McAfee Policy Auditor 5.2.0 Installation Guide

McAfee®

Contents

Introduction

This guide describes installing McAfee® Policy Auditor 5.2.0 for use with ePolicy Orchestrator® version 4.0 Patch 5, or version 4.5. The Setup also installs McAfee Benchmark Editor 5.2.0, a tool that is used by Policy Auditor and other products managed by ePolicy Orchestrator.

Contents

Product components

The Setup installs two extensions that work in the ePolicy Orchestrator environment: Policy Auditor 5.2 and Benchmark Editor 5.2.

Policy Auditor 5.2

Policy Auditor 5.2 automates internal and external IT audits. It audits systems by comparing settings and software to information that describes the desired state of a system. When a system is audited, Policy Auditor provides a score, rating, and detailed information about how well the system conforms to its desired state.

You can create custom audits or use standard industry and government audits like Sarbanes-Oxley (SOX) or the Health Insurance Portability and Accountability Act of 1996 (HIPAA). An audit can check system settings such as password length, password complexity, and open or closed ports. It can also check software for the presence of the latest software updates and settings for web browsers and Microsoft Office.

You can create audits, schedule when and how often they are run, and view detailed reports on the current and historical status of your systems. The customizable reporting system provides quick access to information such as policy audit status, exposure to threats, and overall risk. You can also create your own reports.

Benchmark Editor 5.2

Benchmark Editor 5.2 is a tool for managing your security benchmarks. Benchmarks are documents containing an organized set of rules that describe the desired state of a set of systems. The documents are written in the open-source XML standard format XCCDF (eXtensible Configuration Checklist Description Format). Rules contain one or more checks that standardize the three main steps of the assessment process:

- Representing configuration information of systems for testing.

- Analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, and so on).
- Reporting the results of this assessment.

Finding documentation for McAfee enterprise products

To access the documentation for your McAfee products, use the McAfee ServicePortal.

1. Go to the McAfee ServicePortal (http://mysupport.mcafee.com) and, under **Support by Reading**, click **Product Documentation**.
2. Select a **Product**.
3. Select a **Version**.
4. Select a product document.

Product documentation by phase

McAfee documentation provides the information you need during each phase of product implementation, from installing a new product to maintaining existing ones. Depending on the product, additional documents might also be available. After a product is released, information regarding the product is entered into the online KnowledgeBase, available through the McAfee ServicePortal.

Installation phase — Before, during, and after installation

- *Release Notes*
- *Installation Guide*

Setup phase — Using the product

- *Product Guide*
- *Online Help*

Maintenance phase — Maintaining the software

- *KnowledgeBase* (http://mysupport.mcafee.com)

What's new in this release

This release of Policy Auditor includes the following new features or enhancements:

- **AIX Support** — Policy Auditor can audit systems running AIX 5.3 and 6.1 on Power5 and Power6 processor architectures.
- **Findings** — Findings are audit results that include additional information about the state of a system that is helpful to security officers and network administrators when fixing issues. Findings can include three types of information:
  - **Violations** — Reporting violations provides more information in the audit results. For example, if an audit expects a password with at least 8 characters but finds a password with only 6 characters, the audit shows the actual and expected results. Since an audit may report thousands of violations. Policy Auditor establishes a violation limit that reduces the number of violations that can be displayed to conserve database resources.

- **Compliant** — A message displayed when the system complies with the audit.
- **Incomplete** — A message displayed when the results gathered are not complete because they exceed the violation limit.

Product installation overview

Policy Auditor is installed only in an ePolicy Orchestrator environment. An ePO management server and database must be in place. For details on system requirements and instructions for setting up the ePolicy Orchestrator environment, see the *ePolicy Orchestrator 4.0 Installation Guide* or the *ePolicy Orchestrator 4.5 Installation Guide*.

With the ePO server in place, install any needed prerequisites, then install Policy Auditor by running its Setup program.

The final step is to configure Policy Auditor, Benchmark Editor, and other extensions that enhance the capabilities of Policy Auditor.

System Requirements

Before you install McAfee Policy Auditor, verify that each component meets the minimum system requirements.

