Product Guide

McAfee® Agent 4.8.0

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq 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.

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

Using the 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.
- **Users** — People who use the computer where the software is running and can access some or all of its features.
- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.

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

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

Introducing McAfee Agent

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

1 About the McAfee Agent

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

The McAfee Agent consists of an ePolicy Orchestrator extension and a number of client side packages that correspond to the client operating systems supported by the agent.

The term *agent* is used in three contexts within ePolicy Orchestrator:

- Agent — The basic operating mode for the McAfee Agent, providing a communication channel to ePolicy Orchestrator and local services for other point-products.
- SuperAgent — An agent that acts as a source of content updates to other agents in the same network.
- Agent Handler — An ePolicy Orchestrator server component that you can install in various network locations to help manage agent communication, balance the load, and update products.

Contents

McAfee Agent

After being installed on a client system, the agent provides a communication channel from McAfee managed point-products to an ePolicy Orchestrator server.

In addition, the agent provides local services to these point-products and to products developed by McAfee Security Innovation Alliance partners.

While enabling products to focus on enforcing their policies, the McAfee Agent delivers services that include updating, logging, reporting events and properties, task scheduling, communication, policy storage, and product deployment.

Install the agent on systems you intend to manage with ePolicy Orchestrator. Systems can be managed by ePolicy Orchestrator only if they have an agent installed.

While running silently in the background, the agent:

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

SuperAgent

A SuperAgent is an agent that acts as an intermediary between the McAfee ePO server and other agents in the same network broadcast segment. You can only convert a Windows agent to SuperAgent.

For more information about SuperAgents and their functionality see *SuperAgents and how they work*.

Agent Handler

An Agent Handler is an ePolicy Orchestrator server component that is responsible for managing communication between agents and the ePolicy Orchestrator server.

Each ePolicy Orchestrator server contains a master Agent Handler. Additional Agent Handlers can be installed independently of your main McAfee ePolicy Orchestrator server on systems throughout your network.

Setting up additional Agent Handlers can:

- Help support an increased number of systems managed by a single, logical ePolicy Orchestrator server.
- Provide load-balanced communication with a large number of agents, including geographically distributed agents.
- Allow configuration of an alternate Agent Handler during an agent-server communication failure.

Installing, upgrading, and removing the agent

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

2 Installing the agent

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

Contents

System requirements

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

System requirements

- Installed disk space — 29-32 MB (minimum), excluding log files
- Memory — 256 MB RAM (minimum)
- Processor speed — 500 MHz (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

Operating systems	Processor
Apple Macintosh OS X 10.5 (Leopard)	Intel
Apple Macintosh OS X 10.6 (Snow Leopard)	Intel
Apple Macintosh OS X 10.7 (Lion)	Intel
Apple Macintosh OS X 10.8 (Mountain Lion)	Intel
HP-UX 11i v1 (build 11.11)	PA-RISC
HP-UX 11i v2 (build 11.23)	
HP-UX 11i v3	

Operating systems	Processor
HP-UX 11i v2 (build 11.23)	Itanium
HP-UX 11i v3	
IBM AIX 5.3 (TL6 or later)	Power 5, 6, 7
IBM AIX 6.1	Power 5, 6, 7
IBM AIX 7.1	Power 5, 6, 7
Red Hat Linux Enterprise 3	x86, x64 or compatible
Red Hat Linux Enterprise 4	
Red Hat Linux Enterprise 5	
Red Hat Linux Enterprise 6	
Solaris 9; 32- bit or 64-bit	SPARC
Solaris 10; 64-bit	
Solaris 11; 64-bit	
Oracle Enterprise Linux 5 and 6	x86, x64 or compatible
Scientific Linux 5.7 and 6.3	x86, x64 or compatible
SuSE Linux Enterprise Server/Desktop 8 SP 4	x86, x64 or compatible
SuSE Enterprise Server/Desktop 9 SP 4	
SuSE Enterprise Server/Desktop 10 w/SP4	
SuSE Enterprise Server/Desktop 11 and SP2	
SuSE Linux Enterprise Real Time Extension 9-11	
Open SuSE 10-12	
CentOS Linux 4.0-4.9	
CentOS Linux 5.0-5.8	
CentOS Linux 6.0	
Fedora Core Linux 10-16	
Ubuntu Linux 8.04-12.10	
Debian 5 and 6	
Windows 2003 Server (or R2); 32-bit; Enterprise, Standard, or Web Editions; SP 1 and 2	• Itanium 2 • Intel Pentium • Intel Celeron (recommended) or compatible • x86, x64 or compatible
Windows 2003 Server (or R2); 64-bit; Enterprise, Standard, or Web Editions; SP 2	
Windows 7 Home Premium; 32-bit or 64-bit; General Availability release (GA); includes XP mode	• Intel Pentium • Intel Celeron (recommended) or compatible • x86, x64 or compatible
Windows 7 Professional; 32-bit or 64-bit; GA; includes XP mode	
Windows 7 Ultimate; 32-bit or 64-bit; GA; includes XP mode	
Windows Embedded Standard 2009 (Disk-Based)	
Windows Embedded POS Ready 2009 (Disk-Based)	
Windows Embedded POS (WEPOS)	
Windows Vista Home Premium; 32-bit or 64-bit; GA, SP 1 or 2	

Operating systems	Processor
Windows Vista Home Basic; 32-bit or 64-bit; GA, SP 1 or 2	
Windows Vista Business; 32-bit or 64-bit; GA, SP 1 or 2	
Windows Vista Enterprise; 32-bit or 64-bit; GA, SP 1 or 2	
Windows Vista Ultimate; 32-bit or 64-bit; GA, SP 1 or 2	
Windows 2008 Server; Standard; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server Enterprise; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server Datacenter; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server, Web; 32-bit or 64-bit; GA or SP 2	
Windows 2008 Server, Core; 32-bit or 64-bit; GA or SP 2	
Windows 2008 R2	
Windows 8 Professional 32-bit or 64-bit	
Windows 8 Enterprise 32-bit or 64-bit	
Windows 2012 server 64-bit;	
Windows XP Embedded; SP2 (Disk-Based)	
Windows XP Home Edition; 32-bit or 64-bit; SP2 or 3	
Windows XP Professional; 32-bit or 64-bit; SP2 or 3	
Windows XP Tablet PC Edition; 32-bit or 64-bit; SP3	

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 ePolicy Orchestrator and must be installed locally.

Additional supported platforms

You can install the agent on these supported virtual platforms:

- Windows 2008 Server Hyper-V
- ESX
- VMware Workstation
- VMware player
- Citrix XenServer
- Citrix XenDesktop
- VMware Server

The agent is supported on the following McAfee security appliances:

- McAfee Email and Web Security Appliance 3100 and 3200 on Intel processor

Supported languages

The agent is translated into multiple languages.

The Windows client systems support these languages:

- Brazilian (Portuguese)
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
- Turkish

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

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 one or both of the suggestions to ensure that all characters for each language are properly displayed in the agent monitor.

