Product Guide

McAfee Agent 4.6.0
for use with ePolicy Orchestrator 4.5.0
COPYRIGHT
Copyright © 2010 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS
AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSION SHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

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

Preface 7
About this guide .................................. 7
Audience .................................. 7
Conventions .................................. 7
Finding product documentation ................. 8

Introduction to McAfee Agent 4.6

1 About the McAfee Agent 11
McAfee Agent ................................... 11
SuperAgent .................................... 12
Agent Handler ................................... 12
System requirements .............................. 12
Languages supported by the McAfee Agent .......... 15

Installing, upgrading, and removing the agent

2 Installing the agent 19
Installation versus deployment .................... 19
When to install from ePolicy Orchestrator ........... 21
When to install using Windows login scripts .......... 22
Agent installation folder ............................ 23
Installing the agent extension and packages into ePolicy Orchestrator 24
Agent installation package .............................. 25
Creating custom agent installation packages .......... 26
Agent installation command-line options ............. 26
Assigning values to custom properties ............... 28
Running agent command line tools as an administrator on Windows .......... 28
Installing on Windows systems ....................... 29
Installing on Windows from ePolicy Orchestrator ........ 29
Installing on Windows using third-party deployment methods .......... 30
Installing on Windows manually ..................... 31
Installing on Windows with login scripts ............ 32
Installing on UNIX-based and Macintosh systems .......... 33
Installing on UNIX-based and Macintosh operating systems from ePolicy Orchestrator .... 33
Installing on UNIX-based and Macintosh operating systems manually .......... 34
Installing on Ubuntu operating systems ............ 35
Including the agent on an image .................... 36
Removing an agent GUID from the Windows registry ...... 36
How to identify duplicate agent GUIDs ............... 36
Correcting duplicate agent GUIDs ................... 37

3 Upgrading and restoring agents 39
Upgrading versus updating ............................. 39
Upgrading agents using a product deployment task ........................................ 40
Upgrading an unmanaged agent on Ubuntu .................................................. 40
Restoring a previous version of the agent on Windows ................................ 41
Restoring a previous version of the agent on UNIX-based and Macintosh systems .... 41

4 Changing agent management modes ...................................................... 43
When to change agent management modes .................................................. 43
Changing the agent mode on Windows ........................................................ 44
  Changing from unmanaged to managed mode in Windows ......................... 44
  Changing from managed to unmanaged mode in Windows ......................... 44
Changing the agent mode on UNIX-based and Macintosh systems .................. 44
  Changing from unmanaged to managed mode on UNIX-based platforms .......... 45
  Changing from managed to unmanaged mode on UNIX-based platforms .......... 45

5 Removing the McAfee Agent ....................................................................... 47
Removing agents when deleting systems from the System Tree ....................... 47
Removing agents when deleting groups from the System Tree ........................ 47
Removing agents from systems in query results ............................................ 48
Removing the agent from a Windows command prompt ................................. 48
Uninstalling from non-Windows operating systems ....................................... 48

Using the agent

6 Configuring agent policies ........................................................................ 53
Agent policy settings .................................................................................. 53
  Priority event forwarding ........................................................................ 54
  Selecting a repository .............................................................................. 55
  Changing the agent user interface and event log language ......................... 56
Proxy settings for the agent ........................................................................ 56
  Configuring proxy settings for the agent ................................................... 56
Retrieving system properties ........................................................................ 57
Configuring selected systems for updating ................................................... 58

7 Working with the agent from the McAfee ePO server ................................ 59
Agent-server communication ........................................................................ 59
  Agent-server communication interval ....................................................... 60
  Agent-server communication interruption handling .................................... 60
  Wake-up calls and tasks ............................................................................ 61
  SuperAgents and broadcast wake-up calls ............................................... 61
  SuperAgent caching and communication interruptions ............................... 62
Viewing agent and product properties ........................................................ 63
Responding to policy events ......................................................................... 63
Running client tasks immediately ................................................................ 64
Sending manual wake-up calls to systems ................................................... 65
Sending manual wake-up calls to a group ..................................................... 65
Locate inactive agents .................................................................................. 66
 Queries provided by McAfee Agent ............................................................. 66
Windows system and product properties reported by the agent ...................... 67

8 Running agent tasks from the managed system ........................................ 69
Using the system tray icon ........................................................................... 69
  What the system tray icon does ............................................................... 69
  Making the system tray icon visible .......................................................... 70
  Enabling user access to updating functionality ........................................... 70
Running a manual update ............................................................................ 71
Enforcing policies ....................................................................................... 71
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating policies</td>
<td>71</td>
</tr>
<tr>
<td>Sending properties to the McAfee ePO server</td>
<td>72</td>
</tr>
<tr>
<td>Sending events to the McAfee ePO server on-demand</td>
<td>72</td>
</tr>
<tr>
<td>Updates from the managed system</td>
<td>72</td>
</tr>
<tr>
<td>Viewing version numbers and settings</td>
<td>73</td>
</tr>
<tr>
<td>Agent command-line options</td>
<td>73</td>
</tr>
<tr>
<td><strong>9 Agent activity logs</strong></td>
<td></td>
</tr>
<tr>
<td>About the agent activity logs</td>
<td>75</td>
</tr>
<tr>
<td>Viewing the agent activity log from the managed system</td>
<td>75</td>
</tr>
<tr>
<td>Viewing the agent activity log from the McAfee ePO server</td>
<td>76</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>77</td>
</tr>
</tbody>
</table>
Preface

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

Contents

- About this guide
- Finding product documentation

About this guide

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

Audience

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

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses the following typographical conventions and icons.

- **Book title or Emphasis**
  - Title of a book, chapter, or topic; introduction of a new term; emphasis.
- **Bold**
  - Text that is strongly emphasized.
- **User input or Path**
  - Commands and other text that the user types; the path of a folder or program.
  - A code sample.
- **User interface**
  - Words in the user interface including options, menus, buttons, and dialog boxes.
- **Hypertext blue**
  - A live link to a topic or to a 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.
Finding 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


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

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a Product, then select a Version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introduction to McAfee Agent 4.6

Chapter 1  About the McAfee Agent
1

About the McAfee Agent

The McAfee Agent is the client-side component providing secure communication between ePolicy Orchestrator and managed products.

