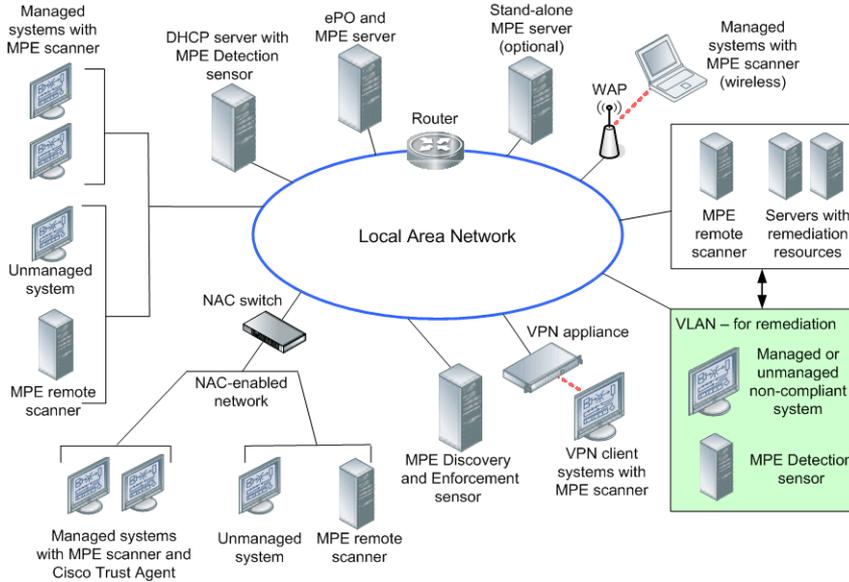




McAfee Policy Enforcer is a system security solution that defines, assesses, and enforces IT security policies to control how managed and unmanaged systems access LAN, VPN and NAC networks. It protects corporate networks by blocking access to systems that do not comply with IT security policies. McAfee Policy Enforcer provides robust policy creation, fast and accurate compliance assessment, and remediation capabilities to enforce compliance to your system security policy.

Components of McAfee Policy Enforcer

The main components of McAfee Policy Enforcer (MPE) are the **server**, **sensor** and **scanner**. Components can be deployed only to *managed systems*, which are systems with the ePolicy Orchestrator (ePO) agent installed. *Unmanaged systems* do not have the ePO agent installed.



MPE server

- Installed on all ePO servers (*integrated*).
- Optionally installed on separate servers (*stand-alone*) to off-load processing.
- Manages communications with the distributed components.
- Installs into the ePO console.
- Uses task management features of ePolicy Orchestrator.
- Stand-alone servers manage their own sensors and scanners.

MPE sensor

- Performs topology discovery and mapping, broadcast detection, and DHCP detection
- Performs switch enforcement for unmanaged systems.
- Deployed to managed systems only.

MPE scanner

- Deployed to managed systems only.
- Always scans the local computer.

Local scanner:

- Performs compliance assessment of the local system.
- Performs self-enforcement.

Remote scanner:

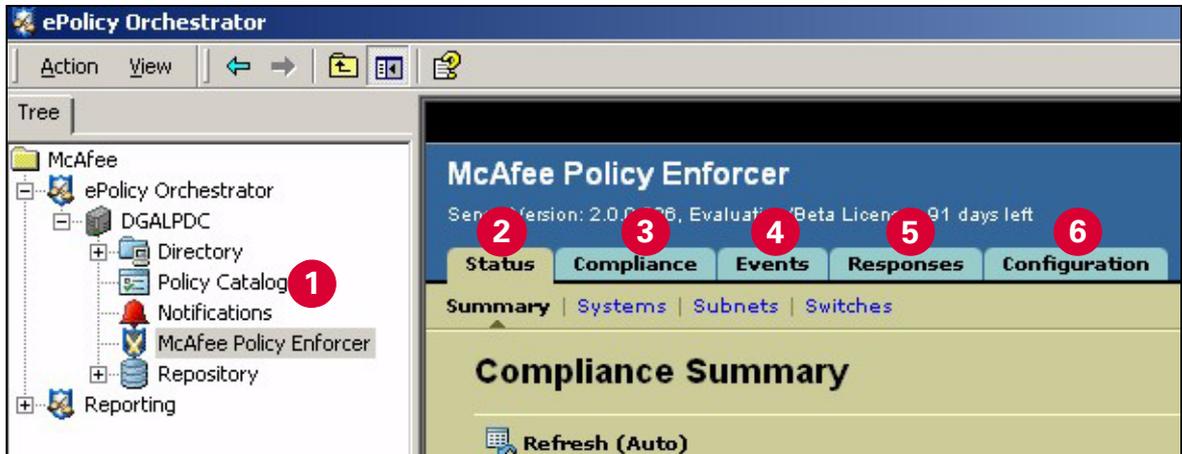
- Performs compliance assessment of itself and remote systems.
- Performs remote scans on unmanaged hosts, and hosts without an active scanner.
- Performs self-enforcement.

Remediation portal

- Brings noncompliant systems into compliance with your McAfee Policy Enforcer policy.
- Hosts ActiveX scanner for unmanaged systems.

Tasks and the McAfee Policy Enforcer interface

McAfee Policy Enforcer installs into the ePolicy Orchestrator console tree. What you select in the console tree controls what appears in the details pane.



1 Policy Catalog

Configure MPE sensor policies

- Set which MPE server manages the sensor and the communication intervals for primary and secondary sensors.
- Set the type of detection (broadcast, DHCP).
- Establish network adapter bindings (which parts of the network the sensor listens to).
- Enable topology discovery and mapping, and switch enforcement.
- Specify settings for switches and routers involved in discovery and enforcement, such as community strings.

Configure MPE scanner policies

- Set which MPE server manages the scanner.
- Enable remote scanning and provide credentials.
- Enable continuous compliance scanning and the time interval.
- Create the remediation list for scanners configured with this policy.

2 Status page

- Monitor compliance status and data for systems, subnets, and switches.
- Manually deploy sensors to specific subnets.
- Manually set an action to be performed on a system.
- Get details for individual systems, subnets, and switches.
- Manually set VLANs for switch ports.

3 Compliance page

- Define a compliance policy for LAN, VPN, and NAC connections.
 - Create one or more rule sets.
 - Create one or more rules for each rule set.
 - Define specific computer conditions for rule sets.
- Define trusted system rules.
- Define quarantine settings, such as VLAN number (*LAN policy only*).
- Specify which VPN installation packages to build (*VPN policy only*).
- Define multiple enforcement zones.

4 Events page

- Monitor all events that occur in your MPE-controlled network.
- Monitor the status of actions that have been triggered in response to events.

5 Responses page

- Monitor responses as they occur.
- Set automatic responses for specific events that occur in your MPE-controlled network.

6 Configuration page

- Set MPE server configuration properties.
- Import and export exception systems lists, automatic responses, and compliance policies.
- Add and test e-mail contacts.
- Add, test, and register external commands and programs.

Getting information



Where to go for threat information, product documentation, and technical support.

Threat Center

McAfee Avert® Labs helps you maintain the highest possible level of security. 100 researchers in 14 countries continuously monitor the latest threats and provide remediation, so that you can stay ahead of the latest threats and respond quickly to emergencies.

http://www.mcafee.com/us/threat_center/default.asp

Documentation

Documentation for McAfee Policy Enforcer and ePolicy Orchestrator is available in PDF format at:

<http://www.mcafee.com/us/enterprise/downloads/index.html>

McAfee Policy Enforcer

Release Notes, Product Guide, and Installation Guide.

ePolicy Orchestrator

Release Notes, Product Guide, Quick Reference Card, Installation Guide, Hardware Sizing and Bandwidth Usage Guide, Reporting Guide, and Walkthrough Guide.

Enterprise Support

Customer Care for the business user. Access websites for customer service and technical support.

<http://www.mcafee.com/us/enterprise/support/index.html>

McAfee Policy Enforcer Features

The features of McAfee Policy Enforcer can be categorized into these basic functions.

Define network security compliance

- Create rules that define the requirements for network access.
- Create separate compliance policies for LAN, VPN, and NAC connections.
- Provides hundreds of compliance checks.

Detect all network systems

System detection

- Sensors perform both broadcast and DHCP detection of systems with either static or dynamic IP addresses.

Topology discovery and mapping

- Sensors perform automatic discovery and mapping of all routers, switches, and systems in your network.

Assess compliance

- Local scanners assess compliance of managed systems.
- Remote scanners assess compliance of unmanaged systems and systems without a local scanner.
- For managed and unmanaged systems, assessment can be performed at the time of the network access request, and at regular intervals using continuous compliance scanning.
- Local policy assessment with an MPE scanner on managed systems.
- Remote policy assessment of unmanaged systems, and systems without a local scanner.
- ActiveX downloadable scanner assesses unmanaged systems without needing a remote scanner.

Enforce compliance policy

- Enforce separate compliance policies for LAN, VPN, and NAC connections.
- Self enforcement (using a built-in firewall) of managed systems.
- Switch enforcement for unmanaged systems.
- Integration with Cisco NAC enforcement framework 2.0.
- Enforce to different zones according to severity of noncompliance.

Remediate noncompliant systems

- Specify the network resources available to noncompliant systems that require remediation.
- Allow noncompliant systems to bring themselves into compliance with your McAfee Policy Enforcer policy.
- Execute automatic remediation actions.

Additional features

Audit compliance policy while fine-tuning rules and rule sets

Alerts and notifications

- An event history table provides information about events that occur in your MPE-managed network environment.
- E-mail alerts (or ePO notifications) can be sent to key personnel based on event types.

Automatic and manual responses to events

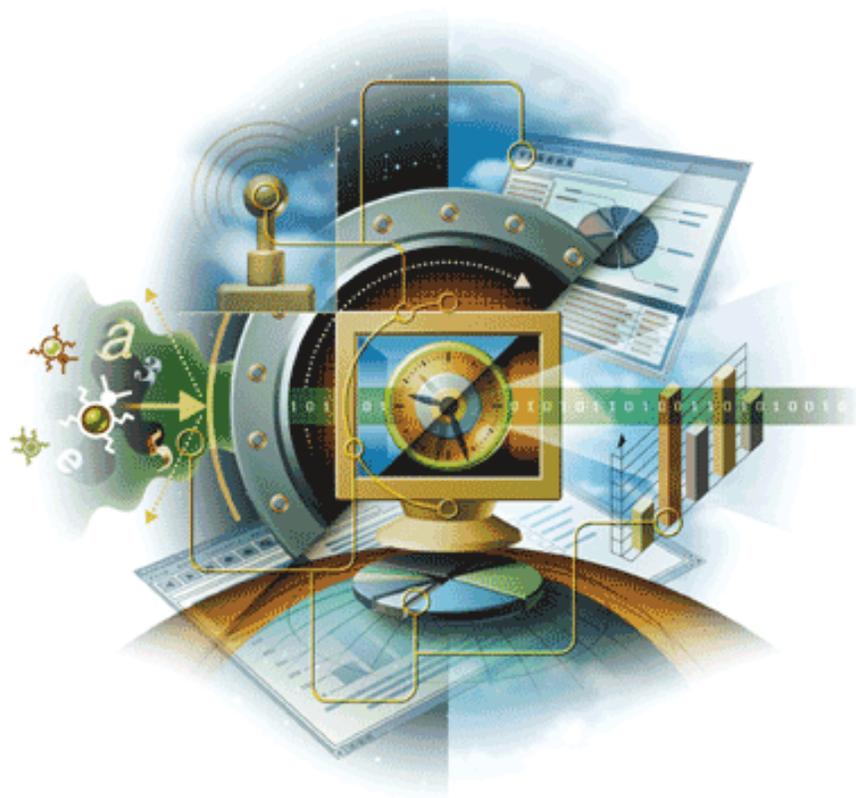
- Responses (actions) can be configured for specific events, such as quarantining or scanning a system, or running an external command.

Compliance and enforcement monitoring

- Summary tables provide status regarding system compliance, and employ numerous display filters.
- Get complete details about any system or switch on the network.
- Monitor switch enforcement events.
- Take manual action on specified systems.

McAfee® Policy Enforcer

version 2.0



McAfee® System Protection

Industry-leading intrusion prevention solutions

McAfee®

McAfee® Policy Enforcer

version 2.0

McAfee®
System Protection

Industry-leading intrusion prevention solutions

McAfee®

COPYRIGHT

Copyright © 2006 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

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLED E), DESIGN (STYLED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color 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 ACCOMPANIES 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 MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright ©2000 CrystalClear Software, Inc.
- FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003.
- Software copyrighted by Gisle Aas. © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, ©1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martinj Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, ©2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, ©2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.
- Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992.
- Software copyrighted by Cambridge Broadband Ltd., © 2001-2003.
- Software copyrighted by Sparta, Inc., © 2003-2004.
- Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004.
- Software copyrighted by Simon Josefsson, © 2003.
- Software copyrighted by Thomas Jacob, © 2003-2004.
- Software copyrighted by Advanced Software Engineering Limited, © 2004.
- Software copyrighted by Todd C. Miller, © 1998.
- Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.
- Software developed by the JDOM Project (<http://www.jdom.org/>).
- TinyXml is released under the zlib license: This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution.

Contents

1	Installation	7
	Installing the software	7
	What is installed	7
	Before you begin	8
	Install the software	8
	Start the console	10
	Start remote consoles	10
	What to do after installation	10
	Beta and evaluation software	12
	What happens when the license expires	12
	Installing a standalone MPE server	13
	When to install a standalone MPE server	13
	What is installed	13
	Before you begin	13
	Install a standalone MPE server	14
	What to do after installation	15
	Installing and customizing the remediation portal	16
	What is installed	16
	Before you begin	17
	Install the remediation portal	17
	Customizing the remediation portal	18
	Customize an existing portal	21
	Opening the remediation portal	22
	What to do after installation	22
	Rescan code for <head> section	24
	Rescan code for <body> section	25
	Migrating Policy Enforcer software	26
	Migrate from Policy Enforcer 1.0 to version 2.0	26
	Migrate to a licensed version	27
2	Uninstallation	28
	Uninstalling the software	28
	What is uninstalled	28
	Before you begin	29
	Uninstall the software	29
	Uninstalling a standalone MPE server	29
	What is uninstalled	29
	Uninstall a standalone MPE server	30
	Uninstalling the remediation portal	30
	What is uninstalled	30
	Uninstall the remediation portal	30
3	Planning	31
	Requirements	31
	McAfee Policy Enforcer software requirements	31
	Standalone MPE server requirements	31
	MPE sensor requirements	32
	MPE scanner requirements	33
	VPN-connected computer requirements	34

VPN appliance requirements	35
Remediation portal requirements	35
Switch requirements	36
Router requirements	36
ePO server and console requirements	36
ePO remote console requirements	37
Things to know before installation	38
Cluster on ePO server	38
Cluster on standalone MPE server	38
Firewall software	39
MDAC 2.8	40
Planning your deployment	41
Assemble a team	41
Evaluate compliance scenarios	42
Where to deploy sensors and scanners	53

1

Installation

Installing Policy Enforcer software and components

This section includes information about different types of McAfee Policy Enforcer (MPE) installation and migration including:

- [Installing the software](#)
- [Installing a standalone MPE server](#)
- [Installing and customizing the remediation portal](#)
- [Migrating Policy Enforcer software](#)

See the *McAfee Policy Enforcer Product Guide* for descriptions of McAfee Policy Enforcer components, features, and functionality.

Installing the software

This section describes the MPE installation process, and it provides additional information on installation procedures and considerations.

What is installed

The McAfee Policy Enforcer software installs an integrated MPE server on an existing ePolicy Orchestrator 3.6.1 server computer. You can also install the remediation portal.

During the installation, Policy Enforcer sensor and MPE scanner installation files and policy pages are added to the ePO master repository. The McAfee Policy Enforcer reports are also added to the ePO server.

The **Policy Enforcer Scanner Update Task** is created in the **Directory** during the installation. This client task updates all check packages on managed systems daily at 12 A.M., by default.

The Rogue System Detection interface is replaced with the Policy Enforcer interface, but the rogue system sensor 1.0.0 policy page and Rogue System Detection reports remain. This allows you to continue to manage and report on existing rogue system sensors while you deploy the McAfee Policy Enforcer software.

McAfee System Compliance Profiler software is unaffected when you install Policy Enforcer.

Policy Enforcer includes a deployment package for ePolicy Orchestrator that enables the installation of a Cisco Trust Agent (CTA).

Before you begin

- Verify that the computer meets the minimum hardware and software requirements, see [page 31](#).
- If the ePO server computer is a member of a Microsoft Cluster Server (MSCS) cluster, see [page 38](#).
- If you use personal firewall software, see [page 39](#).
- Although you can install the software on systems with Terminal Services, you cannot use Terminal Services to install this software. You must use **Add/Remove Programs**. For instructions, see the Microsoft product documentation.
- You can install the Policy Enforcer on systems running these virtual machine programs:
 - Microsoft Virtual Server 2005 Enterprise.
 - Microsoft Virtual Server 2005 Standard.
 - VMware Workstation 4.5 or later.

Install the software

For beta and evaluation versions of the software, the installation process differs slightly from these steps. For more information, see [In the McAfee Policy Enforcer 2.0.0 Setup wizard, click Next to begin the migration. A message appears indicating that the migration was completed successfully. on page 27.](#)

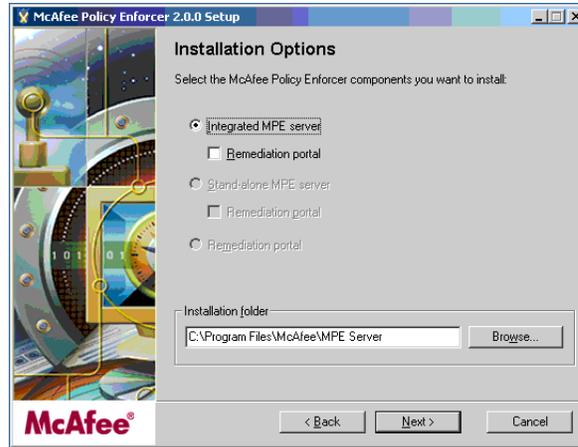
- 1 Insert the CD into the CD-ROM drive of the computer.
- 2 In the autorun window, select the desired language, then select **Install McAfee Policy Enforcer 2.0**.
- 3 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Next** to begin the installation.
- 4 In the **McAfee End User License Agreement** dialog box, select the appropriate license type and the country in which you purchased the software. The license type must match the license you purchased. If you are unsure which license you purchased, contact the person who sold you the software.

Read the entire license agreement carefully, select **I accept the terms in the license agreement** to agree to the license terms, then click **OK**.



If the license agreement does not display correctly, read the appropriate license in the LicenseAgreement.pdf file supplied with the ePolicy Orchestrator software.

- 5 In the **Installation Options** dialog box:
 - a Select **Integrated Policy Enforcer server**.
 - b To install the remediation portal on this computer now, select **Remediation portal**.
 - c Accept the default installation path of the MPE server or click **Browse**.
 - d Click **Next**.

Figure 1-1 Installation Options dialog box

6 In the **Database Server Account** dialog box, click **Next**. Setup verifies that it can connect to the ePO database using the specified authentication method and user account.

7 The **HTTP Configuration** dialog box displays the port numbers used for communication to the server.

- **Scanner-to-server and sensor-to-server communication port** — Displays the port number (default is 8444) that the ePO server uses for inbound communication with the MPE scanner and sensor.
- **Remediation portal communication port** — Displays the port number (default is 81) that noncompliant systems use for outbound communication with the ePO server or standalone MPE server that is handling rescan requests.

