frminst_&lt;hostname&gt;.log</td>
</tr>
<tr>
<td>macmnsvc_&lt;hostname&gt;.log</td>
<td>Frminst_&lt;hostname&gt;_Error.log</td>
</tr>
<tr>
<td>macompatsvc_&lt;hostname&gt;.log</td>
<td>MFEAgent.msi.&lt;system time stamp&gt;.log</td>
</tr>
<tr>
<td>mcScript.log</td>
<td>Vscore_install_vscore_&lt;systemtime&gt;.log</td>
</tr>
<tr>
<td>marepomirror.log</td>
<td>Vscore_uninstall_vscore_&lt;systemtime&gt;.log</td>
</tr>
<tr>
<td>UpdaterUI.log</td>
<td></td>
</tr>
<tr>
<td>UpdaterUI_Error.log</td>
<td></td>
</tr>
</tbody>
</table>

McAfee Agent doesn’t maintain log files for non-Windows installation. You can view these install logs on the command-line console only when installing McAfee Agent.

The agent logs are saved in these locations.

- **On Windows client systems:** `<Documents and Settings>\All Users\Application Data\McAfee\Agent\Logs`
  
  If the operating system does not have a Documents and Settings folder, the default location is `<ProgramData>\McAfee\Agent\Logs`

- **Non-Windows client systems:** `/var/McAfee/agent/logs`

On Windows client systems, the install logs are saved in `%TEMP%\McAfeeLogs`. 
You can define a size limit of these log files. On the Logging tab of the McAfee Agent policy pages, you can configure the level of agent activity that is recorded. You can also configure the roll over count that specifies the number of files the logs will be backed up in. Enabling detailed logging allows McAfee Agent to record its activities with more details that can help you during troubleshooting (for example, at log level 8 in previous versions of McAfee Agent).

In the Logging policy, if Enabled application logging is deselected McAfee Agent stops logging any application data. It is recommended that you enable this option for troubleshooting.

View McAfee Agent activity log from the managed system

The activity log is a condensed log and can be seen on the Windows client system using McAfee Agent tray icon (McTray).

Task
1. On the managed system, right-click the McAfee Agent icon in the system tray, then select McAfee Agent Status Monitor.

2. If you want to save the contents of the McAfee Agent activity log to a file, click Save Contents to Desktop.

   A file called Agent_Monitor.log is saved on your desktop.

3. When finished viewing the McAfee Agent activity log, click Close.
Frequently asked questions

Here are answers to frequently asked questions.

McAfee Smart Installer

**Is the McAfee Smart Installer URL accessible on the internet?**

You can access the McAfee Smart Installer URL using the internet if your McAfee ePO server is accessible over a public network.

**Can I restrict the McAfee Smart Installer URL to be used only specific number of times or number of days?**

The McAfee Smart Installer URL can be used for a predefined number of times.

**Can I run the McAfee Smart Installer if I don't have administrator rights on the client system?**

No, user should have administrator rights to install McAfee Agent on client systems.

Peer-to-Peer communication

**Is peer-to-peer information displayed on the Agent monitor?**

No, these details are available in the detailed logs.

**How many concurrent connections does a peer-to-peer server support?**

A peer-to-peer server supports 10 connections concurrently.

**How will a peer-to-peer client get updated content?**

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

**What type of content does a peer-to-peer server serve?**

A peer-to-peer server can serve all the content available in its McAfee ePO repositories.

**Can I configure the disk quota for peer-to-peer content?**

Yes, see *Peer-to-Peer service* for more details.

General

**Why do I see many McAfee Agent processes for Linux?**

The McAfee runtime environment uses Linux Native threads through the Light Weight Process implementation. Utilizing Linux Native threads causes each thread to show as a separate process on the client computer.

**How the McAfee ePO server sorts McAfee Agent at the first connection?**
When McAfee Agent is installed on a system, a unique GUID is created based on the MAC address and computer name of the system. McAfee Agent will then connect to the McAfee ePO server within a randomized few seconds interval.

At that connection, the McAfee ePO server will use these system properties to see if McAfee Agent is currently populated in the System Tree. A new object is created in the System Tree if no match is found by this search. The location for the new object is also based on this sort order.