The McAfee Agent comprises an ePolicy Orchestrator extension and a number of packages corresponding to the various client operating systems supported by the agent.

The term agent is used in three different 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 also tasked with acting as an intermediary between ePolicy Orchestrator and other local agents, reducing network traffic between locations.
- Agent Handler — A server you can install in various network locations to help manage agent communication, load balancing, and product updates.

Contents

- McAfee Agent
- SuperAgent
- Agent Handler
- System requirements
- Languages supported by the McAfee Agent

 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.

In organizations that are distributed across different locations, SuperAgents can be useful in minimizing network traffic between locations. The SuperAgent caches information received from an ePolicy Orchestrator server or the Master Repository, and distributes it to the agents in its network subnet. The Lazy Caching feature can reduce network traffic even further by causing SuperAgents to retrieve data from ePolicy Orchestrator servers only when requested by a local agent node.

A SuperAgent can also broadcast 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 pings the agents in its subnet. Agents located in a segment with no SuperAgent do not receive the wake-up call. This is an alternative to sending ordinary agent wake-up calls to each agent in the network, with the advantage that it reduces wide-area network traffic.

Agent Handler

An Agent Handler is a server responsible for managing communication between agents and an server.

ePolicy Orchestrator

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

Setting up additional Agent handlers can:

• Help support an increased number of products and systems managed by a single, logical ePolicy Orchestrator server in situations where the CPU on the database server is not overloaded.
• Provide load-balanced communication with a large number of agents, including geographically distributed agents.

System requirements

Make sure your client systems meet the system requirements for McAfee Agent 4.6, including the operating systems and processors it supports.

System requirements

• Installed disk space — 29-32 MB, excluding log files
• Memory — 256 MB RAM
• Processor speed — 500 MHz minimum
## Supported operating systems and processors

<table>
<thead>
<tr>
<th>Operating systems</th>
<th>Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Macintosh OS X Tiger</td>
<td>• Intel</td>
</tr>
<tr>
<td></td>
<td>• PowerPC</td>
</tr>
<tr>
<td>Apple Macintosh OS X Leopard</td>
<td>• Intel</td>
</tr>
<tr>
<td></td>
<td>• PowerPC</td>
</tr>
<tr>
<td>Apple Macintosh OS X Snow Leopard</td>
<td>Intel processor</td>
</tr>
<tr>
<td>HP-UX 11i v1 (build 11.11)</td>
<td>PA-RISC</td>
</tr>
<tr>
<td>HP-UX 11i v2 (build 11.23)</td>
<td></td>
</tr>
<tr>
<td>IBM AIX 5.3 (TL8 or later)</td>
<td>Power 5</td>
</tr>
<tr>
<td>IBM AIX 6.1</td>
<td>Power 5</td>
</tr>
<tr>
<td>McAfee Email and Web Security 3100</td>
<td>Intel processor</td>
</tr>
<tr>
<td>McAfee Email and Web Security 3200</td>
<td></td>
</tr>
<tr>
<td>Red Hat Linux Enterprise 4</td>
<td>x86, x64 or compatible</td>
</tr>
<tr>
<td>Red Hat Linux Enterprise 5</td>
<td></td>
</tr>
<tr>
<td>Solaris 9; 32-bit or 64-bit</td>
<td>SPARC</td>
</tr>
<tr>
<td>Solaris 10; 64-bit</td>
<td></td>
</tr>
<tr>
<td>SuSE Linux 8.2</td>
<td></td>
</tr>
<tr>
<td>SuSE Enterprise Server/Desktop 9</td>
<td>x86, x64 or compatible</td>
</tr>
<tr>
<td>SuSE Enterprise Server/Desktop 10 w/SP3</td>
<td></td>
</tr>
<tr>
<td>SuSE Enterprise Server/Desktop 11</td>
<td></td>
</tr>
<tr>
<td>CentOS Linux 4.0-4.8</td>
<td></td>
</tr>
<tr>
<td>CentOS Linux 5.0-5.4</td>
<td></td>
</tr>
<tr>
<td>Fedora Core Linux 10, 11, and 12</td>
<td></td>
</tr>
<tr>
<td>Ubuntu Linux 8.04, 8.10, 9.04, and 9.10</td>
<td></td>
</tr>
<tr>
<td>Windows 2003 Server (or R2); 32-bit;</td>
<td>• Itanium 2</td>
</tr>
<tr>
<td>Enterprise, Standard, or Web Editions;</td>
<td>• Intel Pentium</td>
</tr>
<tr>
<td>SP 1 or 2</td>
<td>• Intel Celeron (recommended)</td>
</tr>
<tr>
<td>Windows 2003 Server (or R2); 64-bit;</td>
<td>• x86, x64 or compatible</td>
</tr>
<tr>
<td>Enterprise, Standard, or Web Editions;</td>
<td></td>
</tr>
<tr>
<td>SP 2</td>
<td></td>
</tr>
<tr>
<td>Operating systems</td>
<td>Processor</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Windows 7 Home Premium; 32-bit or 64-bit; GA</td>
<td>• Intel Pentium</td>
</tr>
<tr>
<td>Windows 7 Professional; 32-bit or 64-bit; GA</td>
<td>• Intel Celeron (recommended) or compatible</td>
</tr>
<tr>
<td>Windows 7 Ultimate; 32-bit or 64-bit; GA; includes XP mode</td>
<td>• x86, x64 or compatible</td>
</tr>
<tr>
<td>Windows Vista Home Premium; 32-bit or 64-bit; GA, SP 1 or 2</td>
<td></td>
</tr>
<tr>
<td>Windows Vista Home Basic; 32-bit or 64-bit; GA, SP 1 or 2</td>
<td></td>
</tr>
<tr>
<td>Windows Vista Business; 32-bit or 64-bit; GA, SP 1 or 2</td>
<td></td>
</tr>
<tr>
<td>Windows Vista Enterprise; 32-bit or 64-bit; GA, SP 1 or 2</td>
<td></td>
</tr>
<tr>
<td>Windows Vista Ultimate; 32-bit or 64-bit; GA, SP 1 or 2</td>
<td></td>
</tr>
<tr>
<td>Windows 2008 Server; Standard; 32-bit or 64-bit; GA or SP 2</td>
<td></td>
</tr>
<tr>
<td>Windows 2008 Server Enterprise; 32-bit or 64-bit; GA or SP 2</td>
<td></td>
</tr>
<tr>
<td>Windows 2008 Server Datacenter; 32-bit or 64-bit; GA or SP 2</td>
<td></td>
</tr>
<tr>
<td>Windows 2008 Server, Web; 32-bit or 64-bit; GA or SP 2</td>
<td></td>
</tr>
<tr>
<td>Windows 2008 Server, Core; 32-bit or 64-bit; GA or SP 2</td>
<td></td>
</tr>
<tr>
<td>Windows XP Home Edition; 32-bit or 64-bit; SP2 or 3</td>
<td></td>
</tr>
<tr>
<td>Windows XP Professional; 32-bit or 64-bit; SP2 or 3</td>
<td></td>
</tr>
<tr>
<td>Windows XP Tablet PC Edition; 32-bit or 64-bit; SP3</td>
<td></td>
</tr>
</tbody>
</table>

