McAfee®
An Intel Company

Product Guide

McAfee Agent 5.0.0

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

Introducing McAfee Agent

Installing, upgrading, and removing the agent

Using McAfee Agent

Preface

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

Contents

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.

Important/Caution: Valuable 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

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 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*

1 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.

The term *Agent* is used in these contexts within McAfee ePO:

* Agent — The basic operating mode for McAfee Agent, providing a communication channel to McAfee ePO and local services for other managed products.

* SuperAgent — A distributed repository whose content replication is managed by the McAfee ePO server. The SuperAgent caches information received from an McAfee ePO server, the Master Repository, a HTTP, or a FTP repository, and distributes it to the agents.

  It is recommended to configure a SuperAgent in every subnet when managing agents in larger networks. For more information about SuperAgents and their functionality see *SuperAgents and how they work*.

Contents

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.

> ℹ️ McAfee Agent 5.0.0 can be used only with the McAfee ePO server 5.1.1 or later. You can manage previous versions of McAfee Agent with the 5.0.0 extension, but previous versions of the Agent extensions cannot manage McAfee Agent 5.0.0 clients.

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 5.1.1 or later, the Manifest-based policy feature will help improve the scalability of McAfee ePO platform. In 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 polices 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.

SuperAgent support

McAfee Agent 5.0.0 supports SuperAgent on Windows, Linux, and Macintosh operating systems.

See *SuperAgent and how it works* for more details.

Remote provisioning

You can now use remote provisioning to:

- Convert an unmanaged McAfee Agent to managed – Use the command line switch to convert McAfee Agent mode from unmanaged to managed (that is, provision to a McAfee ePO server).

- Migrate from one McAfee ePO server to another – Use the command line switch to migrate McAfee Agent from one McAfee ePO server to another.

See *Changing agent management modes* for more details.

McAfee Agent feature support

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

Feature	Windows	Non-Windows
SuperAgent	Yes	Yes
64-bit Native	Partially ⓘ 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.	Linux only
Run Client Task Now	Yes	Yes
Relay server	Yes	Yes
Peer-to-Peer	Yes	Yes
Policy-enabled application service logging	Yes	Yes
Policy-enabled debug logging	Yes	Yes
Configurable log rotation	Yes	Yes
Remote log access	Yes	Yes
User-based policy	Yes	Macintosh only
McAfee Agent deployment from the McAfee ePO server	Yes	Linux and Macintosh only
McAfee Agent upgrade from the McAfee ePO server	Yes	Yes
McAfee Smart Installer	Yes	Yes
Property collection	Yes	Yes
Policy enforcement	Yes	Yes
Task enforcement	Yes	Yes
McAfee Agent Wake-up	Yes	Yes
Product Update	Yes	Yes
Product Deployment	Yes	Yes
Event Forwarding	Yes	Yes
Data Channel support	Yes	Yes
IPv4, IPv6 , and mixed mode compatibility	Yes	Yes
Managed product Plugin Architecture support	Yes	Yes
Secure Communication	Yes	Yes
Managed and unmanaged mode	Yes	Yes
Agent Handler accessibility	Yes	Yes

Feature	Windows	Non-Windows
CmdAgent	Yes	Yes
Run Immediately scheduling	Yes	Yes
Run Once scheduling	Yes	Yes
Run missed task scheduling	Yes	Yes
System startup scheduling	Yes	No
At logon scheduling	Yes	No
Automatic McAfee Agent uninstall from the McAfee ePO server	Yes	No
Cluster node property reporting	Yes	No
Mirror Task (For VirusScan Enterprise only)	Yes	No
UNC repository updating	Yes	No
McAfee Agent status monitor	Yes	No
McTray application support	Yes	No

Installing, upgrading, and removing the agent

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

2 Installing McAfee Agent

There are various ways to install McAfee Agent on your client systems. The method you choose depends on the operating system, first-time installation or upgrade, and tools used.

You will need these components to install McAfee Agent on clients systems.

- McAfee ePO extension — A zip file that can be installed on the McAfee ePO server. Installing McAfee Agent allows you to customize product features on the McAfee ePO server.

- McAfee Agent software package — A zip file that contains product installation files, which are compressed in a secure format. The McAfee ePO server can deploy these packages to any of your managed systems, once they are checked in to the **Master Repository**.

- McAfee Agent key updater package — This distributes the new master keys when an update is received from the McAfee ePO managed repositories. McAfee Agent uses agent-server secure communication (ASSC) keys to communicate securely with the server. You can generate new ASSC keys and use them as a master set. Existing agents that use other keys in the Agent-server secure communication keys list do not change to the new master key unless there is a client agent key updater task scheduled and run. McAfee Agent key updater package is multi-platform and updates both master public key (srpubkey.bin) and corresponding request key (reqseckey.bin)

consists of a McAfee ePO extension and a number of client-side packages that correspond to the client operating systems supported by the agent.

McAfee Agent 5.0.0 is backward compatible and works with all the managed products that were using McAfee Agent 4.8.x.

Contents

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.

> ⓘ McAfee Agent does not support deployment to Windows 2003 Server SP 1 from the McAfee ePO server and must be installed locally.

Additional supported platforms

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

- Windows 2008 Server Hyper-V
- ESX
- VMware Workstation
- VMware player

- Citrix XenServer
- Citrix XenDesktop
- VMware Server

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:

Language	Language code
Brazilian (Portuguese)	0416
Chinese (Simplified)	0804
Chinese (Traditional)	0404
Czech	0405
Danish	0406
Dutch	0413
English	0409
Finnish	040b
French	040c
German	0407

Language	Language code
Italian	0410
Japanese	0411
Korean	0412
Norwegian	0414
Polish	0415
Portuguese	0416
Russian	0419
Spanish (Spain–Modern Sort)	0c0a
Spanish (Spain-Traditional Sort)	040a
Swedish	041d
Turkish	041f

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.

Install McAfee Agent extension and packages into the McAfee ePO server

Before McAfee Agent can be installed on the managed systems, the extension, the software package, and key updater package must be added to the McAfee ePO server.

> **i** You can manage previous versions of McAfee Agent with 5.0.0 extension, but previous version extensions cannot manage McAfee Agent 5.0.0 client.

Task

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

1 Download McAfee Agent extension, `EPOAGENTMETA.zip`, McAfee Agent packages, and the key updater packages to the system containing the McAfee ePO server.

You can download McAfee Agent packages from McAfee ePO Software Manager. See McAfee ePO product documentation for more details.

McAfee Agent comes with different packages for each supported operating system.

Name	Description
`MA500WIN.zip`	Windows package
`MA500LNX.zip`	Linux package
`MA500MAC.zip`	Macintosh package
`MA500WIN_Embedded.zip`	Windows Embedded Credentials package
`help_ma_500.zip`	McAfee ePO help extension
`EPOAGENTMETA.zip`	McAfee ePO extension
`AgentKeyUpdate.zip`	Key updater package

2 Install McAfee Agent and help extension:

   a In McAfee ePO, click **Menu | Software | Extensions**.

   b Click **Install Extensions**.

   c Browse to the location containing `EPOAGENTMETA.zip`, select it, then click **OK**. The **Install Extensions** summary page appears.

   d Click **OK** to complete the installation of the extension.

   Repeat step **a** through **d** to install help extension.

   > When upgrading from McAfee Agent 4.8 help extension to 5.0, uninstall the agent 4.8 help extension then perform step **a** through **d** to install 5.0 help extension.

3 Check in the appropriate agent packages to the McAfee ePO repository.

   a Click **Menu | Software | Master Repository**. A list of packages in the repository appears.

   b Click **Actions**, then select **Check In Package** from the drop-down menu.

   c Browse to one of the agent packages listed above, select it, then click **Next**.

   d Ensure that **Current** is selected in the **Branch** field, then click **Save**.

   e Repeat steps **a** through **d** for each agent package you need to check in to the repository.

Methods of installing McAfee Agent

McAfee Agent can be deployed to client systems in a number of ways. Some involve using versions of McAfee Agent already installed on the client system, but not managed by an McAfee ePO server.

Use this table to choose an appropriate method and follow the required action.

Method	Action	Notes
McAfee ePO	The McAfee ePO administrator specifies the systems and selects one of the **Push Agents** options when adding a new system, or **Deploy Agents** for systems already in the **System Tree**.	• Selecting many systems can temporarily affect network throughput. • You must specify credentials with administrator rights to the target systems.
Manual (using the `FramePkg.exe` installer)	The network administrator installs McAfee Agent on each managed system individually.	• Allows for information such as custom properties to be added on an individual system basis. • Once McAfee Agent is installed, use the McAfee ePO server to upgrade products and update product content.
Third-party software such as Microsoft Systems Management Server (SMS), Microsoft Group Policy Objects (GPO), or IBM Tivoli,	Configure your third-party software to distribute McAfee Agent installation package, which is located on your McAfee ePO server.	• McAfee Agent installation package contains necessary security keys and the site list. • See third-party instructions.
Login scripts (Windows only)	The network administrator creates an installation or upgrade script, which runs at each logon to a system.	• The user must log on to the system to trigger the installation or upgrade. • The installation package must be in a location accessible to the system.
Customized McAfee Smart installer	The McAfee ePO administrator creates a customized McAfee Smart installer and distributes it to managed node users for manual installation.	• The managed node users must have administrator rights to install McAfee Agent manually. • Enabling Peer-to-Peer servers helps reduce load on the McAfee ePO server. See *Peer-to-Peer service* for more details. • Once McAfee Agent is installed, assigned policies and client tasks are enforced on the managed node.
Deployment task	Use the McAfee ePO server **System Tree** to upgrade McAfee Agent on selected target systems.	• McAfee Agent must already be present on the target system. • Enabling Peer-to-Peer servers helps reduce load on the McAfee ePO server. See *Peer-to-Peer service* for more details.
An image containing McAfee Agent	The administrator removes McAfee Agent GUID using the command line switch, then creates an image that contains McAfee Agent and deploys the image.	• Removing the GUID allows McAfee Agent to generate a new GUID upon the first agent-server communication. • Failure to remove the GUID results in "sequencing errors" from the multiple identical systems

Method	Action	Notes
Unmanaged McAfee products on Windows systems	Using the **System Tree**, the McAfee ePO administrator selects the systems to be converted from unmanaged status to managed status and selects **Actions**	**Agent**	**Deploy Agents**.	• McAfee Agent must already be present on the target system in unmanaged mode.
Unmanaged McAfee products on non-Windows platforms	Type the following command on the system containing McAfee Agent you want to convert from unmanaged to managed status: `<agent install path>/bin/ maconfig -provision -managed -dir <Path of location containing agentfipmode, srpubkey.bin, reqseckey.bin and Sitelist.xml>`	• You must have root privileges to perform this action. • You must use the `srpubkey.bin`, `reqseckey.bin` and `SiteList.xml` files from the McAfee ePO server.