- Configure your Operating Systems to use Unicode support for the agent.
- Install the appropriate Operating System language packs on the systems that need to display language specific characters.

Installation vs. deployment

The terms *installation* and *deployment* both describe the process of equipping one or more computers with the McAfee Agent.

However, there is a difference:

- *Installation* means placing the agent on a computer where no agent is present. Administrator privileges are required to install the agent.
- *Deployment* means upgrading the agent or placing the managed products and their upgrades on one or more client systems where an agent is already present.

Installing the agent

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

Method	Action	Notes
ePolicy Orchestrator	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 a large number of systems can temporarily affect network throughput. • You must specify credentials with administrator rights to the target systems.
Manual	The network administrator installs the agent on each managed system individually.	• Allows for information such as custom properties to be added on an individual system basis. • Once the agent is installed, use ePolicy Orchestrator 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 the agent installation package, which is located on your McAfee ePO server.	• The 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 agent manually. • Once the agent is installed, assigned policies and client tasks will be enforced on the managed node.

Deploying the agent

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

Method	Action	Notes
Deployment task	Use the McAfee ePO System Tree to upgrade the agent on selected target systems.	• An agent must already be present on the target system.
An image containing the agent (Windows)	The administrator removes the agent GUID and MAC address from the agent section of the registry, then creates an image that contains the agent and deploys the image.	• Removing the GUID and MAC address allows the agent to generate a new GUID and MAC address upon the first agent-server communication. • Failure to remove the GUID and MAC address 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**.	• An agent must already be present on the target system in unmanaged mode.
Unmanaged McAfee products on UNIX-based platforms	Type the following command on the system containing the agent you want to convert from unmanaged to managed status: `<agent install path>/bin/msaconfig -m -d <Path of location containing agentfipsmode, srpubkey.bin , reqseckey.bin and SiteList.xml>` If you are using McAfee ePO server 4.6, export `agentfipsmode` file along with the mentioned files and rename the `reqseckey.bin` and `srpubkey.bin` to `req2048seckey.bin` and `sr2048pubkey.bin` respectively.	• 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.

When to deploy from ePolicy Orchestrator

There are specific settings that must be configured on your ePolicy Orchestrator before deploying McAfee Agent.

Deploying the McAfee Agent from ePolicy Orchestrator can support many systems simultaneously.

- Systems must already be added to the System Tree.

  If you have not yet created the System Tree groups, you can deploy the 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 in order to install agents.
- The McAfee ePO server must be able to communicate with the target systems.

  Before beginning a large agent deployment, ping some targets by machine name in each segment of your network to verify that the server can communicate. If the targeted systems respond to the ping, ePolicy Orchestrator can reach the segments.

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

- Network access must be enabled on Windows XP Home and Windows 7 Home client systems. Deploy the agent from ePolicy Orchestrator or install a custom agent installation package on systems running Windows XP Home.

The push deployment feature can install to many systems simultaneously, but can only install a single version of the agent at a time. To install to multiple target operating systems or multiple agent versions, you must configure multiple deployment tasks.

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 the agent on Windows systems.

Network login scripts can be used to make sure that every system logging on to your network is running an agent. You can create a login script to call a batch file that checks if the agent is installed on systems attempting to log on to the network. If no agent is present, the batch file installs the agent before allowing the system to log on. Within 10 minutes of being installed, the agent calls in to the server for updated policies and ePolicy Orchestrator 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 the agent.

Deploying agent using the McAfee Smart installer

You can create a customized McAfee Smart installer by selecting the required operating system, agent version, and Agent Handler.

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 the agent on their system.

The executable file contains the `coninfo.xml` file where the ePolicy Orchestrator server details and a unique token for the agent are saved.

The McAfee Smart installer supports IPv6 environments.

Running the executable on the client system extracts the ePolicy Orchestrator server details and the agent unique token from the `coninfo.xml` file. The client system tries to connect to the ePolicy Orchestrator server to download the configuration files. If the connection succeeds the client system downloads and installs the agent.

If the installer is unable to connect to the ePolicy Orchestrator server directly, it uses the proxy server setting configured on the client system to download and install the 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 ePolicy Orchestrator server directly or using the proxy server, it broadcasts a message to discover an agent with relay capability in its network. The RelayServer responds to the message and establishes connection with the client system. See *Agent relay capability* section for more details.

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

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

Agent installation folder

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

Operating system	Location	Contents
Windows	`<System_Drive>\Program Files\McAfee\Common Framework`	The folder is the same on both managed systems and the ePolicy Orchestrator server itself.
	`<System drive>:\Document and Settings\All Users\Application Data\McAfee\Common Framework`	The folder contains all the agent logs and agent working area.
Windows Vista, Windows 2008 Server, and Windows 7 64-bit	`<System_Drive>\Program Files (x86)\McAfee\Common Framework`	The folder is the same on both managed systems and the ePolicy Orchestrator server itself.
	`<System drive>:\Program Data\McAfee\Common Framework`	The folder contains all the agent logs and agent working area.
AIX	`/opt/McAfee/cma/`	All binaries, logs, agent working area
	`/etc/cma.d/`	Configuration and management information (including GUID and agent version) needed to manage point-products.
	`/etc/`	cma.conf Configuration and management information in xml format, allowing point-products to read.
	`/usr/sbin/`	cma Script for starting and stopping the agent, manually and when called by the system.
HP-UX	`/opt/McAfee/cma/`	All binaries, logs, agent working area.

Operating system	Location	Contents
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/sbin/init.d/cma	cma Script for starting and stopping the agent, manually and when called by the system.
Linux	/opt/McAfee/cma/	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/etc/init.d/	cma Script for starting and stopping the agent, manually and when called by the system.
Macintosh	/Library/McAfee/cma	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/Library/StartupItems/cma/	cma Script for starting and stopping the agent, manually and when called by the system.
Solaris	/opt/McAfee/cma/	All binaries, logs, agent working area.
	/etc/cma.d/	Configuration and management information (including GUID and agent version) needed to manage point-products.
	/etc/	cma.conf Configuration and management information in xml format, allowing point-products to read.
	/etc/init.d/	cma Script for starting and stopping the agent, manually and when called by the system.

Install the agent extension and packages into ePolicy Orchestrator

Before the agent can be installed on the managed systems, both the extension and the software package must be added to ePolicy Orchestrator.

Task

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

1 Download the agent extension, `ePOAgentMeta.zip`, and the agent packages to the system containing the McAfee ePO server.

If using ePolicy Orchestrator server 4.6 or later, you can download the agent packages from the Software Manager. See ePolicy Orchestrator product documentation for more details.

The agent comes with different packages for each supported operating system.

Name	Description
`MA480AIX.zip`	IBM AIX agent package
`MA480HPX.zip`	HP-UX agent package
`MA480LNX.zip`	Linux agent package
`MA480MAC.zip`	Macintosh agent package
`MA480SOL.zip`	Solaris agent package
`MA480WIN.zip`	Windows agent package
`MA480WIN_Embedded.zip`	Windows Embedded agent package
`help_msa_480.zip`	McAfee Agent ePO help extension
`EPOAGENTMETA.zip`	McAfee Agent ePO extension
`AgentKeyUpdate.zip`	McAfee Agent key updater package

2 Install the agent extension:

a In ePolicy Orchestrator, 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.