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

**Additional supported platforms**

The agent is supported on the following virtualization platforms:
- Windows 2008 Server Hyper-V
- ESX
- XenServer

The agent is supported on the following McAfee security appliances:
- McAfee Email and Web Security 3100 and 3200
Languages supported by the McAfee Agent

The agent is localized into multiple languages.

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
Installing, upgrading, and removing the agent

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

Chapter 2  Installing the agent
Chapter 3  Upgrading and restoring agents
Chapter 4  Changing agent management modes
Chapter 5  Removing the McAfee Agent
Installing the agent

The agent software can be placed on client systems in various ways. The method you choose depends on three factors: operating system, first-time installation versus upgrade, and the tools used to install the software.

This section provides the instructions required to place the agent software on a client system for any set of circumstances.

Contents

- Installation versus deployment
- Installing the agent extension and packages into ePolicy Orchestrator
- Agent installation package
- Installing on Windows systems
- Installing on UNIX-based and Macintosh systems
- Including the agent on an image

Installation versus 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 placing the agent, or managed products and their upgrades, on one or more computers where an agent is already present.

Installing the agent

This table lists methods for installing the agent, the required actions, and informational notes about each method.
### 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.

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment task</td>
<td>Use the McAfee ePO System Tree to upgrade the agent on selected target systems.</td>
<td>• An agent must already be present on the target system.</td>
</tr>
</tbody>
</table>
| 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 |

### Installing the agent

#### Installation versus deployment

#### Method

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 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. |
### Installation versus deployment

**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 enable: `<agent install path>/bin/msaconfig -m -d <Path of location containing srpubkey.bin, reqseckey.bin and SiteList.xml> [-nostart]` | • 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 install from ePolicy Orchestrator**

There are a number of circumstances that should be in place before deploying the agent through ePolicy Orchestrator.

Installing the agent by deploying it from ePolicy Orchestrator can support many systems simultaneously. To use this feature to its best effect, certain circumstances must already exist.

- Systems must already be added to the System Tree.

  If you have not yet created the System Tree, 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 specified account 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.
• 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.

• Network access must be enabled on Windows XP Home 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 complete multiple deployment tasks.

When to install using Windows login scripts

In some network environments, it is most efficient to use network login scripts to install the agent on Windows systems as they log on to the network.

Using network login scripts is a reliable method 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.
**Agent installation folder**

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td><code>&lt;System_Drive&gt;\Program Files \McAfee\Common Framework</code></td>
<td>The folder is the same on both managed systems and the ePolicy Orchestrator server itself.</td>
</tr>
<tr>
<td></td>
<td><code>/opt/McAfee/cma/</code></td>
<td>All binaries, logs, agent working area</td>
</tr>
<tr>
<td></td>
<td><code>/etc/cma.d/</code></td>
<td>Configuration and management information (including GUID and agent version) needed to manage point-products.</td>
</tr>
<tr>
<td></td>
<td><code>/etc/</code></td>
<td><code>cma.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration and management information in xml format, allowing point-products to read.</td>
</tr>
<tr>
<td></td>
<td><code>/usr/sbin/</code></td>
<td><code>cma</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Script for starting and stopping the agent, manually and when called by the system.</td>
</tr>
<tr>
<td>AIX</td>
<td><code>/opt/McAfee/cma/</code></td>
<td>All binaries, logs, agent working area</td>
</tr>
<tr>
<td></td>
<td><code>/etc/cma.d/</code></td>
<td>Configuration and management information (including GUID and agent version) needed to manage point-products.</td>
</tr>
<tr>
<td></td>
<td><code>/etc/</code></td>
<td><code>cma.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration and management information in xml format, allowing point-products to read.</td>
</tr>
<tr>
<td></td>
<td><code>/sbin/init.d/cma</code></td>
<td><code>cma</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Script for starting and stopping the agent, manually and when called by the system.</td>
</tr>
<tr>
<td>HP-UX</td>
<td><code>/opt/McAfee/cma/</code></td>
<td>All binaries, logs, agent working area</td>
</tr>
<tr>
<td></td>
<td><code>/etc/cma.d/</code></td>
<td>Configuration and management information (including GUID and agent version) needed to manage point-products.</td>
</tr>
<tr>
<td></td>
<td><code>/etc/</code></td>
<td><code>cma.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration and management information in xml format, allowing point-products to read.</td>
</tr>
<tr>
<td></td>
<td><code>/sbin/init.d/cma</code></td>
<td><code>cma</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Script for starting and stopping the agent, manually and when called by the system.</td>
</tr>
<tr>
<td>Linux</td>
<td><code>/opt/McAfee/cma/</code></td>
<td>All binaries, logs, agent working area</td>
</tr>
<tr>
<td></td>
<td><code>/etc/cma.d/</code></td>
<td>Configuration and management information (including GUID and agent version) needed to manage point-products.</td>
</tr>
<tr>
<td></td>
<td><code>/etc/</code></td>
<td><code>cma.conf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration and management information in xml format, allowing point-products to read.</td>
</tr>
<tr>
<td></td>
<td><code>/etc/init.d/</code></td>
<td><code>cma</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Script for starting and stopping the agent, manually and when called by the system.</td>
</tr>
</tbody>
</table>
### Installing the agent extension and packages into ePolicy Orchestrator

Before the agent can be installed on managed systems, it 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.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA460AIX.zip</td>
<td>IBM AIX agent package</td>
</tr>
<tr>
<td>MA460HPX.zip</td>
<td>HP-UX agent package</td>
</tr>
<tr>
<td>MA460LNX.zip</td>
<td>Linux agent package</td>
</tr>
<tr>
<td>MA460MAC.zip</td>
<td>Macintosh agent package</td>
</tr>
<tr>
<td>MA460SOL.zip</td>
<td>Solaris agent package</td>
</tr>
<tr>
<td>MA460WIN.zip</td>
<td>Windows agent package</td>
</tr>
<tr>
<td>MA460WIN_Embedded.zip</td>
<td>Windows XP Embedded agent package</td>
</tr>
</tbody>
</table>
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.