Available only when you select **Remediation portal** in the **Installation Options** dialog box.

Click **Next**.

8 In the **Ready To Install** dialog box, click **Install** to begin the installation. This dialog box includes the estimated time to complete the installation.

The **Executing Setup** dialog box provides the status of the installation.

9 In the **Installation Complete** dialog box, specify the desired options listed below, then click **Finish** to complete the installation.

- To open the console after completing the installation, select **Start McAfee ePolicy Orchestrator console**.
- To view known issues or last-minute changes to the product or its documentation, click **View Readme**.

Start the console

You must be an ePO global or site administrator to view and use the Policy Enforcer.

- 1 Click the **Start** button, then select **Programs | McAfee | McAfee ePolicy Orchestrator 3.6.1 Console**.
- 2 Click **Log on to server**.
- 3 Type the **User name** and **Password** of a global or site administrator user account.
- 4 Click **OK** to start the console.

Start remote consoles

You must be a global or site administrator to view and use the Policy Enforcer.

- 1 Click the **Start** button, then select **Programs | McAfee | McAfee ePolicy Orchestrator 3.6.1 Console**.
- 2 Click **Log on to server**.
- 3 Type the NetBIOS name of the ePO server computer.
- 4 Type the **User name** and **Password** of a global or site administrator user account.
- 5 Type the console-to-application server communication port (default is 8443) used by the ePO server.
- 6 Click **OK** to start the remote console.

What to do after installation

After installation, there are several considerations and required tasks including:

- Ensure current content retrieval and distribution.
- Plan a phased deployment.
- Mark systems as exceptions.
- Log on to the database server using ePO authentication to access the Policy Enforcer reports for the first time.
- Assign product permissions.

Content retrieval and distribution

We recommend using these ePO server tasks to ensure that you always have the most current Policy Enforcer content (check and server update packages):

- Daily (DAT & Engine) repository pull task (also retrieves content).
- Daily incremental repository replication task.
- Weekly full repository replication task.

For more information, see *Server and client tasks you should schedule to run regularly* in the ePolicy Orchestrator 3.6.1 online Help.

The **Policy Enforcer Scanner Update Task** updates all check packages on managed systems daily at 12 A.M. You can modify the settings of this task, or delete it and use another ePO agent update task to distribute check packages to managed systems. For instructions, see *Changing the default MPE scanner update client task* in the Policy Enforcer online Help.

Deployment planning

We recommend using a phased approach to deploy the software, starting with systems of highest concern. Information about deployment has been divided into compliance scenarios. A deployment checklist is provided for each scenario that explains the required components, data, and tasks, see [Planning your deployment on page 41](#).

Exception systems

The compliance policy does not apply to exception systems such as printers, routers, switches, VoIP phone adapters, and VPN appliances. Remember, any system with an IP address is detected and reported by the sensor. After systems have been detected and scanned, you can mark them as exceptions manually or automatically, based on specific conditions such as IP address range, MAC address, organizational unique identifier (OUI) family, network access device (NAD) type (router or switch), operating system, or scan result. Exception systems are never scanned and always allowed full access to the network.

We recommend marking systems as exceptions while auditing and fine-tuning the compliance policy, and before enforcing compliance. For instructions, see *Marking systems as exceptions* in the Policy Enforcer online Help.

First-time report access

To access the Policy Enforcer reports for the first time, log on to the database server using ePO authentication. You can then use any authentication type to log on to the database server and run reports. The Policy Enforcer reports only appear under the database server; they do not appear under **Report Repository**. For instructions, see *Accessing reports for the first time* in the Policy Enforcer online Help.

Product permissions

You can assign permissions to different areas of the Policy Enforcer software to ePO site administrators. Global administrators are automatically assigned all McAfee Policy Enforcer permissions. Global and site reviewers cannot access the McAfee Policy Enforcer software. For instructions, see *Assigning product permissions to user accounts* in the Policy Enforcer online Help.

Rogue System Detection

If you are already using Rogue System Detection in ePolicy Orchestrator, you can continue to detect rogue systems without any configuration changes. Rogue systems are unauthorized systems or systems not being managed by this ePO server that are accessing the network locally. For more information, see [Compliance audit of managed systems on page 42](#).

Beta and evaluation software

For beta and evaluation versions of the software, the installation process differs slightly from the steps presented in this guide, as follows:

- A dialog box appears before the license agreement, identifying how long you are licensed to use the beta or evaluation software. Click **OK** to continue to the license agreement.
- The license agreement always displays in English — regardless of your system's language — and the license type options are disabled.

When you are using the software, a reminder appears several times as the end of the license period nears, showing the number of days remaining before the license expires. Depending on the type of software, you can:

- **Beta software** — Click **Beta Contact** to access the beta feedback page on the McAfee website, where you can supply your comments about the beta software.
- **Evaluation software** — Click **Buy** to access the McAfee website, where you can purchase a licensed version of the software.

What happens when the license expires

When the license expires, the Rogue System Detection interface reappears. Although the McAfee Policy Enforcer tree icon remains, the interface can no longer be accessed.

The MPE sensor stops performing all functions, except broadcast detection during the next agent-server communication. The **Policy Enforcer Sensor Installation** client task remains and continues to be sent to and enforced on target systems.

The MPE scanner continues to scan systems using the current compliance policy and to report compliance status to the ePO server. The settings for the MPE scanner in the **Deployment** client task are unchanged and continue to be sent to and enforced on target systems.

All McAfee Policy Enforcer installation files, policy pages, and reports remain.

Installing a standalone MPE server

This section includes information on when to install a standalone MPE server including:

- When to install a standalone MPE server
- What is installed
- Before you begin

When to install a standalone MPE server

We recommend installing a standalone MPE server on a different system if the ePO server is at capacity. Standalone MPE servers off-load processing to another system, and send and receive data from the sensors and scanners that they are managing. For more information, see the *McAfee Policy Enforcer 2.0 Bandwidth and Performance Guide*.

You can also use a standalone MPE server to handle rescan requests from noncompliant systems. For instructions, see [Install the remediation portal on page 17](#).

What is installed

The standalone MPE server installs the MPE server only; there is no interface.

Before you begin

Install the McAfee Policy Enforcer software on the ePO server system; see [page 7](#).

You need to be prepared with:

- The NetBIOS name of the ePO server system.
- The console-to-application server communication port (default is 8443) used during the installation of the ePO server and console.
- A global administrator user account.
- Verify that the system meets the minimum hardware and software requirements, see [page 31](#).
- If you are installing the standalone MPE server on a system running Windows 2000, see [page 40](#).
- If the standalone MPE server system is a member of a Microsoft Cluster Server (MSCS) cluster, see [page 38](#).
- If you use personal firewall software, see [page 39](#).

Although you can install the software on systems with Terminal Services, you cannot use Terminal Services to install this software. You must use **Add/Remove Programs**. For instructions, see the Microsoft product documentation.

- You can install the Policy Enforcer on systems running these virtual machine programs:
 - Microsoft Virtual Server 2005 Enterprise.

- Microsoft Virtual Server 2005 Standard.
- VMware Workstation 4.5 or later.

Install a standalone MPE server

For beta and evaluation versions of the software, the installation process differs slightly from these procedures. For more information, see [Migrating Policy Enforcer software on page 26](#).

- 1 Insert the CD into the CD-ROM drive of the system.
- 2 In the autorun window, select the desired language, then select **Install McAfee Policy Enforcer 2.0**.
- 3 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Next** to begin the installation.
- 4 In the **McAfee End User License Agreement** dialog box, select the appropriate license type and the country in which you purchased the software. The license type must match the license you purchased. If you are unsure which license you purchased, contact the person who sold you the software.

Read the entire license agreement carefully, select **I accept the terms in the license agreement** to agree to the license terms, then click **OK**.



If the license agreement does not display correctly, read the appropriate license in the LicenseAgreement.pdf file supplied with the ePolicy Orchestrator software.

- 5 In the **Installation Options** dialog box:
 - a Select **Stand-alone Policy Enforcer server**.
 - b To install the remediation portal on this system now, select **Remediation portal**.
 - c Accept the default installation path of the MPE server (for example, C:\Program Files\McAfee\MPE Server), or click **Browse** to select a different location.
 - d Click **Next**.
- 6 In the **ePolicy Orchestrator Server Information** dialog box, specify the settings of the ePO server:
 - a Type the NetBIOS name of the ePO server system.
 - b Type the console-to-application server communication port (default is 8443) used by the ePO server.
 - c Type the user name and password of a global administrator user account.
 - d Click **Next**.
- 7 In the **Certificate Files Location** dialog box, specify where the certificate files are located on the ePO server system. Use a UNC share or path to a local or mapped drive.
- 8 In the **Database Server Account** dialog box, click **Next**. Setup verifies that it can connect to the ePO database using the specified authentication method and user account, which defaults to the authentication method and user account used to install ePolicy Orchestrator software.

- 9** In the **HTTP Configuration** dialog box, specify the port numbers used for communication to and from the server, and click **Next**.
- **Scanner-to-server and sensor-to-server communication port** — Specifies the port number (default is 8444) that the standalone MPE server uses for inbound communication with the MPE scanner and sensor.
 - **Stand-alone server-to-integrated server communication port** — Specifies the port number (default is 443) that the standalone MPE server uses for outbound communication with the integrated MPE server on the ePO server system.
 - **Remediation portal communication port** — Specifies the port number (default is 80) that noncompliant systems use for outbound communication with the ePO server or standalone MPE server that is handling rescan requests.

Available only when you select **Remediation portal** in the **Installation Options** dialog box.
- 10** In the **Ready To Install** dialog box, click **Install** to begin the installation. This dialog box includes the estimated time to complete the installation.
- The **Executing Setup** dialog box provides the status of the installation.
- 11** In the **Installation Complete** dialog box, specify the desired options listed below, then click **Finish** to complete the installation.
- To open the console after completing the installation, select **Start McAfee ePolicy Orchestrator console**.
 - To view known issues or last-minute changes to the product or its documentation, click **View Readme**.

What to do after installation

After installing a standalone MPE server, you need to change configuration policies for the sensors and scanners.

Management of sensors and scanners from a standalone MPE server

You need to change the configuration policies for MPE or rogue system sensors and MPE scanners that you want to manage from standalone MPE servers. This means providing the NetBIOS name or IP address of the standalone MPE server system and the port number for scanner-to-server and sensor-to-server communication. For instructions, see these topics in the Policy Enforcer online Help:

- *Managing MPE or rogue system sensors from a standalone MPE server.*
- *Managing MPE scanners from a standalone MPE server.*

Installing and customizing the remediation portal

The remediation portal is a set of template files you can customize for your environment. The remediation portal is where noncompliant systems are remedied before being allowed network access. If you have an existing remediation portal, you can use it rather than install the McAfee Policy Enforcer remediation portal. For instructions, see [Customize an existing portal on page 21](#).

Once installed, you can customize the portal template files (see [Customizing the remediation portal on page 18](#)), or you can substitute your own files in the appropriate locations.

Policy Enforcer supports the display of remediation portal files in eight languages. Each language-specific set of files is located in its own directory. The languages, and the two or three letter code are:

Language	Code and directory name
Chinese (Simplified)	chs
Chinese (Traditional)	cht
English	en
French	fr
German	de
Japanese	ja
Korean	ko
Spanish	es

What is installed

The remediation portal can be installed in any one of eight languages. All remediation portal files are installed at the following location, and to language-specific subdirectories:

C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal

The integrated server installs the files to:

C:\Program Files\McAfee\epo\3.6.1\DB\portal

Two files are installed to the above location:

- Default.htm — a home page file that redirects requests to the language-specific home page file (Default.htm located in one of the language directories. Do not modify this file).
- styles.css — the style sheet for all remediation portal files.

Each supported language has its own directory. For example, the directory for the German remediation portal files is:

C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal\de

Each language-specific directory contains a Home page file (Default.htm), a Scan page file (Rescan.htm), local rescan, compliant and noncompliant .htms, a string substitution file (strings.nrc). Image files for the portal are installed to:

C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal\images

The integrated server installs the files to:

C:\Program Files\McAfee\epo\3.6.1\DB\portal

You can install the portal when you install the software or standalone MPE server, or separately on a different system.

If you install the portal on a different system from the ePO server or standalone MPE server, a Tomcat web server is also installed.

If you use an existing portal, you must add our custom remediation code to communicate with the ePO server or standalone MPE server. For instructions, see [Customize an existing portal on page 21](#).

Before you begin

- If you install the portal on a different system from the ePO server or standalone MPE server, verify that it meets the minimum requirements; see [page 35](#).
- If you use personal firewall software; see [page 39](#).

Install the remediation portal

- 1 Insert the CD into the CD-ROM drive of the system.
- 2 In the autorun window, select the desired language, then select **Install McAfee Policy Enforcer 2.0**.
- 3 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Next** to begin the installation.
- 4 In the **McAfee End User License Agreement** dialog box, select the appropriate license type and the country in which you purchased the software. The license type must match the license you purchased. If you are unsure which license you purchased, contact the person who sold you the software.

Read the entire license agreement carefully, select **I accept the terms in the license agreement** to agree to the license terms, then click **OK**.



If the license agreement does not display correctly, read the appropriate license in the LicenseAgreement.pdf file supplied with the ePolicy Orchestrator software.

- 5 In the **Installation Options** dialog box:
 - a Select **Remediation portal**.
 - b Modify or accept the default installation path of the uninstallation program (for example, C:\Program Files\McAfee\MPE Server), or click **Browse** to select a different location.
 - c Click **Next**.
- 6 In the **HTTP Configuration** dialog box, specify the port number (default is 80 or 81) that noncompliant systems use for outbound communication with the server that is accepting rescan requests. This can be the integrated MPE server installed on the ePO server, or a standalone MPE server.

Click **Next**.

- 7 In the **Ready To Install** dialog box, click **Install** to begin the installation. The dialog box includes the estimated time to complete the installation.

The **Executing Setup** dialog box provides the status of the installation.

- 8 In the **Installation Complete** dialog box, click **View Readme** to view known issues or last-minute changes to the product or its documentation, then click **Finish** to complete the installation.

When pointing to the integrated server, the Rescan.htm file is updated automatically during the installation with the name of the MPE server that will accept rescan requests from quarantined systems, and the console-to-application server communication port number (default is 8443) of the ePO server.

Customizing the remediation portal

To customize the remediation portal, you modify text or other HTML elements in the Default.htm file and the Strings.nrc file in the appropriate language-specific directory. You can also use an existing portal. For instructions, see [Customize an existing portal on page 21](#).

Modifications you might consider are:

- Customizing the compliance policy definition and remediation steps.
- Adding your corporate links to the navigation frame.
- Changing the company name, logo, and company contact information.

Customize the Default.htm file

The Default.htm files in the language-specific directories provide a template for creating your own remediation home page.

In the Default.htm file, you customize the text that explains why end users have been redirected to the remediation portal. This text defines the rules of the compliance policy and outlines the steps end users must follow to update their systems.

Depending on your compliance policy definition, you may want to add or remove certain entries from this file. You can also rewrite this file to follow your corporate guidelines, add your own instructions and information, or substitute any text in this file.

The beginning of the Default.htm file contains explanatory information about what text to modify, and tasks to perform. The file gets a large portion of its text from the Strings.nrc file. To modify the text being displayed, modify the appropriate string variable in the Strings.nrc file.

- 1 Open the language-specific directory for the language you will use for displaying remediation information. For example, if your remediation portal will display English, go to:

```
C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal\en
```

- 2 Open the Default.htm file in a text editor.

If you installed the portal at the same time as the software, the default location is:

```
C:\Program Files\McAfee\ePO\3.6.1\DB\Portal\en
```

3 Modify the Default.htm file with URLs or other corporate information, such as your corporate home page, legal department home page, and to images such as your corporate logo.

4 Locate all text that is bracketed by a set of two curly braces; for example: {{YOUR_COMPANY}}. The replacement text identifiers in the Default.htm file are:

Corporate information:

- {{YOUR_CORPORATE_HOMEPAGE}}
- {{YOUR_CORPORATE_LOGO}}
- {{YOUR_COMPANY}}
- {{YOUR_SECURITY_HOMEPAGE}}
- {{YOUR_LEGAL_HOMEPAGE}}
- {{YOUR_EMPLOYMENT_HOMEPAGE}}

Adding links to the navigation frame:

- {{YOUR_OTHER_URL_1}}
- {{YOUR_OTHER_URL_2}}
- {{YOUR_OTHER_URL_3}}
- {{YOUR_OTHER_URL_4}}
- {{YOUR_OTHER_URL_5}}
- {{YOUR_OTHER_URL_6}}

Compliance policy definition and remediation steps:

- {{YOUR_ANTIVIRUS_URL}}
- {{YOUR_ENGINE_URL}}
- {{YOUR_DAT_URL}}
- {{YOUR_AGENT_URL}}
- {{YOUR_ADDITIONAL_PRODUCT_URL}}

5 In the <head> section of the Default.htm file, locate the loadResources() function. You need to identify the association between the "labelID_<var-name>" identifiers and the "nrc_<var-name>" string variables in the Strings.nrc file.

6 Save and close the Default.htm file.

Customize the Localrescan.htm files

The localrescan.htm files in the language-specific directories provide a template for hosting the McAfee Policy Enforcer ActiveX downloader.

Customizing these pages is similar to the default.htm page. See [Customize the Default.htm file on page 18](#) for instructions. Follow the same directions to customize items like the company logo, corporate information, and other URLs that are displayed to the user. For the ActiveX component, you need to configure the MPE_SERVER_Name.

This ActiveX component downloads the MPE scanner on the user's system and executes a single scan, then removes the MPE scanner after the scan is complete. In the localrescan.htm file, you can customize the text that explains to users that the system is currently being scanned.

Depending on the scan results, the component navigates to one of these pages:

- rescancompliant.htm page
The component navigates here if the user is compliant with your policy. On this page, customize the text that explains that the user is compliant with the company policies and is allowed full network access.
- rescannoncompliant.htm page
The component navigates here if the user is noncompliant with your policy. On this page, customize the text that explains that the user is noncompliant with the company policies and will not be allowed full network access.
- rescanerror.htm page
The component navigates here if an error occurs while attempting to download the MPE scanner or while scanning the system. On this page, customize the text that explains that an error has occurred while attempting to scan the user's system.

Customize the Strings.nrc file

The Strings.nrc file is a Unicode text file that contains definitions of string variables used in the Default.htm and Rescan.htm files.

You can add links to web pages that users might find useful to the navigation frame that appears on the left side of the Home and Scan pages.

- 1 Open the language-specific directory for the language you use for displaying remediation information. For example, if your remediation portal displays in English, go to:

```
C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal\en
```
- 2 Open the Strings.nrc file in a text editor. This is a Unicode file.
- 3 Locate the "nrc_<var-name>" variable that specifies the text used in the Default.htm file.lines of code.
- 4 Modify the headings and text as necessary.
- 5 Change {{YOUR_OTHER_URL_X}} and {{YOUR_OTHER_PAGE_X}} to the desired web addresses and link text, respectively.

- 6 Save and close both files.

Using the Rescan.htm file

The Scan page, Rescan.htm, is automatically modified during installation with the name of the server where the remediation portal was installed, and the port number of the console-to-application server communication port of the ePO server.