3 Check in the appropriate agent packages to the ePolicy Orchestrator 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-d for each agent package you need to check in to the repository.

Install the help extension

You can install the help extension separately on the McAfee ePO server using the **Software** tab. The help extension is a .ZIP file.

Task

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

1 Log on to the McAfee ePO server as an administrator.

2 Click **Menu** | **Software** | **Extensions** | **Install Extension**. The Install Extension dialog box appears.

3 Click **Browse** and select the extension file **help_msa_480.ZIP**, then click **OK**. The Install Extension page appears with the extension name and version details.

4 Click **OK**.

Agent installation package

An agent installation package (`FramePkg.exe` or `install.sh`) is created when you install ePolicy Orchestrator or check in an agent package. You can install the agent on the client systems using the installation package.

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

- The 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, the paths of the agent installation package on the server are:

Operating System	Location
Windows	`C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3000\Install\0409\FramePkg.exe`
AIX	`C:\ProgramFiles\McAfee\ePolicyOrchestrator\DB\Software\Current \EPOAGENT4000AIXX\Install\0409\install.sh`
HPUX	`C:\ProgramFiles\McAfee\ePolicyOrchestrator\DB\Software\Current \EPOAGENT4000hpux\Install\0409\install.sh`
Linux	`C:\ProgramFiles\McAfee\ePolicyOrchestrator\DB\Software\Current \EPOAGENT3700LYNX\Install\0409\install.sh`
Solaris	`C:\ProgramFiles\McAfee\ePolicyOrchestrator\DB\Software\Current \EPOAGENT3700SLRS\Install\0409\install.sh`
Macintosh	`C:\ProgramFiles\McAfee\ePolicyOrchestrator\DB\Software\Current \EPOAGENT3700MACX\Install\0409\install.sh`

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

- You specifically create one within ePolicy Orchestrator
- Agent packages are checked in to any branch of the repository (Previous, Current, or Evaluation)
- Encryption key changes

The default agent installation package contains no embedded 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 ePolicy Orchestrator server. This McAfee Smart installer can be distributed to client system users for agent installation.

Create custom agent installation packages

Custom installation packages can be used to install the agent on systems that are not managed by ePolicy Orchestrator.

If you use a distribution method other than deployment capabilities (such as login scripts or third-party deployment software), you can create a custom agent 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 the agent.

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.

Task

For option definitions, click **?** 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 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.

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

- You can create customized McAfee Smart installer only with ePolicy Orchestrator 5.0 and McAfee Agent 4.8 or later.
- Ensure that the McAfee Agent extension is installed and the software package is checked in to the ePolicy Orchestrator 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.

Task

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

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 the agent installer.

3 Select the appropriate operating system and 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**.

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.

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.

Agent installation command-line options

Depending on whether the agent is already installed, you can use command-line options when you run the agent installation package (`FramePkg.exe`) or the 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 the agent.

This table describes all of the agent installation command-line options. These options are not case-sensitive, but their values are. 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 agent data files. The default location is: `<Documents and Settings>\All Users\Application Data\McAfee\Common Framework`. If the operating system does not have a `Documents and Settings` folder, the default location is `C:\ProgramData\McAfee\Common Framework`. Example: `FRAMEPKG /INSTALL=AGENT /DATADIR=<AGENT DATA PATH>`
/DOMAIN/ USERNAME/ PASSWORD	Specifies a domain, and account credentials used to install the agent. The account must have rights to create and start services on the desired 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 the desired system, use the system's name as the domain. Example: `FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=jdoe /PASSWORD=password`

Command	Description
/FORCEINSTALL	Specifies that the existing agent is uninstalled, then the new agent is installed. Use this option only to change the installation directory or to downgrade the agent. When using this option, McAfee recommends specifying a different directory for the new installation (/INSTDIR). Example: `FRAMEPKG /INSTALL=AGENT /FORCEINSTALL /INSTDIR=c:\newagentdirectory`
/INSTALL=AGENT	Installs and enables the 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 the agent is enabled. This command-line option upgrades the agent. You can use this command to install agent in unmanaged mode. An Embedded credential package cannot be used to install the agent in unmanaged mode. Example: `FRAMEPKG /INSTALL=UPDATER`
/INSTDIR	Specifies the installation folder on the desired system. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default location is: `<DRIVE>:\program files\mcafee\common framework` Example: `FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent` On Windows Vista, Windows 2008 Server and Windows 7 64-bit client systems, the default location is: `<DRIVE>:\program files (x86)\mcafee\common framework`
/REMOVE=AGENT	Removes the agent if not in use. If in use, the agent changes to *updater* mode. Example: `FRMINST /REMOVE=AGENT`
/RESETLANGUAGE	Resets the agent language to its default operating system language.
/SILENT or /S	Installs the agent in silent mode, hiding the installation from the end user. Example: `FRAMEPKG /INSTALL=AGENT /SILENT`
/SITEINFO	Specifies the folder path to a specific repository list (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 language version of the agent that you want to install. If you install multiple language versions, the locale selected in operating system determines the language version that displays. Example: `FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404` If errors occur during installation, all error messages are displayed in English no matter what `/USELANGUAGE` parameters are set.

Install agent using customized McAfee Smart installer

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

Before you begin

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

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

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

Task

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

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 the 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 the agent download.
Other supported non-Windows operating systems	• Run the agent installer from the folder where the it is downloaded `./<McAfeeSmartInstall.sh>` The installation log `McAfeeSmartInstall_<date>_<time>.log` is saved in the folder where you downloaded the agent installer.

Command-line options for installing URL-based agent manually

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

Before you begin

The `glibc-32bit` library should be installed on the Linux 64-bit client systems.

Task

For option definitions, click **?** 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 agent data files. The default location is: `<Documents and Settings>\All Users\Application Data\McAfee\Common Framework`. If the operating system does not have a `Documents and Settings` folder, the default location is `C:\ProgramData\McAfee\Common Framework`. Example: `McAfeeSmartInstall.exe -d "Data path"` 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\common framework` Example: `McAfeeSmartInstall.exe -i "Install path"` 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 `C:\DOCUME~1\ADMINI~1\LOCALS~1\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.

Parameter	Description
`-f`	Forces agent installation This command-line parameter is supported only on Windows operating system.
`-s`	Installs the agent in silent mode This command-line parameter is supported on Windows and Macintosh operating systems.
`-v`	Installs the agent in the VDI mode This command-line parameter is supported only on Windows operating system.
`?`	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.

Assign values to custom properties

You can specify up to four custom properties when installing the agent using command line. These values override values set by the ePolicy Orchestrator administrator.

Custom properties 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 McAfee ePO server.