## Agent installation package

An agent installation package (**FramePkg.exe**) is created when you install ePolicy Orchestrator or check in an agent 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)

By default, the path of the agent installation package on the server is:

```
C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe
```

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.

Creating custom agent installation packages
Custom installation packages are useful for agent installation tasks performed outside 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 or install.sh). 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 operating system.
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.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| /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 |
| /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.  
Example: FRAMEPKG /INSTALL=AGENT |
| /INSTALL=UPDATER | Enables the AutoUpdate 7.0 component if it has already been installed, and does not change whether the agent is enabled. This command-line option upgrades the agent.  
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 |
| /REMOVE=AGENT | Removes the agent if not in use. If in use, the agent changes to updater mode.  
Example: FRMINST /REMOVE=AGENT |
| /SILENT or /S | Installs the agent in silent mode, hiding the installation from the end user.  
Example: FRAMEPKG /INSTALL=AGENT /SILENT |
## Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/SITEINFO</td>
<td>Specifies the folder path to a specific repository list (SiteList.xml) file. Example: FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\TMP \SITELIST.XML</td>
</tr>
<tr>
<td>/USELANGUAGE</td>
<td>Specifies the language version of the agent that you want to install. If you select 0409 or a locale other than the 12 languages with locale IDs, the software appears in English. If you install multiple language versions, the locale selected in operating system determines the language version that displays. Example: FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404</td>
</tr>
</tbody>
</table>

If errors occur during installation, all error messages are displayed in English no matter what /USELANGUAGE parameters are set.

### Assigning values to custom properties

You can specify up to four custom properties during installation of the agent at the 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.

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

- **Windows operating systems:** FrmInst.exe /CustomProps1="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/.

### Running agent command line tools as an administrator on Windows

The agent command line tools (frminst.exe and framepkg.exe) require administrator privileges. To avoid forgetting this, you can configure them to always run with administrator privileges.

**Task**

1. On the target Windows system, open Windows Explorer and navigate to your McAfee Agent installation folder.
   The agent installation folder defaults to C:\Program Files\McAfee\Common Framework.

2. Right-click on FrmInst.exe and select Properties.

3. On the Compatibility tab, select Run this program as an administrator.
4 Click OK.

5 Repeat these steps for FramePkg.exe.

Installing on Windows systems

If you are operating in a Windows environment, you can install the agent 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.

Tasks

- Installing on Windows from ePolicy Orchestrator on page 29

  Installing agents on your Windows systems using ePolicy Orchestrator is a quick way to modify a number of systems simultaneously.

- Installing on Windows using third-party deployment methods on page 30

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

- Installing on Windows manually on page 31

  This method is appropriate if your organization requires that software be installed on systems manually.

- Installing on Windows with login scripts on page 32

  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.

Installing on Windows from ePolicy Orchestrator

Installing agents on your Windows systems using ePolicy Orchestrator is a quick way to modify a number of systems simultaneously.

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.

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.

Installing 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 (for example, Everyone or Users), then click Add.
   g. Click Add.

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

---

**Installing on Windows manually**
This method is appropriate if your organization requires that software be installed on systems manually.

You can 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.

### Installing 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

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

Each system runs the script when it logs on to the network and, if necessary, installs the agent.

Installing on UNIX-based and Macintosh systems

Different agent installation methods are available depending on the operating system running on the client system.

On HP-UX, AIX, 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.

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
- Installing on UNIX-based and Macintosh operating systems from ePolicy Orchestrator
- Installing on UNIX-based and Macintosh operating systems manually
- Installing on Ubuntu operating systems

Installing 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 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 10.6 (Snow Leopard)
- Red Hat Enterprise Linux versions 4 and 5

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 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.

Installing on UNIX-based and Macintosh operating systems manually
The agent must be installed manually on AIX, HP-UX, Solaris, and some Linux systems, and can be installed manually on Macintosh and other 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:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT4000AIXX\Install\0409</td>
</tr>
<tr>
<td>HPUX</td>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT4000HPUX\Install\0409</td>
</tr>
<tr>
<td>Linux</td>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3700LYNX\Install\0409</td>
</tr>
<tr>
<td>Macintosh</td>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3700MACX\Install\0409</td>
</tr>
<tr>
<td>Solaris</td>
<td>C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3700SLRS\Install\0409</td>
</tr>
</tbody>
</table>

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

4 Run these commands, giving root credentials when requested:

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

Installing on Ubuntu operating systems

The agent must be installed manually on systems running the Ubuntu operating system.

There are two ways to install the agent on Ubuntu, in managed or unmanaged mode. 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

Task

1 Copy the installer to the client system.

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

3 Choose the installation mode and run one of the following sets of commands.
   - Install the agent in managed mode.
     ```bash
     $chmod +x ./installdeb.sh
     $sudo ./installdeb.sh -i
     ```
   - Install the agent in unmanaged mode.
     ```bash
dpkg -i MFErt.i686.deb
dpkg -i MFEmca.i686.deb
     ```
Including 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.

When you include the McAfee Agent on an image, you must remove its GUID from the registry. This allows subsequently installed agent images to generate their own GUID at their first agent-server communication.

Tasks
- Removing an agent GUID from the Windows registry on page 36
  When installing an agent on an image, you must remove its GUID from the registry to avoid duplicating GUIDs in the future.
- How to identify duplicate agent GUIDs on page 36
  No two agents can share the same GUID.
- Correcting duplicate agent GUIDs on page 37
  Agents with duplicate GUIDs can be automatically identified and removed with a server task.