Typically, you should not have to modify this file.

Customize an existing portal

If you already have a portal in place, you can customize it to accept user credentials and send rescan requests to the ePO server or a standalone MPE server. You need to add the specified code to the appropriate HTML pages on your company portal. You also need to provide this data:

- The NetBIOS name of the ePO server or standalone MPE server that is accepting rescan requests. If the server system is a member of a cluster, use the NetBIOS name of the virtual server.
 - The console-to-application server communication port number (default is 8443) of the ePO server.
- 1 Add the code in the RescanCodeForHead.htm file to the <head> section to the appropriate HTML page. This file is available in the installation directory. If you installed the portal separately from the Policy Enforcer software, the default location is:

C:\Program Files\McAfee\ePO\3.6.1\Samples

If you installed the portal at the same time as the software, the default location is:

C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal\Samples

This code is also provided under [Rescan code for <head> section on page 24](#).

- 2 Add the code in the RescanCodeForBody.htm file to the <body> section of the appropriate HTML page. This file is available in the installation directory. This code is provided under [Rescan code for <body> section on page 25](#).

- 3 Locate these lines of code in the code you added in [Step 2](#):

```
<form name="theForm" method="post"  
action="https://{MPE_SERVER_NAME}:8443/snowcap/rescan.go">
```

- 4 Change {{MPE_SERVER_NAME}} to the NetBIOS name of the ePO server or standalone MPE server that is accepting rescan requests.
- 5 Change 8443 to the console-to-application server communication port of the ePO server.
- 6 Save and close the files.

Opening the remediation portal

To open the remediation portal, go to this web address on the integrated server (case-sensitive):

`https://<MPE_SERVER_NAME>:8443/Portal/default.htm`

- where <MPE_SERVER_NAME> is the NetBIOS name of the ePO server or standalone MPE server that is accepting rescan requests.
- where 8443 is the console-to-application server communication port of the ePO server. If you changed the port number from the default, use that port number instead.

What to do after installation

Whether you are using an existing portal or the one provided with the Policy Enforcer, you need to complete these post-installation tasks.

Using the remediation portal

You need to ensure that users of noncompliant systems can remediate their systems to bring them into compliance.

- **Remediation instructions** — Ensure that users of noncompliant systems know what steps to take to remediate their systems.
- **Remediation resources access** — Ensure that noncompliant systems have access to every URL on the remediation portal.
- **Remediation portal access** — Ensure that noncompliant systems have access to the remediation portal.
- **Portal URL for users** — Ensure that users of noncompliant systems know the URL of the remediation portal.

The process depends on the enforcement type: self-enforcement, switch enforcement, or VPN enforcement. Typically, managed systems use self-enforcement, unmanaged systems use switch enforcement, and VPN-connected systems use VPN enforcement.

Systems that use Cisco NAC enforcement may use the McAfee Policy Enforcer remediation features if an administrator configures it in the Cisco ACS server.

Table 1-1 Remediation instructions

Enforcement type	Process
Self-enforcement	<p>When you define the noncompliance action for a compliance rule and the Enforcement Type for the rule is set to LAN, the local message automatically displays the list of failed checks. You can include additional information in the local message that assists users in remediating their systems. For instructions, see <i>Defining the compliance policy</i> in the Policy Enforcer online Help.</p> <p>You can also add remediation instructions to the remediation portal. For instructions, see Customizing the remediation portal on page 18 or Customize an existing portal on page 21.</p>
Switch enforcement	Add remediation instructions to the remediation portal. For instructions, see Customizing the remediation portal on page 18 or Customize an existing portal on page 21 .
VPN enforcement	<p>When you define the noncompliance action for a compliance rule and the Enforcement Type for the rule is set to VPN, the local message automatically displays the list of failed checks. You can include additional information in the local message that assists users in remediating their systems. For instructions, see <i>Defining the compliance policy</i> in the Policy Enforcer online Help.</p>

Table 1-2 Remediation resources access

Enforcement type	Process
Self-enforcement	Add the servers hosting each URL to the remediation list. For instructions, see <i>Defining the remediation list</i> in the Policy Enforcer online Help.
Switch enforcement	Ensure that the remediation VLAN has access to the servers hosting each URL; see network personnel.
VPN enforcement	These systems cannot access the remediation portal. Some VPN vendors support remediation. For information, see the VPN vendor product documentation.

Table 1-3 Remediation portal access

Enforcement type	Process
Self-enforcement	Add the server hosting the remediation portal to the remediation list. For instructions, see <i>Defining the remediation list</i> in the Policy Enforcer online Help.
Switch enforcement	Ensure that the separate VLAN for remediation has access to the server hosting the remediation portal; see network personnel.
VPN enforcement	These systems cannot access the remediation portal. Some VPN vendors support remediation. For information, see the VPN vendor product documentation.

Table 1-4 Portal URL for users

Enforcement type	Process
Self-enforcement	Add the URL to the remediation portal to the local message in every rule in your compliance policy. For instructions, see <i>Defining the compliance policy</i> in the Policy Enforcer online Help.
Switch enforcement	Set up a browser redirection on the remediation portal web server; go to solution ID KB46354 on the McAfee KnowledgeBase for example methods.
VPN enforcement	These systems cannot access the remediation portal. Some VPN vendors support remediation. For information, see the VPN vendor product documentation.

Rescan code for <head> section

```
<!-- The following javascript validation code should be included on any
custom rescan request page. -->
<!-- You will find accompanying <form> code for the body of the page in
the sample file RescanCodeForBody.htm -->
```

```
<script language="JavaScript">
function enableControls() {
    var btnRescan          = document.getElementById("btnRescan");
    var useSameCredentials =
document.getElementById("useSameCredentials");
    var account           = document.getElementById("account");
    var password          = document.getElementById("password");

    btnRescan.disabled = false;
    if ( useSameCredentials.checked )
    {
        disableText(account, true);
        disableText(password, true);
    }
    else
    {
        disableText(account, false);
        disableText(password, false);
        if ( !validateDomainAndUser(account.value) )
        {
            btnRescan.disabled = true;
        }
        if ( !validatePassword(password.value) )
        {
            btnRescan.disabled = true;
        }
    }
}
function validateDomainAndUser(duStr)
{
    if ( duStr.length < 1 )
    {
        return false;
    }

    var matchResult = duStr.match(/^[\.a-zA-Z0-9_-]+\[\[\.a-zA-Z0-9_-]+\$/);
    return (matchResult != null);
}

function validatePassword(pwStr)
{
    if ( pwStr.length < 1 )
    {
        return false;
    }
    return true;
}
```

```

function disableText(textControl, disabledState)
{
    textControl.disabled = disabledState;
    if ( disabledState ) {
        textControl.style.backgroundColor = "#dddddd";
    } else {
        textControl.style.backgroundColor = "";
    }
}

</script>

```

Rescan code for <body> section

```

<!-- To make effective use of this form, you should also include the
javascript found in the sample -->
<!-- file RescanCodeForHead.htm and include it in the <head> section of
your document. -->
<!-- The following 'onload' handler should be called in the body tag of
your page -->
<body onload="enableControls()">
<!-- This form should be included in its entirety in your custom rescan
request page. -->
<!-- You may optionally omit the <div> tag or make adjustments based on
your site's own css policy -->
<!-- If you have installed the ePO / MPE server with a different
Console-to-Application Server -->
<!-- communication port than 8443, please adjust the action below
accordingly. -->
<div class="rescanForm">
    <!-- NOTE: {{MPE_SERVER_NAME}} is the hostname of your ePO / McAfee
Policy Enforcer Server -->
    <!-- This server should be routable from the quarantine area / VLAN. -->
    <form name="theForm" method="post"
action="https://{{MPE_SERVER_NAME}}:8443/snowcap/rescan.go">
        <table cellSpacing=0 cellPadding=0 border=0>
            <tr>
                <td colspan=2>
                    <!-- Use same credentials again -->
                    <input type="checkbox" checked id="useSameCredentials"
name="useSameCredentials"
                    onclick="enableControls()">
                    <label for="useSameCredentials">Managed System: Use
existing credentials</label><p>
                </td>
            </tr>
            <tr>
                <td>
                    <!-- Administrator account -->
                    <td><label>Administrator account (domain\user):</label></td>
                <td>
                    <input type="text" class="formText" size=24 maxlength=85
id="account" name="account"
                    onchange="enableControls()"
onkeyup="enableControls()">
                </td>
            </tr>
        </table>
    </div>

```

```

<tr>
  <!-- Administrator password -->
  <td><label>Password:</label></td>
  <td>
    <input type="password" class="formText" size=24
maxlength=127 id="password" name="password"
    onchange="enableControls()"
onkeyup="enableControls()">
  </td>
</tr>
<!-- Rescan and Cancel buttons -->
<td colspan=3>
  <br>
  <input type="submit" value="Scan" class="formButton"
id="btnRescan" name="btnRescan">

  <!-- The onclick handler should be adjusted to direct
the user to any applicable cancel page -->
  <input type="button" value="Cancel" class="formButton"
id="btnCancel" name="btnCancel"
onclick="window.navigate('default.htm')">
  </td>
</tr>
</table>
</form>
</div>

```

Migrating Policy Enforcer software

This section includes information on migrating from previous or pre-release versions of the software.

Migrate from Policy Enforcer 1.0 to version 2.0

If you have installed Policy Enforcer version 1.0 Patch 2, note that data is migrated to support new features. The display and placement of data has changed, as follows:

- In version 1.x, there were two compliance policies based on LAN and VPN policy types. In version 2.0, there is *one* compliance policy.
- The policy types moved to the Rule Set level and are now called Assessment Result Modules to take into account NAC enforcement. Rule sets and Assessment Result Modules have a many-to-many relationship. This means many rule sets can apply to Assessment Result Modules and vice versa.
- During the data migration, the rule sets (including rules, checks, and TrustedMachineRules) for LAN and VPN are merged into one compliance policy. The upgrade software compares rule set names. If there are any duplications, the rule set names are appended with `_LAN` or `_VPN` before being merged.

Similarly, if any trusted machine rules have duplicate names, they are renamed by appending `_LAN` or `_VPN` before they are merged.



Policy types have not been deleted during the migration, but that they now reside on the rule set level.

- Version 2.0 supports multiple quarantine zones. The existing quarantine VLAN number is read and stored in a newly created default quarantine zone (Access Zone).

All the existing Rule Sets and Rules which had quarantine zones are assigned to the newly created default quarantine zone.



Version 2.0 retains all scanner and sensor NAP policies on the server. Any customized sensor and scanner NAP policies are migrated from earlier releases and they are fully functional.

Migrate to a licensed version

If you have a pre-release of the software (joint development, beta, or release candidate), you must uninstall it before you can install a licensed version. For instructions, see [Uninstalling the software on page 28](#).

If you have an evaluation version of the software, you can migrate it to a licensed version. To do so, you must be logged on as a local administrator or a member of the **Administrators** group.

- 1 Close all ePO consoles.
- 2 Insert the CD into the CD-ROM drive of the system.
- 3 In the autorun window, select the desired language, then select **Install McAfee Policy Enforcer 2.0**.



Be sure that the Setup program you are using is for the licensed version of the software.

- 4 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Next** to begin the migration. A message appears indicating that the migration was completed successfully.

2

Uninstallation

This section describes the uninstallation process for removing software applications.

- [Uninstalling the software](#)
- [Uninstalling a standalone MPE server](#)
- [Uninstalling the remediation portal](#)

Uninstalling the software

This section includes information on the following topics:

- [What is uninstalled](#)
- [Before you begin](#)
- [Uninstall the software](#)

What is uninstalled

Uninstalling McAfee Policy Enforcer software removes the integrated MPE server and the remediation portal, if installed. For instructions, see [Uninstalling the remediation portal on page 30](#). The MPE sensor 2.0.0 and MPE scanner 2.0.0 installation files and policy page are deleted from the ePO master repository. Policy Enforcer reports are also deleted from the ePO server.

The McAfee Policy Enforcer interface is replaced with the Rogue System Detection interface during the uninstallation, and the rogue system sensor 1.0.0 installation files and policy page and Rogue System Detection reports remain.

The McAfee System Compliance Profiler software is unaffected when you remove McAfee Policy Enforcer.

Restart the system at the end of the software uninstallation.

McAfee does not support the uninstallation of the Cisco Trust Agent (CTA). Refer to Cisco documentation for additional information on uninstalling CTA.

Before you begin

- 1 Uninstall the MPE sensors from the LAN. For instructions, see *Uninstalling MPE or rogue system sensors* or *Uninstalling MPE sensors manually* in the Policy Enforcer online Help.
- 2 Uninstall the MPE scanners from the LAN and VPN-connected systems. For instructions, see *Uninstalling MPE scanners* or *Uninstalling MPE scanners manually* in the Policy Enforcer online Help.
- 3 Remove configuration changes from VPN appliances. For instructions, see *Removing configuration changes* for the corresponding VPN vendor in the Policy Enforcer online Help.
- 4 Uninstall any standalone MPE servers; see [page 29](#).

Uninstall the software

- 1 Close all ePO consoles.
- 2 Close all database management software, for example, SQL Enterprise Manager.
- 3 Use **Add/Remove Programs** in the **Control Panel** to remove the **McAfee Policy Enforcer 2.0.0** for McAfee ePolicy Orchestrator 3.6.1.1 software.
- 4 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Remove**.
- 5 Click **Finish** when done.

Uninstalling a standalone MPE server

This section includes information on the following topics:

- [What is uninstalled](#)
- [Uninstall a standalone MPE server](#)

What is uninstalled

Before removing a standalone MPE server, be sure to redirect sensors and scanners that it currently manages to another standalone MPE server or the ePO server. For instructions, see these topics in the Policy Enforcer online Help:

- *Managing MPE or rogue system sensors from a standalone MPE server.*
- *Managing MPE scanners from a standalone MPE server.*

Removing a standalone MPE server uninstalls the MPE server and the remediation portal, if installed. For instructions, see [Uninstalling the remediation portal on page 30](#).

Restart the system at the end of the software uninstallation.

Uninstall a standalone MPE server

- 1 Use **Add/Remove Programs** in the **Control Panel** to remove the **McAfee Policy Enforcer 2.0.0 Stand-alone Server**.
- 2 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Remove**.
- 3 Click **Finish** when done.

Uninstalling the remediation portal

This section includes information on the following topics:

- [What is uninstalled](#)
- [Uninstall the remediation portal](#)

What is uninstalled

If you installed the remediation portal when you installed the software or standalone MPE server, the entire contents of the remediation portal installation directory is removed. The default location is:

C:\Program Files\Common Files\McAfee\Tomcat\WebApps\Portal

If you installed the portal at the same time as the software, the default location is:

C:\Program Files\McAfee\ePO\3.6.1\DB\Portal

If you installed the portal on a different system from the ePO server or standalone MPE server, the web server is also removed.

Restart the system at the end of the uninstallation.

If you were using an existing portal, you need to remove the custom remediation code. For more information, see [Customize an existing portal on page 21](#).

Uninstall the remediation portal

- 1 Use **Add/Remove Programs** in the **Control Panel** to remove the **McAfee Policy Enforcer 2.0.0 Remediation Portal** software.
- 2 In the **McAfee Policy Enforcer 2.0.0 Setup** wizard, click **Remove**.
- 3 Click **Finish** when done.

3

Planning

Requirements, preinstallation, and deployment scenarios

This section describes the planning process.

- [Requirements](#)
- [Things to know before installation](#)
- [Planning your deployment](#)

Requirements

The following topics list the hardware and software requirements for using McAfee Policy Enforcer.

McAfee Policy Enforcer software requirements

Product — ePolicy Orchestrator 3.6.1. For a list of ePolicy Orchestrator 3.6.1 requirements, see [ePO server and console requirements on page 36](#) and [ePO remote console requirements on page 37](#).

VirusScan Enterprise — If McAfee VirusScan® Enterprise 8.0i is installed on the ePO server, you must install VirusScan Enterprise 8.0i, Patch 11 or later.

Standalone MPE server requirements

Browser — Microsoft Internet Explorer 6.0 or later.

Database software — MDAC 2.8 (Windows 2000 only).

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.



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

File system — NTFS (NT file system) partition (recommended).

Free disk space — 500MB (first-time installation); 1GB (upgrade); 2GB recommended.

IP address — Static IP address (recommended).

Memory — 512MB RAM (minimum); 1GB (recommended).

Monitor — 1024x768, 256-color, VGA monitor.

NIC (network interface card) — 100Mbit or higher.

Operating system:

- Windows 2000 Advanced Server, Service Pack 3 or later.
- Windows 2000 Server, Service Pack 3 or later.
- Windows 2000 Terminal Services, Service Pack 3 or later.
- Windows Server 2003 Enterprise, Service Pack 1 or later.
- Windows Server 2003 Standard, Service Pack 1 or later.
- Windows Server 2003 Web, Service Pack 1 or later.

Processor:

- Intel Pentium compatible.
- 450MHz or higher.

VirusScan Enterprise — If VirusScan Enterprise 8.0i is installed on the standalone MPE server, you must install VirusScan Enterprise 8.0i, Patch 11 or later.

MPE sensor requirements

Browser — Internet Explorer 6.0 or later.

File system — NTFS partition (recommended).

Free disk space — 65MB or higher.

Host computer — Server computer (recommended).

Memory — 512MB or higher RAM.

Network environment — TCP/IP.

NIC (network interface card):

- Ethernet interface that supports 802.3, Ethernet II, or 802.11 protocol.
- 100Mbit or higher.

Operating system:

- Windows 2000 Professional, Service Pack 3 or later.
- Windows 2000 Advanced Server, Service Pack 3 or later.
- Windows 2000 Server, Service Pack 3 or later.
- Windows 2000 Terminal Services, Service Pack 3 or later.
- Windows XP Professional, Service Pack 1 or later.
- Windows Server 2003 Enterprise.

- Windows Server 2003 Standard.
- Windows Server 2003 Web.

Processor:

- Intel Pentium compatible.
- 300MHz or higher.

Product — ePO agent 3.5.5 or later.

MPE scanner requirements

Computers on which you are installing the MPE scanner must meet these minimum requirements. Systems being scanned remotely have no specific requirements.

Browser — Internet Explorer 6.0 or later.

Host computer — Server computer (recommended).

Memory (when scanning remote systems) — 512MB or higher RAM.

Operating system (when scanning remote systems):

- Windows 2000 Professional, Service Pack 3 or later without *MS05-019.
- Windows 2000 Advanced Server, Service Pack 3 or later without *MS05-019.
- Windows 2000 Server, Service Pack 3 or later without *MS05-019.
- Windows 2000 Terminal Services, Service Pack 3 or later without *MS05-019.
- Windows XP Professional with no service pack without *MS05-019 and with †Internet Connection Firewall disabled.
- Windows XP Professional, Service Pack 1 or later without *MS05-019 and with †Internet Connection Firewall disabled.
- Windows Server 2003 Enterprise, Service Pack 1 or later without *MS05-019 and with †Windows Firewall disabled.
- Windows Server 2003 Standard, Service Pack 1 or later without *MS05-019 and with †Windows Firewall disabled.
- Windows Server 2003 Web, Service Pack 1 or later without *MS05-019 and with †Windows Firewall disabled.

* The scanner cannot be installed on computers running Microsoft Security Bulletin MS05-019 because it inadvertently disables raw socket support.