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"`

  - In Windows, custom property values are stored in the registry at `HKLM\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent\CustomProps\`

- **UNIX-based operating systems:** `msaconfig -CustomProps1 "Property 1" -CustomProps2 "Property 2" -CustomProps3 "Property 3" -CustomProps4 "Property 4"`

  Custom property values are stored in `CustomProps.xml`, an editable file located at `/McAfee/cma/scratch/`.

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 ePolicy Orchestrator* on page 33
  Installing McAfee Agent on your Windows systems using ePolicy Orchestrator can support many systems simultaneously.
- *Install on Windows using third-party deployment methods* on page 34
  Installing the agent using third-party deployment methods requires an installation package created for that environment.
- *Install on Windows manually* on page 35
  You can manually install the 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 36
  Using Windows login scripts to install the agent can be an efficient way to make sure all systems in your network have an agent installed.
- *Install using Group Policy Object* on page 36
  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 ePolicy Orchestrator

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

Before you begin

The agent extension must be installed on the ePolicy Orchestrator server and appropriate agent and key updater packages must be added to the Master Repository before installing agent onto a Windows system.

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 the agent during the import.

Task

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

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

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

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

You can only install one version of the agent onto 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 agent is removed in its entirety, including policies, tasks, events, and logs before the new 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.

Install on Windows manually

You can manually install the 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 the agent on their own systems, distribute the agent 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.

Task

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

1 Copy the agent 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 the agent is installed.

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

Within ten minutes, the agent calls in to the McAfee ePO server for the first time.

4 As needed, bypass the ten-minute interval by forcing the agent to call. Use this command at an administrator command prompt:

```
cmdagent /p
```

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

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

Install on Windows with login scripts

Using Windows login scripts to install the agent can be an efficient way to make sure all systems in your network have an 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 the agent has been installed in the expected location and, if not, run `FramePkg.exe` to install the agent. Below is a sample batch file that does this. This example checks the default installation folder for an agent file and, if not present, installs the new agent.

  ```
  IF EXIST "C:\Program Files\McAfee\Common Framework\FRAMEWORKSERVICE.EXE" GOTO END_BATCH
  \\MyServer\Agent\UPDATE$\FRAMEPKG.EXE /INSTALL=AGENT
  :END_BATCH
  ```

  `FramePkg.exe` requires administrator rights to install properly, so we recommend the version of `FramePkg.exe` with embedded credentials. The installation folders for your distribution might be different than in this example, depending on where you have specified to install the agent.

Task

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

   - Systems logging on to the network are automatically directed to this folder to run the agent installation package and install the agent. The default location for the agent installation packages for Windows is: `C:\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**.

McAfee Agent does not support Per-User installations.

Install on UNIX-based and Macintosh systems

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

On HP-UX, AIX, Solaris, and most Linux systems, the agent is installed manually using an installation script (install.sh) that McAfee ePO creates when you check in the agent to the McAfee ePO Master Repository and indicate the operating system in use.

Ubuntu Linux client systems have a slightly different manual installation method.

You can download platform specific HP-UX installation files from these locations:

- For Itanium systems — `C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software \Current\EPOAGENT4000HPUX\Install\0409\installhpia.sh`
- For PA-RISC systems — `C:\Program Files\McAfee\ePolicy Orchestrator\db\Software \Current\EPOAGENT4000HPUX\Install\0409\installhppa.sh`

The agent can be installed from ePolicy Orchestrator on Macintosh OS X and Red Hat Enterprise Linux client systems.

Once the agent is in place on client systems, you can run an agent deployment task to schedule updates to the agent as well as deploy products for management by McAfee ePO.

Contents

Install on UNIX-based and Macintosh operating systems from ePolicy Orchestrator

Installing agents 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 UNIX-based operating systems support installing the agent from ePolicy Orchestrator.

- Apple Macintosh OS/X versions 10.5 (Leopard) and later
- Red Hat Enterprise Linux versions 4 and later
- Ubuntu Linux 8.04 and later

Enable SSH on the Unix-based and Macintosh client systems before installing agent from McAfee ePO.

Comment the following line in the `/etc/sudoers` file on a Red Hat operating systems.

```
Default requiretty
```

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 UNIX-based system.

Task

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

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

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

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

You can only install one version of the agent onto 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 UNIX-based and Macintosh operating systems manually

The agent must be installed manually on AIX, HP-UX, Solaris, and some Linux systems. Manual installation of agent is also supported on Macintosh and Linux systems.

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 UNIX-based system.

Task

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 `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 required files is:

Operating System	Location
AIX	`C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT4000AIXX\Install\0409`
HPUX	`C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT4000HPUX\Install\0409`
Linux	`C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3700LYNX\Install\0409`
Macintosh	`C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3700MACX\Install\0409`
Solaris	`C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3700SLRS\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 40
  The agent can be installed manually or pushed from an ePolicy Orchestrator server on managed systems running Ubuntu operating system.
- *Install agent in unmanaged mode on Ubuntu systems* on page 40
  The agent can be installed manually or pushed from an ePolicy Orchestrator 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 agent in unmanaged mode on Ubuntu systems

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

The installers (install.sh and installdeb.sh) and 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 `MFErt.i686.deb` and `MFEcma.i686.deb` to the client system.

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

3 Run these commands, giving root credentials when requested:

```
dpkg -i MFErt.i686.deb
dpkg -i MFEcma.i686.deb
```

Install on Unix-based systems using script options

Installing the agent on Unix-based and Macintosh systems using the install script (install.sh) supports the following options.

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

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

Include the agent on an image

The 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.

Tasks

- *Correct duplicate agent GUIDs* on page 41
  Agents with duplicate GUIDs can be automatically identified and removed with a server task.

Identify duplicate agent GUIDs

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

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

Install agent on a non-persistent virtual image

Creating a new agent identifier each time a non-persistent virtual image is started results in duplicate Agent GUID. To avoid duplication of GUIDs agent can be installed in VDI mode on the virtual images.

Installing agent in the VDI mode deprovisions the virtual image every time its shut down and enables the McAfee ePO server to save the deprovisioned agents in its database.

Task

For option definitions, click **?** 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 **McAfee Agent for Windows 4.8.0** as **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 the agent installer on the virtual image and the run the following command to install the agent in VDI mode:

```
FramePkg.exe /Install=Agent /enableVDIMode
```

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

To verify if the 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 agent. The value of the system property **Vdi** should be **Yes**.

3 Upgrading and restoring agents

If you have been using an older version of ePolicy Orchestrator and have previous agent versions in your environment, you can upgrade those agents once you've installed your new McAfee ePO server.

Periodically, McAfee releases newer versions of the agent that can be deployed and managed using ePolicy Orchestrator. When the agent installation package is available, you can download it from the McAfee download site or the Software Manager, check it in to the master repository, then use the deployment task to upgrade the agent.

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

Contents

Upgrading vs. updating

Upgrading involves changing software version numbers, while updating involves changing data.

Upgrading is not the same as *updating*. *Upgrading* the agent means installing a newer version of the agent over an older version, for example, replacing McAfee Agent 4.5 with McAfee Agent 4.6. *Updating* means getting the most up-to-date DATs and signatures that products use to identify and disarm threats.