McAfee Agent files and folders

Installing McAfee Agent places files in different locations depending on the operating system.

Folder content	Operating system	Location
Installation files	Windows (32-bit and 64-bit)	`<PROGRAMFILES>\McAfee\Agent`
	Linux	`/opt/McAfee/agent/`
	Macintosh	`/Library/McAfee/agent`
Data files	Windows (32-bit and 64-bit)	`<Documents and Settings>\All Users \Application Data\McAfee\Agent` If the operating system does not have a Documents and Settings folder, the default location is `<System _Drive>\ProgramData\McAfee\Agent`
	Linux and Macintosh	`/var/McAfee/agent/`
Configuration and management information (including GUID and agent version) needed to manage products	Linux and Macintosh	`/etc/ma.d/`
Script for starting and stopping the agent manually and when called by the system.	Linux	`/etc/init.d/ma`
	Macintosh	`/Library/StartupItems/ma`
Install log files	Windows	`%TEMP%\McAfeeLogs`
Agent log files	Windows	`<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 `<System _Drive>\ProgramData\McAfee\Agent\Logs`
	Linux and Macintosh	`/var/McAfee/agent/logs`

Folder content	Operating system	Location
Peer-to-Peer repository path	Windows	`<Documents and Settings>\All Users \Application Data\McAfee\Agent\data\mcafeeP2P` If the operating system does not have a Documents and Settings folder, the default location is `<System _Drive>\ProgramData\McAfee\Agent`
	Linux and Macintosh	`/var/McAfee/agent/data/mcafeeP2P`
Lacy cache repository path	Windows	`<Documents and Settings>\All Users \Application Data\McAfee\Agent\data \McAfeeHttp` If the operating system does not have a Documents and Settings folder, the default location is `<System _Drive>\ProgramData\McAfee\Agent`
	Linux and Macintosh	`/var/McAfee/agent/data/McAfeeHttp`
Database path	Windows	`<Documents and Settings>\All Users \Application Data\McAfee\Agent\db` If the operating system does not have a Documents and Settings folder, the default location is `<System _Drive>\ProgramData\McAfee\Agent`
	Linux and Macintosh	`/var/McAfee/agent/db`

McAfee Agent installation package

McAfee Agent installation package (`FramePkg.exe` or `install.sh`) is created when you install McAfee ePO or check in McAfee Agent package. You can install McAfee Agent on the client systems using the installation package.

This file is a customized installation package for McAfee Agent that report to your McAfee ePO server. The package contains information necessary for McAfee Agent to communicate with the server. Specifically, this package includes:

- McAfee Agent installer
- `SiteList.xml` file
- `srpubkey.bin` (the server public key)
- `reqseckey.bin` (the initial request key)

- `req2048seckey.bin`
- `sr2048pubkey.bin`
- `agentfipsmode` file

By default, McAfee Agent installation packages are located at `<System Drive>\Program Files \McAfee\ePolicy Orchestrator\DB\Software\Current\<Product Id>\Install\0409`. Product IDs for supported operating systems are:

Operating System	Product ID
Windows	`EPOAGENT3000`
Linux	`EPOAGENT3700LYNX`
Macintosh	`EPOAGENT3700MACX`

The Windows installation package is `FramePkg.exe` and `install.sh` for non-Windows.

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

- You specifically create one within McAfee ePO

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

- Encryption key changes

The default McAfee Agent installation package doesn't contain user credentials. When executed on the targeted system, the installation uses the account of the currently logged-on user.

You can create custom installation packages containing embedded credentials if required by your environment.

> Because an installer package created for this purpose has embedded credentials, access to it should be severely restricted. Installer packages with embedded credentials should only be used in very specific situations where another deployment method is not available. For additional, important information about the use of embedded credentials, see McAfee KB65538

You can also create a customized McAfee Smart installer using McAfee ePO server. This McAfee Smart installer can be distributed to client system users for McAfee Agent installation.

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.

Install on Windows systems

You can install the agent on Windows systems directly from the ePolicy Orchestrator console.

Alternatively, you can

- Copy the agent installation package onto removable media or into a network share for manual or login script installation on your Windows systems

- Copy the customized McAfee Smart installer to download and install agent manually on the managed nodes

Tasks

- *Install on Windows from the McAfee ePO server* on page 26
  Installing McAfee Agent on your Windows systems using McAfee ePO can support many systems simultaneously.

- *Install on Windows using third-party deployment methods* on page 27
  Installing the agent using third-party deployment methods requires an installation package created for that environment.

- *Create custom installation packages* on page 29
  Custom installation packages can be used to install McAfee Agent on systems that are not managed by the McAfee ePO server.

- *Install on Windows manually* on page 29
  You can manually install McAfee Agent on the system, or distribute the `FramePkg.exe` installer for users to run the installation program themselves.

- *Install on Windows with login scripts* on page 32
  Using Windows login scripts to install McAfee Agent can be an efficient way to make sure all systems in your network have McAfee Agent installed.

- *Install using Group Policy Object* on page 33
  The agent supports deployment using Window's Group Policy Objects on client systems in their network. The administrator must copy the agent Group Policy Object files and msi file to a shared path (UNC path) accessible to each client system on which you want to install the agent.

Install on Windows from the McAfee ePO server

Installing McAfee Agent on your Windows systems using McAfee ePO can support many systems simultaneously.

> **Before you begin**
>
> - McAfee Agent extension must be installed on the McAfee ePO server and appropriate software and key updater packages must be added to the Master Repository before installing on a Windows system.
>
> - See *Deploying from McAfee ePO server* for more information.

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

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

Task

1   Click **Menu | Systems | System Tree**, then select the groups or systems where you want to deploy McAfee Agent.

2   Click **Actions | Agent | Deploy Agents**.

3   Select the appropriate **Agent version** drop-down list given the target operating system, and select a version from that list.

> You can only install one version of McAfee Agent on one type of operating system with this task. If you need to install on multiple operating systems or versions, repeat this task for each additional target operating system or version.

4 Select these options as appropriate:

- **Install only on systems that do not already have an agent managed by this ePO server**

- **Force installation over existing version**

  > ⓘ If you use the force installation option, the existing McAfee Agent is removed in its entirety, including policies, tasks, events, and logs before the new McAfee Agent is installed.

5 To change the installation path from the default, enter the target path in the **Installation path** option.

6 Type valid credentials in the **Domain**, **User name**, and **Password** and **Confirm password** fields.

If you want these entries to be the default for future deployments, select **Remember my credentials for future deployments**.

7 If you do not want the defaults, enter appropriate values into the **Number of attempts**, **Retry interval**, and **Abort after** options.

8 If you want the deployment to use a specific Agent Handler, select it from the drop-down list. If not, select **All Agent Handlers**.

9 Click **OK**.

The **Server Task log** page appears with the **Deploy McAfee Agent** task listed.

Install on Windows using third-party deployment methods

Installing the agent using third-party deployment methods requires an installation package created for that environment.

> **Before you begin**
>
> The agent extension must be installed on the ePolicy Orchestrator server and appropriate agent packages added to the Master Repository before the agent can be installed onto a Windows system.

Task

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

1 Create an installation package:

a Click **Menu | Systems | System Tree**.

b Click **System Tree Actions**, then select **New Systems** from the drop-down menu.

c Select **Create and download agent installation package**.

d Deselect **Use Credentials**.

  > ⓘ If deselected, you receive the default package. If selected, you can specify required credentials.

e Click **OK**.

f Select `FramePkg.exe` and save it to the desktop.

2 To embed credentials on systems not belonging to a domain, modify the local security policy on the target systems:

a Log on to the target system using an account with local administrator permissions.

b From the command line, run `SECPOL.MSC` to open the **Local Security Settings** dialog box.

    c   In the **System Tree** under **Security Settings | Local Policies,** select **User Rights Assignment.**

    d   In the **Policy** column of the details pane, double-click **Impersonate a client after authentication** to open the **Local Security Policy Setting** dialog box.

    e   Click **Add User or Group** to open the **Select Users or Groups** dialog box.

    f   Select the user or group that the user is likely to run as, then click **Add.**

    g   Click **Add.**

You are now ready to use your third-party software to distribute the installation package, `FramePkg .exe.`

> 🛈 By default User Access Control is enabled on Windows Vista and later operating systems. The administrator should add permission to the user or turn off User Access Control to install the agent manually on client systems.

When to install using Windows login scripts

In environments where the client systems log on to the network, network login scripts can be used to install McAfee Agent on Windows systems.

Network login scripts can be used to make sure that every system logging on to your network is running McAfee Agent. You can create a login script to call a batch file that checks if McAfee Agent is installed on systems attempting to log on to the network. If no McAfee Agent is present, the batch file installs the it before allowing the system to log on. Within ten seconds of being installed, McAfee Agent calls in to the server for updated policies and McAfee ePO tasks, and the system is added to the **System Tree.**

This method is appropriate when:

- Domain names or sorting filters are assigned to the segments of your **System Tree.**

- You already have a managed environment and want to ensure that new systems logging on to the network become managed as a result.

- You already have a managed environment and want to ensure that systems are running a current version of McAfee Agent.

Create custom installation packages

Custom installation packages can be used to install McAfee Agent on systems that are not managed by the McAfee ePO server.

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

> - Because an installer package created for this purpose has embedded credentials, access to it should be severely restricted. Installer packages with embedded credentials should only be used in very specific situations where another deployment method is not available. For additional, important information about the use of embedded credentials, see McAfee KB65538.
>
> - Microsoft Windows XP Service Pack 2 and later do not allow embedded administrator credentials until the package file name has been added to the exception list of the Windows firewall.

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

Task

1   Click **Menu | Systems | System Tree**, then from the **System Tree Actions** drop-down menu, select **New Systems**.

2   Next to **How to add systems**, select **Create and download agent installation package.**

3   Select the appropriate Windows version.

4   Select or deselect **Use Credentials**. If selected, type the appropriate **Credentials for agent installation,**

   If you want these credentials to be remembered the next time you complete this task, click **Remember my credentials for future deployments**.

5   Click **OK**.

6   When prompted, select the file to be downloaded. Click to open the file, or right-click to save the file.

7   Distribute the custom installation package file as needed.

Install on Windows manually

You can manually install McAfee Agent on the system, or distribute the `FramePkg.exe` installer for users to run the installation program themselves.

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

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

Task

1   Copy the installation package, `FramePkg.exe`, from your McAfee ePO server to a shared folder on a network server accessible by the target system.

2   On the target system, navigate to and right-click `FramePkg.exe`, select **Run as administrator**, and wait a few moments while McAfee Agent is installed.

3   Click **OK** to complete the installation.

Within ten seconds, McAfee Agent calls in to the McAfee ePO server for the first time.

> ⓘ   Systems on which McAfee Agent is installed manually are located initially in the **Lost & Found** group of the McAfee ePO **System Tree**.