Server requirements

You must meet all hardware requirements as outlined in the ePolicy Orchestrator product guide for your software version.

ePolicy Orchestrator requirements

McAfee Policy Auditor requires ePolicy Orchestrator 4.0.5 (ePolicy Orchestrator 4.0, Patch 5) or ePolicy Orchestrator 4.5 to install and operate.

ePolicy Orchestrator 4.0 operating systems supported

- Windows 2000 Advanced Server with Service Pack 4 or later
- Windows 2000 Server with Service Pack 4 or later
- Windows Server 2003 Enterprise with Service Pack 1 or later
- Windows Server 2003 Standard with Service Pack 1 or later
- Windows Server 2003 Web with Service Pack 1 or later
- Windows Server 2003 R2 Enterprise
- Windows Server 2003 R2 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard

ePolicy Orchestrator 4.5 operating systems supported

- Windows Server 2003 Enterprise with Service Pack 2 or later
- Windows Server 2003 Standard with Service Pack 2 or later

- Windows Server 2003 Web with Service Pack 2 or later
- Windows Server 2003 R2 Enterprise with Service Pack 2 or later
- Windows Server 2003 R2 Standard with Service Pack 2 or later
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard

NOTE: The installation is blocked if you attempt to install on a version of Windows earlier than Server 2003. In addition, ePolicy Orchestrator stops functioning if, after having been installed on Windows Server 2003, the server is upgraded to Windows Server 2008.

Domain controllers

The server must have a trust relationship with the Primary Domain Controller (PDC) on the network. For instructions, see the Microsoft product documentation.

Ports

- McAfee recommends avoiding the use of Port 80 for HTTP communication via ePolicy Orchestrator because it is the primary port used by many web-based activities. It is a popular target for malicious exploitation and is often disabled by the system administrator in response to a security violation or outbreak.

  NOTE: Ensure that the ports you choose are not already in use on the ePolicy Orchestrator server.

  NOTE: Installing the software on a Primary Domain Controller (PDC) is supported, but not recommended.

- Notify network administrators of the ports you intend to use for HTTP and HTTPS communication with ePolicy Orchestrator.

Supported virtual infrastructure software

ePolicy Orchestrator 4.0	ePolicy Orchestrator 4.5
• VMware ESX 3.0.x	• VMware ESX 3.5.x • Microsoft Virtual Server 2005 R2 with Service Pack 1 • Windows Server 2008 Hyper-V

Supported platforms for the McAfee Policy Auditor agent plug-in

The McAfee Policy Auditor agent plug-in supports the following enterprise platforms:

Operating system	X86 support	X64 support	Other processors	Notes
Windows 2000 Server	X			
Windows 2000 Advanced Server	X			
Windows 2000 Professional	X			

Operating system	X86 support	X64 support	Other processors	Notes
Windows XP Professional	X	X		Native 32- and 64-bit agent
Windows Server 2003 Standard Edition	X	X		Native 32- and 64-bit agent
Windows Server 2003 Enterprise Edition	X	X		Native 32- and 64-bit agent
Windows Vista	X	X		Native 32- and 64-bit agent
Windows 2008 Server	X	X		Native 32- and 64-bit agent
Mac OS X 10.4	X	X	PowerPC	Universal binary
Mac OS X 10.5	X	X	PowerPC	Universal binary
HP-UX 11i v1			RISC	
HP-UX 11i v2			RISC	
AIX 5.3 TL8 SP5			Power5, Power6	
AIX 6.1 TL2 SP0			Power5, Power6	
Solaris 8			SPARC	
Solaris 9			SPARC	
Solaris 10			SPARC	
Red Hat Linux AS, ES, WS 4.0	X	X		32-bit agent on 64-bit hardware
Red Hat Enterprise Linux 5.0, 5.1	X	X		32-bit agent on 64-bit hardware

Agentless audit support

Agentless audits allow you to audit systems that do not have the McAfee Policy Auditor agent plug-in installed. In order to perform agentless audits, you must have a McAfee Foundstone 6.7 server or a McAfee Vulnerability Manager 6.8 server that is accessible over your network.

Agentless audit considerations

When determining how to implement agentless auditing, you need to consider your current ePO server installation, whether you already have Foundstone 6.7 installed, and your plans for upgrading your ePO server.