- If you use ePolicy Orchestrator to deploy agents in your network, the procedure differs slightly depending which previous version of the agent you are upgrading.
- If you are upgrading your agents and your network is very large, consider the size of the agent installation package file and your available bandwidth before deciding how many agents 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 agents, consider scheduling the task to run at different times for different groups in the **System Tree**.

The procedure for upgrading the agent may change depending on which agent version is running on your managed systems.

Some previous agent versions do not support all features in ePolicy Orchestrator 5.0. For full ePolicy Orchestrator functionality, upgrade to agent version 5.0 or later.

Upgrading agents by a method other than using ePolicy Orchestrator, such as upgrading manually or using network login scripts, is identical to installing agents for the first time.

Upgrade agents using a product deployment task

The **Product Deployment** client task in ePolicy Orchestrator can be used to upgrade the agents on a group of systems in the **System Tree**.

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

Task

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

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 the task should be sent to all computers or to 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 the agent to deploy and, if needed, additional command-line parameters.
7. If you are working in a Windows environment, select whether to run the task at each policy enforcement interval.
8. 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.

   - You can postpone the update only on Windows client systems.
   - You can't run the task at every policy enforcement when a deployment is postponed.
   - You can't postpone the task if you want to run the task at every policy enforcement.
9. Click **Next** to open the **Schedule** page.
10. Schedule the task as needed, then click **Next**.
11. Verify the task's details, then click **Save**.

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

Upgrade an unmanaged agent on Ubuntu

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

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

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

This process supports upgrading an unmanaged McAfee Agent from version 4.5 to version 4.6. Agents running in managed mode can be upgraded with a deployment task in ePolicy Orchestrator.

Task

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

1. Copy the installer files (`MFRrt.i686.deb` and `MFEcma.i686.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:

```
dpkg -I --force-confnew MFErt.i686.deb
dpkg -I --force-confnew MFEcma.i686.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 UNIX-based and Macintosh 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, the agent installations in your network are running in updater mode.

Contents

When to change agent management modes

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

To start managing these products with ePolicy Orchestrator, you can enable the agent that is already on the system by changing its management mode.

Changing the existing agent on each system to managed mode saves significant network bandwidth over deploying the agent installation package. However, existing McAfee products were probably installed with an older version of the agent, and these 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 ePolicy Orchestrator to updater (unmanaged) mode. Information is provided for changing from managed mode to unmanaged mode.

Before changing the agent mode, consider the following:

- By default, `FrmInst.exe` is installed on the McAfee ePO server in this location: `C:\Program Files\McAfee\Common Framework`.
- You should not change the agent installation folder without removing and reinstalling the agent. Agents that you enable might be in a different folder than 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 will have to move them from that location.

- You must export the `SiteList.xml`, `reqseckey.bin`, and `srpubkey.bin` (repository list file) from the McAfee ePO server and copy to the target systems. The repository list contains network address and other information that the agent requires to call in to the server after being installed.

  If you are using McAfee ePO server 4.6 and higher, 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.

- `SiteList.xml` must be placed in the same location as `srpubkey.bin` and `reqseckey.bin`.

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 48
  Two methods are available for changing the agent mode on Windows systems.
- *Change from managed to unmanaged mode in Windows* on page 48
  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 the agent mode on Windows systems.

- To perform the simple and fast method that involves sending a 5 MB file across the network, perform the following 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 perform the more complex and time-consuming method that involves sending a 400 KB file across the network, perform the following steps:
  a. Export `sitelist.xml`, `srpubkey.bin` and `reqseckey.bin` from the McAfee ePO server to a temporary location on the target system.

     If you are using McAfee ePO server 4.6 and higher, export `agentfipsmode` file along with the mentioned files and rename the `reqseckey.bin` and `srpubkey.bin` to `req2048seckey.bin` and `sr2048pubkey.bin` respectively.

  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.

Change from managed to unmanaged mode in Windows

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

Task

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

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 ePolicy Orchestrator and now functions only as an updater.

Change the agent mode on UNIX-based and Macintosh systems

Agents can be toggled between unmanaged mode to managed mode.

Tasks

- *Change from unmanaged to managed mode on UNIX-based platforms* on page 49
  Changing the agent mode on non-Windows systems must be done manually.
- *Change from managed to unmanaged mode on UNIX-based platforms* on page 50
  Changing the agent mode on non-Windows systems must be done manually.

Change from unmanaged to managed mode on UNIX-based platforms

Changing the agent mode on non-Windows systems must be done manually.

This procedure can also be used to change which McAfee ePO server or Agent Handler an agent communicates with.

Task

1 On the target system, locate the `msaconfig` file in the binaries subfolder of the `cma` folder.

Operating system	Default location
HP-UX, Linux, AIX, and Solaris	`/opt/McAfee/cma/bin`
Macintosh	`/Library/McAfee/cma/bin`

2 Open a terminal window on the target system.

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

If you are using McAfee ePO server 4.6 and above, export `agentfipsmode` file along with the above mentioned files and rename the `reqseckey.bin` and `srpubkey.bin` to `req2048seckey.bin` and `sr2048pubkey.bin` respectively.

4 Run the following command:

```
/opt/McAfee/cma/bin/msaconfig -m -d <path of location containing
srpubkey.bin, reqseckey.bin and SiteList.xml> [-nostart]
```

The optional `-nostart` parameter indicates that the agent does not restart after changing mode.

Change from managed to unmanaged mode on UNIX-based platforms

Changing the agent mode on non-Windows systems must be done manually.

Task

1 On the target system, locate the `msaconfig` file in the binaries subfolder of the `cma` folder.

Operating system	Default location
HP-UX, Linux, AIX, and Solaris	`/opt/McAfee/cma/bin`
Macintosh	`/Library/McAfee/cma/bin`

2 Open a terminal window on the target system.

3 Run the following command:

```
/opt/McAfee/cma/bin/msaconfig -u [-nostart]
```

The optional `[-nostart]` parameter indicates that the agent does not restart after changing mode.

5 Removing the McAfee Agent

After deleting an agent, the system is deleted from the System Tree and the agent is removed during the next agent-server communication.
Keep in mind that if point-products still reside on systems after attempting to remove the agent, the agent continues to run unmanaged in updater mode in order to maintain those point-products.

You cannot remove the agent using the Product Deployment task, which can remove products such as VirusScan Enterprise.

Contents

Remove agents when deleting systems from the System Tree

The agent is removed from systems when you delete those systems from the System Tree.

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

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

The agent is removed from all systems in a group when you delete that group from the System Tree.

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

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

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 agents from systems listed in the results of a query (for example, the Agent Versions Summary query).

Task

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

1. Run the desired 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 point-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. The default location of this file is:

   `C:\Program Files\McAfee\Common Framework`

Remove agents from non-Windows operating systems

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

The task involves:

- Removing the agent from the system.
- Removing the system names from the McAfee ePO System Tree.

Task

For option definitions, click **?** 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
AIX	`rpm -e MFEcma`
HP-UX	`swremove MFEcma`

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/cma/uninstall.sh`
Solaris	`pkgrm MFEcma`

3 On the ePolicy Orchestrator server, click **Menu** | **Systems** | **System Tree**, then select the systems from which you have just uninstalled the agent.

4 From the **Actions** drop-down menu, select **Directory Management**, then select **Delete** from the submenu.

Using the agent

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

6 Configuring agent policies

Agent policy settings determine the performance and behavior of an agent in your environment.

Contents

Agent policy settings

The agent provides configuration pages for setting policy options that are organized into four categories: **General**, **Repository**, **Product Improvement Program** and **Troubleshooting**.

Agent 4.5 had one policy categories: **General**. When upgrading the agent from version 4.5 to version 4.6 and later, McAfee-supplied policies (for example **McAfee Default** and **My Default**) are broken into four categories: **General**, **Repository**, **Troubleshooting**, and **Product Improvement Program**. This is not done to user-created policies. Previously-existing user-created policies are only broken into **General** and **Repository** categories and do not receive a **Troubleshooting** policy category.

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

When upgrading from ePolicy Orchestrator server 4.5 to 4.6 and later, the Agent Extension is also upgraded from 4.5 to 4.6 and later. McAfee-supplied agent policies (**McAfee Default** and **My Default**) are broken into four categories: **General**, **Repository**, **Troubleshooting**, and **Product Improvement Program**. Any policy created by a user using Agent 4.5 are spilt into **General** and **Repository** categories during upgrade.

General policies

Settings available for **General** policies are divided into five tabs.

Tab	Settings
General	• Policy enforcement interval • Use of system tray icon in Windows environments • 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
SuperAgent	• Create SuperAgent and broadcast wake-up calls to SuperAgent in Windows environments • The repository path where the SuperAgent goes for product and update packages • Enabling lazy caching • Specify time interval to flush lazy cache • Enabling RelayServer on agent
Events	• Enabling/disabling Priority event forwarding • Level of priority events forwarded • Interval between event uploads • Maximum number of events per upload
Logging	• Enabling/disabling of logging • Setting the log file size limit • Level of logging detail • Setting remote access to logging
Updates	• Custom update log file location • Specifying post-update options • Downgrading DAT files • Selecting repository branches

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	Agent user interface and log file language

Product Improvement Program

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

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

Priority event forwarding

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

During normal operation, the 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 the agent enforces policies locally, to critical events, such as when a virus is detected and not cleaned. A typical deployment of agents in a large network can generate thousands of these events an hour.

Specific event severities are determined by the product that generates the events. 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 the agent sends lower priority events to the McAfee ePO server on subsequent Agent to Server communication intervals.

You can enable priority uploading of events on the **Events** tab of the McAfee Agent policy pages.

Retrieve system properties

You can use the agent to retrieve system properties from managed systems.

At each agent-server communication, the 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:

- The 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 the 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.

Agent wake-up client task is supported only on the Windows platform. Use System Tree actions to the wake up the agent on Unix-based and Macintosh 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 on a policy name to update it.
4. Deselect **Retrieve all system and product properties (recommended)** 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 the agent policy, even if previously sent.

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

10 Click **Save**.

Select a repository

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

The 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. It also allows you to determine whether old files in a SuperAgent's lazy cache are retained or purged.

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 **Repository** in the **Category** drop-down list.

3 Click **Actions**, then select **New Policy** to create a new policy, or select **Duplicate** in the **Actions** column for the **My Default** policy name to create a new 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-managed repository list), or **Use other repository list** (a locally controlled repository list that is not managed by ePolicy Orchestrator).

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 agents to update from any distributed repository ensures that they get the update from some location.

The agent selects a repository each time a change occurs in the repository list, IP address, or Repository policy option.

Tasks

- *Configure proxy settings for the agent* on page 61
  You might need to configure proxy settings if an agent is having trouble accessing the Internet.

Proxy settings for the agent

To access the McAfee update sites, the agent must be able to access the Internet. Use the 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 an 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 an 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.

Task

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

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 **My Default**, or any other 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**.

Repository Package Management

Contents

About Repository Package Management

This feature allows you schedule repository packages at a specific time. You can only view packages that you have access to, regardless of the repository contents.

Manage the deployed server

Pull new DATs from McAfee, test them on a group of pilot systems, and then automatically move the DAT from Evaluation to the Current branch.

Task

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

1 From the ePolicy Orchestrator console, select **Menu** | **Software** | **Master Repository** | **Pull Now**.

2 Start a repository pull to copy the Evaluation version of DAT to the Master Repository.

3 Use a Client Task to deploy the new DAT to the TestSystem group in the System Tree.

4 Allow the DAT to run for a specified amount of time, then automatically move the DAT from Evaluation to the Current Branch.

5 Create an automatic response that monitors the pilot systems:

- If no errors occur, then automatically move the DAT file to the Current branch of the Master Repository, select all Agent Handlers, then deploy it.
- If errors occur, then notify the administrator and stop the automatic deployment.

Change the agent user interface and event log language

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

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

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

Task

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

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

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

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

The **McAfee Default** policy can't be modified.

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

5 Click **Save**.

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

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

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.

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**.

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

The agent has to talk to an ePolicy Orchestrator server or Agent Handler periodically to ensure all settings are current, send events and so on.

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

When the agent is first installed, it calls in to the server at a random time within six seconds. Thereafter, the agent calls in whenever one of the following occurs:

- The Agent-to-server communication interval (ASCI) elapses.
- A scheduled wake-up task runs on the client systems.
- Communication is initiated manually from the managed system.
- Agent wake-up calls sent from the ePolicy Orchestrator server

Agent-server communication Interval

The agent-server communication interval (ASCI) determines how often the McAfee Agent calls in to the McAfee ePO server.

The agent-server communication interval is set on the **General** tab of the McAfee Agent Policy page. The default setting of 60 minutes means that the agent contacts the server once every hour. When deciding whether to modify the interval, consider that the 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.