Removing an agent GUID from the Windows registry

When installing an agent on an image, you must remove its GUID from the registry to avoid duplicating GUIDs in the future.

If you don't follow this step, all deployed images with agents share the same GUID, and must be changed manually. In a large organization, this is impractical. Although you can configure the McAfee ePO server to identify replicated GUIDs and assign a new GUID at the next agent-server communication, the action consumes considerable processing bandwidth.

- On the imaged system, locate the registry key for the agent and remove it.
  The registry keys are located at: HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent\AgentGUID

How to 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 or the other 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**.

### Correcting 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. To open the Server Task Builder, click **Menu | Automation | Server Tasks**, then click **Edit** in the row labeled **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**. To run this task now, click **Run** instead of **Edit**, and the task runs immediately. You are shown the **Server Task Log** page after it finishes.

2. On the **Description** page, select **Enabled**.
   - To run the task with the default configuration displayed on the **Actions** and **Schedule** tabs, click **Save**.
   - To configure the **Actions** and **Schedule** tabs, click **Next**.

3. On the **Actions** page, select **Run Query** from the **Actions** drop-down list.

4. Next to the **Query** field, click **...**, select one of the following options under System Management, 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 the following options, 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**.
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, check it in to the master repository, then use the deployment task to upgrade the agent.

Contents

- Upgrading versus updating
- Upgrading agents using a product deployment task
- Upgrading an unmanged agent on Ubuntu
- Restoring a previous version of the agent on Windows
- Restoring a previous version of the agent on UNIX-based and Macintosh systems

Upgrading versus updating

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

The term *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 4.6. For full ePolicy Orchestrator functionality, upgrade to agent version 4.6 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.
Upgrading agents using a product deployment task

Deploying a newer version of the agent with the Product Deployment client task is the same task that is used to deploy products to systems that are already running agents.

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  Click Next to open the Schedule page.
9  Schedule the task as needed, then click Next.
10  Verify the task’s details, then click Save.

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

Upgrading an unmanged 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 MFEmca.i686.deb) to the client system.
2. Open a terminal window on the client system. Navigate to the folder containing the installer.
3. Execute the following commands:
   ```
   dpkg -i --force-confnew MFRrt.i686.deb
   dpkg -i --force-confnew MFEmca.i686.deb
   ```

**Restoring 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.

**Restoring 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.
You might have previously used McAfee products in your network. If so, you likely already have agent installations in your network running in updater mode.

Contents

- When to change agent management modes
- Changing the agent mode on Windows
- Changing the agent mode on UNIX-based and Macintosh systems

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 copy the SiteList.xml (repository list file) from the McAfee ePO server 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.

- SiteList.xml must be placed in the same location as srpubkey.bin and reqseckey.bin.
Changing the agent mode on Windows

Agents can be changed from unmanaged mode to managed. Agents can also be reverted to unmanaged mode if necessary.

Tasks

• **Changing from unmanaged to managed mode in Windows on page 44**
  Two methods are available for changing the agent mode on Windows systems. One is simple but uses a large amount of bandwidth, the other is more complex but uses significantly less bandwidth.

• **Changing from managed to unmanaged mode in Windows on page 44**
  Changing Windows systems to unmanaged mode involves removing the systems from the System Tree.

Changing from unmanaged to managed mode in Windows

Two methods are available for changing the agent mode on Windows systems. One is simple but uses a large amount of bandwidth, the other is more complex but uses significantly less bandwidth.

• 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 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. Copy sitelist.xml, srpubkey.bin and reqseckey.bin from the McAfee ePO server to a temporary location on the target system.
  b. Run C:\Program Files\McAfee\Common Framework\frminst.exe on the target system. This requires administrator privileges.

Changing 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.

Changing the agent mode on UNIX-based and Macintosh systems

Agents can be changed from unmanaged mode to managed. Agents can also be reverted to unmanaged mode if necessary.
Tasks

- Changing from unmanaged to managed mode on UNIX-based platforms on page 45
  Changing the agent mode on non-Windows systems must be done manually.

- Changing from managed to unmanaged mode on UNIX-based platforms on page 45
  Changing the agent mode on non-Windows systems must be done manually.

Changing 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.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX, Linux, and Solaris</td>
<td>/opt/McAfee/cma/bin</td>
</tr>
<tr>
<td>Macintosh</td>
<td>/Library/McAfee/cma/bin</td>
</tr>
</tbody>
</table>