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

Command-line options for installing McAfee Agent on Windows

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

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

This table describes all of McAfee Agent installation command-line options. These options are not case-sensitive. Both `FramePkg.exe` and `FrmInst.exe` require administrator privileges, so they must be run from within an administrator command prompt or configured to always run as administrator.

FramePkg.exe and FrmInst.exe command-line options

Command	Description
/DATADIR	Specifies the folder on the system to store McAfee Agent data files. The default location is: `<Documents and Settings>\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: `FRAMEPKG /INSTALL=AGENT /DATADIR=D:\AgentData`
/DOMAIN /USERNAME /PASSWORD	Specifies a domain, and account credentials used to install McAfee Agent. The account must have rights to create and start services on a system. If left unspecified, the credentials of the currently logged-on account are used. If you want to use an account that is local to a system, use the system's name as the domain. Example: `FRAMEPKG /INSTALL=AGENT /DOMAIN=mydomain.com /USERNAME=jdoe / PASSWORD=password`
/FORCEINSTALL	Specifies that the existing McAfee Agent is uninstalled, then the new McAfee Agent is installed. Use this option only to change the installation directory or to downgrade McAfee Agent. When using this option, McAfee recommends specifying a different directory for the new installation (/INSTDIR). Example: `FRAMEPKG /INSTALL=AGENT /FORCEINSTALL /INSTDIR=D:\McAfeeAgent`

Command	Description	
/INSTALL	/INSTALL=AGENT	Installs and enables McAfee Agent in managed mode. Example: `FRAMEPKG /INSTALL=AGENT`
	/INSTALL=UPDATER	Enables the AutoUpdate component if it has already been installed, and does not change whether McAfee Agent is enabled. This command-line option upgrades McAfee Agent. You can use this command to install McAfee Agent in unmanaged mode. ⓘ An Embedded credential package cannot be used to install McAfee Agent in unmanaged mode. Example: `FRAMEPKG /INSTALL=UPDATER`
	/INSTALL=AGENT/ FORCE32BITSERVICES	Installs McAfee Agent in a 32-bit mode on a 64-bit operating system. Example: `/INSTALL=AGENT/FORCE32BITSERVICES`
/INSTDIR	Specifies the installation folder on the system. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default location is: `<DRIVE>:\program files\mcafee\Agent` Example: `FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent`	
REMOVE	Removes McAfee Agent if not in use. If in use, McAfee Agent changes to *updater* mode. Example: `FRMINST /REMOVE=AGENT`	
/FORCEUNINSTALL	Removes McAfee Agent forcibly from the client system. Example: `FRAMEPKG.EXE /FORCEUNINSTALL`	
/RESETLANGUAGE	Resets McAfee Agent language to its default operating system language.	
/SILENT or /S	Installs McAfee Agent in non-interactive mode, hiding the installation from the end user. Example: `FRAMEPKG /INSTALL=AGENT /SILENT`	
/SITEINFO	Specifies the folder path to a specific repository list (McAfee Agent installer, `reqseckey.bin` (the initial request key), `srpubkey.bin` (the server public key), `req2048seckey.bin`, `sr2048pubkey.bin`, `SiteList.xml` file, and `agentfipsmode` file). Example: `FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\TMP\SITELIST.XML`	
/USELANGUAGE	Specifies the locale ID of McAfee Agent that you want to install. Use the switch to change current McAfee Agent language to any supported language. Example: `FRAMEPKG /INSTALL=AGENT /USELANGUAGE=0404` ⓘ If errors occur during installation, all error messages are displayed in English irrespective of the installed locale.	

Install on Windows with login scripts

Using Windows login scripts to install McAfee Agent can be an efficient way to make sure all systems in your network have McAfee Agent installed.

Before you begin

- McAfee recommends first creating segments of your **System Tree** that use either network domain names or sorting filters that add the expected systems to the desired groups. If you don't, all systems are added to the **Lost & Found** group, and you must move them manually.

- Consult your operating system documentation for writing login scripts. The details of the login script depend on your needs. This task uses a basic example.

- Create a batch file (`ePO.bat`) that contains commands you want to execute on systems when they log on to the network. The content of the batch file depends on your needs, but its purpose is to check whether McAfee Agent has been installed in the expected location and, if not, run `FramePkg.exe` to install McAfee Agent. Below is a sample batch file that does this. This example checks the default installation folder for McAfee Agent files and, if not present, installs the McAfee Agent.

```
@ECHO OFF
SETLOCAL
set MA_KEY_NAME="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\Agent"
set MA_VALUE_NAME=InstallPath

FOR /F "usebackq skip=2 tokens=1,2*" %%A IN (
 `REG QUERY %MA_KEY_NAME% /v %MA_VALUE_NAME% 2^>nul`) DO (
    set Home="%%C"
)

IF DEFINED home SET home=%home:"=%
if defined Home echo "McAfee Agent 5.0 is already installed"
if NOT defined Home "\\MyServer\Agent$\Update\FramePkg.exe /install=agent"
exit /b 0
```

💡   `FramePkg.exe` requires administrator rights to install properly.

Task

1 Copy McAfee Agent installation package, `FramePkg.exe`, from your McAfee ePO server to a shared folder on a network server, where all systems have permissions.

> ℹ️
> - Systems logging on to the network are automatically directed to this folder to run McAfee Agent installation package and install McAfee Agent. The default location for the installation packages for Windows is: `<Program Files>\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe`
>
> - Embedded credential package always runs in silent mode and does not display any error message when an installation fails.

2 Save the batch file you created, `ePO.bat`, to the `NETLOGON$` folder of your primary domain controller (PDC) server. The batch file runs from the PDC every time a system logs on to the network.

3 Add a line to your login script that calls the batch file on your PDC server.

The line would look similar to this example: `CALL \\<PDC>\NETLOGON$\EPO.BAT`

Install using Group Policy Object

The agent supports deployment using Window's Group Policy Objects on client systems in their network. The administrator must copy the agent Group Policy Object files and msi file to a shared path (UNC path) accessible to each client system on which you want to install the agent.

Task

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

1 Download `Framepkg.exe` from the ePolicy Orchestrator server to a shared folder on a network server, where all systems have permissions.

2 Execute the following command:

```
Framepkg.exe /gengpomsi /SiteInfo=<sharedpath>\SiteList.xml /
FrmInstLogLoc=<localtempDir>\<filename>.log
```

The following files are extracted to your local drive.

- MFEagent.msi
- Sitelist.xml
- srpubkey.bin
- reqseckey.bin

- agentfipsmode
- sr2048pubkey.bin
- req2048seckey.bin

3 Copy the extracted files to a shared UNC location specified in siteinfo path.

4 Create a new Group Policy Object.

Refer to Microsoft documentation for instructions.

5 Click **Computer Configuration** | **Policies** | **Software Settings**.

6 Right-click **Software installation**, then click **New** | **Package**.

7 When prompted for a package, browse to the shared UNC path, then select `MFEAgent.msi`.

8 Select the **Deployment Method** as **Assigned**.

> (i) McAfee Agent does not support Per-User installations.

Install on Linux and Macintosh systems

McAfee Agent can be installed manually, using McAfee ePO, or using the custom agent installation URL.

On Linux systems, McAfee Agent is installed manually using an installation script (install.sh) that McAfee ePO creates when you check in the McAfee Agent software package in the McAfee ePO Master Repository and indicate the operating system in use. Ubuntu Linux client systems have a slightly different manual installation method, which is discussed in later sections in the document.

McAfee Agent can be installed from McAfee ePO on Macintosh OS X and Red Hat Enterprise Linux client systems.

Once McAfee Agent is installed on client systems, you can run a **Product Deployment** task to schedule updates to McAfee Agent as well as deploy other managed products.

Contents

‣ *Install on non-Windows operating systems from the McAfee ePO server*

‣ *Install on non-Windows operating systems manually*
‣ *Install on Ubuntu operating systems*
‣ *Install on non-Windows systems using script options*

Install on non-Windows operating systems from the McAfee ePO server

Installing McAfee Agent on your Macintosh or Red Hat Linux systems is a quick way to modify and manage a number of systems simultaneously.

> **Before you begin**
>
> The following non-Windows operating systems support installing McAfee Agent from the McAfee ePO server.
>
> • Apple Macintosh OSX versions 10.6 (Leopard) and later
>
> • Red Hat Enterprise Linux versions 4 and later
>
> Enable SSH on the non-Windows client systems before installing McAfee Agent from McAfee ePO.
>
> > (i) • You must have root permissions to install McAfee ePO on non-Windows system.
> >
> > • McAfee Agent extension must be installed on the McAfee ePO server and appropriate packages must be added to the Master Repository before installing McAfee Agent on a non-Windows system.
> >
> > Comment the following line in the `/etc/sudoers` file on a Red Hat operating systems.
> >
> > ```
> > Default requiretty
> > ```

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

Task

1 Click **Menu** | **Systems** | **System Tree**, then select the groups or systems where you want to deploy McAfee Agent.

2 Click **Actions** | **Agent** | **Deploy Agents**.

3 Select the appropriate **Agent version** drop-down list given the target operating system, and select a version from that list.

> 💡 You can only install one version of McAfee Agent on one type of operating system with this task. If you need to install on multiple operating systems or versions, repeat this task for each additional target operating system or version.

4 Select **Install only on systems that do not already have an agent managed by this ePO server**.

5 Type valid credentials in the **User name**, and **Password** and **Confirm password** fields.

If you want these entries to be the default for future deployments, select **Remember my credentials for future deployments**.

6 If you do not want the defaults, enter appropriate values into the **Number of attempts**, **Retry interval**, and **Abort after** options.

7 If you want the deployment to use a specific Agent Handler, select it from the drop-down list. If not, select **All Agent Handlers**.

8 Click **OK**.

Install on non-Windows operating systems manually

McAfee Agent must be installed manually on Macintosh and Linux systems.

> **Before you begin**
>
> The agent extension must be installed on the McAfee ePO server and appropriate agent packages added to the Master Repository before the agent can be installed onto a non-Windows system.

Task

1 Open the repository in McAfee ePO by selecting **Menu | Software | Master Repository**. Choose a repository from the **Preset** drop-down list.

2 From the selected repository branch, copy the `install.sh` file to the target systems.

The path includes the name of the selected repository. For example, if checked in to the Current branch of the McAfee ePO software repository, the path of the Macintosh files is: `C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3700MACX\Install\0409`

3 Open **Terminal**, then switch to the location where you copied the `install.sh` file.

4 Run these commands, giving root credentials when requested:

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

Install on Ubuntu operating systems

The agent can be installed on Ubuntu in managed or unmanaged mode. You can download the installer from an ePolicy Orchestrator server or from the local drive on the ePolicy Orchestrator server.