- Enforces policies.
- The Agent Handler or the ePolicy Orchestrator server sends new policies and tasks to the client. This action might trigger other resource-consuming actions.
- Many systems managed by ePolicy Orchestrator.
- Your organization has stringent threat response requirements.
- Inadequate available bandwidth.

In general, if your environment includes these variables, you want to perform agent-server communications less frequently. For 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.

The McAfee Agent cycles through the following connection methods six times or until one of a set of responses is returned.

1. IP address
2. Fully qualified domain name
3. NetBIOS

The agent iterates through those three connection methods in that order up to six times for a total of 18 connection attempts. There is no delay between connection attempts. The agent stops this cycle if a connection attempt results in any of the following:

- No error
- Download failed
- Upload failed
- Agent is shutting down
- Transfer aborted
- Server busy (status code from McAfee ePO server)
- Upload success (status code from McAfee ePO server)
- Agent needs new keys

- No package to receive (status code from McAfee ePO server)
- Agent needs to regenerate GUID (status code from McAfee ePO server)

Other results such as connection refused, failed to connect, connection timeout, or other errors causes the agent to retry immediately using connection method in the list until the next ASCI nears.

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.

The agent wake-up client task is supported only on Windows platforms. Use System Tree actions to wake-up agents on Unix-based and Macintosh OS.

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

- **Manually from the server** — This is the most common approach and requires the agent wake-up communication port be open.
- **On a schedule set by the administrator** — This approach is useful when manual agent-to-server communication is disabled by policy. The administrator can create and deploy a wake-up *task*, which wakes up the agent and initiates Agent-Server Communication.

Some reasons for issuing an agent 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** 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 agent on a Windows system to a SuperAgent, it can issue wake-up calls to designated network broadcast segments. SuperAgents distribute the bandwidth impact of the agent 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 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.

SuperAgents and how they work

A SuperAgent is an agent that acts as an intermediary between the McAfee ePO server and other agents in the same network broadcast segment. You can only convert a Windows agent to SuperAgent.

The SuperAgent caches information received from an ePolicy Orchestrator server, the Master Repository, or a mirrored Distributed Repository, and distributes it to the agents in its network subnet. The Lazy Caching feature allows SuperAgents to retrieve data from ePolicy Orchestrator servers only when requested by a local agent node. Creating a hierarchy of SuperAgent along with lazy caching further saves bandwidth and minimizes the wide-area network traffic.

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 ePolicy Orchestrator server, then wakes up the agents in its subnet.

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.

SuperAgents and broadcast wake-up calls

Use agent wake-up calls to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent.

SuperAgents distribute the bandwidth load of concurrent wake-up calls. Instead of sending agent wake-up calls from the server to every 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 all agents in the same broadcast segment.
3. All notified agents (regular agents notified by a SuperAgent and all SuperAgents) exchange data with the ePolicy Orchestrator server or Agent Handler.

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

SuperAgent deployment tips

To deploy enough SuperAgents to the appropriate locations, first determine the broadcast segments in your environment and select a system (preferably a server) in each segment to host a SuperAgent. If you use SuperAgents, make sure all agents are assigned a SuperAgent.

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:

- The agent wake-up communication port (8081 by default).
- The agent broadcast communication port (8082 by default).

Convert agents to SuperAgents

During the global updating process, when the SuperAgent receives an update from the ePolicy Orchestrator server it sends wake-up calls to all the agents in its network. Configure SuperAgent policy settings to convert an agent to SuperAgent.

Task

For option definitions, click **?** 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 the desired General policy.

From this location, you can edit the selected policy, or create a new 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 wide-area network (WAN) usage.

If an agent has been converted to a SuperAgent, it can cache content from the McAfee ePO server, the distributed repository, or other SuperAgents to distribute locally to other agents, reducing WAN bandwidth. To activate this, turn on **LazyCaching** in the **McAfee Agent** | **SuperAgent** policy options page which you access from **Menu** | **Policy** | **Policy Catalog**.

The SuperAgents 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 caches that content. From that point on, the cache is updated whenever a newer version of the package requested 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 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 cache is flushed

SuperAgents flush content from their cache in two situations.

- If the **Checking new repository content interval** has expired since the last time updates were requested, the SuperAgent downloads updates from the Master Repository, processes them, and completely flushes the cache if any new content is available.
- When a global update occurs, SuperAgents receive a wake-up call that flushes all content in the cache.

- SuperAgents are flushed every 30 minutes by default. When the SuperAgent flushes its cache, it deletes every file in its repository not listed in `Replica.log`. This includes any personal files you might have put in that folder.
- SuperAgent caching in conjunction with repository replication is not recommended.

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.

SuperAgent Caching should not be used in conjunction 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.

SuperAgent and its hierarchy

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

A SuperAgent caches the content updates from the ePolicy Orchestrator server or distributed repository and distributes it to the agents in the network reducing the wide area network traffic. It is always ideal to have more than one SuperAgent to balance the network load.

Ensure that you enable Lazy caching before you setting the SuperAgent hierarchy.

Creating a hierarchy of SuperAgents

You can use the Repository policy to create the hierarchy. It is recommended to have a three level hierarchy of SuperAgents in your network.

Creating a hierarchy of SuperAgent avoids repetitive download of the content update from the ePolicy Orchestrator server or distributed repository. For example, in a client network with two SuperAgents (SuperAgent 1 and SuperAgent 2) and a distributed repository, configure the hierarchy in such a way that the client systems receives the content updates from the SuperAgent 1. The SuperAgent 1 receives and caches updates from SuperAgent 2, then the SuperAgent 2 receives and caches updates from the distributed repository.

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. See *Enable SuperAgent wake-up call broadcast* for more details.

If the SuperAgents don't serve agents with latest content update, agents reject the content update received from SuperAgent and fall back to the next repository configured in the policy.

Arrange SuperAgent in hierarchy

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

Task

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

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. If you want 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 SuperAgents in hierarchy.

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. See *Collect McAfee Agent Statistics* for more details.

Agent relay capability

If your network configuration blocks communication between the McAfee Agent and the McAfee ePO server, the agent can't receive content updates, policies, or send events.

Relay capability can be enabled on agents that have direct connectivity to the ePolicy Orchestrator server or Agent Handlers to bridge communication between the client systems and the McAfee ePO server. You can configure more than one agent as a RelayServer to maintain network load balance.

- You can enable relay capability on McAfee Agent 4.8 or later.
- The ePolicy Orchestrator server can only initiate communication (for example, Show agent logs) with a directly connected agent.
- Relay capability is not supported on AIX systems.

Communicating through RelayServers

Enabling relay capability in your network converts an agent to a RelayServer. An agent with relay capability can access the ePolicy Orchestrator server or the distributed repository.

When an agent fails to connect to the ePolicy Orchestrator server or the Agent Handler directly, it broadcasts a message to discover an agent with relay capability in its network. The RelayServers respond to the message and agent establishes connection with the server that first responded.

If an agent fails to connect to the ePolicy Orchestrator server or the Agent Handler directly, it tries to connect to the first RelayServer which responded to the discovery message. The agent discovers the RelayServers in the network at every ASCI and caches the details of the first five unique RelayServers that responded to the discovery message. If the current RelayServer fails to connect with the ePolicy Orchestrator server or doesn't have the required content update, agent connects to the next RelayServer available in its cache.

- Agents require User Datagram Protocol (UDP) to discover RelayServers in the network.
- RelayServer connects only with the ePolicy Orchestrator server or the distributed repositories that are listed in its `SiteList.xml` file. McAfee recommends you to include the RelayServers `sitelist.xml` as a super-set of the site lists of all agents that are configured to connect through this RelayServer.

On a Windows client system, after the relay capability is enabled through the policy a new service **MfeServiceMgr.exe** is installed. This service can be started or stopped to control relay capability on the client system.

Once the agent has completed uploading or downloading content from the ePolicy Orchestrator server, the RelayServer then disconnects the agent and the ePolicy Orchestrator server.