Agentless auditing system	Notes
McAfee Foundstone 6.7	• Works with the ePolicy Orchestrator 4.0 Patch 5 environment. • Does not work with the ePolicy Orchestrator 4.5 environment. • Prompts you to install a specific version of Java when configuring its integration with Policy Auditor.

Agentless auditing system	Notes
McAfee Vulnerability Manager 6.8	• Works with the ePolicy Orchestrator 4.0 Patch 5 environment and the ePolicy Orchestrator 4.5 environment. • Does not require you to install Java. • Does not support all of the features of McAfee Agent 5.2.

McAfee Foundstone 6.7 integration requirements

Policy Auditor can register a McAfee Foundstone 6.7 server to conduct agentless audits. To take advantage of this ability, you must install Rogue System Detection as well as an extension that integrates Policy Auditor and McAfee Foundstone 6.7.

- **Operating environment** — You must have ePolicy Orchestrator 4.0 Patch 5.
- **Rogue System Detection 2.0** — You must install Rogue System Detection version 2.0 for rogue systems to appear in the ePO server.
- **Rogue System Detection Patch 2** — You must upgrade Rogue System Detection 2.0 to version 2.0.2 to integrate Policy Auditor with Vulnerability Manager.
- **Foundstone ePO Extension** — You must install this extension so that Policy Auditor and McAfee Foundstone 6.7 can communicate seamlessly.

McAfee Vulnerability Manager 6.8 integration requirements

Policy Auditor can register a McAfee Vulnerability Manager 6.8 server to conduct agentless audits. To take advantage of this ability, you must install Rogue System Detection as well as an extension that integrates Policy Auditor and Vulnerability Manager 6.8.

- **Operating environment** — You must have one of the following:
  - ePolicy Orchestrator 4.0 Patch 5 — Vulnerability Manager 6.8 works with the ePO 4.0 server to conduct agentless audits.
  - ePolicy Orchestrator 4.5 — Vulnerability Manager 6.8 works with the ePO 4.5 server to conduct agentless audits.
- **Rogue System Detection 2.0** — You must install Rogue System Detection version 2.0 for rogue systems to appear in the ePO server.
- **Rogue System Detection Patch 2** — You must upgrade Rogue System Detection 2.0 to version 2.0.2 to integrate Policy Auditor with Vulnerability Manager.
- **Foundstone ePO Data Integration Extension** — You must install this extension so that Policy Auditor and Vulnerability Manager can communicate seamlessly.

  NOTE: The Foundstone ePO Data Integration Extension extension is not supported on Windows 2008.

Policy Auditor database considerations

Using Policy Auditor with a database

You need to install a database before you install Policy Auditor. If no database is present, the Policy Auditor Setup offers to install SQL Server 2005 Express.

- Any of the following databases, if previously installed, meet this requirement.
  - MSDE 2000 (ePolicy Orchestrator 4.0 only).
  - SQL 2000 (ePolicy Orchestrator 4.0 only).
  - SQL Server 2005 Express with Patch 2.
  - SQL Server 2005.
  - SQL Server 2008 (ePolicy Orchestrator 4.5 only).

NOTE: If you are currently using SQL 2000 or MSDE 2000 for your ePolicy Orchestrator 4.0 database, you must upgrade to SQL Server 2005, SQL Server 2005 Express with Patch 2, or higher before upgrading to ePolicy Orchestrator 4.5. McAfee does not recommend using SQL Server 2005 Express if the ePO server is managing more than 5,000 systems.

If no other databases are installed, the Policy Auditor Setup detects that no database is present and prompts you to install SQL Server 2005 Express.

These tables provide additional information about the database choices and other software requirements.