Tasks

- *Install agent in managed mode on Ubuntu systems* on page 35
  The agent can be installed manually or pushed from an ePolicy Orchestrator server on managed systems running Ubuntu operating system.
- *Install McAfee Agent in unmanaged mode on Ubuntu systems* on page 36
  McAfee Agent can be installed manually or pushed from an McAfee ePO server on unmanaged systems running Ubuntu operating system.

Install agent in managed mode on Ubuntu systems

The agent can be installed manually or pushed from an ePolicy Orchestrator server on managed systems running Ubuntu operating system.

Task

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

1 Open the repository in ePolicy Orchestrator by selecting **Menu | Software | Master Repository**. Choose a repository from the **Preset** drop-down list.

2 From the selected repository branch, copy the `installdeb.sh` file to the target systems.

3 Open **Terminal**, then switch to the location where you copied the `installdeb.sh` file.

4 Run these commands, giving root credentials when requested:

```
$chmod +x ./installdeb.sh
$sudo ./installdeb.sh -i
```

Install McAfee Agent in unmanaged mode on Ubuntu systems

McAfee Agent can be installed manually or pushed from an McAfee ePO server on unmanaged systems running Ubuntu operating system.

The installers (install.sh and installdeb.sh) and McAfee Agent package are found at the following location on the McAfee ePO server:

`<epo server install location>\McAfee\ePolicy Orchestrator\DB\Software\Current`
`\EPOAGENT3700LYNX\Install\0409`

Task

1 Copy the installer files (32-bit files: `MFErt.i686.deb` and `MFEma.i686.deb` and 64-bit files: `MFErt`
`.x86_64.deb` and `MFEma.x86_64.deb`) to the client system.

2 Open a terminal window on the client system. Navigate to the folder containing the installer.

3 Run the following commands:

On 32-bit systems:

```
dpkg -I --force-confnew MFErt.i686.deb
dpkg -I --force-confnew MFEma.i686.deb
```

On 64-bit systems:

```
dpkg -I --force-confnew MFErt.x86_64.deb
dpkg -I --force-confnew MFEma.x86_64.deb
```

Install on non-Windows systems using script options

Installing McAfee Agent on non-Windows systems using the install script (install.sh) supports the following options.

Table 2-1 Supported install script (install.sh) options

Option	Function	Linux	Macintosh
-b	Upgrades the agent only. The server information is not updated	x	x
-h	Shows help	x	x
-i	Performs a new installation	x	x
-u	Upgrades entire install	x	x

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.

McAfee Agent then installs other McAfee products through the deployment tasks and enforces new policies assigned to the managed node fetched during the first ASCI.

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 If you want the installer to use a specific Agent Handler, select it from the drop-down list. If not, select **All Agent Handlers**.

> **ℹ** If you selected **All Agent Handler**, the agent configuration files will be downloaded from primary Agent Handler or the ePolicy Orchestrator server and the all the Agent Handlers will be listed in the `Sitelist.xml` for further download of installation files.

5 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.

> **ℹ** The install.zip file cannot be downloaded from the FTP or UNC servers.

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	Steps to install
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>` ⓘ The installation log `McAfeeSmartInstall_<date>_<time>.log` is saved in the folder where you downloaded McAfee Agent installer.

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>`

Parameter	Description
`-d "Data path"`	Overrides the path of McAfee Agent data files. The default location is: `<Documents and Settings>\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` ⓘ This command-line parameter is supported only on Windows operating systems.
`-i "Install path"`	Overrides the default folder where installation files are saved. You can use Windows system variables, such as `<SYSTEM_DRIVE>`. If not specified, the default location is: `<DRIVE>:\Program Files\McAfee\Agent` Example: `McAfeeSmartInstall.exe -i D:\McAfeeAgent` ⓘ This command-line parameter is supported only on Windows operating systems.
`-g`	Generates the debug log `McAfeeSmartInstall_<date>_<time>.log`. • On Windows client system, the log file is saved in `<Documents and Settings>\<User>\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.
`-a "Proxy address" -p "Proxy port"`	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. ⓘ This command-line parameter is supported on Windows and Macintosh operating systems.
`-k`	Switches off the peer and certificate verification of the https server from where the installer downloads the configuration file.
`-u "Proxy user name" -w "Proxy password"`	Specifies the user name and password for the authenticated proxy server ⓘ This command-line parameter is supported on Windows and Macintosh operating systems.
`-f`	Forces McAfee Agent installation ⓘ This command-line parameter is supported only on Windows operating system.
`-s`	Installs McAfee Agent in silent mode ⓘ This command-line parameter is supported on Windows and Macintosh operating systems.

Parameter	Description
-v	Installs McAfee Agent in the VDI mode.
?	Displays the help for command-line options.
	ⓘ This command-line parameter is not supported on Macintosh operating systems.

ⓘ   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.

Options	Definition
Choose Columns	Opens the Choose Columns page allowing you to select the columns that will be displayed in the Agent Deployment page.
Create Agent Deployment Url	Opens Agent Deployment URL page allowing you to create new URL for Agent Deployment.
Delete Agent Deployment Url	Deletes the selected Agent Deployment URL.
Enable/Disable Agent Deployment Url	Enables or disables the client system users from deploying the agent using the URL.
Export Table	Displays the Export page allowing you to choose the way the table is exported.
View Agent Deployment Url	Displays the Agent Deployment URL.

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 Next to **How to add systems**, select **Create and download agent installation package**.

3 Select a **Agent version**.

4 Select or deselect **Use Credentials**, then click **OK**. If selected, type the appropriate **Credentials for agent installation**.

If you want these credentials to be remembered the next time you complete this task, click **Remember my credentials for future deployments**.

5 When prompted, select the file to be downloaded. Right click and save the file.

6 Copy McAfee Agent installer on the virtual image and the 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**.

Assign values to custom properties

Custom properties are a set of properties that are reported back to the McAfee ePO server and are displayed in the system properties. These properties can be used to enhance custom reporting on systems or to allow custom tagging with the McAfee ePO server.

You can specify up to four custom properties when installing McAfee Agent using command line. These values override values set by the McAfee ePO administrator.

> The custom properties field does not support use of double quotation marks (") with in the custom property text. However, you can use the single quotation mark (') as an alternative. For example:
>
> ```
> FrmInst.exe /CustomProps1="Custom Property 'quoted text' 1"
> ```

At the command line, type the string that is appropriate for your operating system:

- **Windows operating systems:** `FrmInst.exe /CustomProps1="Custom Property 1" / CustomProps2="Property 2" /CustomProps3="Property 3" /CustomProps4="Property 4"`

- **Non-Windows operating systems:** `maconfig -custom -prop1 "Property 1" -prop2 "Property 2" -prop3 "Property 3" - prop4 "Property 4"`

Processes used by McAfee Agent 5.0.0

The table lists the processes used by McAfee Agent 5.0.0.

Windows Processes/ Applications	Non-Windows Processes	Service name	Service display name	Description
masvc.exe	masvc	Masvc	McAfee Agent Service	Performs functions such as property collection, policy enforcement, scheduling of tasks, agent server communication, and trigger update session
macmnsvc.exe	macmnsvc	Macmnsvc	McAfee Agent Common Services	Hosts multiple McAfee Agent services such as Peer-to-Peer server, Wake-up, and RelayServer
macompatsvc.exe	macompatsvc	McAfeeFramework	McAfee Agent Backwards Compatibility Service	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.
cmdagent.exe	cmdagent	N/A	N/A	This is a command line program that invokes McAfee Agent To know more about switches available with this command, use `cmdagent.exe /?`
FrmInst.exe	N/A	N/A	N/A	MA installation program To know more about switches available with this command, use `FrmInst.exe /?`
maconfig.exe	maconfig	N/A	N/A	This is a command line program used to configure different options of McAfee Agent To know more about switches available with this command, use `maconfig –help`
McScanCheck.exe	McScanCheck	N/A	N/A	Command line program used by McScript_InUse.exe to perform DAT or engine updates.

Windows Processes/ Applications	Non-Windows Processes	Service name	Service display name	Description
McScript_InUse.exe	Mue_InUse	N/A	N/A	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.
UpdaterUI.exe	N/A	N/A	N/A	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.
ma_mirror_task.exe	N/A	N/A	N/A	Performs repository mirroring for VirusScan Enterprise
FramePkg.exe	N/A	N/A	N/A	McAfee Agent installer
McTray.exe	N/A	N/A	N/A	System tray icon management tool. It runs under the same user session and is started by UdaterUI.exe.

Include McAfee Agent on an image

McAfee Agent can be installed on an image that is subsequently deployed to multiple systems. You must take precautions to make sure the agent functions properly in this scenario.

No two McAfee Agent can share the same GUID. The most common way McAfee Agent ends up with duplicate GUIDs is if it was installed on an image without having its GUID removed, and that image was deployed onto more than one system.

To ensure the GUIDs are not duplicated, run this command on the system image where McAfee Agent is installed and will be used to deploy on more than one client systems.

```
maconfig -enforce -noguid
```

Identify duplicate agent GUIDs

When client systems with duplicate GUIDs attempt to communicate with an Agent Handler, they generate sequencing errors, which indicate a GUID problem. The **Managed Systems** query result type tracks these information about the sequence errors.

• The number of sequence errors for each system in the **Managed Systems Sequence Errors** property.

• The date and time of the last sequence error in the **Managed Systems Last Sequence Error** property.

The tracked information is incorporated into one of the available predefined queries:

- **Systems with High Sequence Errors**

- **Systems with no Recent Sequence Errors**

Two predefined tasks help manage GUID problems.

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

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

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

  Sequencing errors can occur occasionally for inconsequential reasons. This task clears the count of sequencing errors in systems that have not had any recent sequencing errors. This cleanup task does not remove any problematic GUIDs. The threshold value for defining recent is set in the query **Systems with no Recent Sequence Errors**

Correct duplicate agent GUIDs

Agents with duplicate GUIDs can be automatically identified and removed with a server task.

You can schedule this task to run periodically, or run it immediately.

Task

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

1 Click **Menu | Automation | Server Tasks**, then edit the **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs** task.

   ⓘ   To run this task immediately, click **Run**. The **Server Task Log** page appears after running the task.

2 On the **Description** page, select **Enabled**.

   - To run the task with the default configuration, click **Save**.

   - To configure the **Actions** and **Schedule** tabs, click **Next**.

3 On the Actions page, select **Actions | Run Query**.

4 Select one of these queries from the **System Management** category, then click **OK**.

   - **System with high Sequence errors**

   - **Systems with no recent Sequence errors**

5 From the **Sub-Actions** drop-down list, select one of these, then click **Next**.

   - **Clear Agent GUID Sequence Error Count**

   - **Move Agent GUID to Duplicate List and Delete systems**

6 Set a schedule for running the task, then click **Next**.

7 Review your settings, then click **Save**.

3 Upgrading and restoring agents

If you are using an older version of McAfee ePO and have previous agent versions in your environment, you can upgrade those agents once you install your new McAfee ePO server.