Enable relay capability

You can 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 `cmamesh` process and the service manager port to the `iptables` and `ip6tables`.

Task

For option definitions, click **?** 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 the desired General policy.

   From this location, you can edit the selected policy, or create a new 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 **Enable RelayServer** to enable relay capability.

   - Ensure that you configure the **Service Manager port** to **8083**.
   - McAfee recommends that you enable relay capability within the organization's network.
   - RelayServers cannot connect to the ePolicy Orchestrator servers using proxy settings.
8. Click **Save**.
9. Send an agent wake-up call.

   - 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.
   - On a Windows client system, the log file `SvcMgr_<system name>.log` is saved in `C:\ProgramData\McAfee\Common Framework\DB`.

Collect McAfee Agent statistics

You can run McAfee Agent Statistics client task on the managed nodes to collect the RelayServer and SuperAgent hierarchy statistics.

Task

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

1. Click **Menu** | **Systems** | **System Tree** | **Systems**, then select a group under 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**. The Client Task Assignment Builder page appears.
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**.

Options	Definition
RelayServer Statistics	Collects these statistics from the client systems: • Number of failed connections from the RelayServers to the ePolicy Orchestrator server or distributed repositories • number of connections rejected by the RelayServer after the maximum allowed connections
SuperAgent Hierarchical Update Statistics	Collects the network bandwidth saved by use of SuperAgent hierarchy

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

Disable relay capability

You can use the General policy to disable the relay capability on the agent.

For option definitions, click **?** 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 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.

5 On the **SuperAgent** tab, deselect **Enable RelayServer** to disable the relay capability on the client system.

6 Click **Save**.

7 Send an agent wake-up call.

Respond to policy events

You can set up an automatic response in ePolicy Orchestrator that is filtered to see only policy events.

Task

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

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 click **Next**.

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

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

Option	Definition
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 point 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 point 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 the desired behavior depending on action type, then click **Next**.

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

An automatic response has now been created that will perform the described action when a policy event occurs.

Run client tasks immediately

When ePolicy Orchestrator 4.6 and later is communicating with McAfee Agent 4.6 and later, you can run client tasks immediately using the run tasks now.

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.

The **Run Client Task Now** is supported only on Windows client systems.

Task

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

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.

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 as 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 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 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 **?** in the interface.

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

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

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication. The query results allow you take a variety of actions with respect to the systems identified, including ping, delete, wake up, and re-deploy an agent.

Windows system and product properties reported by the agent

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

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

View agent and product properties

A common troubleshooting task is to verify that the policy changes you made match the properties retrieved from a system.

Task

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

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 ribbon at the top of the System Information page contains Summary, Properties, and Threat Events windows. It also displays System Properties, Products, Threat Events, McAfee Agent, Rogue System Detection, and Related Items tabs.

Queries provided by McAfee Agent

McAfee Agent adds a number of standard queries to your ePolicy Orchestrator environment.

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

Table 7-1 Queries provided by McAfee Agent

Query	Description
Agent Communication Summary	A pie chart of managed systems indicating whether the agents have communicated with the McAfee ePO server within the past day.
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.
Managed nodes having point product policy enforcement failures	A single group bar chart showing the maximum managed nodes (specified in the Query Builder wizard) having at least one policy enforcement failure. You can query for point product policy enforcement failures on McAfee ePO server 5.0 or later.
Managed nodes having point product property collection failures	A single group bar chart showing the maximum managed nodes (specified in the Query Builder wizard) having at least one property collection failure. You can query for point product property collection failures on McAfee ePO server 5.0 or later.
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.

8 Running agent tasks from the managed system

If you can access the managed system where the agent is installed, you can view and manage some features of the agent.

The agent interface is available on the managed 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

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. This feature is available only if specifically 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 the agent communicates, and the software products being managed.

Making the system tray icon visible

You can hide the system tray icon to restrict the use of agent and other point-products.

Task

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

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, for example **My Default**.

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 4.5 or later 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.

Task

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

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, for example **My Default**.

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**.

Run a manual update

Updates can be run manually from a client system.

Product updates can include:

- 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

Task

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

The agent performs an update from the repository defined in the agent policy.

The agent will pull 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.

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

View version numbers and settings

Information about agent settings can be found on the managed system.

This is useful for troubleshooting when installing new agent versions, or to confirm that the installed agent is the same version as the one displayed in the agent properties on the server.

Each installed point product provides information to the **About** dialog. The following information is provided by the agent:

- Agent version number
- Current system mode (Managed, Unmanaged, or SuperAgent)
- Date and time of Last security update check
- Date and time of Last agent-server communication
- Agent-server communication interval
- Policy Enforcement Interval
- 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 the agent.

Agent command-line options

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

Different Command Agent tools are available for Windows, Unix based, and Macintosh Operating systems.

- Windows — `CmdAgent.exe`
- Unix based and Macintosh — `cmdagent`

The Command Agent tool is installed on the managed system at the time of 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 agent installation folder. By default, this location is:

- Windows — `C:\Program Files\McAfee\Common Framework`
- Unix based — `/opt/McAfee/cma/bin`
- Macintosh —`/Library/McAfee/cma/bin`

Command-line options

Parameter	Description
/C	Checks for new policies. The agent contacts the McAfee ePO server for new or updated policies, then enforces them immediately upon receipt.
/E	Prompts the agent to enforce policies locally.
/P	Sends properties to the McAfee ePO server.
/S	Displays the Agent Monitor.
/F	Forwards events from Unix based and Macintosh client systems to ePO server.

9 Agent activity logs

The agent activity log files are useful for determining agent status or for troubleshooting. Two log files record agent activity and are located in the agent installation folders on the managed system.

Contents

About the agent activity logs

The agent maintains two log files that track its actions.

Agent activity log

This log file records agent activity related to things such as policy enforcement, agent-server communication, and event forwarding. You can define a size limit of this log file. On the Logging tab of the McAfee Agent policy pages, you can configure the level of agent activity that is recorded.

The agent activity log is an XML file named `agent_<system>.xml`, where `<system>` is the NetBIOS name of the system where the agent is installed.

Detailed agent activity log

The detailed activity log contains troubleshooting messages. This file has a 1 MB default size limit. When this log file reaches 1 MB, a backup copy is made (`agent_<system>_backup.log`).

On Windows systems, the detailed agent activity log is named `agent_<system>.log` file, where `<system>` is the NetBIOS name of the system on which the agent is installed.

On UNIX-based systems, the detailed log files are found in the folder `/opt/McAfee/cma/scratch/etc` and they are named `log`, `log.1`, `log.2`,…, `log.5`. The higher the log number, the older the file.

View the agent activity log from the managed system

The agent activity log can be seen on the Windows client system using the Agent tray icon (McTray).

The agent icon is available in the system tray only if the **Show McAfee system tray icon (Windows only)** policy is set in ePolicy Orchestrator 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 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 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:

- **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**.

Index

G

I

L

M

N

O

P

Q

R

S

T

U

W