<table>
<thead>
<tr>
<th>System properties used when Sorting Criteria is disabled</th>
<th>System properties used when Sorting Criteria is enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent GUID</td>
<td>Agent GUID</td>
</tr>
<tr>
<td>Domain Name</td>
<td>IP address and Tags evaluated for the computer</td>
</tr>
<tr>
<td>Computer Name</td>
<td>Domain Name</td>
</tr>
<tr>
<td>IP address</td>
<td>Computer Name</td>
</tr>
</tbody>
</table>

If an entry is found that is listed within the search order, McAfee Agent lists the client system in the correct group. If it does not find any of the above, it would then list the client in the Lost and Found group at the My Organization level.

**What are the ports used by McAfee Agent**

<table>
<thead>
<tr>
<th>Ports</th>
<th>Protocols</th>
<th>Traffic direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>8081</td>
<td>TCP</td>
<td>Peer-to-peer server serves content, Relay connections established.</td>
</tr>
<tr>
<td>8082</td>
<td>UDP</td>
<td>Peer-to-peer server discovery, Relay server discovery.</td>
</tr>
<tr>
<td>8083</td>
<td>UDP</td>
<td>Relay server discovery for previous versions of McAfee Agent.</td>
</tr>
</tbody>
</table>

If both Peer to Peer and Relay server are disabled then these ports are not open.
Index

A
about this guide 5
agent
  command-line options 51
  introduction to 9
  maintenance 37
  relay capability 38
  relay capability, disable 39
  relay capability, enable 39
  removal methods 25, 26
  removing from systems in query results 26
  settings, viewing 50
  system requirements 15
  tasks, running from managed systems 47
  uninstalling 25
  user interface 47
agent activity logs 54
agent distribution
  FrmInst.exe command-line 26
Agent Handlers
  introduction to 9
agent installation
  CmdAgent.exe 51
  un installing 25
Agent Monitor 50
agent-server communication
  about 37
ASCI (See agent-server communication interval) 37

B
best practices
  agent-server communication interval 37

C
Command Agent tool (CmdAgent.exe) 51
command-line options
  agent 51
  CmdAgent.exe 51
  FrmInst.exe 26
conventions and icons used in this guide 5

D
Data Execution Prevention 15
DEP, See Data Execution Prevention
disable agent relay capability 39
documentation
  audience for this guide 5
  product-specific, finding 6
  typographical conventions and icons 5

E
enable agent relay capability 39
events
  forwarding, agent configuration and 33

F
frequently asked questions 55

G
global updating
  event forwarding and agent settings 33
  groups
    deleting from System Tree 25

I
icon, system tray, See system tray icon
inactive agents 44

L
languages
  multiple, support for 16

M
managed systems
  agent-server communication 37
  running an update task manually 49, 50
  viewing agent activity log 54
McAfee Agent
  properties, viewing 46
  statistics 42
McAfee ServicePortal, accessing 6
Index

N
notifications
  event forwarding and agent settings 33

O
operating systems
  McAfee Agent 15

P
passwords
  installing agents, command-line options 51
peer-to-peer; best practice 41
policies
  enforcing 49
  update settings 50
  verifying changes 46
policies, McAfee Agent
  options for policy pages 31
  settings, about 31
product properties 44
properties
  McAfee Agent, viewing from the console 46
  minimal vs. full 33
  product 44
  retrieving from managed systems 33
  sending to ePO server 50
  system 44
  verifying policy changes 46
proxy settings
  agent policies 33
  configuring for the agent 34

Q
queries
  removing agents in results of 26

R
relay capability 38
relay capability, disable 39
relay capability, enable 39
removal
  agent, from UNIX systems 26
requirements
  operating systems 15
  processors 15

S
ServicePortal, finding product documentation 6
SPIPE 37
status
  security 47
supported languages 16
system requirements 15
system tray icon
  allow users to update from 48
  options 47
  security status 47
  using 47
  visibility 48
System Tree
  deleting systems from 25
  removing agents 25
  removing agents from systems 25
systems
  properties 44

T
technical support, finding product information 6
troubleshooting
  verifying properties of the McAfee Agent and products 46

U
uninstallation
  agent, from UNIX systems 26
UNIX
  uninstalling the agent from 26
updates
  allow users via system tray icon 48
  running tasks manually 49, 50
  security 47
updating
  global, event forwarding and agent settings 33
  manually 49, 50
user interface, agent 47

V
virtual image
  non-persistent 22

W
Windows
  running a manual update 49