Periodically, McAfee releases newer versions of the agent that can be deployed and managed using McAfee ePO. When the agent installation package and the extension is available, you can download it from the McAfee download site or the Software Manager. Check in the installation package in to the master repository and install the new extension, then use the **Product Deployment** task to upgradeMcAfee Agent.

You can create a customized McAfee Smart installer to upgrade McAfee Agent on the client systems.

You can upgrade from McAfee Agent 4.x.x to 5.0.0.

Contents

‣ *Upgrading vs. updating*
‣ *Upgrade McAfee Agent using a product deployment task*
‣ *Upgrade an unmanaged McAfee Agent on Ubuntu*
‣ *Restore a previous version of the agent on Windows*
‣ *Restore a previous version of the agent on non-Windows systems*

Upgrading vs. updating

This document refers upgrading as installing a newer version of the existing software and updating as changing data.

Upgrading is not the same as *updating*. *Upgrading* means installing a newer version of McAfee Agent over an older version, for example, replacing McAfee Agent 4.8 with McAfee Agent 5.0.0. *Updating* means getting the most up-to-date DATs and signatures that products use to identify and disarm threats.

- If you use the McAfee ePO server to deploy McAfee Agent in your network, the procedure differs slightly depending which previous version of McAfee Agent you are upgrading.

- If you are upgrading your McAfee Agent and your network is very large, consider the size of the installation package file and your available bandwidth before deciding how many to upgrade at once. Consider using a phased approach. For example, upgrade one group in your **System Tree** at a time. In addition to balancing network traffic, this approach makes tracking progress and troubleshooting easier.

- If you use a product deployment client task to upgrade McAfee Agent, consider scheduling the task to run at different times for different groups in the **System Tree**.

The procedure for upgrading may change depending on the version of McAfee Agent running on your managed systems.

> (i) Some previous McAfee Agent versions do not support all features in McAfee ePO 5.1.1. For full McAfee ePO functionality, upgrade to McAfee Agent version 5.0.0 or later.

Upgrading McAfee Agent by a method other than using the McAfee ePO server, such as upgrading manually or using network login scripts, is identical to installing McAfee Agent for the first time.

Upgrade McAfee Agent using a product deployment task

The **Product Deployment** client task in McAfee ePO can be used to upgrade McAfee Agent on a group of systems in the **System Tree**.

> **Before you begin**
>
> Appropriate McAfee Agent packages must be added to the Master Repository before they can be used to upgrade existing McAfee Agent installations.

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

Task

1 Click **Menu | Systems | System Tree**.

2 On the **Client Tasks** tab, click **Actions**, then select **New Task** from the drop-down menu.

   The **Client Task Builder** wizard opens to the **Description** page.

3 Name the task, then select **Product Deployment** from the drop-down list and select whether to send the task to all computers or tagged computers only.

4 Click **Next** to open the **Configuration** page.

5 Select the target platform.

6 Use the drop-down lists in the **Products and Components** area to specify the version of McAfee Agent to deploy and, if needed, additional command-line parameters.

7 Select **Allow end users to postpone this update** to enable the user to postpone the update. For example, if users are in the middle of an important task, they can postpone the update to finish the task, or at least close any open applications.

> (i) • You can postpone the update only on Windows client systems.

8 Click **Next** to open the **Schedule** page.

9 Schedule the task as needed, then click **Next**.

10 Verify the task's details, then click **Save**.

The new deployment task is sent to the client computers at the next agent-server communication. Every time the task executes, it checks to determine whether to install the specified McAfee Agent.

Upgrade an unmanaged McAfee Agent on Ubuntu

Upgrading an McAfee Agent running in unmanaged mode on Ubuntu must be done manually.

The installer and McAfee Agent package is found at the following location on the McAfee ePO server:

```
<epo server install location>\DB\Software\Current\EPOAGENT3700LYNX\Install\0409
```

This process supports upgrading an unmanaged McAfee Agent from version 4.8.0 to version 5.0.0. McAfee Agent running in managed mode can be upgraded with a deployment task in McAfee ePO.

Task

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

1 Copy the installer files (32-bit files: `MFErt.i686.deb` and `MFEma.i686.deb` and 64-bit files: `MFErt.x86_64.deb` and `MFEma.x86_64.deb`) to the client system.

2 Open a terminal window on the client system. Navigate to the folder containing the installer.

3 Run the following commands:

On 32-bit systems:

```
dpkg -I --force-confnew MFErt.i686.deb
dpkg -I --force-confnew MFEma.i686.deb
```

On 64-bit systems:

```
dpkg -I --force-confnew MFErt.x86_64.deb
dpkg -I --force-confnew MFEma.x86_64.deb
```

Restore a previous version of the agent on Windows

It is possible to restore a previous version of the agent in a Windows environment. You might do this after testing a new version of the agent.

Task

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

1 Click **Menu | Systems | System Tree**, then select the systems on which you want to install a previous version of the agent.

2 Click **Actions | Agent | Deploy Agents**.

3 From the **Agent version** drop-down list on the **Deploy Agent** page, select the agent you want to restore, then do the following:

   a Select **Force installation over existing version**.

   b Specify the target installation path for the forced installation.

   c Enter user credentials for agent installation.

   d Provide the **Number of attempts**; **Retry interval**; and **Abort after** information.

   e Select whether the connection used for the deployment is to use a specific Agent Handler or all Agent Handlers.

4 Click **OK** to send the agent installation package to the selected systems.

Restore a previous version of the agent on non-Windows systems

Restoring a previous version of the agent on non-Windows systems involves uninstalling the current agent version and installing the previous one.

Task

1   On the client system, uninstall the currently installed version of the agent.

2   On the client system, install the earlier version of the agent.

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

4 Changing agent management modes

McAfee Agent operates in two modes. managed and unmanaged. If you have previously not managed McAfee products in your network, McAfee Agent installations in your network are running in updater mode.

- Managed mode — In this mode McAfee Agent connects and communicates with the McAfee ePO server to manage its and other McAfee product updates.

- Unmanaged mode — In this mode McAfee Agent doesn't connect or communicate with the McAfee ePO server, but only pulls updates from McAfee HTTP or FTP servers.

Contents

When to change McAfee Agent management modes

Some of the more recent McAfee products that use AutoUpdate, such as VirusScan Enterprise, are installed with McAfee Agent in *updater* mode.

To start managing these products with the McAfee ePO server, you can enable McAfee Agent that is already on the system by changing its management mode.

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

In some situations, you might want to change a system that has been managed by McAfee ePO to updater (unmanaged) mode. Information is provided for changing from managed mode to unmanaged mode.

Before changing the McAfee Agent mode, consider the following:

- By default, `FrmInst.exe` is installed on client system in this location: `C:\Program Files\McAfee
\Agent.`

- Do not change the McAfee Agent installation folder without removing and reinstalling McAfee Agent. McAfee Agents that you enable might be in a different folder than McAfee Agents that you deploy in your network by another method.

- Assigning sorting filters or domain names to specific **System Tree** segments saves time. Without such designations, systems are placed in **Lost&Found** and you must move them from that location.

- Export `agentfipsmode` file from `C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software
\Current\EPOAGENT3000\Install\0409\` along with the mentioned files and rename the `reqseckey.bin` and `srpubkey.bin` to `req2048seckey.bin` and `sr2048pubkey.bin` respectively.

Change the agent mode on Windows

Agents can be changed from unmanaged mode to managed or vice versa.

Tasks

- *Change from unmanaged to managed mode in Windows* on page 52
  Two methods are available for changing McAfee Agent mode on Windows systems.
- *Change from managed to unmanaged mode in Windows* on page 52
  Changing Windows systems to unmanaged mode involves removing the systems from the System Tree.

Change from unmanaged to managed mode in Windows

Two methods are available for changing McAfee Agent mode on Windows systems.

- To send the installer file `Framepkg.exe` across the network, perform these steps.

  a Export `Framepkg.exe` from McAfee ePO server to a temporary location on the target system, (that is, the system to be converted from unmanaged to managed mode).

  b Run `Framepkg.exe` on the client system. This requires administrator privileges.

- To send the `Sitelist.xml` file across the network, perform these steps. This more complex and time-consuming method and involves sending a 400 KB file across the network.

  a Export `Sitelist.xml`, `srpubkey.bin`, `reqseckey.bin`, `req2048seckey.bin`, and `sr2048pubkey.bin` from the McAfee ePO server to a temporary location on the target system.

  b Run `C:\Program Files\McAfee\Common Framework\frminst.exe /install=agent /siteinfo =<full path>\SiteList.xml` on the target system. This requires administrator privileges.

- Use the command line switch to convert McAfee Agent mode from unmanaged to managed (that is, provision to aMcAfee ePO server)

```
maconfig.exe -provision -managed -auto -dir "temp location to copy keys"
 -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]
```

For example,

```
maconfig -provision -managed -auto -dir "/tmp/keys"
 -epo ePOServerMachine [-user admin] [password password123]
```

Change from managed to unmanaged mode in Windows

Changing Windows systems to unmanaged mode involves removing the systems from the System Tree.

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

Task

1 Click **Menu** | **Systems** | **System Tree**.

2 Select the systems to change to unmanaged mode.

3 Click **Actions**, select **Directory Management**, then click **Delete**.

4 Confirm the deletion. The selected system is no longer managed by McAfee ePO and now functions only as an updater.

This uninstalls McAfee Agent if there are no other managed products installed on the system.

Change McAfee Agent mode on non-Windows systems

McAfee Agent can be toggled between unmanaged mode to managed mode.

Tasks

- *Change from unmanaged to managed mode on non-Windows platforms* on page 53
  Changing McAfee Agent mode on non-Windows systems must be done manually.

- *Change from managed to unmanaged mode on non-Windows platforms* on page 53
  Changing McAfee Agent mode on non-Windows systems must be done manually.

Change from unmanaged to managed mode on non-Windows platforms

Changing McAfee Agent mode on non-Windows systems must be done manually.

> **i** This procedure can also be used to change which McAfee ePO server or Agent Handler McAfee Agent communicates with.

Task

1 On the target system, locate the `maconfig` file in the binaries subfolder of the `ma` folder.

Operating system	Default location
Linux	`/opt/McAfee/agent/bin`
Macintosh	`/Library/McAfee/agent/bin`

2 Open a terminal window on the target system.

3 Export `sitelist.xml`, `srpubkey.bin`, `reqseckey.bin`, `req2048seckey.bin`, and `sr2048pubkey.bin` from the McAfee ePO server to a temporary location on the target system.

4 Run the following command:

```
maconfig -provision -managed -auto -dir "temp location to copy keys"
 -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]
```

For example,

```
maconfig -provision -managed -auto -dir "/tmp/keys"
 -epo ePOServerMachine [-user admin] [password password123]
```

Change from managed to unmanaged mode on non-Windows platforms

Changing McAfee Agent mode on non-Windows systems must be done manually.