† Scanner host computers cannot scan remote systems when the Internet Connection Firewall or Windows Firewall is enabled [specifically the Internet Connection Firewall (ICS)/Internet Connection Sharing (ICS) service or Application Layer Gateway Service, respectively] because these services prevent TCP packets from being sent to specific ports.

Operating system (when scanning only the local computer):

- Windows 2000 Professional, Service Pack 3 or later.
- Windows 2000 Advanced Server, Service Pack 3 or later.
- Windows 2000 Server, Service Pack 3 or later.
- Windows 2000 Terminal Services, Service Pack 3 or later.
- Windows XP Professional, Service Pack 1 or later.
- Windows Server 2003 Enterprise, Service Pack 1 or later.
- Windows Server 2003 Standard, Service Pack 1 or later.
- Windows Server 2003 Web, Service Pack 1 or later.

Product — ePO agent 3.5.5 or later.

VPN-connected computer requirements

IPSec VPN

VPN client software:

- Check Point VPN-1 SecureClient.



Check Point VPN-1 SecuRemote does not support Secure Configuration Verification (SCV) and, thus, cannot be supported.

- Nortel VPN Client.
- Nortel VPN Tunnel Guard agent.

Products:

- ePO agent 3.5.5 or later.
- MPE scanner 2.0.0 or later.

SSL VPN

VPN client software:

- No client software required.

VPN appliance requirements

IPSec VPN

Free disk space — 5MB or higher.

VPN software:

- Check Point VPN-1 Pro.
- Nortel VPN Router 600, 1010, 1050, 1100, 1700, 1740, 2700, or 5000 series.
- Nortel VPN Gateway 3050 or 3070 series.

SSL VPN

Free disk space — 5MB or higher.

VPN software:

- Juniper Networks Remote Access 500 series.
- Juniper Networks Secure Access 700, 1000, 2000, 3000, 4000, or 6000 series.

Products:

- VPN installation package.

Remediation portal requirements

If you install the remediation portal on a different computer from the ePO server or standalone MPE server, it must meet these minimum requirements:

Browser — Internet Explorer 6.0 or later.

Free disk space — 200MB or higher.

IP address — Static IP address (recommended).

Memory — 384MB or higher RAM.

Operating system:

- Windows 2000 Advanced Server, Service Pack 3 or later.
- Windows 2000 Server, Service Pack 3 or later.
- Windows 2000 Terminal Services, Service Pack 3 or later.
- Windows Server 2003 Enterprise, Service Pack 1 or later.
- Windows Server 2003 Standard, Service Pack 1 or later.
- Windows Server 2003 Web, Service Pack 1 or later.

Processor:

- Intel Pentium compatible.
- 300MHz or higher.

Switch requirements

Protocols:

- SNMP (Simple Network Management Protocol) 2.0c or later.
- STP (Spanning-Tree Protocol).
- CDP (Cisco Discovery Protocol); (recommended).

Vendors — For a list of switch vendors on which topology discovery and switch enforcement are supported, go to solution ID [KB46328](#) on the McAfee KnowledgeBase.

Router requirements

Protocols:

- SNMP (Simple Network Management Protocol) 2.0c or later.

ePO server and console requirements

Browser — Internet Explorer 6.0 or later.

Dedicated server — If managing more than 250 client computers, we recommend using a dedicated server.

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.



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

File system — NTFS partition (recommended).

Free disk space — 500MB minimum (first-time installation); 1GB minimum (upgrade); 2GB (recommended).

IP address — Static IP address (recommended).

Memory — 512MB RAM (minimum); 1GB (recommended).

Monitor — 1024x768, 256-color, VGA monitor.

NIC (network interface card) — 100Mbit or higher.

Operating system:

- Windows 2000 Advanced Server, Service Pack 3 or later.
- Windows 2000 Server, Service Pack 3 or later.
- Windows Server 2003 Enterprise.
- Windows Server 2003 Standard.
- Windows Server 2003 Web.

Processor:

- Intel Pentium compatible.
- 450MHz or higher.

ePO remote console requirements

Browser — Internet Explorer 6.0 or later.

File system — NTFS or FAT partition.

Free disk space — 250MB.

Memory — 128MB RAM.

Monitor — 1024x768, 256-color, VGA monitor.

NIC (network interface card) — 10Mbit or higher.

Processor — Intel Pentium compatible.

Operating system:

- Windows 2000 Advanced Server, Service Pack 3 or later.
- Windows 2000 Professional, Service Pack 3 or later.
- Windows 2000 Server, Service Pack 3 or later.
- Windows 2000 Terminal Server.
- Windows XP Professional, Service Pack 1 or later.
- Windows Server 2003 Enterprise with or without service packs.
- Windows Server 2003 Standard with or without service packs.
- Windows Server 2003 Web with or without service packs.

Things to know before installation

This section describes the requirements to meet before installing the software including the following topics:

- [Cluster on ePO server](#)
- [Cluster on standalone MPE server](#)
- [Firewall software](#)
- [MDAC 2.8](#)

Cluster on ePO server

If the ePO server system is a member of an MSCS cluster, do the following to install the McAfee Policy Enforcer software:

- 1 Stop these ePolicy Orchestrator services, then change their startup type to **Manual**:
 - McAfee ePolicy Orchestrator 3.6.1 Application Server
 - McAfee ePolicy Orchestrator 3.6.1 Event Parser
 - McAfee ePolicy Orchestrator 3.6.1 Server
- 2 Install the McAfee Policy Enforcer software on each cluster member. No configuration changes are needed.
- 3 Test the cluster:
 - a Select the ePO group, and select **Bring online**.
 - b Right-click any of the resources for the ePO group, then select **Initiate Failover**. The resources should fail and come back online.
- 4 Take note of the virtual server name. You need to enter it in the MPE sensor and scanner configuration policies to define the server managing those sensors and scanners.

Cluster on standalone MPE server

If the standalone MPE server system is a member of an MSCS cluster, do the following to install a standalone MPE server:

- 1 Install the standalone MPE server on each cluster member. No configuration changes are needed.
- 2 Test the cluster:
 - a Select the ePO group, and select **Bring online**.
 - b Right-click any of the resources for the ePO group, then select **Initiate Failover**. The resources should fail and come back online.
- 3 Take note of the virtual server name. You need to enter it in the MPE sensor and scanner configuration policies to define the server managing those sensors and scanners.

Firewall software

If you use personal firewall software, ensure that the communication ports you specify during the installation accept the appropriate type of communication. The software uses these ports to communicate between its components.

Table 3-1 Communication with the MPE server

Communication	Process	Protocol	Default port	*Inbound/ †Outbound
Remediation portal-to-server	---	HTTPS	81 or 80	Inbound
Scanner-to-server	MPEScanner.exe	HTTPS TCP	8444	Inbound
Sensor-to-server	MPESensor.exe	HTTPS TCP	8444	Inbound
Server-to-database	Tomcat.exe	TCP TDS	1433	Outbound
Standalone server-to-integrated server	---	HTTPS	443	Outbound

*Communication is relative to the integrated or standalone MPE server.

†Communication is relative to the standalone MPE server.

Table 3-2 Sensor (MPESensor.exe) communication

Communication	Protocol	Default port	*Inbound/ Outbound
Broadcast detection (listen only)	ARP	none	Passive
DHCP detection (listen only)	UDP	67 68	Passive
Enforcement (sensor-to-NADs)	UDP	161	Outbound
Discovery of starting switch and router (listen only)	CDP STP	none	Passive
Topology discovery (sensor-to-NADs)	UDP SNMP	161	Outbound

*Communication is relative to the sensor host system.

Table 3-3 Scanner services

Scanner Services	*Inbound/ Outbound
MPEScanner.exe	Both
FSAssessment.exe	Both
FSDiscovery.exe	Both

*Communication is relative to the scanner host system.

MDAC 2.8

If you are installing a standalone MPE server on a system running Windows 2000, MDAC 2.8 must also be installed to ensure database connectivity.

Determine the version number of MDAC

- 1 Locate the Msdadc.dll file that corresponds to the database software. The default location is:

C:\Program Files\Common Files\System\Ole Db

- 2 Right-click the Msdadc.dll file, then select **Properties**. The <FILE> **Properties** dialog box appears.
- 3 Click the **Version** tab, select **ProductVersion** under **Item name**, and check the version number under **Value**.

Installing MDAC

We distribute the MDAC 2.8 Setup program on the product CD and in the product package available for download. It can be found in these locations:

On the product CD

Setup\MDAC\MDAC_Typ_<LANGUAGE>.exe

- Where <LANGUAGE> equals EN for English, FR for French, DE for German, JP for Japanese, and ES for Spanish.

In the downloaded product package

Setup\MDAC\MDAC_Typ.exe

At press time, the Chinese (Simplified), Chinese (Traditional), and Korean language versions of the Setup program were available on the Microsoft website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6c050fe3-c795-4b7d-b037-185d0506396c&DisplayLang=en>

At press time, instructions for installation were available on the Microsoft website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6c050fe3-c795-4b7d-b037-185d0506396c&DisplayLang=en>

Planning your deployment

When planning your deployment of the distributed components of Policy Enforcer, important considerations include the type of systems you want to protect, how they connect to the network, network environment constraints, and corporate policies. These considerations determine the functionality and where to deploy the McAfee Policy Enforcer components.

To plan your deployment, we recommend that you:

- [Assemble a team.](#)
- [Evaluate compliance scenarios.](#)
- [Where to deploy sensors and scanners.](#)

Assemble a team

Because the Policy Enforcer software works closely with network components, its deployment requires coordination within your company. For this reason, we recommend that you assemble a cross-functional team. This team might include:

- IT support personnel and network engineers.
- The VPN system security administrator.
- The NAC system security administrator.
- The ePolicy Orchestrator administrator.
- The compliance policy administrator.
- The network security administrator.

Each compliance scenario here includes:

- The systems and connection types being protected.
- Required Policy Enforcer components and their functionality.
- Required network components.
- Required network data.
- A checklist of deployment tasks.

Reviewing each compliance scenario will help you determine the makeup of the team. For example, if you are using a remediation portal, you might involve the web services department.

Evaluate compliance scenarios

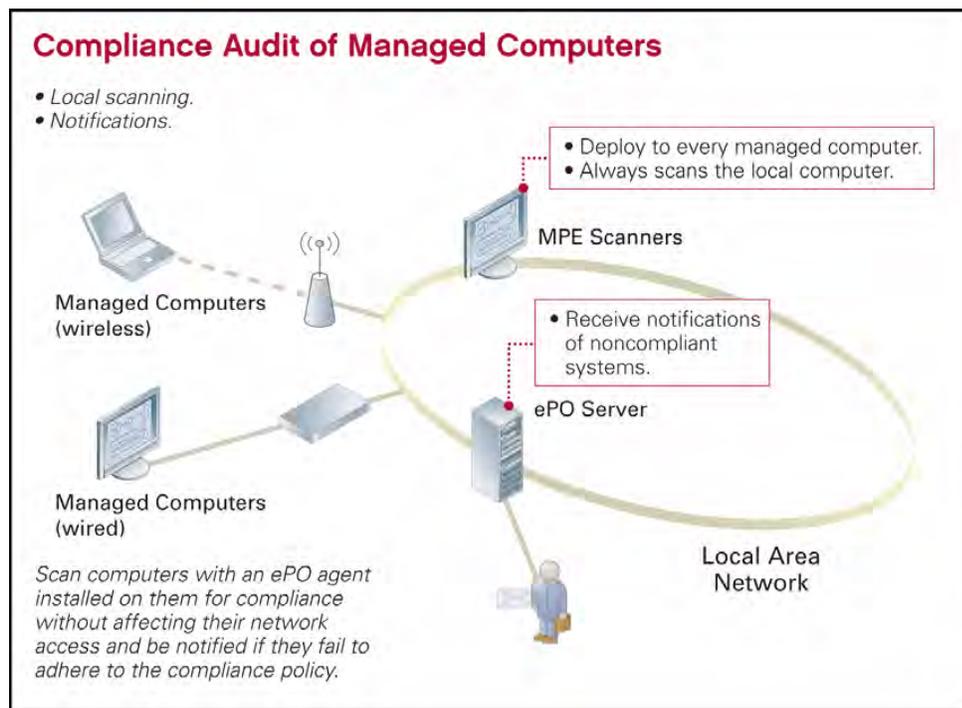
Choose from these compliance scenarios based on your needs and constraints:

- Compliance audit of managed systems.
- Local compliance enforcement of managed systems.
- Compliance audit of unmanaged systems.
- Remote compliance enforcement of unmanaged systems.
- Compliance audit of VPN-connected systems.
- Compliance enforcement of VPN-connected systems.
- Compliance audit and enforcement of NAC-connected systems.

Compliance audit of managed systems

You can scan managed systems that are accessing the network locally (wired or wireless) without affecting their network access, and be notified if they fail to adhere to the compliance policy.

You need to deploy an MPE scanner to every managed system on the LAN that you want to protect. For information, see [Where to deploy sensors and scanners on page 53](#).



Deployment checklist

To implement this compliance scenario, do the following:

1 Verify requirements.

- Scanner host systems; see [page 33](#).

2 Complete these tasks.

- Deploy scanners.
- Define the compliance policy.
- Set the compliance policy to audit mode.
- Receive notifications of noncompliant systems.

Local compliance enforcement of managed systems

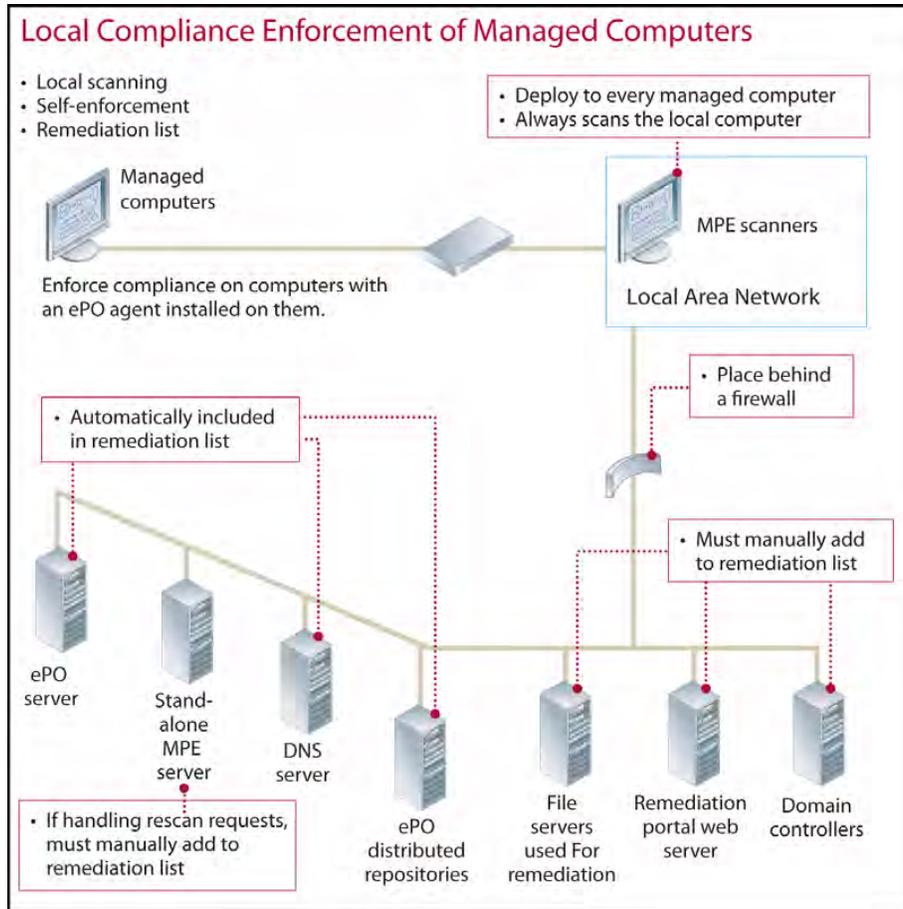
You can enforce compliance on managed systems that are accessing the network locally. If you are already reporting on the compliance status of managed systems on the LAN, set the LAN policy to enforce mode to start enforcing compliance on these systems.

You need to deploy an MPE scanner to every managed system on the LAN that you want to protect, see [Where to deploy sensors and scanners on page 53](#).

To display remediation steps to users of noncompliant systems, you need a remediation portal. You can use an existing portal or the one provided with the Policy Enforcer software.

You also need a list of the network resources noncompliant systems can access for remediation. The remediation list always includes the system's ePO server, the scanner host system, DNS servers, and ePO distributed repositories. You must manually add standalone MPE servers (if handling rescan requests from noncompliant systems), any file servers used for remediation, the server hosting the remediation portal, and the primary and backup domain controllers.

The network resources in the remediation list need to be protected. We recommend placing these resources behind a firewall to prevent scanner host systems from spreading infections.



Deployment checklist

To implement this compliance scenario, do the following:

1 Verify requirements.

- Scanner host systems; see [page 33](#).

2 Gather data.

- URL for the remediation portal.
- SNMP community string for the sensor.
- VLANs for use for enforcement zones.
- List of network resources by DNS name, fully-qualified domain name (FQDN), or IP address.



Because different FQDNs (for example, www.mcafee.com and mcafee.com) resolve to different IP addresses, you must add each one to the remediation list to enable access. We recommend that IP addresses are preferred for internal resources and all resources available via the Internet should use FQDN.

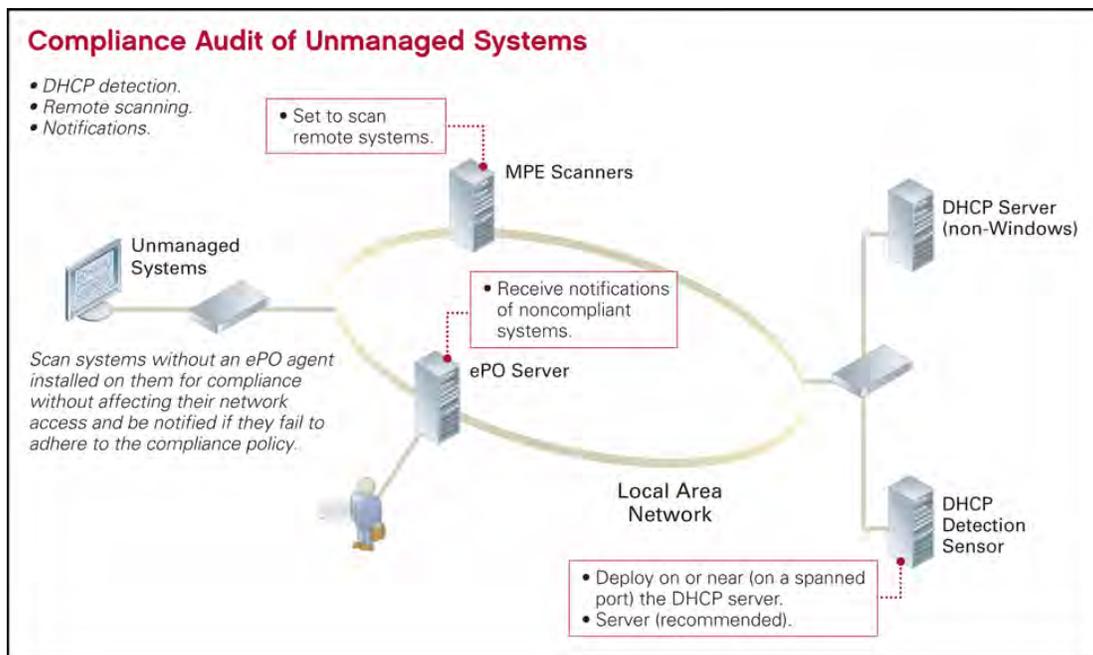
3 Complete these tasks.