2. Open a terminal window on the target system.

3. Run the following command:

   ```bash
   /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.

Changing 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.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX, Linux, and Solaris</td>
<td>/opt/McAfee/cma/bin</td>
</tr>
<tr>
<td>Macintosh</td>
<td>/Library/McAfee/cma/bin</td>
</tr>
</tbody>
</table>

2. Open a terminal window on the target system.

3. Run the following command:

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

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

After deleting an agent, the system is deleted from the System Tree and the agent 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

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

Removing 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. Confirm the deletion, then click OK.

Removing 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.

Removing 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. Confirm the deletion, then click OK.

Removing 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

Uninstalling 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.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>rpm -e MFEcma</td>
</tr>
<tr>
<td>HP-UX</td>
<td>swremove MFEcma</td>
</tr>
</tbody>
</table>
| Linux            | rpm -e MFEcma  
|                  | rpm -e MFErt  |
|                  | ⚠ Run the commands in the listed order. |
| Ubuntu           | dpkg --remove MFErt.i686.deb  
|                  | dpkg --remove MFEcma.i686.deb  |
|                  | ⚠ Run the commands in the listed order. |
| Macintosh        | /Library/McAfee/cma/uninstall.sh |
| Solaris          | pkg rm 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

Chapter 6  Configuring agent policies
Chapter 7  Working with the agent from the McAfee ePO server
Chapter 8  Running agent tasks from the managed system
Chapter 9  Agent activity logs
Configuring agent policies

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

Contents

- Agent policy settings
- Proxy settings for the agent
- Retrieving system properties
- Configuring selected systems for updating

Agent policy settings

The agent provides seven configuration pages for setting policy options. These pages are organized into three categories: General, Repository, and Troubleshooting.

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.

Agent 4.5 had one policy categories: General. When upgrading the agent from version 4.5 to version 4.6, McAfee-supplied policies (for example McAfee Default and My Default) are broken into three categories: General, Repository, and Troubleshooting. 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.

General policies

Settings available for General policies are divided into four tabs.
<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
</table>
| General      | • Policy enforcement interval  
• Use of system tray icon in Windows environments  
• Agent and SuperAgent wake-up call support  
• The repository path where the SuperAgent goes for product and update packages  
• Whether to accept connections only from the McAfee ePO server  
• Creation of SuperAgents in Windows environments  
• Enabling lazy caching  
• Yielding of the CPU to other processes in Windows environments  
• Rebooting options after product deployment in Windows environments  
• Agent-server communication  
• Sending full or minimal system properties and product properties |
| Events       | Priority event forwarding                                                                                                                  |
| 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  
• Defining repository branches                                                                 |

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

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

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

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Agent user interface and log file language</td>
</tr>
</tbody>
</table>

**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.

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

### Selecting a repository

Repositories are selected within a policy.

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 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:

<table>
<thead>
<tr>
<th>Selection method</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping time</td>
<td>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.</td>
</tr>
<tr>
<td>Subnet distance</td>
<td>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.</td>
</tr>
<tr>
<td>Use order in repository list</td>
<td>A user-defined list of repositories based on locally determined preferences. You can sequence and enable or disable specific distributed repositories on the <strong>Repositories</strong> tab of the McAfee Agent policy pages. Allowing agents to update from any distributed repository ensures that they get the update from some location.</td>
</tr>
</tbody>
</table>

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

**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 cannot 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.

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)

- **Use Internet Explorer proxy settings** — 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.

- **Configure the proxy settings manually** — 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.

Configuring 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.
   - On Windows systems you can select **Use Internet Explorer proxy settings** 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**.

---

**Retrieving 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.
- 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.

**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 Send full product properties in addition to system properties to send system properties and minimal product properties.
   This is selected by default.

5 Click Save.

6 Click Menu | Policy | Client Task Catalog.

7 In the Client Task Types list, select McAfee Agent Wakeup.

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

Configuring 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.

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 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.

3 Click OK.
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 agent properties can be viewed.

Contents
- Agent-server communication
- Viewing agent and product properties
- Responding to policy events
- Running client tasks immediately
- Sending manual wake-up calls to systems
- Sending manual wake-up calls to a group
- Locate inactive agents
- Queries provided by McAfee Agent
- Windows system and product properties reported by the agent

Agent-server communication

The agent has to talk to an ePolicy Orchestrator server periodically to ensure all settings are current. These communications are referred to as agent-server communication. During each agent-server communication, the agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the agent, and the repository list if it has changed since the last agent-server communication. The agent enforces the new policies locally on the managed system and applies any task or repository changes.

ePolicy Orchestrator 4.0 uses a proprietary network protocol. Versions 4.5 and later use an industry-standard Transport Layer Security (TLS) network protocol for secure network transmissions.

After the agent is installed, it calls in to the server at a random time within ten minutes. Thereafter, the agent calls in whenever one of the following situations occurs:

- The agent-server communication interval (ASCI) lapses.
- At agent startup.
- Agent wake-up calls are sent from McAfee ePO or Agent Handlers.
- Communication is initiated manually from the managed system (Windows only).
Agent-server communication interval

The agent-server communication interval determines how often the agent calls in to the server.

The agent-server communication interval (ASCI) 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 what the agent does at each ASCI:

• The agent collects and sends its properties to the server or Agent Handler.
• The agent sends the events that have occurred since the last agent-server communication.
• The server or Agent Handler sends new policies and tasks to the client. This action might dictate other resource-consuming actions, such as an immediate DAT download.
• The agent enforces policies.

Although these activities do not burden any one computer, a number of factors can cause the cumulative demand on the network, McAfee ePO servers, or on Agent Handlers to be significant.
• A large number of systems being managed by ePolicy Orchestrator.
• Your organization has stringent threat response requirements.
• The network or physical location of clients in relation to servers or Agent Handlers is highly distributed.
• Inadequate available bandwidth.

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

Agent-server communication interruption handling

Agent-server communication follows a specific algorithm designed to work around issues that might cause a problem connecting with an ePolicy Orchestrator server.