Task

1 On the target system, locate the `maconfig` file in the binaries subfolder of the `ma` folder.

Operating system	Default location
Linux	`/opt/McAfee/agent`
Macintosh	`/Library/McAfee/agent`

2   Open a terminal window on the target system.

3   Run the following command:

```
/opt/McAfee/agent/maconfig -provision -unmanaged -nostart
```

> The optional -nostart parameter indicates that McAfee Agent does not restart after changing mode.

5 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.

> (i) You cannot remove McAfee Agent using the **Product Deployment** task, which can remove products such as VirusScan Enterprise.

Contents

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.

Operating system	Commands

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.

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.

6 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 Repository policy*

McAfee Agent policy settings

McAfee Agent provides configuration pages for setting policy options that are organized into these categories: **General**, **Repository**, **Product Improvement Program** 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 5.1.1 or later, only the difference in the policy settings is downloaded from the server.

General policy

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

Tab	Settings
General	• Policy enforcement interval • Use of system tray icon in Windows environments • McAfee Agent and **SuperAgent** wake-up call support • Whether to accept connections only from the McAfee ePO server • Yielding of the CPU to other processes in Windows environments • Rebooting options after product deployment in Windows environments • Agent-server communication • Retrieving all system and product properties • Restricting McAfee Agent processes, services, and registry keys modification.
SuperAgent	• Create **SuperAgent** and broadcast wake-up calls to **SuperAgent** • The repository path where the **SuperAgent** goes for product and update packages • Enabling lazy caching • Specify time interval to flush lazy cache memory • Specify the disk space for the lazy cache • Specify the time interval to purge the files from the disk • Enabling RelayServer on McAfee Agent • Enabling discovery of relay serves
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 • Enabling/disabling remote logging • Setting remote access to logging

Tab	Settings
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

> When importing **My Default General** policy from the McAfee ePO 4.6.6 server to the McAfee ePO 5.1.1 server, the policy values for **Peer-to-Peer** feature are replicated from **McAfee Default** policy rather than **My Default** policy in the McAfee ePO 5.1.1 server.

Repository policies

Settings available for **Repository** policies are divided into two tabs.

Tab	Settings
Repositories	Repository selection
Proxy	Proxy configuration

Troubleshooting policies

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

Tab	Settings
General	McAfee Agent user interface and log language

Product Improvement Program

Settings available for **Product Improvement Program** policies are contained within a single tab.

For more details on using Product Improvement Program, see Product Improvement Program product documentation.

Tab	Settings
Product Improvement Program	Allowing Product Improvement Program to collect anonymous diagnostic and usage data.

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

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

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.

If you plan to use **Automatic Responses**, McAfee recommends that you enable priority uploading of higher severity events for those features to function as intended because McAfee Agent sends lower priority events to the McAfee ePO server on later agent-server communication intervals.

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.

Event ID	Description	Severity
2401	Common update success	3
2402	Common update fail	4
2411	Deployment success	3
2412	Deployment fail	4
2413	McAfee Agent uninstall attempt	3
2422	Policy enforce fail	3
2427	Props collect fail	3

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.

- The task setting that specifies whether to retrieve all properties defined by McAfee Agent policy, or only properties that have changed since the last agent-server communication. This setting is available when configuring an immediate or scheduled wake-up call.

Use **System Tree** actions to wake up McAfee Agent on non-Windows operating systems.

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**.

6   Click **Menu | Policy | Client Task Catalog**.

7   In the **Client Task Types** list, select **McAfee Agent Wake-up**.

8   Click the name of an existing task, or click **Actions | New Task** and choose a **McAfee Agent Wake-up** task.

9   In **Options**, select **Send all properties defined by the agent policy** to retrieve all properties as defined by McAfee Agent policy, even if previously sent.

    The default is **Send only properties that have changed since the last agent-server communication**, which sends only new information to the server.

10 Click **Save**.

Configuring Repository policy

You can configure **Repository** policy to manage repository usage and proxy server settings used by McAfee Agent

Tasks

- *Select a repository* on page 65
  Repositories are selected within a policy. McAfee products are updated from the repositories you specify in the Repository policies.

Select a repository

Repositories are selected within a policy. McAfee products are updated from the repositories you specify in the Repository policies.

See ePO product documentation for details on Repositories and different types of repositories.

McAfee Agent can update from any repository in its repository list based on the policy setting. This repository management tool allows you to specify the most efficient means for designating a source repository for updates. It allows you to select repositories based on ping time, subnet distance, or from a preset list.

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

Task

1   Click **Menu | Policy | Policy Catalog**.

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

3   Click **Actions**, then select **New Policy** to create a policy, or select **Duplicate** in the **Actions** column for the **My Default** policy name to create a policy based on the default.

4   Type a name for the policy, then click **OK**.

5 On the **Repositories** tab, select whether to **Use this repository list** (the McAfee ePO server managed repository list), or **Use other repository list** (a locally controlled repository list that is not managed by the McAfee ePOserver).

6 Choose a basis for selecting a repository:

Selection method	Definition
Ping time	The shortest round-trip elapsed time between sending an echo request to a remote ICMP-enabled system and receiving a response from that system. Ping timeout can be used to control the maximum time taken. The default is 30 seconds, minimum is 5, and maximum is 60.
Subnet distance	The fewest hops an ICMP packet makes while traversing the network from a local system to a remote system. The maximum number of hops can be used to control the packet traversal. The default is 15 hops, minimum is 1, and maximum is 30.
Use order in repository list	A user-defined list of repositories based on locally determined preferences. You can sequence and enable or disable specific distributed repositories on the **Repositories** tab of the McAfee Agent policy pages. Allowing McAfee Agent to update from any distributed repository ensures that they get the update from some location.

> McAfee Agent selects a repository each time a change occurs in the repository list, IP address, or Repository policy option.

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**.

7 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 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 McAfee Agent, and the repository list if it has changed since the last agent-server communication. McAfee Agent enforces the new policies locally on the managed system and applies any task or repository changes.

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:

• The agent-server communication interval (ASCI) elapses.

• McAfee Agent wake-up calls are sent from the McAfee ePO server or Agent Handlers.

• A scheduled wake-up task runs on the client systems.

- Communication is initiated manually from the managed system (using Agent Status monitor or command line).

- McAfee Agent wake-up calls sent from the McAfee ePO server.

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 or McAfee ePO servers, or on Agent Handlers 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 in relation to servers or Agent Handlers 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

Wake-up calls and tasks

A McAfee Agent wake-up call triggers an immediate agent-server Communication rather than waiting for the current Agent-Server Communication Interval (ASCI) to elapse.

> (i) Use **System Tree** actions to wake-up McAfee Agent on non-Windows operating system.

There are two ways to issue a wake-up call:

- **Manually from the server** — This is the most common approach and requires McAfee Agent wake-up communication port be open.

- **On a schedule set by the administrator** — This approach is useful when manual agent-server communication is disabled by policy. The administrator can create and deploy a wake-up *task*, which wakes up McAfee Agent and initiates agent-server Communication.

Some reasons for issuing a wake-up call are:

- You make a policy change that you want to enforce immediately, without waiting for the scheduled ASCI to expire.

- You created a new task that you want to run immediately. The **Run Task Now** option creates a task, then assigns it to specified client systems and sends wake-up calls.

- A query generated a report indicating that a client is out of compliance, and you want to test its status as part of a troubleshooting procedure.

If you have converted a particular McAfee Agent to a **SuperAgent**, it can issue wake-up calls to designated network broadcast segments. **SuperAgent** distributes the bandwidth impact of the wake-up call.

Send manual wake-up calls to individual systems

Manually sending an agent or SuperAgent wake-up call to systems in the **System Tree** is useful when you make policy changes and you want agents to call in to send or receive updated information before the next agent to server communication.

Task

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

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

2 Select the systems from the list, then click **Actions | Agent | Wake Up Agents**.

3 Make sure the systems you selected appear in the **Target Systems** section.

4 Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call** as appropriate.

5 Accept the default **Randomization** (0 minutes) or type a different value (0 - 60 minutes). Consider the number of systems that are receiving the wake-up call when it is sent immediately, and how much bandwidth is available. If you type `0`, agents respond immediately.

6 To send incremental product properties as a result of this wake-up call, deselect **Get full product properties...**. The default is to send full product properties.

7 To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.

8 Enter a **Number of attempts, Retry interval**, and **Abort after** settings for this wake-up call if you do not want the default values.

9 Select whether to wake-up agent using **All Agent Handlers** or **Last Connected Agent Handlers**.

10 Click **OK** to send the agent or SuperAgent wake-up call.

Send manual wake-up calls to a group

An agent or SuperAgent wake-up call can be sent to an entire **System Tree** group in a single task. This is useful when you have made policy changes and want agents to call in to send or receive the updated information before the next agent to server communication.

Task

For option definitions, click ? in the interface.

1 Click **Menu | Systems | System Tree**.

2 Select the target group from the **System Tree** and click the **Group Details** tab.

3 Click **Actions | Wake Up Agents**.

4 Make sure the selected group appears next to **Target group**.

5 Select whether to send the agent wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.

6 Next to **Type**, select whether to send an **Agent wake-up call** or **SuperAgent wake-up call**.

7 Accept the default **Randomization** (0 minutes), or type a different value (0 - 60 minutes). If you type `0`, agents awaken immediately.

8 To send minimal product properties as a result of this wake-up call, deselect **Get full product properties…**. The default is to send full product properties.

9 To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.

10 Click **OK** to send the agent or SuperAgent wake-up call.

SuperAgent and how it works

A SuperAgent is a distributed repository whose content replication is managed by the McAfee ePO server.

The SuperAgent caches information received from an McAfee ePO server, the Master Repository, a HTTP, or a FTP repository, and distributes it to the agents in its broadcast domain. It is recommended to configure a **SuperAgent** in every broadcast domain when managing agents in larger networks.

The Lazy Caching feature allows SuperAgent to retrieve data from the McAfee ePO servers only when requested by a local agent node. Creating a hierarchy of SuperAgent along with lazy caching further saves bandwidth and minimizes the load on the McAfee ePO server. To activate this, turn on **LazyCaching** in the **McAfee Agent | SuperAgent** policy options page, which you access from **Menu | Policy | Policy Catalog.**

A SuperAgent also broadcasts wake-up calls to other agents located on the same network subnet. The SuperAgent receives a wake-up call from the McAfee ePO server, then wakes up the agents in its subnet.

> (i)   This is an alternative to sending ordinary agent wake-up calls to each agent in the network or sending agent wake-up task to each computer.

SuperAgent **and broadcast wake-up calls**

Use wake-up calls to initiate agent-server communication, consider converting McAfee Agent on each broadcast domain into a **SuperAgent**.