- Install remediation portal; see [page 16](#).
- Deploy scanners.
- Define the remediation list for managed systems.
- Define the compliance policy.
- Set the compliance policy to enforce mode.

Compliance audit of unmanaged systems

You can scan unmanaged systems without affecting their network access. You are notified if the systems fail to adhere to the compliance policy. You can also scan managed systems — without a scanner — using this scenario; however, we recommend using local scanning and self-enforcement on managed systems.

You need to use an MPE sensor for DHCP detection and deploy it on or near the DHCP server. You also need to deploy one MPE scanner that have been enabled to scan remote systems. For information, see [Where to deploy sensors and scanners on page 53](#).



Deployment checklist

To implement this compliance scenario, do the following:

1 Verify requirements.

- Sensor host systems; see [page 32](#).
- Scanner host systems; see [page 33](#).
- Switches; see [page 36](#).
- Routers; see [page 36](#).

2 Gather data.

- Read-only SNMP community for all switches.
- Read-only SNMP community for all routers.
- Read-write SNMP community for all access layer switches.

3 Complete these tasks.

- Deploy sensors.
- Configure the DHCP detection sensor.
- Deploy scanners.
- Define the compliance policy.
- Set the compliance policy to audit mode.
- Enable scanning of remote systems.
- Receive notifications of noncompliant systems.

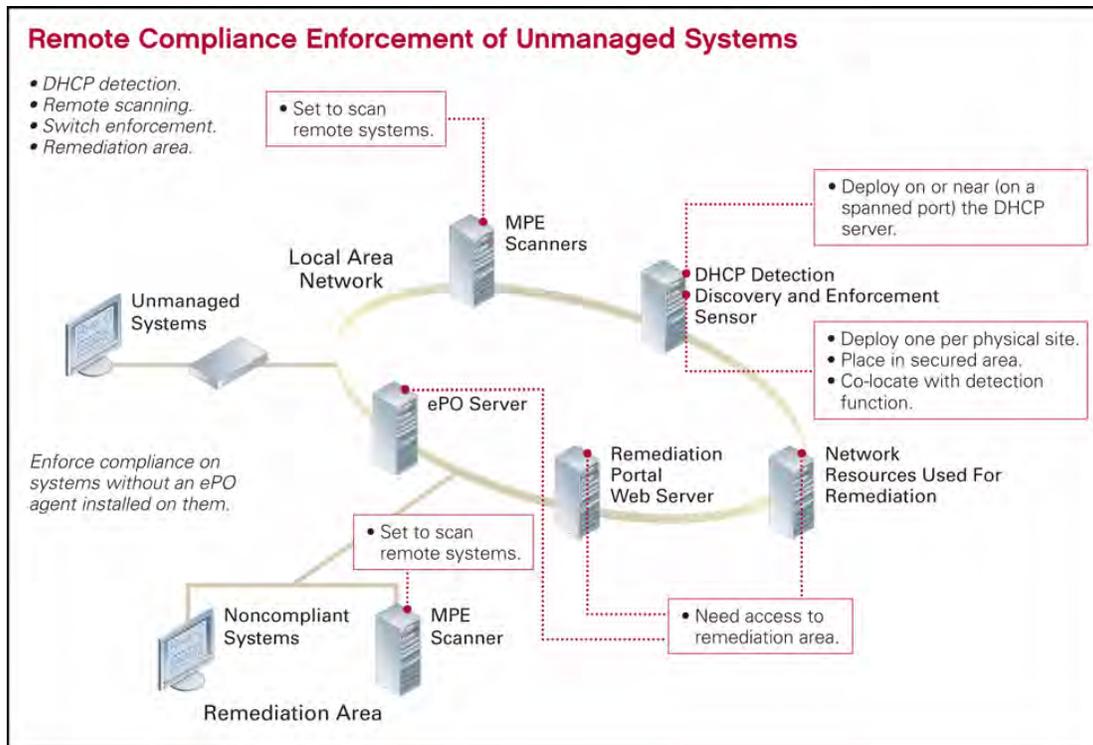
Remote compliance enforcement of unmanaged systems

You can enforce compliance on unmanaged systems that are accessing the network locally. If you are already reporting on the compliance status of unmanaged systems on the LAN, set the LAN policy to enforce mode to start enforcing compliance on these systems.

You need to use an MPE sensor for DHCP detection and discovery and enforcement and deploy it on or near the DHCP server. You also need to deploy MPE scanners enabled to scan remote systems: one per physical site and one in the remediation area. For information, see [Where to deploy sensors and scanners on page 53](#).

To display remediation steps to end users of noncompliant systems, you need a remediation portal and a browser redirection on the web server hosting the portal. You can use an existing portal or the one provided with the McAfee Policy Enforcer software.

You also need a separate VLAN on the network to send noncompliant systems for remediation. A detection, mapping sensor is required on the remediation VLAN. The remediation area needs access to the ePO server system, the server hosting the remediation portal, and any other network resources end users need to access to update their systems.



Deployment checklist

To implement this compliance scenario, do the following:

1 Verify requirements.

- Sensor host systems; see [page 32](#).
- Scanner host systems; see [page 33](#).
- Switches; see [page 36](#).
- Routers; see [page 36](#).

2 Gather data.

- Read-only SNMP community for all switches.
- Read-only SNMP community for all routers.
- Read-write SNMP community for all access layer switches.
- VLAN value of remediation area.
- URL for the remediation portal.

3 Complete these tasks.

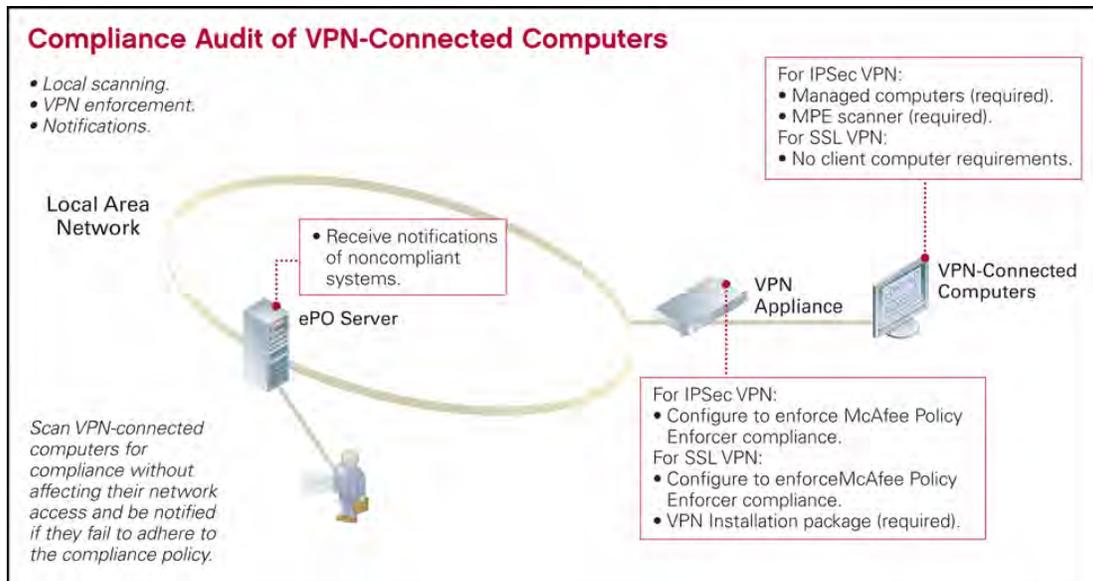
- Install remediation portal; see [page 16](#).
- Set up a browser redirection on the remediation portal web server; go to solution ID [KB46354](#) on the McAfee KnowledgeBase for example methods.
- Define the remediation area; see network personnel.
- Give network resources used for remediation access to the remediation area; see network personnel.
- Deploy sensors.
- Configure the DHCP detection sensor.
- Configure the discovery and enforcement sensor.
- Deploy scanners.
- Enable scanning of remote systems.
- Define the compliance policy.
- Set the compliance policy to enforce mode.

Compliance audit of VPN-connected systems

You can scan VPN-connected systems that are accessing the network remotely using supported VPN vendors without affecting their network access, and be notified if they fail to adhere to the compliance policy.

For IPSec VPN, you must define the compliance policy, configure the VPN appliance, allow VPN-connected systems access to the VPN appliance, and install the MPE scanner on the VPN client system.

For SSL VPN, you must define the compliance policy, configure the VPN appliance, allow VPN-connected systems access to the VPN appliance, create the VPN installation package, and copy it to the VPN appliance.



Deployment checklist

To implement this compliance scenario, do the following:

1 Verify requirements.

- VPN appliance; see [page 35](#).
- VPN-connected systems; see [page 34](#).

2 Complete these tasks.

- Define the compliance policy.
- Set the compliance policy to audit mode.
- Configure the VPN appliance.
- Allow VPN-connected systems access to the VPN appliance.
- Deploy the scanner (IPSec VPN only).
- Create the VPN installation package (SSL VPN only).

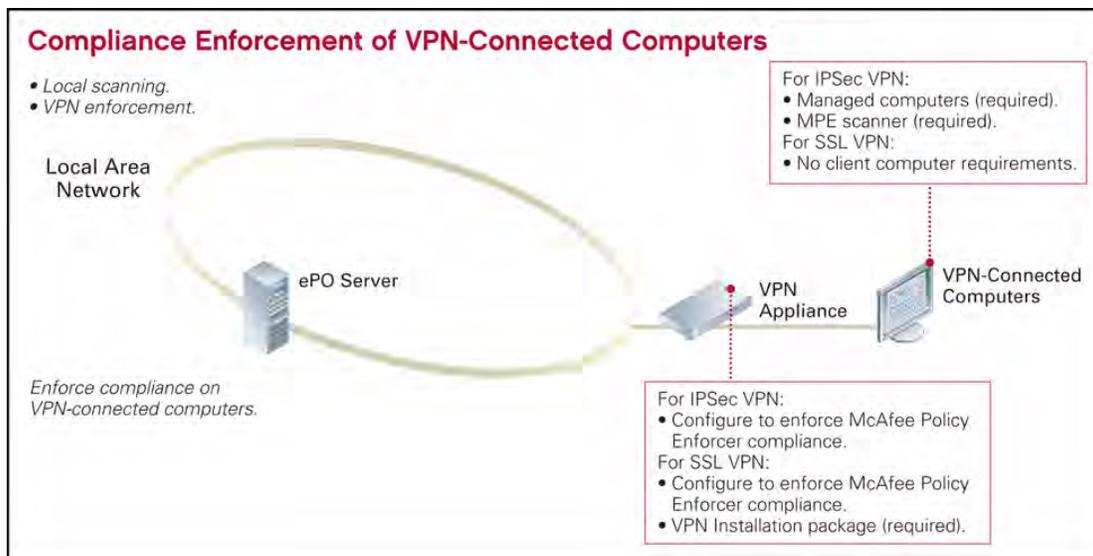
Compliance enforcement of VPN-connected systems

You can enforce compliance on VPN-connected systems that are accessing the network remotely. Enforcing compliance is only supported on systems accessing the network using supported VPN vendors.

If you are already reporting on the compliance status of managed systems connecting through VPN, set the VPN policy to enforce mode to start enforcing compliance on these systems. For some vendors, you might also need to change settings on the VPN appliance to enforce compliance.

For IPSec VPN, you must define the compliance policy, configure the VPN appliance, and install the MPE scanner on the VPN client system.

For SSL VPN, you must define the compliance policy, configure the VPN appliance, allow VPN-connected systems access to the VPN appliance, and create the VPN installation package and copy it to the VPN appliance.



Deployment checklist

To implement this compliance scenario, do the following:

1 Verify requirements.

- VPN appliance; see [page 35](#).
- VPN-connected systems; see [page 34](#).

2 Complete the tasks.

- Define the compliance policy.
- Set the compliance policy to enforce mode.
- Configure the VPN appliance.
- Allow VPN-connected systems access to the VPN appliance.
- Deploy the scanner (IPSec VPN only).
- Create the VPN installation package (SSL VPN only).

Compliance audit and enforcement of NAC-connected managed and unmanaged systems

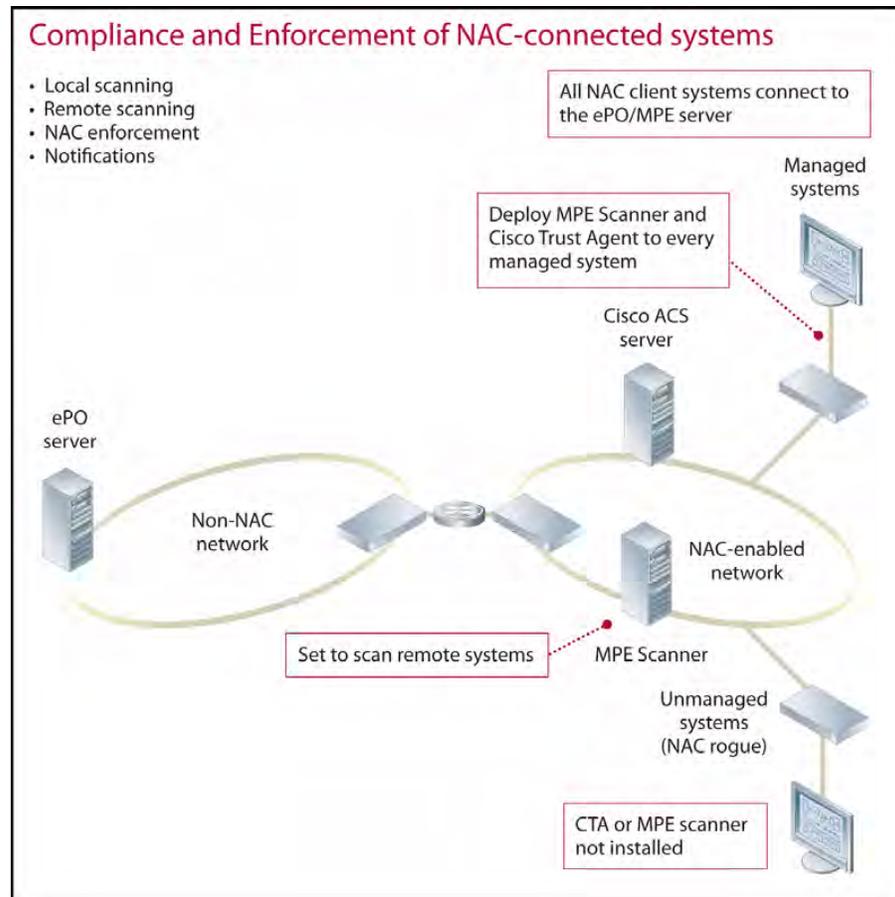
You can scan managed and unmanaged systems that are accessing the network via a NAC-enabled network device without affecting their network access. You are also notified if the systems fail to adhere to the compliance policy.

You can also enforce compliance on managed and unmanaged systems that are accessing the network via a NAC-enabled network device. If you are already reporting on the compliance status of managed and unmanaged systems in a NAC environment, set the NAC policy to enforce mode to start enforcing compliance on these systems.

You need to deploy an MPE scanner to every managed system in the NAC environment that you want to protect. For information, see [Where to deploy sensors and scanners on page 53](#).

To display remediation steps to users of noncompliant systems, you need a remediation portal. You can use an existing portal or the one provided with the McAfee Policy Enforcer software.

You also need a list of the network resources noncompliant systems can access for remediation. Access to these systems needs to be configured in the Cisco ACS Server control panel. This list should include the system's ePO server, the remote scanner host system, DNS server, ePO distributed repositories, any standalone MPE servers (if handling rescan requests from noncompliant systems), any file servers used for remediation, the server hosting the remediation portal, and the primary and backup domain controllers.



Deployment checklist

To implement this compliance scenario, do the following:

- 1 Verify requirements.**
 - Scanner host systems; see page 27.
- 2 Gather data.**
 - URL for the remediation portal.
 - Cisco ACS Server configuration

3 Complete these tasks.

- Ensure that a Cisco Trust Agent (CTA) is already deployed to managed systems
- Import Policy Enforcer NAC attributes into Cisco ACS Server
- Configure Cisco ACS Server to integrate with MPE Server
- Configure Cisco ACS Server to allow noncompliant systems access to specific network resources
- Deploy scanners.
- Enable scanning of remote systems.
- Define the compliance policy.
- Set the compliance policy to audit or enforce mode.
- Receive notifications of noncompliant systems.

Where to deploy sensors and scanners

Read about our recommendations for where to deploy MPE sensors and scanners:

- Determining detection type and where to deploy detection sensors.
- Where to deploy discovery and enforcement sensors.
- Determining scanning mode and where to deploy scanners.

Determining detection type and where to deploy detection sensors

Whether you want to protect systems with static or dynamic IP addresses determines the type of detection to use. Broadcast detection finds systems with both dynamic and static IP addresses within one subnet. DHCP detection finds system with dynamic IP addresses assigned by the DHCP server.

Table 3-4 What each detection type finds and where to deploy detection sensors

Detection type	Detects	Does not detect	Where to deploy
Broadcast	Dynamic and static IP addresses	Anything outside the subnet	One on each subnet
DHCP	Dynamic IP addresses	Static IP addresses	One on or *near the DHCP server

*Near meaning on a spanned port.

DHCP detection? — If yes, we recommend enabling DHCP detection, topology discovery and mapping, and switch enforcement on one sensor, and deploying it on or near the DHCP server.

Existing rogue system sensors? — If yes, you can continue to use rogue system sensors for broadcast detection until you want to upgrade them to MPE sensors. Remember that rogue system sensors only support broadcast detection; they do not support DHCP detection.

We recommend upgrading any existing rogue system sensors to MPE sensors, then deploying only new MPE sensors.

Host system recommendation — We recommend using a server as the sensor host system, and defining it as a trusted system. Trusted systems are always scanned and reported on, but never quarantined or dropped from the network. For a list of the minimum hardware and software requirements for the sensor, see [MPE sensor requirements on page 32](#).

Where to deploy discovery and enforcement sensors

Deploying discovery and enforcement sensors enables the Policy Enforcer to locate and enforce systems on the network.

SNMP considerations — If there is one read-only SNMP community and one read-write community for all switches, and one read-write community for all access layer switches, deploy one discovery and enforcement sensor per physical site (or DHCP server).

If there are multiple SNMP communities for switches and routers on the LAN, deploy one discovery and enforcement sensor for each set of unique community strings. In this case, we recommend deploying only one sensor per subnet to reduce network traffic and avoid multiple sensors performing discovery on the same subnet. However, we strongly recommend changing the SNMP community on switches and routers to use common strings.

We recommend placing the discovery and enforcement sensor near switches in a secured area on the network. Although communication between the sensor and server is secure, SNMP communication is not. The sensor uses a read-write community string to change the network access mode (allow, quarantine, or drop) on switch ports.

Access layer, core, or distribution switches? — We recommend only using access layer switches to perform switch enforcement. Use none or different community strings on core and distribution switches from access layer switches. Use a separate read-write community string or none at all on your distribution and core switches.

DHCP detection? — If yes, we recommend enabling DHCP detection, topology discovery and mapping, and switch enforcement on one sensor and deploying it on or near the DHCP server.