Table 1: Database considerations

Database	Requirements	Notes
SQL Server 2005 and SQL Server 2008	Dedicated server and network connection	Needed if managing more than 5,000 computers.
	Local database server	If the database and ePO server are on the same system, McAfee recommends setting up your server to use a using a fixed virtual memory size that is approximately two-thirds of the total memory allotted for SQL Server. For example, if the computer has 1 GB of RAM, set 660 MB as the fixed memory size for SQL Server.
	Licenses	A license is required for each processor on the computer where SQL Server is installed. If the minimum number of SQL Server licenses is not available, you might have difficulty installing or starting the ePolicy Orchestrator software.
MSDE 2000 (ePolicy Orchestrator 4.0 only)	Service Pack 3	Ensure that the database is not installed on a backup domain controller (BDC).
SQL Server 2000 (ePolicy Orchestrator 4.0 only)	Service Pack 3	Ensure that the database is not installed on a backup domain controller (BDC).

Database	Requirements	Notes
SQL Server 2005 Express	• .NET Framework 2.0 • .NET Framework 2.0 Service Pack 2	You must acquire and install .NET Framework 2.0 SP2.

Table 2: Additional software considerations

Software	Notes
MSXML 6.0	You must acquire and install. **1** From the Internet Explorer **Tools** menu, select **Windows Update**. **2** Click **Custom**, then select **Software, Optional**. **3** Select **MSXML6**. If it is not in the list, it is already installed on your server. **4** Select **Review and install updates**, then click **Install Updates**.
Internet Explorer 6 SP1 or later	You must acquire and install.
.NET Framework 2.0 SP2	You must acquire and install if using SQL Server 2005 Express.
MDAC 2.8	If not previously installed, the installation wizard installs automatically.
SQL Server 2005 Backward Compatibility	If not previously installed, the installation wizard installs automatically.
SQL Server 2005 Express	If no other database has been previously installed, this database can be installed automatically at user's selection.
Microsoft updates	Update the ePolicy Orchestrator server and the database server with the most current updates and patches.
MSI 3.1	The installation fails if using a version of MSI earlier than MSI 3.1.

Database installation documented in this guide

The only database installation scenario described in detail is a first-time installation of SQL Server 2005 Express. In this scenario, the Policy Auditor Setup installs both Policy Auditor and the database on the same server. If the database is to be installed on a different server than the ePolicy Orchestrator software, manual installation is required on the remote servers.

Other relevant database installations and upgrades

McAfee recommends making specific maintenance settings to ePolicy Orchestrator databases. For instructions, see *Maintaining ePolicy Orchestrator databases* in the ePolicy Orchestrator product guide for the version that you are using.

See the documentation provided by the database manufacturer for information about the following installation scenarios:

- Installing SQL Server 2005
- Installing SQL Server 2008
- Upgrading from MSDE to SQL Server 2005
- Upgrading from MSDE 2000 to SQL Server 2005
- Upgrading from MSDE 2000 to SQL Server 2005 Express

SQL Server

- **Dedicated server and network connection** — Use a dedicated server and network connection if managing more than 5,000 client computers.
- **SQL Server licenses** — If using SQL Server, a SQL Server license is required for each processor on the computer where SQL Server is installed.

  CAUTION: If the minimum number of SQL Server licenses is not available after you install the SQL Server software, you might have a problem installing or starting the ePolicy Orchestrator software.

Browsers supported

ePolicy Orchestrator 4.0	ePolicy Orchestrator 4.5
• Microsoft Internet Explorer 6.0 with Service Pack 1 or later. • Microsoft Internet Explorer 7.0.	• Microsoft Internet Explorer 6.0 with Service Pack 1 or later. • Microsoft Internet Explorer 7.0. • Microsoft Internet Explorer 8.0. • Firefox 3.0.

Proxy servers

If using a proxy, bypass the proxy server:

1. In Internet Explorer, click **Tools | Internet Options**.
2. Select the **Connections** tab and click **LAN Settings**.
3. Select **Use a proxy server for your LAN**, then select **Bypass proxy server for local addresses**.
4. Click **OK**, then click **OK** again.

McAfee Agent versions supported

- McAfee Agent 4.0 and ePolicy Orchestrator 4.0 work together to support all legacy features.
- McAfee Agent 4.0 (release plus all patches) works with ePolicy Orchestrator 4.5. However, several of the new features of ePolicy Orchestrator 4.5 (SSL/TLS, Data Channel, Update Now, IPv6 support, Agent Handler, Custom Props) and McAfee Agent 4.5 (SSL/TLS, Data Channel, LPC/IPC, Custom Props) do not work.
- McAfee Agent 4.5 and ePolicy Orchestrator 4.5 work together to support all legacy and new features.
- McAfee Agent 4.5 and ePolicy Orchestrator 4.0 work together to support all legacy features. However, several of the new features of ePolicy Orchestrator 4.5 (SSL/TLS, Data Channel, Update Now, IPv6 support, Agent Handler, Custom Props) and McAfee Agent 4.5 (SSL/TLS, Data Channel, LPC/IPC, Custom Props) do not work.