SuperAgent distributes the bandwidth load of concurrent wake-up calls. Instead of sending wake-up calls from the server to every McAfee Agent, the server sends the **SuperAgent** wake-up call to **SuperAgents** in the selected System Tree segment.

The process is:

1   Server sends a wake-up call to all **SuperAgents**.

2   **SuperAgents** broadcast a wake-up call to McAfee Agent in the same broadcast domain.

3   All notified McAfee Agent (McAfee Agent notified by a **SuperAgent** and all **SuperAgents**) exchange data with the McAfee ePO server or Agent Handler.

When you send a **SuperAgent** wake-up call, McAfee Agent without an operating **SuperAgent** on their broadcast domain are not prompted to communicate with the server.

SuperAgent **deployment tips**

To deploy enough **SuperAgents** to the appropriate locations, first determine the broadcast domains in your environment and select a system (preferably a server) in each domain to host a **SuperAgent**. If you use **SuperAgents**, make sure every McAfee Agent is assigned a **SuperAgent**.

McAfee Agent and **SuperAgent** wake-up calls use the same secure channels. Make sure the following ports are not blocked by a firewall on the client:

- McAfee Agent wake-up communication port (8081 by default).

- McAfee Agent broadcast communication port (8082 by default).

Convert McAfee Agent to SuperAgent

During the global updating process, when the **SuperAgent** receives an update from the McAfee ePO server, it sends wake-up calls to all McAfee Agent in its network. Configure **SuperAgent** policy settings to convert McAfee Agent to **SuperAgent**.
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.

> (i)   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 **Convert agents to SuperAgents** to enable broadcast of wake-up calls.

8 Click **Save**.

9 Send an agent wake-up call.

SuperAgent caching and communication interruptions

The SuperAgent caches the contents of its repository in a specific manner designed to minimize the load on the McAfee ePO server.

If an agent has been converted to a SuperAgent, it can cache content from the McAfee ePO server, the distributed repository, or other SuperAgent to distribute locally to other agents, reducing load on the McAfee ePO server.

> ⓘ
> - SuperAgent caching in conjunction with repository replication is not recommended.
> - The SuperAgent cannot cache content from McAfee HTTP or FTP repositories.

How the cache works

When a client system first requests content, the SuperAgent assigned to that system downloads the requested content from its configured repositories and caches that content. The cache is updated whenever a newer version of the requested package is available in the Master Repository. When a hierarchical structure of SuperAgent is created, the child SuperAgent receives the requested the content update from its parent's cache.

The SuperAgent is guaranteed only to store content required by the agents assigned to it because it does not pull any content from the repositories until requested from a client. This minimizes traffic between the SuperAgent and the repositories. While the SuperAgent is retrieving content from the repository, client system requests for that content are paused.

> ⚠
> The SuperAgent must have access to the repository. Without this access, agents receiving updates from the SuperAgent never receive new content. Make sure that your SuperAgent policy includes access to the repository.

Agents configured to use the SuperAgent as their repository receive the content cached in the SuperAgent instead of directly from the McAfee ePO server. This improves agent system performance by keeping the majority of network traffic local to the SuperAgent and its clients.

If the SuperAgent is reconfigured to use a new repository, the cache is updated to reflect the new repository.

When the lazy cache content is purged

You can configure the SuperAgent to purge cache content that are not in use. The cache content is downloaded when a client system requests for an update. The previous content update files may still be available in the local disk but may not be listed in the `Replica.log` file. If a file is not listed in `Replica.log` it is purged because it will not be requested by any client system.

> ⓘ
> The `Replica.log` file contains information about files and folder in its respective directory. Every directory in the repository contains a `Replica.log` file.

By default the cache content is purged every day. You can configure the purging interval using the SuperAgent policy.

How communication interruptions are handled

When a SuperAgent receives a request for content that might be outdated, the SuperAgent attempts to contact the McAfee ePO server to see if new content is available. If the connection attempts time out, the SuperAgent distributes content from its own repository instead. This is done to ensure the requester receives content even if that content might be outdated.

> • Do not use SuperAgent caching with global updating. Both of these features serve the same function in your managed environment; keeping your distributed repositories up-to-date. However, they are not complementary features. Use SuperAgent caching when limiting bandwidth usage is your primary consideration. Use Global Updating when quick enterprise updating is your primary consideration. See ePO product documentation for more details on Global Updating.
>
> • SuperAgent caching in conjunction with repository replication is not recommended.

SuperAgent hierarchy

A hierarchy of SuperAgents can serve agents in the same network with minimum network traffic utilization.

A SuperAgent caches the content updates from the McAfee ePO server or distributed repository and distributes it to the agents in the network reducing the load on the McAfee ePO server. It is always ideal to have more than one SuperAgent to balance the network load.

> Ensure that you enable **Lazy caching** before you set the SuperAgent hierarchy.

Creating a hierarchy of SuperAgents

Use the Repository policy to create the hierarchy. McAfee recommends that you create a three level hierarchy of SuperAgents in your network.

Creating a hierarchy of SuperAgents avoids repetitive download of the content update from the McAfee ePO server or distributed repository. For example, in a client network with multiple SuperAgents (SuperAgent 1, SuperAgent 2, SuperAgent 3, and SuperAgent 4) and a distributed repository, configure the hierarchy in such a way that the client systems receives the content updates from their respective SuperAgents (SuperAgent 2, SuperAgent 3, or SuperAgent 4). The SuperAgent 2, 3, and 4 receive and cache updates from SuperAgent 1, and the SuperAgent 1 receives and caches updates from the distributed repository.

> • In the above example, SuperAgent 2, SuperAgent 3, and SuperAgent 4 are configured as SuperAgents for the client systems in their respective broadcast domain.
>
> • The SuperAgents cannot cache content from McAfee HTTP or FTP repositories.

When creating a hierarchy, ensure that the hierarchy doesn't form a cycle of SuperAgent; for example SuperAgent 1 is configured to pull updates from SuperAgent 2, SuperAgent 2 is configured to pull updates from SuperAgent 3, and SuperAgent 3 in turn is configured to pull updates from SuperAgent 1.

To ensure that the parent SuperAgent is up-to-date with the latest content update, SuperAgent wake-up calls broadcast must be enabled.

> If the SuperAgents don't serve agents with latest content update, agent falls back to the next repository configured in the policy.

Arrange SuperAgents in a hierarchy

General and Repository policies can be modified to enable and set SuperAgent hierarchy.

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 **General**.

2   Click the **My Default** policy to start editing the policy. To create a policy, click **Actions | New Policy**.

The **McAfee Default** policy cannot be modified.

3   On the **SuperAgent** tab, select **Convert agents to SuperAgents** to convert the agent to a **SuperAgent** and update its repository with latest content.

4   Select **Use systems running SuperAgents as distributed repository** to use the systems that host SuperAgents as update repositories for the systems in its broadcast segment then provide the **Repository Path**.

5   Select **Enable Lazy caching** to allow SuperAgents to cache content when it is received from the McAfee ePO server.

6   Click **Save**.

The **Policy Catalog** page lists the **General** policies.

7   Change the **Category** to **Repository**, then click the **My Default** policy to start editing the policy. If you want to create policy, click **Actions | New Policy**.

8   On the Repositories tab, select **Use order in repository list**.

9   Click **Automatically allow clients to access newly-added repositories** to add new SuperAgent repositories to the list, then click **Move to Top** to arrange the SuperAgents in a hierarchy.

> (i) Arrange the hierarchy of the repositories in such a way that the parent SuperAgent is always at the top of the repository list.

10 Click **Save**.

After setting the SuperAgent hierarchy you can create and run the McAfee Agent Statistics task to collect a report of network bandwidth saving.

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 or Agent Handler 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 `macmnsvc` 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**.

9 Send a McAfee Agent wake-up call.

> ℹ️
> - After the first ASCI the status of the RelayServer is updated in the McAfee Agent Properties page or the McTray UI on the client system.
> - The log file `Macmnsvc_<hostname>.log` is saved in these locations.
>   - On a Windows client system — `<ProgramData>\McAfee\Agent\Logs`
>   - On a non-Windows client system — `/var/McAfee/agent/logs`

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**.

7 Send a McAfee Agent wake-up call.

Peer-to-Peer communication

To retrieve updates and install products the McAfee Agent must communicate with the McAfee ePO server. 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.

> **i** 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 server.

> **i** 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.

> **i** 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**.

9 Send a McAfee Agent wake-up call.

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 and **SuperAgent** hierarchy.

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**.

> (i) 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.

> (i) 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.

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

Configure selected systems for updating

You can choose a set of packages that are updated immediately when **Update Now** is selected on one or more systems from ePolicy Orchestrator server.

Typical reasons for using this functionality include:

- Updating selected systems when troubleshooting

- Distributing new DATs or signatures to a large number of systems, or all systems, immediately

- Updating selected products, patches, or service packs that have been deployed previously

Task

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

1   Click **Menu | Systems | System Tree**, then select the systems to be updated.

2   Click **Actions | Agent | Update Now**.

    - Select **All packages** to deploy all update packages in the repository.

    - Select **Selected packages** to specify which update packages to deploy. Deselect the packages that you do not want to deploy.

      > **i**   The ability to deploy patches and service packs from the Evaluation or Previous repositories is designed to allow update testing on a limited subset of systems before doing a broader deployment. McAfee recommends moving approved patches and service packs to the Current repository when they are ready for general deployment.

3   Click **OK**.

Respond to policy events

Set up an automatic response in McAfee ePO that is filtered to see only policy events.

> ℹ️ See ePO product documentation for more details on **Automatic Responses**.

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

Task

1 Click **Menu | Automation | Automatic Responses** to open the Automatic Responses page.

2 Click **Actions | New Response**.

3 Enter a **Name** for the response, and an optional **Description**.

4 Select **ePO Notification Events** for the **Event group**, and **Client**, **Threat**, or **Server** for the **Event type**.

5 Click **Enabled** to enable the response and then click **Next**.

6 From **Available Properties**, select **Event Description**.

7 Click ... in the **Event Description** row and choose one of the following options:

   • **Agent failed to collect properties for any point products** — This event is generated and forwarded when a property collection failure first occurs. A subsequent success event is not generated. Each failing managed product generates a separate event.

   • **Agent failed to enforce policy for any point products** — This event is generated and forwarded when a policy enforcement failure first occurs. A subsequent success event is not generated. Each failing managed product generates a separate event.

8 Enter remaining information into the filter as needed, then click **Next**.

9 Select **Aggregation**, **Grouping**, and **Throttling** options as needed.

10 Choose an action type and enter a behavior depending on the action type, then click **Next**.

11 Review the summarized response behavior. If correct, click **Save**.

The automatic response performs the described action when a policy event occurs.

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 it's 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.

  > **i** 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.

Run client tasks immediately

When the McAfee ePO server communicates with the McAfee Agent, you can run client tasks immediately using the **Run Client Task Now** action.