Host system recommendation — We recommend using a server as the sensor host system and defining it as a trusted system. By default, systems that are hosting enforcement sensors are marked as trusted systems. Trusted systems are always scanned and reported on, but never quarantined or dropped from the network.

For a list of the minimum hardware and software requirements for the sensor, see [MPE sensor requirements on page 32](#).

Management networks and ACLs? — If switches use separate IP address ranges than systems (management network versus user network) and an Access Control List (ACL) is in use, give the sensor host system access to the management network, then add the following data to the ACL:

- Sensor host system's IP address.
- Read-only SNMP community for all switches.
- Read-only SNMP community for all routers.
- Read-write SNMP community for all access layer switches.

In this case, we recommend using a dedicated server with a static IP address as the sensor host system to help ensure SNMP security. We recommend that this dedicated server use one NIC for the management network and another for the user network to retain security between networks.

Determining scanning mode and where to deploy scanners

Company policy and a phased deployment plan will likely determine whether you choose to scan systems locally, remotely, or both. For example, if you need approval to install software on systems using the corporate image, you might choose to use remote scanning because only one server per physical site is needed to host the scanner. Scanning the local system requires installing software on each system.

Regardless of the scanning mode you choose, we recommend deploying the scanner to systems of highest concern first.

Local or remote scanning? — Scanning the local system has these advantages over scanning remote systems:

- The majority of checks in the compliance policy require credentials. Because credentials are always available on scanner host systems, all checks can be performed when scanning the local system.
- Systems are never allowed access to the network until they are deemed compliant by the scanner. In contrast, systems being scanned remotely might have access to the network for a short time while their compliance status is being determined.
- Overall load on the network is reduced.

For these reasons, we recommend scanning the local system, especially server systems. However, not all systems can be scanned locally. Systems running older operating systems and unmanaged systems must be scanned remotely.

Host system recommendation — When scanning remote systems, we recommend using a server as the scanner host system, and defining it as a trusted system. By default, scanner host systems that are scanning remote systems are marked as trusted systems. Trusted systems are always scanned and reported on, but never quarantined or dropped from the network. In this case, we also recommend using a dedicated server as the scanner host system, and deploying the scanner to the same system that is hosting the discovery and enforcement sensor.

For a list of the minimum hardware and software requirements for the scanner, see [MPE scanner requirements on page 33](#).

Internet connection or Windows Firewall and remote scanning? — When scanning remote systems, you must disable the Internet Connection Firewall or Windows Firewall [specifically the **Internet Connection Firewall (ICS)**/**Internet Connection Sharing (ICS)** service or **Application Layer Gateway Service**, respectively] on scanner host systems.

For a list of the minimum hardware and software requirements for the scanner, see [MPE scanner requirements on page 33](#).

Managed or unmanaged? — Scanner host systems must be managed systems.

Unmanaged systems must be scanned remotely.

Operating system? — If scanning remote systems, we recommend using a server running Windows 2000 or 2003 as the scanner host system.

Systems running Windows 95, Windows 98, Windows Me, Windows NT, or non-Windows operating systems cannot be scanner host systems and must be scanned remotely.

Table 3-5 When to scan locally versus remotely

Local scanning	Remote scanning
Systems running these operating systems:	Systems running these operating systems:
<ul style="list-style-type: none"> ■ Windows 2000 server editions (recommended if scanning remote systems). ■ Windows 2000 workstation editions. ■ Windows XP Professional with Windows Firewall disabled. ■ Windows Server 2003 with Internet Connection Firewall disabled. 	<ul style="list-style-type: none"> ■ *Windows 95 (required). ■ *Windows 98 (required). ■ *Windows Me (required). ■ Windows NT (required). ■ *Non-Windows operating systems.
<ul style="list-style-type: none"> ■ Server systems (recommended). 	<ul style="list-style-type: none"> ■ Server systems. ■ Workstation systems.
<ul style="list-style-type: none"> ■ Managed systems (recommended). 	<ul style="list-style-type: none"> ■ Managed systems. ■ Unmanaged systems (required).

*Scanning running these operating systems is limited to operating system identification.

Optimizing scanning — We recommend changing specific registry settings on the scanner host system to optimize its performance in these situations:

- When it is scanning systems running older operating systems.
- When it is scanning a large number of remote systems and it has at least 1GB of RAM.

For instructions, see *Optimizing scanning* in the Policy Enforcer online Help.

Virtual machine? — Install the scanner in every virtual machine session on managed systems to avoid having the network access mode changed on the entire system when it is noncompliant.

700-1466-00

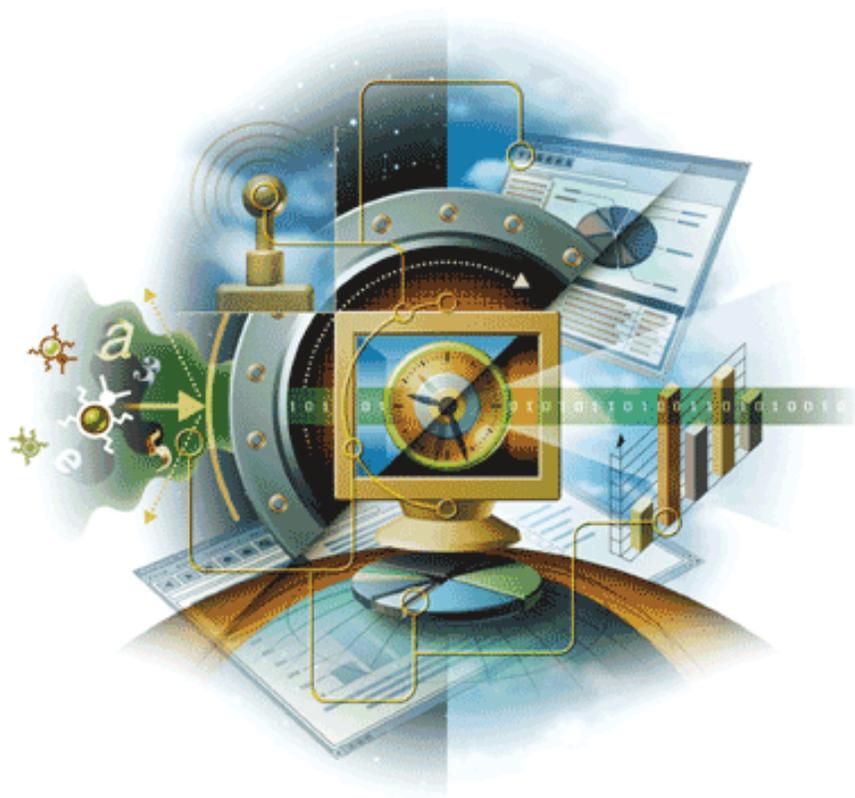
Copyright © 2006 McAfee, Inc. All Rights Reserved.

McAfee[®]

mcafee.com

McAfee® Policy Enforcer

version 2.0



McAfee® System Protection

Industry-leading intrusion prevention solutions

McAfee®



McAfee® Policy Enforcer

version 2.0

McAfee®
System Protection

Industry-leading intrusion prevention solutions

McAfee®

COPYRIGHT

Copyright © 2006 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

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color 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 ACCOMPANIES 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 MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright ©2000 CrystalClear Software, Inc.
- FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In™ Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In™ HTML Export, © 2001 Stellent Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003.
- Software copyrighted by Gisle Aas, © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, ©1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martijn Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, ©2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, ©2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.
- Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992.
- Software copyrighted by Cambridge Broadband Ltd., © 2001-2003.
- Software copyrighted by Sparta, Inc., © 2003-2004.
- Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004.
- Software copyrighted by Simon Josefsson, © 2003.
- Software copyrighted by Thomas Jacob, © 2003-2004.
- Software copyrighted by Advanced Software Engineering Limited, © 2004.
- Software copyrighted by Todd C. Miller, © 1998.
- Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.
- Software developed by the JDOM Project (<http://www.jdom.org/>).
- TinyXml is released under the zlib license: This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution.

Contents

1	Introducing McAfee Policy Enforcer	8
	What is McAfee Policy Enforcer?	8
	Integration with ePolicy Orchestrator	9
	ePolicy Orchestrator policy integration	9
	Managed and unmanaged systems	10
	Rogue System Detection integration	10
	System Compliance Profiler integration	10
	Product permissions	11
	McAfee Policy Enforcer (MPE) components	11
	MPE server	12
	MPE sensor	13
	MPE scanner	13
	Remediation portal	14
	Content updates for McAfee Policy Enforcer	14
	Automatic notification	15
	Content retrieval and distribution	15
	What's new in this release	16
	Cisco NAC enforcement framework support	16
	Multiple enforcement zones	17
	Automatic remediation	18
	On-demand ActiveX scanner	19
	Using the product documentation	20
	Audience	20
	Conventions	20
	Getting product information	21
	Standard documentation	21
	Supplemental documentation	21
	Contact information	22
2	Configuring and Managing MPE Components	23
	Getting started with McAfee Policy Enforcer	23
	Communication flow between MPE components	26
	Configuring and managing MPE servers	27
	Configure MPE servers	27
	MPE server management tasks	27
	How MPE servers work	28
	Integrated MPE server	29
	Standalone MPE servers	30
	Configuring and managing MPE sensors	31
	Configure an MPE sensor policy	31
	MPE Sensor management tasks	33
	How MPE sensors work	35
	Associating MPE sensors with standalone MPE servers	36
	MPE sensors vs. rogue system sensors	36
	Primary and secondary sensors	36
	Topology discovery and mapping	37
	Switch enforcement	41
	How detection works	41
	Configuring and managing scanners	45

Configure a scanner policy	45
The default scanner policy	47
Scanner management tasks	47
How MPE scanners work	48
Local scanners	49
Remote scanners	51
Using continuous compliance scanning	52
3 Compliance Policy Enforcement	53
How compliance policy enforcement works	53
Enforcement methods	54
Self-enforcement	54
Switch enforcement	56
Enforcement types	58
LAN enforcement	58
VPN enforcement	59
Cisco NAC enforcement	60
Enforcement modes	63
Policy enforcement and enforcement zones	64
Quarantining managed systems	65
Quarantining unmanaged systems	66
Enforcement zone priority	66
Manually quarantining a system or switch port	66
4 Compliance Policy Definition	67
Defining a compliance policy	67
How compliance policy definition works	69
How rule sets work	70
Rule set computer conditions	71
How rules work	71
McAfee default rules	72
Checks	73
How are checks evaluated?	74
Comparing exception systems and trusted systems	75
5 Remediation	76
What is needed to perform remediation?	76
Configuring and managing remediation	77
How does remediation work?	78
The remediation portal	80
Accessing the remediation portal	81
The remediation list	81
Automatic remediation	82
Rescanning a system in an enforcement zone	83
Remediation of managed systems	83
Remediation of unmanaged systems	85
Remediation for VPN enforcement	87
6 Actions, Notifications, Troubleshooting	88
Status of systems compliance summary	88
Status of systems	89
Status of subnets	89
Status of switches	89
Custom filter	90
Automatic responses	90
Actions	91
Reports	92
Accessing reports for the first time	92
McAfee Policy Enforcer report templates	92
Troubleshooting tools	93

	Scanner log files	93
	Sensor log files	94
	Packet capture of network traffic	95
	NAC-related troubleshooting	95
7	Cisco NAC Integration	96
	MPE components in a NAC environment	97
	Setup requirements for Cisco NAC	99
	Deploy the Cisco Trust Agent	100
	Set credentials for ACS authentication	101
	Cisco ACS server configuration	101
	Import ADF file to ACS server	102
	Configuration for NAC managed systems	102
	Configuration for NAC Agentless Hosts	104
8	VPN Integration	106
	Configuring IPSec VPN products	106
	Check Point	106
	Nortel	108
	Configuring SSL VPN Products	110
	Creating the Juniper SSL VPN installation package	110
	Juniper	110
	Allowing VPN-connected computers access to the VPN appliance	112
A	Frequently Asked Questions	113
	How does McAfee Policy Enforcer work with fast user switching?	113
	How do I deploy the discovery and enforcement sensor securely?	114
	What happens to laptops at a coffee shop or hotel? Are these systems quarantined?	114
	Does McAfee Policy Enforcer work with Cisco Network Admission Control?	114
	Does McAfee Policy Enforcer work with the 802.1x protocol?	115
	What happens to computers connected to the network via unsupported VPN software?	115
	What happens to VoIP phones on the network?	115
	What happens when multiple systems are connected to the same port of unmanaged switches, hubs, or WAPs?	116
	When should deploy one sensor per subnet?	116
	Does McAfee Policy Enforcer work with multiple NICs?	116
	Where do I find bandwidth and performance data on McAfee Policy Enforcer?	116
	Glossary	117
	Index	127

1

Introducing McAfee Policy Enforcer

Topics in this section:

- [What is McAfee Policy Enforcer?](#)
- [Integration with ePolicy Orchestrator](#)
- [McAfee Policy Enforcer \(MPE\) components](#)
- [Content updates for McAfee Policy Enforcer](#)
- [What's new in this release](#)
- [Using the product documentation](#)
- [Getting product information](#)
- [Contact information](#)

What is McAfee Policy Enforcer?



McAfee® Policy Enforcer is security software that protects corporate networks by blocking access to systems that do not comply with IT security policies. The software integrates with McAfee ePolicy Orchestrator®, and provides robust policy creation, device detection and mapping, fast and accurate compliance assessment, network access control, and remediation capabilities for managed and unmanaged systems.

McAfee Policy Enforcer software:

- **Defines network security compliance** — Provides complete control when defining compliance for every system on your network. You control the level of network access given to noncompliant systems.
- **Detects all network systems** — Detects new systems when they request access to or communicate on the network.
- **Assesses compliance** — Scans systems to determine whether they meet the minimum requirements of the compliance policy.
- **Enforces compliance policy** — Allows systems full network access, puts systems in an enforcement zone, or drops systems entirely based on scan results. You can change the network access mode on systems manually or automatically in response to an event.
- **Remediates noncompliant systems** — Displays remediation steps to users of noncompliant systems. After updating their systems, users can rescan their systems from the remediation portal.

Policy Enforcer is designed for use by network and security administrators on networks that use McAfee ePolicy Orchestrator.

Integration with ePolicy Orchestrator

Policy Enforcer integrates with ePolicy Orchestrator software, and uses its deployment, update, notification, and management features. Policy Enforcer installs seamlessly on existing ePolicy Orchestrator (ePO) servers.

The Policy Enforcer interface is accessed from the ePO console. Although most Policy Enforcer functions are controlled by the MPE server, the ePO server manages:

- Communications between the MPE distributed components (sensors and scanners) and the ePO central data repository.
- Sending compliance policy updates to scanners.

For instance, if the Policy Enforcer compliance policy changes, it is the ePO server that manages the communication and distribution of this change to all managed systems on the network. All MPE scanners are updated with the new policy at the next agent-server communication.

The following table lists some of the important tasks that are managed by the ePolicy Orchestrator software. The ePolicy Orchestrator Compliance Check server task is unaffected when you install Policy Enforcer.

For more information on...	See these topics in the ePolicy Orchestrator online Help...
Agent deployment	<i>Distributing Agents</i>
Client tasks	<i>Configuring Product Policies and Tasks</i>
Distributed repositories	<i>Creating Repositories</i>
Notifications	<i>ePolicy Orchestrator Notifications</i>
Product policies	<i>Configuring Product Policies and Tasks</i>
Server tasks	<i>Configuring ePolicy Orchestrator Servers</i>
Updating	<i>Deploying Software and Updates</i>
User accounts	<i>Configuring ePolicy Orchestrator Servers</i>
Reports	<i>Reporting</i>

ePolicy Orchestrator policy integration

ePolicy Orchestrator defines configuration policies for systems connected to your network. For example, you can require systems to have anti-virus and anti-spyware products installed, or specific operating system service packs and patches.

Policy Enforcer adds to the ePolicy Orchestrator policy features by allowing you to define a *compliance* policy that can quarantine or drop noncompliant systems from your network. For example, you can require that specific network security products, operating system patches, and threat checks be present on systems accessing your network. Typically, you would define your Policy Enforcer compliance rules to match your ePolicy Orchestrator configuration rules.

Managed and unmanaged systems

Policy Enforcer adopts the same concept of managed and unmanaged systems used by ePolicy Orchestrator.

- Unmanaged — no ePO agent installed.
- Managed — ePO agent installed.

The ePO agent is a program that performs background tasks on managed computers, mediates all requests between the server and managed products on these computers, and reports back to the server on the status of these tasks.

Rogue System Detection integration

Once Policy Enforcer is installed, the Rogue System Detection interface within ePolicy Orchestrator is replaced. The rogue system sensor 1.0.0 policy page and Rogue System Detection reports remain, allowing you to manage and report on existing rogue system sensors while you deploy Policy Enforcer components.

Although you can continue to use rogue system sensors for broadcast detection after installing Policy Enforcer, McAfee recommends upgrading existing rogue system sensors to MPE sensors, and only deploying new MPE sensors.

For more information on...	See these topics...
Rogue System Detection and rogue system sensors	<i>Rogue System Detection</i> in the ePolicy Orchestrator online Help.
Rogue System Detection reports	<i>Report and Query Templates</i> in the ePolicy Orchestrator online Help.
Working with rogue system sensors within Policy Enforcer	MPE sensors vs. rogue system sensors on page 36.

If you are already using Rogue System Detection in ePolicy Orchestrator, you can continue to detect rogue systems without making any configuration changes. For more information, see *Rogue System Detection* under *Planning Your Deployment* in the *McAfee Policy Enforcer 2.0 Installation Guide*.

System Compliance Profiler integration

The McAfee System Compliance Profiler® software, including its on-demand scan client task, is unaffected when you install Policy Enforcer.

Product permissions

Policy Enforcer uses a product permission model similar to ePolicy Orchestrator. See [Configure MPE servers on page 27](#).

ePolicy Orchestrator role	Policy Enforcer access permission
Global administrator	Automatically has access to all areas and functionality.
Site administrator	Can be assigned access to specific areas and functionality.
Global and Site reviewers	No access.

McAfee Policy Enforcer (MPE) components

The components of McAfee Policy Enforcer are:

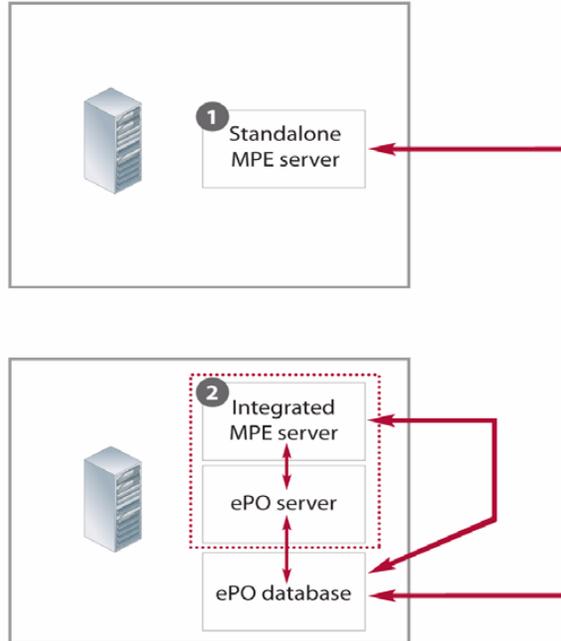
- [MPE server](#)
- [MPE sensor](#)
- [MPE scanner](#)
- [Remediation portal](#)

The MPE server works with the ePO server and database. The MPE sensor and MPE scanner are distributed components that rely on the ePO agent and the MPE server to receive policy configuration. The remediation portal is required to put noncompliant systems in an enforcement zone.