Windows agent plug-in requirements

Hardware and network requirements

- **Processor** — Intel Pentium-class, Celeron, or compatible processor; 166 MHz processor or higher.
- **Free disk space (agent)** — 300 MB.
- **Free disk space (products)** — Sufficient disk space on client computers for each McAfee product that you plan to deploy. For more information, see the corresponding product documentation.
- **Free Memory** — 20 MB RAM.
- **Network environment** — Microsoft or Novell NetWare networks. NetWare networks require TCP\IP.
- **NIC** — Network interface card; 10 MB or higher.

Windows Operating systems supported

- Windows 2000 Professional
- Windows 2000 Advanced Server with Service Pack 1, 2, 3, or 4
- Windows 2000 Datacenter Server with Service Pack 1, 2, 3, or 4
- Windows 2000 Professional with Service Pack 1, 2, 3, or 4
- Windows 2000 Server with Service Pack 1, 2, 3, or 4
- Windows Server 2003 Enterprise
- Windows Server 2003 Standard
- Windows Server 2003 Web
- Windows XP Home with Service Pack 1
- Windows XP Professional with Service Pack 1
- Windows Vista
- Windows Server 2008

Non-Windows agent plug-in requirements

These are the non-Windows systems supported by the McAfee Policy Auditor agent plug-in.

- Red Hat Linux AS, ES, WS 4.0
- Red Hat Enterprise Linux 5.0, 5.1
- Solaris 8, 9, 10
- Macintosh OS X 10.4, 10.5
- HP-UX 11i v1
- HP-UX 11i v2
- AIX 5.3 TL8 SP5
- AIX 6.1 TL2 SP0

Distributed repositories

- **Free disk space** — 100 MB on the drive where the repository is stored.
- **Memory** — 256 MB minimum.

Common Criteria considerations

This page is intended for use by government agencies that are required to use only National Information Assurance Partnership (NIAP) Common Criteria validated security products. It describes functional modifications that meet specific Common Criteria requirements, and provides advice on best practices for satisfying those requirements.

Server access

Physical access to the server must be restricted to authorized personnel that have been adequately trained to manage the system.

The server must be located in a physically secure facility with access limited to authorized personnel.

Functionality on multiple platforms

The combination of ePolicy Orchestrator and Policy Auditor 5.2 functions identically on all platforms where ePolicy Orchestrator operates.

Encryption

All packages created and distributed by McAfee are signed with a key pair using the DSA (Digital Signature Algorithm) signature verification system, and are encrypted using 168-bit 3DES encryption. A key is used to encrypt or decrypt sensitive data.

The ePolicy Orchestrator repository list (SiteList.xml) file contains the names of all the repositories you are managing. The repository list includes the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository list to the agent during agent-server communication.

The Security Keys page in ePolicy Orchestrator allows you to manage encryption for repositories and for agent-server communications.

Applications running under the ePolicy Orchestrator environment use a Secure Socket Layer (SSL) sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks.

HTTPS and SSL support the use of X.509 digital certificates from the server so that a user can authenticate the sender.

Passwords

When a new ePolicy Orchestrator user is created, the Add New User interface allows for use of NT authentication, which has previously been set at the network level, or a new ePolicy Orchestrator authentication credential can be created.

Administrators who must adhere to the requirements of the National Information Assurance Partnership (NIAP) Common Criteria Validation Scheme (CCEVS) are directed to assign passwords

employing ePolicy Orchestrator authentication only. McAfee is recommends that the network IT administrator assign passwords that meet the following requirements:

- Must be at least 10 characters in length.
- Must contain at least three of the following four character groups:
  - English uppercase characters (A-Z).
  - English lowercase characters (a-z).
  - Numerals (0-9).
  - Non-alphanumeric characters, such as !, $, #, %.