McAfee Agent puts tasks into a queue when they are scheduled to run instead of immediately executing them. While a task can be queued up immediately, it only starts executing if no other tasks are ahead of it in the queue. Tasks created during the **Run Client Task Now** procedure are run and the task is deleted from the client after it finishes.

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

Task

1 Click **Menu | Systems | System Tree.**

2 Select one or more systems on which to run a task.

3 Click **Actions | Agent | Run Client Task Now.**

4 Select the **Product** as **McAfee Agent** and the **Task Type**.

5 To run an existing task, click the **Task Name** then click **Run Task Now.**

6 To define a new task, click **Create New Task.**

   a Enter the information appropriate to the task you are creating.

   > **i** If you create a McAfee Agent **Product Deployment** or **Product Update** task during this procedure, one of the available options is **Run at every policy enforcement**. This option has no effect because the task is deleted after it finishes.

The **Running Client Task Status** page appears, and displays the state of all running tasks. When the tasks are complete, the results can be viewed in the **Audit Log** and **Server Task Log**.

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 30 days. You can duplicate this default query and modify it to specify hours, days, weeks, quarters, or years.

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication. The query results allow you take various actions on the systems identified, including ping, delete, wake up, and redeploy McAfee Agent.

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 GUID	Is 64 Bit OS	Server Key
CPU Serial Number	Is Laptop	Sequence Errors
CPU Speed (MHz)	Last Sequence Error	Subnet Address
CPU Type	Last Communication	Subnet Mask
Custom Props 1-4	LDAP Location	System Description
Communication Type	MAC Address	System Location
Default Language	Managed State	System Name
Description	Management Type	System Tree Sorting
DNS Name	Number Of CPUs	Tags
Domain Name	Operating System	Time Zone
Excluded Tags	OS Build Number	To Be Transferred
Free Disk Space	OS OEM Identifier	Total Disk Space
Free Memory	OS Platform	Total Physical Memory
Free System Drive Space	OS Service Pack Version	Used Disk Space
Installed Products	OS Type	User Name
IP Address	OS Version	Vdi
IPX Address		

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.

Agent GUID	**Installed Path**
Agent-Server Secure Communication Key Hash	**IsLazyCachingEnabled**
Agent-to-Server Communication Interval	**Language**
Agent Wake-Up Call	**Last Policy Enforcement Status**
Agent Wake-Up Communication Port	**Last Property Collection Status**
Cluster Node	**License Status**
Cluster Service State	**Peer-to-Peer**
Cluster Name	**Peer-to-Peer Repository Directory**
Cluster Host	**Prompt User When a Reboot is Required**
Cluster Member Nodes	**Policy Enforcement Interval**
Cluster Quorum Resource Path	**Product Version**
Cluster IP Address	**Plugin Version**
DAT Version	**Run Now Supported**
Engine Version	**Service Pack**
Force Automatic Reboot After	**Show McAfee Tray Icon**
Hotfix/Patch Version	**RelayServer**
	SuperAgent Functionality
	SuperAgent Repository
	SuperAgent Lazychache
	SuperAgent Repository Directory
	SuperAgent Wake-Up Communication Port

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.

Queries provided by the McAfee Agent

The McAfee ePO server provides a number of standard queries related to the McAfee Agent.

The following queries are installed into the Agent Management shared group.

Table 7-1 Queries provided by McAfee Agent

Query	Description
Agent Communication Summary	A pie chart of managed systems indicating whether each McAfee Agent has communicated with the McAfee ePO server within the past day.
Agent Handler Status	A pie chart displaying Agent Handler communication status within the last hour.
Agent Statistics information	A bar chart displaying these McAfee Agent statistics: • Number of failed connections to the RelayServers • Number of attempts made to connect to the RelayServer after the maximum allowed connections • Network bandwidth saved by use of SuperAgent hierarchy
Agent Versions Summary	A pie chart of installed agents by version number on managed systems.
Inactive Agents	A table listing all managed systems whose agents have not communicated within the last month.
Repositories and Percentage Utilization	A pie chart displaying individual repository utilization as a percentage of all repositories.
Repository Usage Based on DAT and Engine Pulling	A stacked bar chart displaying DAT and Engine pulling per repository.
Systems per Agent Handler	A pie chart displaying the number of managed systems per Agent Handler.

8 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.

> **i** 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.

Option	Function
Update Security	Triggers immediate updating of all installed McAfee software products. This includes application of patches and hotfixes, as well as DAT and signature updates. **i** This feature is available only if enabled in the agent policy.
Quick Settings	Links to certain product menu items that are frequently used.
Manage Features	Displays links to the administrative console of managed products.
Scan Computer for	Launches McAfee programs, such as VirusScan Enterprise, that scan systems on-demand and detect malicious software.

Option	Function
View Security Status	Displays the current system status of managed McAfee products, including current events.
McAfee Agent Status Monitor	Triggers the Agent Status Monitor, which: • Displays information on the collection and transmission of properties. • Sends events. • Enforces policies. • Collect and send properties. • Checks for new policies and tasks.
About...	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.
Agent status	Displays if the system managed or unmanaged. If it is a managed system, displays if these features are enabled. • SuperAgent • Peer-to-Peer • Relay capability

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**.

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.

6 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.

> **ⓘ** 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

- Current system mode (Managed or Unmanaged)

- SuperAgent status (SuperAgent, 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`

> **i**
> - 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

Parameter	Description
/c	Checks for new policies. McAfee Agent contacts the McAfee ePO server for new or updated policies, then enforces them immediately upon receipt.
/e	Prompts McAfee Agent to enforce policies locally.
/p	Sends properties to the McAfee ePO server.
/s	Displays the McAfee Agent monitor on Windows client systems.
/f	Forwards events from client systems to the McAfee ePO server.
/i	McAfee Agent information
/h	Lists all the switches with their description

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.

9 McAfee Agent activity logs

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.

Contents
- *About the McAfee Agent activity logs*
- *View McAfee Agent activity log from the managed system*
- *View the agent activity log from 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

Agent logs	Windows install logs
`masvc_<hostname>.log`	`Frminst_<hostname>.log`
`macmnsvc_<hostname>.log`	`Frminst_<hostname>_Error.log`
`macompatsvc_<hostname>.log`	`MFEAgent.msi.<system time stamp>.log`
`mcScript.log`	`Vscore_install_vscore_<systemtime>.log`
`marepomirror.log`	`Vscore_uninstall_vscore_<systemtime>.log`
`UpdaterUI.log`	
`UpdaterUI_Error.log`	

> (i) 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).

> (i) 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.

Configuring the **Remote Logging** options on the **Logging** policy tab allows you to enable or disable the activity logging to be displayed on the McAfee ePO server console. You can also configure the access to view these remote logs and the number of lines to be displayed in the log.

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).

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

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**.

View the agent activity log from the McAfee ePO server

You can view the agent activity log of a Windows managed system from the McAfee ePO server.

> **Before you begin**
> Be sure that the McAfee Agent policy settings are set to the following:
> * Ensure that McAfee Agent can communicate with the McAfee ePO server.
> * **Accept connections only from McAfee ePO server** is deselected (McAfee Agent policy pages, **General** tab).
> * **Enable remote access to log** is selected (McAfee Agent policy pages, **Logging** tab).

Task

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

1   Click **Menu | Systems | System Tree**, then select the system.

2   From the **Actions** drop-menu, select **Agent**, then select **Show Agent Log**.

3   To view the backup copy of the detailed log, click **previous**.

A 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.

Remote Provisioning

Is there a temporary credential available that can be shared with end user for remote provisioning? I do not want to share my McAfee ePO administrator credentials.

No, user requires administrator credentials to connect to McAfee ePO server.

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 can I change the language of McAfee Agent during installation?

Run this command on the client system.

framepkg.exe /install=agent /uselanguage=<Locale ID>

Are there best practices or important considerations for upgrading McAfee Agent?

Any action that generates network traffic must be carefully considered. Because the McAfee ePO server is used to deploy products, updates, and McAfee Agents, an McAfee ePO administrator's actions could negatively affect the network. Though the McAfee Agent installation package is not large by itself, it can have significant impact on a network if sent to thousands of systems at one time. Therefore, apply careful planning to any deployment effort.

Before checking in the new package, make sure you

* Disable Global Updating — Checking in a McAfee Agent package with Global Updating enabled can cause the new version of the McAfee Agent to be deployed even if the **Product Deployment** task is not enabled.

* Disable the **Product Deployment** Task — If the **Product Deployment** task is still enabled from the previous deployment, then the new version will cause deployments to begin according to the configured schedule. To reduce the risk of existing task execution, the task change should be sent to client systems before checking in the new package.

Consider these before deploying the McAfee Agent

* Enable **Product Deployment** task below Directory level — Do not set the **Product Deployment** task at the root level. Schedule **Product Deployment** tasks at a Site level, or even at the Group level, if required, to reduce the number of systems downloading the new McAfee Agent at the same time.

* Randomize **Product Deployment** tasks — Do not configure the **Product Deployment** task to start at a set time for the entire Site. Using the randomization feature in the task will allow the network traffic to be spread out over a selected period of time.

How can I redirect the communication from a McAfee Agent to a new McAfee ePO server?

You can use one these install methods to redirect communication from a McAfee Agent to a new McAfee ePO server. See McAfee ePO product documentation for alternate methods.

Method	Action
Using `FrmInst.exe` ⓘ This method is supported only on Windows.	**1** On McAfee ePO Server, navigate to `C:\Program Files\McAfee\ePO \DB\Software\Current\ePOAgent3000\Install\0409` on the McAfee ePO server. **2** Copy these files to a temporary location on the client system. • SiteList.xml file • agentfipsmode file • sr2048pubkey.bin • reqseckey.bin (the initial request key) • srpubkey.bin (the server public key) • req2048seckey.bin **3** Run this command on the client system. `FrmInst.exe /SiteInfo=<Temporary_folder_path>\SiteList.xml`

Using remote provisioning commands	Run this command on the client system.
	
	`maconfig -provision -managed -auto -dir "temp location to copy keys"`
	`  -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]`
	
	For example,
	
	`maconfig -provision -managed -auto -dir "/temp"`
	`  -epo ePOServerMachine [-user admin] [password password123]`

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.

System properties used when Sorting Criteria is disabled	System properties used when Sorting Criteria is enabled
Agent GUID	Agent GUID
Domain Name	IP address and Tags evaluated for the computer
Computer Name	Domain Name
IP address	Computer Name

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

Ports	Protocols	Traffic direction
8081	TCP	Inbound connection from the McAfee ePO server or Agent Handler. Peer-to-peer server serves content, Relay connections established.
8082	UDP	Inbound connection to McAfee Agent. Peer-to-peer server discovery, Relay server discovery.
8083	UDP	Relay server discovery for previous versions of McAfee Agent.

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

Index