Communication interruptions can happen for many reasons, and the agent-server connection algorithm is designed to re-attempt communication if its first attempt fails.

The agent cycles through the following connection methods up to 6 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)
• Upload success (status code from McAfee ePO)
• No package to receive (status code from McAfee ePO)
• Agent needs to regenerate GUID (status code from McAfee ePO)

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

**Wake-up calls and tasks**

The purpose of an agent wake-up call is to trigger an immediate agent-server communication rather than wait for the current agent-server communication interval to expire.

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 agent-server communication is disabled. The administrator can create and deploy a wake-up task, which triggers a wake-up call on a schedule.

Some reasons for issuing an agent wake-up call are:

- You make a policy change that you want the agent to adopt immediately, without waiting for the ASCI to expire.
- You created a new task that you want the agent to run immediately.
- 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 are have converted a particular Windows system to use as a SuperAgent, it can issue wake-up calls to designated network broadcast segments. SuperAgents distribute the bandwidth impact of the agent wake-up call, and help distribute network traffic.

**SuperAgents and broadcast wake-up calls**

If you operate in a Windows environment and plan to 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 server.

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. Be aware that agents in broadcast segments without SuperAgents do not receive the broadcast wake-up call, so they do not call in to the server in response to a wake-up call. 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).

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 its McAfee ePO server to distribute locally to other agents, reducing WAN bandwidth. To activate this, turn on LazyCaching in the McAfee Agent | General policy options page which you access from Menu | Policy | Policy Catalog.

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.

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

Agents configured to use the SuperAgent as their repository receive the content cached in the SuperAgent repository 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.

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.
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 and other sites listed in Sitelist.xml 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.

Viewing agent and product properties

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

The properties you see depend on whether you configured the agent to send full or minimal properties on the McAfee Agent policy pages.

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 appear. New in ePolicy Orchestrator 4.6 is a ribbon at the top of the System Information page containing Summary, Properties, and Threat Events windows.

Responding to policy events

You can set up an automatic response in ePolicy Orchestrator 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 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 the **Event Description** row and choose one of the following options from the list:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent failed to collect properties for any point products</td>
<td>This event is broadcast when a property collection failure first occurs. A subsequent success event is not broadcast. Each failing point product generates a separate event.</td>
</tr>
<tr>
<td>Agent failed to enforce policy for any point products</td>
<td>This event is broadcast when a policy enforcement failure first occurs. A subsequent success event is not broadcast. Each failing point product generates a separate event.</td>
</tr>
</tbody>
</table>

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.

### Running client tasks immediately

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

ePolicy Orchestrator 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 at the same time 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 after it finishes.

**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** supplying the task and the **Task Type**.

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

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

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

   **i** If you create a **McAfee Agent Product Deployment** or **Product Update** task during this procedure, one of the available options is **Run at every policy enforcement**. This option has no effect 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 Log.
Sending manual wake-up calls to 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 for an update before the next agent-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 section.
4. Next to Wake-up call type, select whether to send an Agent Wake-Up Call or SuperAgent Wake-Up Call.
5. Accept the default Randomization (0 - 60 minutes) or type a different value. Consider the number of systems that are receiving the wake-up call, and how much bandwidth is available. If you type 0, agents respond immediately.
6. 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.
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.

Sending 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 for an update before the next agent-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 - 60 minutes), or type a different value. 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.

---

**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 to take a variety of actions with respect to the systems identified, including ping, delete, wake up, and re-deploy an agent.

---

**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**

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Communication Summary</td>
<td>A pie chart of managed systems indicating whether the agents have communicated with the McAfee ePO server within the past day.</td>
</tr>
<tr>
<td>Agent Handler Status</td>
<td>A pie chart displaying Agent Handler communication status within the last hour.</td>
</tr>
<tr>
<td>Agent Versions Summary</td>
<td>A pie chart of installed agents by version number on managed systems.</td>
</tr>
<tr>
<td>Inactive Agents</td>
<td>A table listing all managed systems whose agents have not communicated within the last month.</td>
</tr>
<tr>
<td>Managed nodes having point product policy enforcement failures</td>
<td>A single group bar chart showing all nodes having at least one policy enforcement failure in the last 24 hours.</td>
</tr>
<tr>
<td>Managed nodes having point product property collection failures</td>
<td>A single group bar chart showing all nodes having at least one property collection failure in the last 24 hours.</td>
</tr>
</tbody>
</table>
Table 7-1 Queries provided by McAfee Agent  (continued)

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repositories and Percentage Utilization</td>
<td>A pie chart displaying individual repository utilization as a percentage of all repositories.</td>
</tr>
<tr>
<td>Repository Usage Based on DAT and Engine Pulling</td>
<td>A stacked bar chart displaying DAT and Engine pulling per repository.</td>
</tr>
<tr>
<td>Systems per Agent Handler</td>
<td>A pie chart displaying the number of managed systems per Agent Handler.</td>
</tr>
</tbody>
</table>

Windows system and product properties reported by the agent

The lists below show the data reported 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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Version</td>
<td>Is 64 Bit OS</td>
</tr>
<tr>
<td>CPU Serial Number</td>
<td>Is Laptop</td>
</tr>
<tr>
<td>CPU Speed (MHz)</td>
<td>Last Communication</td>
</tr>
<tr>
<td>CPU Type</td>
<td>MAC Address</td>
</tr>
<tr>
<td>Custom Props 1-4</td>
<td>Managed State</td>
</tr>
<tr>
<td>Default Language</td>
<td>Management Type</td>
</tr>
<tr>
<td>Description</td>
<td>Number Of CPUs</td>
</tr>
<tr>
<td>DNS Name</td>
<td>Operating System</td>
</tr>
<tr>
<td>Domain Name</td>
<td>OS Build Number</td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>OS OEM Identifier</td>
</tr>
<tr>
<td>Free Memory</td>
<td>OS Platform</td>
</tr>
<tr>
<td>Installed Products</td>
<td>OS Service Pack Version</td>
</tr>
<tr>
<td>IP Address</td>
<td>OS Type</td>
</tr>
<tr>
<td>IPX Address</td>
<td></td>
</tr>
</tbody>
</table>

Product 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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Wake-Up Communication Port</td>
<td>Language</td>
</tr>
<tr>
<td>Agent-to-Server Communication Interval</td>
<td>License Status</td>
</tr>
<tr>
<td>DAT Version</td>
<td>Policy Enforcement Interval</td>
</tr>
<tr>
<td>Engine Version</td>
<td>Product Version</td>
</tr>
<tr>
<td>HotFix/Patch Version</td>
<td>Service Pack</td>
</tr>
</tbody>
</table>
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
- Running a manual update
- Enforcing policies
- Updating policies
- Sending properties to the McAfee ePO server
- Sending events to the McAfee ePO server on-demand
- Updates from the managed system
- Viewing version numbers and settings
- Agent command-line options