User IDs and passwords should be unique. No two users should have the same password. In addition, the User ID used to access ePolicy Orchestrator should be different from any other User ID required for related ePolicy Orchestrator functionality such as SQL administration or creation of distributed repositories.

Administrators must ensure that all user names and passwords are protected by the users in a manner which is consistent with IT security.

Intrusion prevention system

McAfee Host Intrusion Prevention is a preemptive approach to host and network security used to identify and quickly respond to potential threats. Host Intrusion Prevention monitors individual host and network traffic. However, because an attacker might carry out an attack immediately after gaining access, Host Intrusion Prevention can also take immediate action as preset by the network administrator.

Timestamp

ePolicy Orchestrator uses either a *datetime* or *smalldatetime* data type, as appropriate, to record the events and triggers to automatically update the timestamp when any modification takes place. Many tables have a *datetime* or *smalldatetime* data type to indicate when a row was created, and are linked to other tables to preserve the date and time of all modifications.

Email alarm notifications of storage space exhaustion

The ePolicy Orchestrator notification feature transmits alerts to designated email recipients. The administrator must set up four Notifications that require configuration in order to meet the "alarm" requirements of FAU_STG.4.1 and IDS_STG.2.1

- Notification that storage space for new records in the ePOAuditEvent table in the SQL Server database is exhausted.
- Purging of the oldest 20% of the records in the ePOAuditEvent table completed successfully.
- Purging of the oldest 20% of the records in the ePOAuditEvent table failed.
- Notification that storage space for new records in the ENT_IPSEvent table in the SQL Server database is exhausted. When this notification is received, the administrator should purge the database.

The appropriate *ePolicy Orchestrator Product Guide* provides information about purging and archiving the database.

Installation of McAfee Policy Auditor

This chapter provides instructions for installing the Policy Auditor extension on a system where ePolicy Orchestrator software has been installed. Policy Auditor 5.2.0 can be installed as a new installation or as an upgrade from earlier Policy Auditor versions.

Be sure that you have read, understood, and complied with the requirements and recommendations in the *System Requirements* section. This summarizes the process of installing Policy Auditor.

1. If you are not integrating Policy Auditor with McAfee Foundstone 6.7 or McAfee Vulnerability Manager 6.8, you must have one of these environments installed:
   - ePolicy Orchestrator 4.0 Patch 5.
   - ePolicy Orchestrator 4.5
2. If you plan to integrate Policy Auditor with a McAfee Foundstone 6.7 installation, you must have the following environment:
   - ePolicy Orchestrator 4.0 Patch 5 must be installed on your ePO server.
   - Rogue System Detection 2.0, Patch 2 (RSD 2.0.2) must be installed on your ePO 4.0 server.
3. If you plan to integrate Policy Auditor with a McAfee Vulnerability Manager 6.8 installation, you must have the following environment:
   - ePolicy Orchestrator 4.0 Patch 5 or ePolicy Orchestrator 4.5 must be installed on your ePO server.
   - Rogue System Detection 2.0, Patch 2 (RSD 2.0.2) must be installed on your ePO server.
4. Install Policy Auditor. If the ePO server is a member of an MSCS cluster, follow the instructions in *Installing Policy Auditor on an MSCS Cluster*.

Contents

Installing Policy Auditor on an MSCS cluster

Use this task to install Policy Auditor on an ePO server that is a member of an MSCS cluster.

Task

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

1 Stop these ePolicy Orchestrator services, then change their startup type to **Manual**.
   - McAfee ePolicy Orchestrator Application Server.
   - McAfee ePolicy Orchestrator Event Parser.
   - McAfee ePolicy Orchestrator Server.

2 Install Policy Auditor on each cluster member according to the *Installing Policy Auditor on ePolicy Orchestrator* section. No configuration changes are required.

3 Test the cluster:
   a Select the ePO server group, then click **Bring Online**.
   b Right-click any of the resources for the ePO server group, then click **Initiate Failover**. The resources should fail and come back online.

Installing Policy Auditor on ePolicy Orchestrator

Use this task to install Policy Auditor.