MPE server

The server manages communications between it and the MPE distributed components (sensors and scanners), and manages the integration of its functions with the ePO server. You can install the integrated MPE server only, or install additional standalone MPE servers.

Figure 1-1 Integrated and standalone MPE servers with local ePO database



- 1 A standalone MPE server receives data from the sensors and scanners it manages. Sensor and scanner data is transmitted to the ePO database.
- 2 The integrated MPE server:
 - Sends and receives data from the sensors and scanners it manages, if any.
 - Manages the user interface including: status and summary data; sending compliance policy updates to scanners; managing event reporting and automatic responses; and managing configuration policies, properties, and tasks.
 - Transmits data to the ePO database.

The ePO database can be installed on the same system as the ePO server (local database) or on a different system (remote database). You specify the ePO database location when you install Policy Enforcer.

For details, see [How MPE servers work on page 28](#).

MPE sensor

The sensor is a distributed component installed on selected managed systems; servers are recommended.

The MPE sensor performs:

- **Detection** — Detects new systems when they request access to or communicate on the network.
- **Topology discovery and mapping** — Identifies all switches and routers on the LAN and their relationship to each other. Finds the network location of systems — using network topology data — each time they are detected.
- **Switch enforcement** — Based on scan results, changes the network access mode (allowed or quarantined) of systems being scanned remotely. In response to an event, you can also change the network access mode (allow, quarantine, or drop) of systems manually or automatically.

See [How MPE sensors work on page 35](#) for details.

MPE scanner

The scanner is a distributed component installed on managed systems. Scanners can assess systems for compliance on the network locally or remotely. See [How MPE scanners work on page 48](#) for details.

Local scanners

A local scanner assesses only the system on which it is installed for compliance, and provides:

- **Local scanning** — Assesses whether the managed system running locally adheres to the compliance policy.
- **Self-enforcement** — Changes the network access mode (allow, quarantine, or drop) of systems *being scanned locally*, based on scan results.

Remote scanners

A remote scanner is a distributed component that provides the functionality of a local scanner for the system where it is installed, and provides:

- **Remote scanning** — Assesses any system in the same network as the systems to be scanned — without a scanner installed or a functioning scanner — for adherence to the compliance policy.

Remediation portal

The remediation portal is necessary for users of noncompliant systems to install software, patches, or content updates that make their systems compliant with your compliance policy. You can add McAfee's custom remediation code to an existing portal or customize the templates included with Policy Enforcer. The templates support eight languages.

A link to the remediation portal can be included in the noncompliance message of each policy rule. This message is displayed to users of noncompliant managed systems. Noncompliant unmanaged systems do not receive this message, and must be redirected to the remediation portal when users open their Internet browser.

The portal should provide information and links to resources that allow users to remedy any violation of your compliance policy. After updating their systems, users must be able to initiate a rescan from the remediation portal. You can use a remote scanner accessible from your enforcement zones or quarantine VLANs, or use the Policy Enforcer downloadable ActiveX scanner.

For more information, see [Chapter 5, Remediation](#). To install and set up the remediation portal templates, see the *McAfee Policy Enforcer Installation Guide*.

Content updates for McAfee Policy Enforcer

McAfee releases content updates for Policy Enforcer periodically. To ensure that you have the most current protection, McAfee recommends signing up for automatic notification.

Policy Enforcer uses two types of content: a check package and server update package.

Check packages

- **Threat check package** — Includes checks for selected, high-risk virus infections.
- **Microsoft security bulletin check package** — Includes checks for Microsoft security updates, divided into subsets by application, Internet Explorer, and operating system.
- **Compliance check package** — Includes checks for supported anti-spyware, anti-virus, firewall, and host intrusion prevention products, ePO agent, Microsoft service packs, patch management products, potentially unwanted programs, and third-party agents.

Server update package

- **Network access device support** — Extends support for topology discovery and switch enforcement to additional network access devices such as switches. These updates are released on an as-needed basis.
- **Check data** — Includes descriptive information about each check, such as check categories and IDs.

Automatic notification

You can receive automatic notification of content updates for Policy Enforcer using these methods:

- The MSAS service on ServicePortal.
- Weekly security newsletter for Platinum Technical Support customers.

Checks that are new in the last 30 days are highlighted in the compliance policy interface.

Content retrieval and distribution

To ensure you have the most current content from McAfee (check and server update packages), use these ePO server tasks:

ePO server task	Time interval
Repository pull task (DAT and engine)	Daily
Repository replication task	Daily incremental
Repository replication task	Weekly full

The default **Policy Enforcer Scanner Update Task** updates all check packages on managed systems daily at 12 A.M. You can modify the settings of this task, or delete it and use another ePO agent update task to distribute check packages to managed systems. For instructions, see [Scanner management tasks on page 47](#).



If you delete the default task, make sure to set up a replacement.

What's new in this release

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

- [Cisco NAC enforcement framework support](#)
- [Multiple enforcement zones](#)
- [Automatic remediation](#)
- [On-demand ActiveX scanner](#)

Cisco NAC enforcement framework support

Previous release	Cisco Network Admission Control (NAC) enforcement framework was not supported in Policy Enforcer 1.0.
Current release	McAfee Policy Enforcer 2.0 supports Cisco NAC enforcement framework, version 2.0.
Benefits	Cisco NAC support enables customers to use ePolicy Orchestrator with Policy Enforcer as the management console to define, monitor, and manage system security compliance.
Where to find	To use Policy Enforcer in a Cisco NAC enforcement framework, users must configure the Cisco Access Control Server (ACS), and enable the NAC enforcement type for rule sets in their compliance policy.
For more information	<ul style="list-style-type: none">■ Chapter 7, Cisco NAC Integration on page 96.■ Chapter 3, Compliance Policy Enforcement on page 53.

Multiple enforcement zones

Previous release	In Policy Enforcer 1.0, noncompliant systems were quarantined to a single quarantine area, specified by a VLAN.
Current release	McAfee Policy Enforcer 2.0 provides multiple named enforcement zones which can be associated with different rules in the compliance policy.
Benefits	Systems now can be quarantined to specific VLANs. This separates compliant systems from other systems based on their level of non-compliance and employee versus guest status. This feature prevents compliant systems from being infected by noncompliant systems before they are remediated.
Where to find	Enforcement zones are defined by clicking the Policy Enforcer Compliance tab, then clicking the Enforcement Types tab.
For more information	<ul style="list-style-type: none">■ Chapter 3, Compliance Policy Enforcement on page 53.■ Chapter 4, Compliance Policy Definition on page 67.

Automatic remediation

Previous release	In Policy Enforcer 1.0, all remediation of noncompliant systems was performed manually.
Current release	McAfee Policy Enforcer 2.0 includes the ability to initiate commands or actions that run automatically if a system fails a compliance rule.
Benefits	Automated remediation reduces the time to patch systems at risk, and reduces help desk calls for remediation portal questions.
Where to find	This feature is found on the Set Noncompliance Actions page of the Add/Edit Rule wizard.
For more information	<ul style="list-style-type: none">■ Chapter 4, Compliance Policy Definition on page 67■ Chapter 5, Remediation on page 76.

On-demand ActiveX scanner

Previous release	In Policy Enforcer 1.0, a remote scanner handled scanning unmanaged systems and rescan requests from the remediation portal.
Current release	In McAfee Policy Enforcer 2.0, unmanaged systems can be assessed for compliance using the on-demand ActiveX scanner or a remote scanner. Rescan requests from the remediation portal also can be handled by either scanner.
Benefits	<p>Users on an unmanaged system can download the ActiveX scanner, which can perform compliance assessment, then uninstall itself. This functionality works in addition to the existing solution of scanning unmanaged systems using an MPE remote scanner.</p> <p>Administrators can make the ActiveX scanner available on the remediation portal for rescan requests.</p>
Where to find	No setup or other configuration of this component is needed.
For more information	<ul style="list-style-type: none">■ Chapter 3, Compliance Policy Enforcement on page 53.■ Chapter 5, Remediation on page 76.

Using the product documentation

The *Installation Guide* provides requirements, installation instructions, and deployment planning. After installation, the following documentation is provided to assist you.

User reference	User assistance	
Product Guide	MPE user interface	online Help
<ul style="list-style-type: none"> ■ Describes components and features. ■ Explains how functionality works. ■ Lists tasks and where to go in the user interface to do them. 	<ul style="list-style-type: none"> ■ Designed for flow of work. ■ Uses terms that fit workflow. ■ Provides instructional text where appropriate. 	<ul style="list-style-type: none"> ■ Click Help button for user interface term definitions. ■ Step-by-step instructions are provided for each task.

Audience

This information is intended for network and system administrators who are responsible for their company's security program. The information is designed for professionals experienced in networking.

Conventions

This guide uses the following conventions:

Bold	All words from the interface, including options, menus, buttons, and dialog box names.
Condensed	<p>Example: Type the User name and Password of the appropriate account.</p>
Courier	<p>The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).</p> <p>Examples: The default location for the program is: <code>C:\Program Files\McAfee\EPO\3.6.1</code></p> <p>Run this command on the client computer: <code>scan --help</code></p>
<i>Italic</i>	<p>For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material.</p> <p>Example: Refer to the <i>ePolicy Orchestrator Product Guide</i>.</p>
Blue	<p>A web address (URL) and/or a live link.</p> <p>Example: Visit the McAfee website at: http://www.mcafee.com</p>
<TERM>	<p>Angle brackets enclose a generic term.</p> <p>Example: In the console tree, right-click <SERVER>.</p>
	<p>Note: Supplemental information; for example, another method of executing the same command.</p>
	<p>Tip: Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.</p>



Caution: Important advice to protect your computer system, enterprise, software installation, or data.



Warning: Important advice to protect a user from bodily harm when using a hardware product.

Getting product information

Product documentation, with the exception of the Release Notes, comes as Adobe Acrobat .PDF files, and can be downloaded from the McAfee Support ServicePortal:

https://mysupport.mcafee.com/eservice_enu/start.swe?SWECmd=Start

Standard documentation

Installation Guide — System requirements; instructions for installing and starting the software; and deployment scenarios.

Product Guide — Introduction to the product, its features and components; detailed information on how the product works; process flow for using the software; and instructions on configuring the software, deployment, recurring tasks, and operating procedures.

Help — The **Help** menu in the application accesses the entire online Help system; the **Help** button in the application displays information about the current page of the interface, including all field definitions.

Release Notes — *ReadMe*. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.

Quick Reference Card — Contains essential information on basic product features, components, tasks you perform, and where to find them in the interface. *A printed card accompanies the product CD.*

Supplemental documentation

For information about ePolicy Orchestrator software, refer to the product documentation, which can be downloaded from the McAfee Support ServicePortal.

Contact information

Threat Center: McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library

<http://vil.nai.com>

Avert Labs WebImmune & Submit a Sample *(Logon credentials required)*

<https://www.webimmune.net/default.asp>

Avert Labs DAT Notification Service

http://vil.nai.com/vil/signup_DAT_notification.aspx

Download Site <http://www.mcafee.com/us/downloads/>

Product Upgrades *(Valid grant number required)*

Security Updates (DATs, engine)

HotFix and Patch Releases

- **For Security Vulnerabilities** *(Available to the public)*

- **For Products** *(ServicePortal account and valid grant number required)*

Product Evaluation

McAfee Beta Program

Product Documentation

Technical Support <http://www.mcafee.com/us/support/>

KnowledgeBase Search

<http://knowledge.mcafee.com/>

McAfee Technical Support ServicePortal *(Logon credentials required)*

https://mysupport.mcafee.com/eservice_enu/start.swe

Customer Service

Web

<http://www.mcafee.com/us/support/index.html>

<http://www.mcafee.com/us/about/contact/index.html>

Phone — US, Canada, and Latin America toll-free:

+1-888-VIRUS NO or **+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

Professional Services

Enterprise: <http://www.mcafee.com/us/enterprise/services/index.html>

Small and Medium Business: <http://www.mcafee.com/us/smb/services/index.html>

2

Configuring and Managing MPE Components

Topics in this section:

- [Communication flow between MPE components](#)
- [Configuring and managing MPE servers](#)
- [How MPE servers work](#)
- [Configuring and managing MPE sensors](#)
- [How MPE sensors work](#)
- [Configuring and managing scanners](#)
- [How MPE scanners work](#)

Getting started with McAfee Policy Enforcer

You use the ePolicy Orchestrator console to configure, manage, and deploy Policy Enforcer components. This section provides a basic task flow for configuring Policy Enforcer components.

A deployment checklist that details the required components, data, and tasks is provided in *Planning Your Deployment* in the *McAfee Policy Enforcer Installation Guide*.

1 Configure the MPE server

- 1 If necessary, install additional standalone Policy Enforcer servers. (See *Installation Guide*.)
 - Associate a sensor with a standalone Policy Enforcer server
 - Associate a scanner with a standalone Policy Enforcer server
- 2 Specify the basic, email, and external command settings, if known.
- 3 Configure email notifications of noncompliant systems.

See [Configuring and managing MPE servers on page 27](#).

2**Deploy MPE sensors**

- 1 Deploy at least one sensor that performs topology discovery and mapping, and switch enforcement.
 - Configure a sensor policy.
 - Know the read-only community strings used for querying switch and router information via SNMP, and read-write community strings used for switch enforcement.
 - Optionally select/identify a starting switch or router. The default selections are automatic.
- 2 Deploy one or more detection sensors.
 - Configure sensor policies.
- 3 Upgrade and/or replace any Rogue System sensors to Policy Enforcer sensors.

See [Configuring and managing MPE sensors on page 31](#).

3**Set up a remediation portal**

- 1 Identify the server resources to use for remediation of noncompliant systems.
- 2 Set up and/or identify one or more enforcement zones (VLANs) that can be used for quarantining noncompliant systems.
- 3 Set up all of the resources that users need to remediate their problems.
- 4 Provide remediation instructions to correct user problems.

See [Remediation on page 76](#).

4**Deploy MPE scanners**

- 1 Use the ePO deployment task to install scanners on all systems.
 - Configure the scanners for a local policy.
 - Configure the scanners for a remote policy
- 2 Know the resources you want to include in the scanner's remediation list.

See [Configuring and managing scanners on page 45](#).

5**Define a compliance policy**

- 1 Understand how policy enforcement works for each connection type.
- 2 Define one or more enforcement zones.
- 3 Define one or more rule sets, rules, and conditions for compliant systems.

See [Compliance Policy Enforcement on page 53](#) and [Compliance Policy Definition on page 67](#).

6 Set up support and vendor integration

- 1 Define one or more enforcement zones.
- 2 Define enforcement types.
 - Configure Policy Enforcer for VPN connections.
 - Configure Policy Enforcer for a Cisco NAC network environment.
- 3 Create rule sets, rules, and define conditions for compliant systems.

See [Compliance Policy Enforcement on page 53](#) and [Compliance Policy Definition on page 67](#).

7 Audit a compliance policy

- 1 Define *trusted system* rules.
- 2 Identify exception systems.
- 3 Add new rules or edit existing rules and rule sets based on audit results.
- 4 Run the compliance policy as an audit and fine tune policy (e.g. printers).

See [Defining a compliance policy on page 67](#).

8 Enforce the compliance policy

- 1 Access and use Policy Enforcer reports.
- 2 Monitor and tune the enforcement policy.

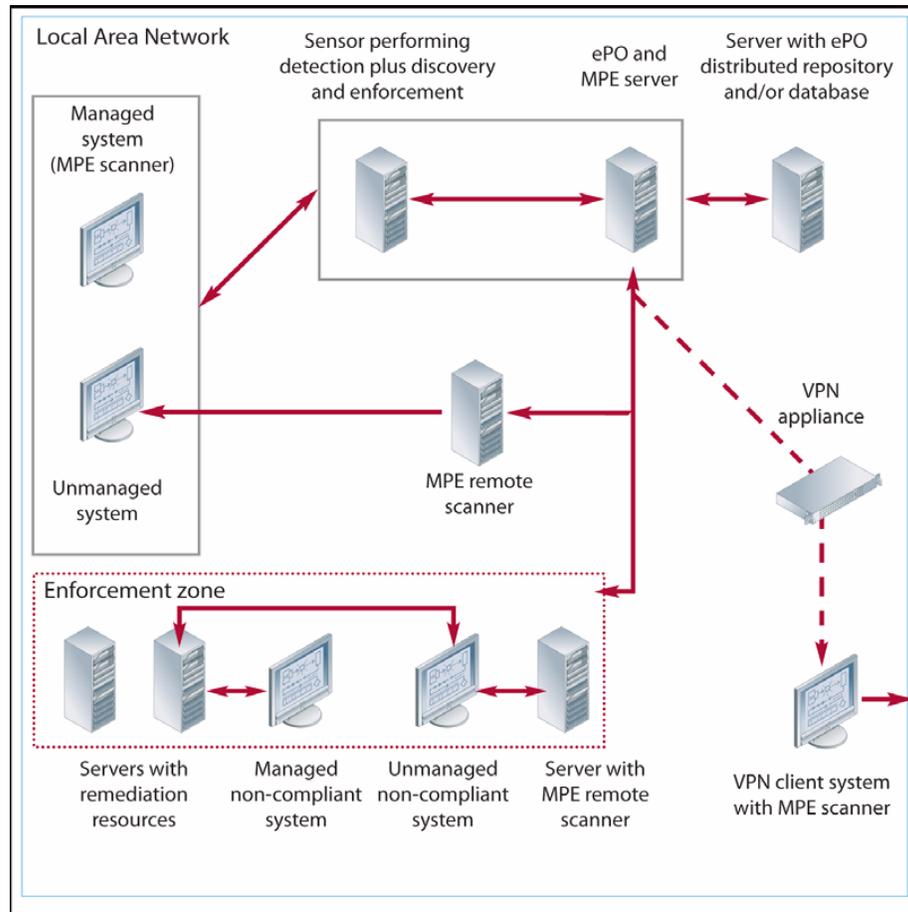
See [Actions, Notifications, Troubleshooting on page 88](#).

Communication flow between MPE components

Figure 2-1 shows the components in a LAN environment, and the communication flow between them.

 Figure 2-1 represents a minimal configuration, and does not represent all possible options. Details about each component can be found in the appropriate sections of this topic.

Figure 2-1 Policy Enforcer components



Systems on the network are detected by sensors. Sensors communicate their findings to the MPE server, which stores the data in the ePO database. If an unmanaged system is detected, the MPE server requests that the nearest remote scanner perform a scan. Local scanners on managed systems send scan results to the MPE server. The server then selects an enforcement action based on policy and configured enforcement mechanisms.

Configuring and managing MPE servers

Configure MPE servers

All MPE server configuration is specified and accessed for the integrated server using the ePO console. Standalone servers are not configured except to specify the ePO database when they are installed.