### Using the system tray icon

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

### What the system tray icon does

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Security</td>
<td>Triggers immediate updating of all installed McAfee software products. This includes application of patches and hotfixes, as well as DAT and signature updates.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="This feature is available only if specifically enabled in the agent policy." /></td>
</tr>
<tr>
<td>Quick Settings</td>
<td>Links to product menu items that are frequently used.</td>
</tr>
<tr>
<td>Manage Features</td>
<td>Displays links to the administrative console of managed products.</td>
</tr>
</tbody>
</table>
Option | Function
--- | ---
Scan Computer for | Launches McAfee programs, such as VirusScan Enterprise, that scan systems on-demand and detect malicious software.
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.
• Downloads and enforces policies.
About... | Displays system and product information for products installed on the system, 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
If you want to restrict a user's ability to use the agent and other point-products, you can hide the system tray icon.

**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**.
Running 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.

Enforcing 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 | Status Monitor**.
2. Click **Enforce Policies**.

The policy enforcement activity is displayed in the **Agent Status Monitor**.

Updating policies

You can manually cause the agent to communicate with the server to update policy settings.

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

The policy-checking activity is displayed in the **Agent Status Monitor**.
Sending 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 **Agent Status Monitor**.

   ![Note]
   
   Agent policy controls whether full or incremental properties are sent.

Sending 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 **Agent Status Monitor**.

   ![Note]
   
   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

Viewing 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
• 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 Windows-only Command Agent tool (CmdAgent.exe) to perform selected agent tasks from the managed system.

CmdAgent.exe is installed on the managed system at the time of agent installation. Perform this task locally on managed systems using this program or the McAfee system tray icon. It must be run within an Administrator command prompt.

The CmdAgent.exe file is located in the agent installation folder. By default, this location is:

C:\Program Files\McAfee\Common Framework

Command-line options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/C</td>
<td>Checks for new policies. The agent contacts the McAfee ePO server for new or updated policies, then enforces them immediately upon receipt.</td>
</tr>
<tr>
<td>/E</td>
<td>Prompts the agent to enforce policies locally.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>/P</td>
<td>Sends properties and events to the McAfee ePO server.</td>
</tr>
<tr>
<td>/S</td>
<td>Displays the Agent Monitor and its options.</td>
</tr>
</tbody>
</table>
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
- Viewing the agent activity log from the managed system
- Viewing the agent activity log from the McAfee ePO server

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`, 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.

Viewing the agent activity log from the managed system

The agent activity log can be seen within the agent on the client system.

The agent icon is available in the system tray only if the Show McAfee system tray icon (Windows only) option is selected 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.
Agent activity logs
Viewing the agent activity log from the McAfee ePO server

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**.

Viewing the agent activity log from the McAfee ePO server

You can view the agent activity log of a 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

## A

- about this guide 7
- agent
  - command-line options 73
  - introduction to 11
  - maintenance 59
  - modes, converting 44
  - properties, viewing 63
  - removal methods 47, 48
  - removing from systems in query results 48
  - restoring a previous UNIX version 41
  - restoring a previous Windows version 41
  - settings, viewing 73
  - system requirements 12
  - tasks, running from managed systems 69
  - uninstalling 47
  - UNIX installation folder 23
  - upgrading with phased approach 40
  - user interface 69
  - wake-up calls 65
- agent activity logs 75, 76
- agent distribution
  - FrmInst.exe command-line 48
- Agent Handlers
  - introduction to 11
- agent installation
  - CmdAgent.exe 73
  - command-line options 26
  - creating custom packages 26
  - deployment methods 19
  - from an image 36
  - manually on Windows 31
  - on UNIX 34
  - on Windows via push technology 29
  - package, location of 25, 32
  - uninstalling 47
  - update packages 40
  - using login scripts 32
- Agent Monitor 72
- agent upgrade 39, 40
- agent-server communication
  - about 59
  - interval, (ASCI) 36
- ASCI (See agent-to-server communication interval) 60

## B

- best practices
  - agent-to-server communication interval 59

## C

- Command Agent tool (CmdAgent.exe) 73
- command-line options
  - agent 73
  - agent installation 26
  - CmdAgent.exe 73
  - FrmInst.exe 48
- conventions and icons used in this guide 7
- credentials
  - required for agent installation 26

## D

- Data Execution Prevention 12
- DEP, See Data Execution Prevention
- deployment
  - installation, definition and methods 19
  - methods 19
  - push technology via 29
  - upgrading agents 40
- documentation
  - audience for this guide 7
  - product-specific, finding 8
  - typographical conventions and icons 7

## E

- events
  - forwarding, agent configuration and 54
- extension files
  - UNIX, agent package file name 34

## F

- FRAMEPKG.EXE 25

## G

- global unique identifier (GUID)
  - duplicate 36
  - scheduling corrective action for duplicates 37
Index

global updating
  event forwarding and agent settings 54
groups
  deleting from System Tree 47
GUID, See global unique identifier

I
icon, system tray, See system tray icon
inactive agents 66
installation folder
  UNIX 23

L
Locale IDs, settings for installation 26
login scripts
  install the agent via 32

M
managed mode
  convert from unmanaged mode in Windows 44
  convert from unmanaged mode on UNIX 45
  convert from updater mode 44
managed systems
  agent-server communication 59
  running an update task manually 71, 72
  viewing agent activity log 75
McAfee ServicePortal, accessing 8

N
notifications
  event forwarding and agent settings 54

O
operating systems
  McAfee Agent and 12

P
packages
  agent file name, for UNIX 34
  creating custom for agent installation 26
passwords
  installing agents, command-line options 73
policies
  enforcing 71
  update settings 71
  verifying changes 63
policies, McAfee Agent
  options for policy pages 53
  settings, about 53
product properties 67
properties
  agent, viewing from the console 63
  properties (continued)
    custom, for the agent 28
    minimal vs. full 57
    product 67
    retrieving from managed systems 57
    sending to ePO server 72
    system 67
    verifying policy changes 63
proxy settings
  agent policies 56
  configuring for the agent 56
push technology
  initial agent deployment via 29

Q
queries
  removing agents in results of 48

R
removal
  agent, from UNIX systems 48
repositories
  selecting a source for updates 55
requirements
  operating systems 12
  processors 12

S
scripts, login for agent installation 32
ServicePortal, finding product documentation 8
SPIPE 59
status
  security 69
SuperAgents
  introduction to 11
  wake-up calls 61, 65
  wake-up calls to System Tree groups 65
system requirements 12
system tray icon
  allow users to update from 70
  options 69
  security status 69
  using 69
  visibility 70
System Tree
  deleting systems from 47
  groups and manual wake-up calls 65
  removing agents 47
  removing agents from systems 47
systems
  properties 67
Technical Support, finding product information 8
troubleshooting
  upgrading agents by group 40
  verifying properties of agent and products 63

uninstallation
  agent, from UNIX systems 48
UNIX
  agent installation folder 23
  agent package file name 34
  converting from managed to unmanaged mode 45
  converting from unmanaged to managed mode 45
  installing the agent on 34
  uninstalling the agent from 48
unmanaged mode
  convert to managed mode in Windows 44
  convert to managed mode on UNIX 45
updater mode
  convert to managed mode in Windows 44
  convert to managed mode on UNIX 45
updates
  agent installation packages 40
updates (continued)
  allow users via system tray icon 70
  for selected systems 58
  running tasks manually 71, 72
  security 69
  upgrading agents 40
updating
  global, event forwarding and agent settings 54
  manually 71, 72
user accounts
  credentials for agent installation 26
user interface, agent 69
wake-up calls
  about 61
  manual 65
  SuperAgents and 61, 65
tasks 61
to System Tree groups 65
Windows
  converting agent mode 44
  running a manual update 71