Before You Begin

- If you are using ePolicy Orchestrator 4.0, Patch 5 must be installed on your ePO server.
- If you plan to integrate Policy Auditor with a McAfee Foundstone 6.7 installation, you must have the following environment:
  - ePolicy Orchestrator 4.0 Patch 5 must be installed on your ePO server.
  - Rogue System Detection 2.0, Patch 2 (RSD 2.0.2) must be installed on your ePO 4.0 server.
- If you plan to integrate Policy Auditor with a McAfee Vulnerability Manager 6.8 installation, you must have the following environment:
  - ePolicy Orchestrator 4.0 Patch 5 or ePolicy Orchestrator 4.5 must be installed on your ePO server.
  - Rogue System Detection 2.0, Patch 2 (RSD 2.0.2) must be installed on your ePO server.

Task

1 Download the product zip file from the McAfee download site, and store it on your ePO server.

2 Unzip the archive, then double-click the **Setup** program. The InstallShield Wizard appears and begins the installation process.

3 If you already have Policy Auditor 5.0 or later installed, a dialog box appears that asks you whether you want to perform an upgrade of Policy Auditor Server. Click **Yes**.

4 In the Setup Requirements window, check that each section displays the message **All required applications were found**. If the required applications were not found, they are listed, and you must exit and install these applications.

5 The installation screen appears. Click **Next**.

6 Accept the default location to install the software, or select a different location on the ePolicy Orchestrator server.

7 Accept the license agreement.

8 Type your ePolicy Orchestrator user name and password in the appropriate fields.

9 Verify that all information is correct, then start the installation.

10 When the installation is complete, click **Finish**.

NOTE: After installing Policy Auditor, the content check-in requires 20 to 25 minutes. Allow approximately 30 minutes to pass after installation before using benchmarks or checks. Click **Reporting | Server Task Log** to verify that the new content has been checked in.

Installing the McAfee Foundstone 6.7 extension

Use this task to install the Foundstone ePO Extension in an ePolicy Orchestrator 4.0 environment. The extension is not supported in an ePolicy Orchestrator 4.5 environment.

NOTE: Install this software only if you plan to integrate Policy Auditor with McAfee Foundstone 6.7.

Before you begin

Rogue System Detection 2.0 Patch 2 must be installed on your ePO server.

Task

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

1 Download the Foundstone ePO Extension zip file from the McAfee download site, and store it on your ePO server.

2 Unzip the file to a convenient location. Read the release notes and the documentation, then double-click the Setup file to begin the installation.

3 Follow the instructions in the Setup and the documentation for Foundstone ePO Extension to complete the installation.

Installing the McAfee Vulnerability Manager 6.8 extension

Use this task to install the Foundstone ePO Data Integration Extension in an ePolicy Orchestrator 4.0 or ePolicy Orchestrator 4.5 environment.

NOTE: Install this software only if you plan to integrate Policy Auditor with Vulnerability Manager 6.8.

Before you begin

Rogue System Detection 2.0 Patch 2 must be installed on your ePO server.

Task

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

1 Download the Foundstone ePO Data Integration Extension zip file from the McAfee download site, and store it on your ePO server.

2 Unzip the file to a convenient location. Read the release notes and the documentation, then double-click the Setup file to begin the installation.

3 Follow the instructions in the Setup and the documentation for Foundstone ePO Data Integration Extension to complete the installation.

Policy Auditor configuration

This is a high-level overview of the configuration process you need to follow after installing Policy Auditor. All of the information can be found in the online help.

1 Go to the *Configuring Benchmark Editor* section under McAfee McAfee Benchmark Editor 5.2.0 and follow the instructions.

2 Go to the *Configuring Policy Auditor* section under McAfee Policy Auditor 5.2.0 and follow the instructions.

3 If you are Integrating Policy Auditor with McAfee Foundstone 6.7 or Vulnerability Manager, see the appropriate McAfee Policy Auditor 5.2.0 Product Guide and follow the instructions.

4 If you are integrating Policy Auditor with your third-party ticketing system, go to the *Managing Issues and Tickets* section under McAfee Policy Auditor 5.2.0 and follow the instructions to configure your installation to work with your ticketing system.

Index

W