- 1 In the console tree under **ePolicy Orchestrator** | <SERVER>, select **McAfee Policy Enforcer**.
- 2 On the **Configuration** tab, configure the available pages:

Page name	Settings
Basic Configuration	<ul style="list-style-type: none"> ■ Set user interface parameters ■ Email server designation ■ System classification parameters ■ Ports to check for an ePO agent ■ Sensor parameters ■ Scanner parameters ■ Import and export of compliance policies, exception lists, and automatic responses
Email Contacts	<ul style="list-style-type: none"> ■ Add, edit, or delete email contacts for automatic responses.
External Commands	<ul style="list-style-type: none"> ■ Add, test, and delete external command lines ■ Add, edit, or delete a registered program

MPE server management tasks

Many of the management tasks for the MPE server need to be done only once, if at all, during installation or when specific network configurations change, such as email server settings.

Server management tasks and where to go in the product to do them are listed below. The online Help provides step-by-step procedures and field definitions.

Task	Description	Where to do it
<i>Set up MPE server user accounts</i>	Assign permissions to areas within McAfee Policy Enforcer software.	ePolicy Orchestrator <desired ePO Server> Users tab
<i>Initiate an immediate agent-server communication</i>	Run ePO and MPE tasks immediately.	ePolicy Orchestrator Directory , then select group or computers and right-click to select Agent Wakeup Call
<i>Retrieving and distributing new Policy Enforcer content</i>	Keep Policy Enforcer content up to date.	Use ePO server tasks (see ePO online Help)
<i>Enable email notifications for automatic responses</i>	Required to receive email notifications of noncompliant systems	McAfee Policy Enforcer Configuration tab Basic Configuration Email Server
<i>Define recipients of email notifications</i>		McAfee Policy Enforcer Configuration tab Email Contacts
<i>Purge Event History</i>	Purge nonessential data to maintain system performance.	McAfee Policy Enforcer Events tab Purge All Events

How MPE servers work

The MPE server is the central management component for all functionality of Policy Enforcer. For example, the MPE server makes enforcement and remote scanning decisions based on the results of sensors and scanners.

Systems on the network are detected by sensors. Sensors communicate their findings to the MPE server, which stores the data in the ePO database. If an unmanaged system is detected, the MPE server sends a request to the nearest remote scanner to perform a scan. Local scanners on managed systems send scan results to the MPE server. The server then selects an enforcement action based on policy and configured enforcement mechanisms.

The MPE server works with the ePO server, database, and agent. It manages its functions with the ePO server and ePO console, and stores and manages its data in the ePO database. The MPE server communicates directly with the ePO agent and assigns tasks. You access the Policy Enforcer interface through the ePolicy Orchestrator console.

An MPE server is installed on the a system where the ePO server is installed. This is called the *integrated* server. You can also install one or more *standalone* MPE servers. However, you manage all Policy Enforcer functionality through the integrated server; there is no interface to standalone servers.

Deploying servers in a cluster

Use the Windows Cluster Manager software. The MPE server has no special requirements for deployment in a cluster.

Topics in this section include:

- [Integrated MPE server on page 29.](#)
- [Standalone MPE servers on page 30.](#)

Integrated MPE server

The integrated MPE server is installed on the same system as the ePO server, so both servers share the processing power. The integrated MPE server is always responsible for managing:

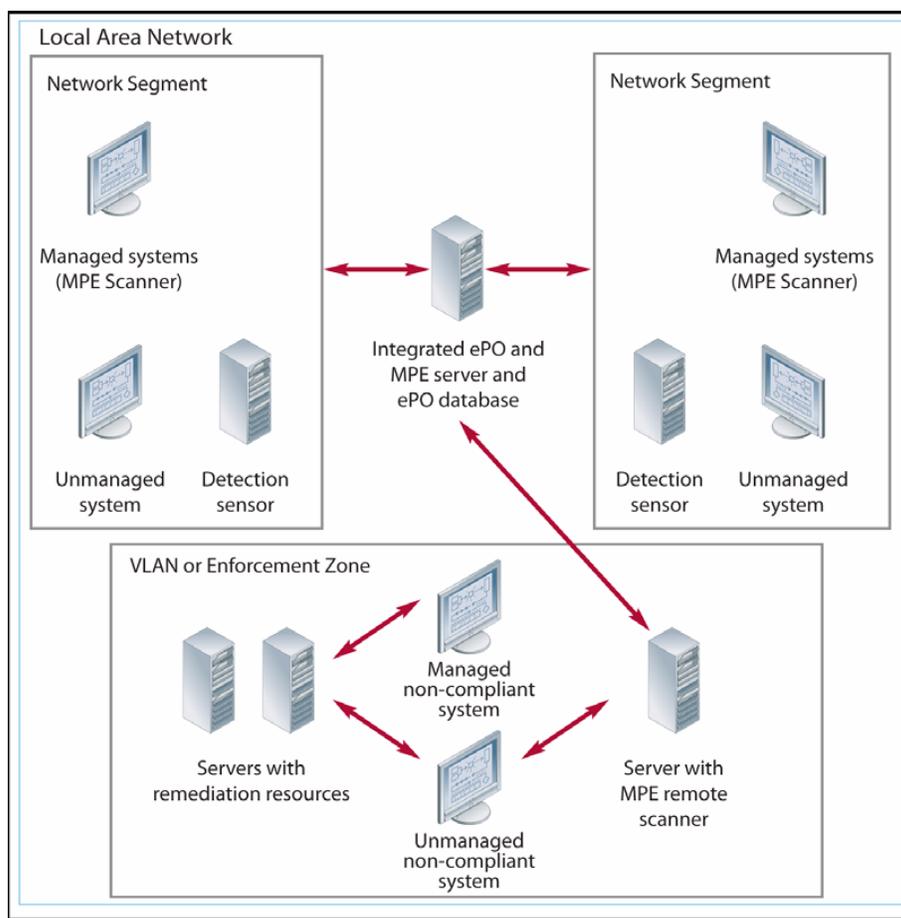
- Status and summary data of systems.
- Event reporting and automatic responses for events and noncompliance.
- The compliance policy for LAN, VPN, and Cisco NAC network connections.
- The configuration of tasks and properties for servers, sensors, and scanners.

Only the integrated MPE server receives content updates. It pulls content only from the ePO central repository.

If the integrated server is the only MPE server you have installed, all sensors and scanners you deploy are managed by, and send their data to, this server. If you have a large network, this can create an unmanageable processing load on a single server. You can distribute the processing load by installing one or more standalone MPE servers, and assigning sets of sensors and scanners to each MPE server.

Figure 2-2 shows a single integrated MPE server with all sensors and scanners in all network segments communicating their data to this one server.

Figure 2-2 Deployment with an integrated server only



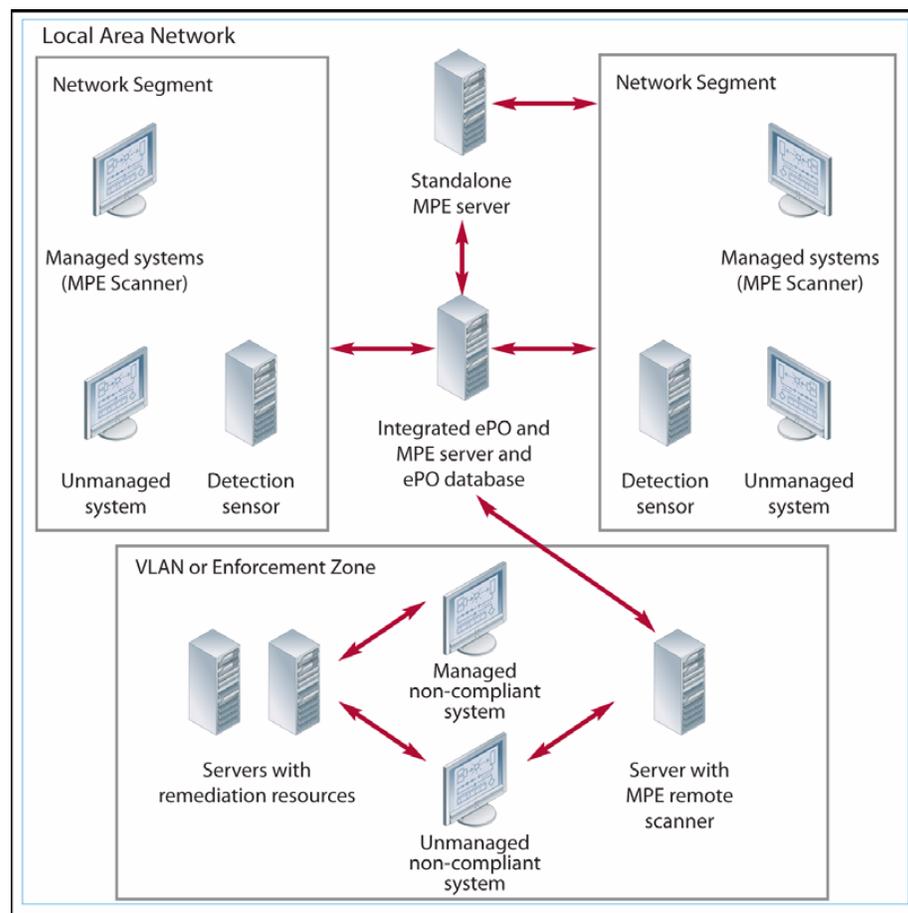
Standalone MPE servers

Standalone MPE servers are installed on host systems separate from the ePO server. Using them distributes network traffic and processing load across multiple systems, and provides configuration flexibility.

Each standalone MPE server manages its own set of sensors and scanners. Any decisions, such as for enforcement and remote scanning, apply only to the sensors and scanners it manages. When deploying sensors and scanners, you designate in the policies which MPE server manages that component. Standalone servers transmit their sensor and scanner data directly to the ePO database.

Figure 2-3 shows that a standalone server can be added to the configuration, and that communications from the MPE distributed components can be directed to specific MPE servers.

Figure 2-3 Deployment with a standalone server



To specify that sensors and scanners report to a particular standalone server, you modify the sensor or scanner configuration policy. See [Configure a scanner policy on page 45](#).

Configuring and managing MPE sensors

Configuring a sensor means to configure a sensor policy to enable the functions you want the sensor to perform. Managing a sensor means to control its installation and performance.

Configure an MPE sensor policy

The sensor policy defines the functionality of an MPE sensor. You can use the default MPE sensor policy as a basis for creating your own policies. The MPE sensor policy is managed using the ePO Policy Catalog. The complete sensor policy is defined by three policy pages: the Global policy page, the Detection policy page, and the Discovery and Enforcement policy page. You then assign the required policies to deployed sensors.

- 1 In the console tree under **ePolicy Orchestrator** | <SERVER> | **Policy Catalog**, select **Policy Enforcer Sensor**. See [Figure 2-4](#).
- 2 Configure the available pages:

Page name	Settings
Global Policies	<ul style="list-style-type: none"> Defines which MPE server manages the sensor. Sets the sensor-to-server communication port. Setting sensor-to-server communication intervals.
Discovery and Enforcement Policies	<ul style="list-style-type: none"> Enabling or disabling topology discovery and mapping. Enabling or disabling switch enforcement. Switch and router discovery and mapping. Switch enforcement. Specifying a starting switch and router. Setting the frequency of topology discovery.
Detection Policies	<ul style="list-style-type: none"> Enabling or disabling the type of detection to use (broadcast, DHCP, or both). Adapter network settings. Reporting settings

The default MPE sensor policy

Policy Enforcer includes a default sensor policy that creates a sensor with the following configuration:

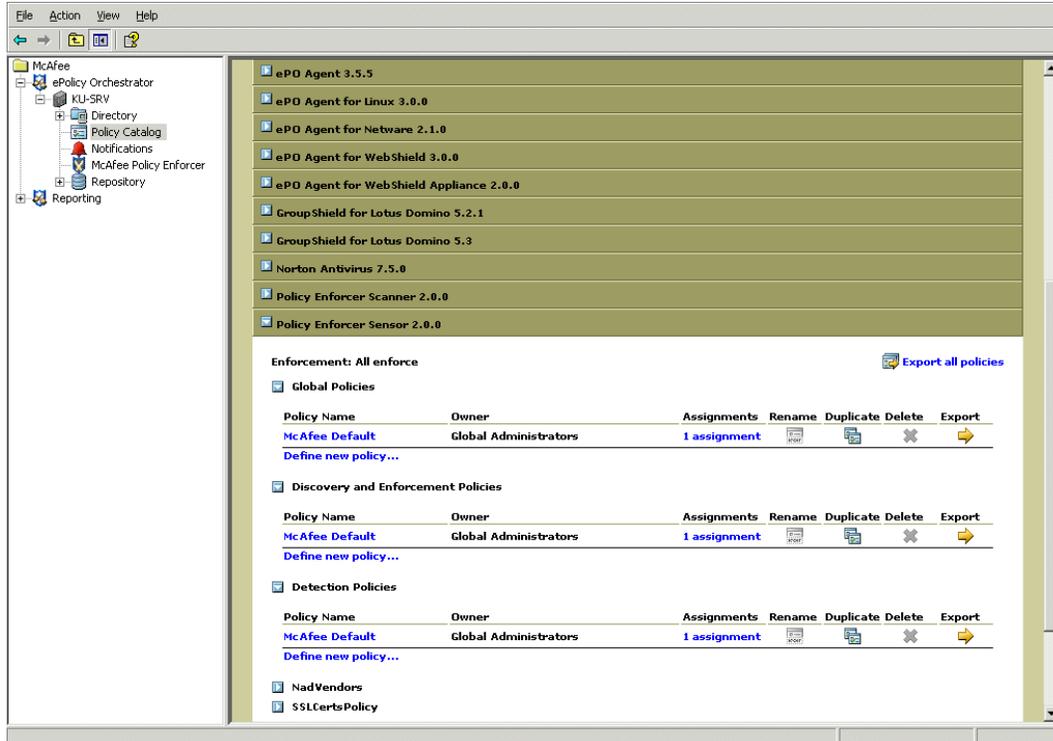
Sensor policy page	Enabled functionality
Global	The sensor reports data to the integrated MPE server, and uses default timing intervals.
Detection	Broadcast and DHCP detection.
Discovery and Enforcement	Topology discovery and mapping. (Switch enforcement is disabled.)

Custom MPE sensor policies

In the sensor policies, you enable the functionality you want the sensor to perform. For example, if you want a sensor to perform topology discovery and mapping, and switch enforcement, but not host detection, you need to create a set of policy pages that enable and disable the appropriate functionality.

You can configure a single sensor to perform all three primary functions (detection, topology discovery and mapping, and switch enforcement). You cannot configure a sensor to perform switch enforcement only because the enforcement functionality relies on the topology data to locate the correct network access device for any specific system.

Figure 2-4 ePolicy Orchestrator | <server> | Policy Catalog | Policy Enforcer Sensor policies



MPE Sensor management tasks

Sensor management tasks and where to go to do them are listed below. The online Help provides step-by-step procedures and field definitions.

Task	Description	Where to do task
<i>Deploying a sensor</i>	Deploy a sensors automatically using the ePO deployment task, or manually to uncovered subnets.	McAfee Policy Enforcer Status tab Subnets List and click Deploy Sensors button. See Figure 2-5 .
<i>Assign a sensor policy</i>	Once you have created one or more sensor policies, you need to assign them to deployed sensors.	ePolicy Orchestrator Directory <select a computer hosting an MPE sensor> Policies tab Policy Enforcer Sensor <select the sensor policy to assign> , then click Edit button.
<i>Associate a sensor with a standalone MPE server</i>	To have a sensor report its data to a standalone MPE server, you must change the server name on the sensor Global policy page.	ePolicy Orchestrator Directory Policy Catalog Policy Enforcer Sensor Global Policies , then define or edit a policy.
<i>Set primary and non-primary sensor options</i>	You can deploy more than one sensor to your network segments so that you have backup in case a sensor becomes non-operational.	ePolicy Orchestrator <SERVER> McAfee Policy Enforcer Configuration tab Basic Configuration Sensor Parameters
<i>Upgrade rogue system sensors to MPE sensors</i>	After installing Policy Enforcer, we recommend upgrading existing rogue system sensors to MPE sensors.	ePolicy Orchestrator <SERVER> McAfee Policy Enforcer Status tab Subnets tab <click a subnet> Subnet Details page Sensors table , then select a rogue system sensor and click Deploy Sensors
<i>Uninstall rogue system or MPE sensors</i>	After installing Policy Enforcer, you can uninstall your rogue system sensors. You might, at times, need to uninstall an MPE sensor.	ePolicy Orchestrator <SERVER> McAfee Policy Enforcer Status tab Subnets tab <click a subnet> Subnet Details page Sensors table , then select a sensor and click Uninstall
<i>View details on switches and ports</i>	You can view all switches and their ports once a sensor has performed an initial discovery and mapping of your network environment.	ePolicy Orchestrator <SERVER> McAfee Policy Enforcer Status tab Switches tab , then select any row. See Figure 2-6 .
<i>Disable UDP port scanning (McAfee Desktop Firewall)</i>	If MPE sensor host computers are running McAfee Desktop Firewall, you must disable UDP port scanning to avoid triggering a UDP port scan.	From Desktop Firewall General Policies page on the Intrusion Detection Settings tab, deselect Port scan (UDP)

Figure 2-5 McAfee Policy Enforcer | Status tab | Subnets List

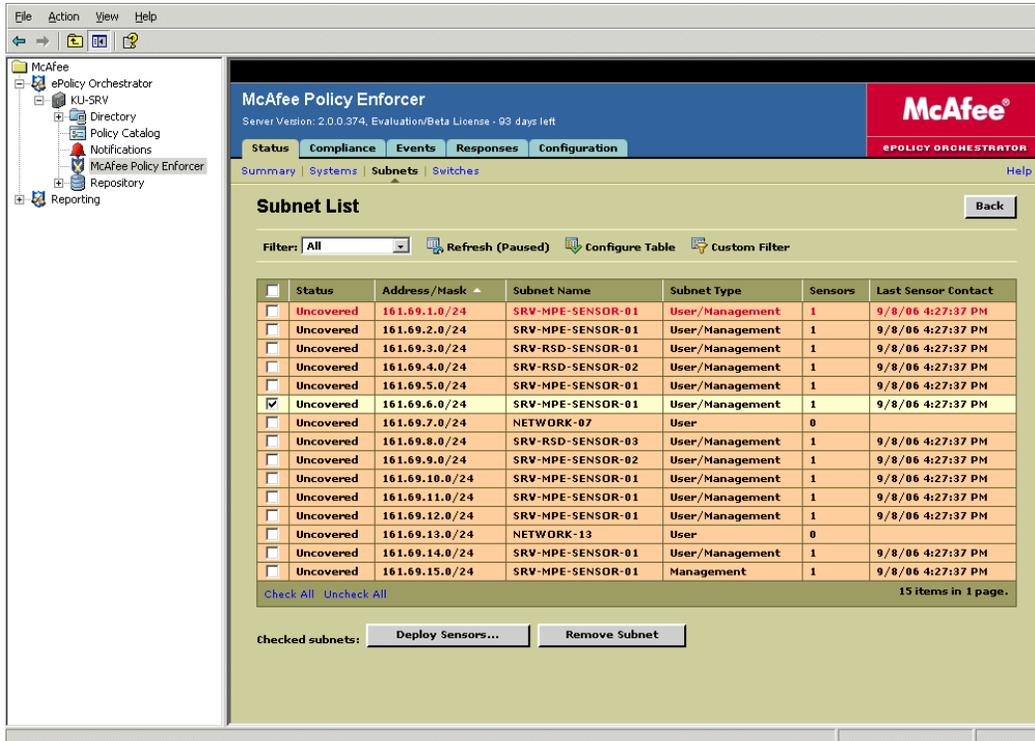
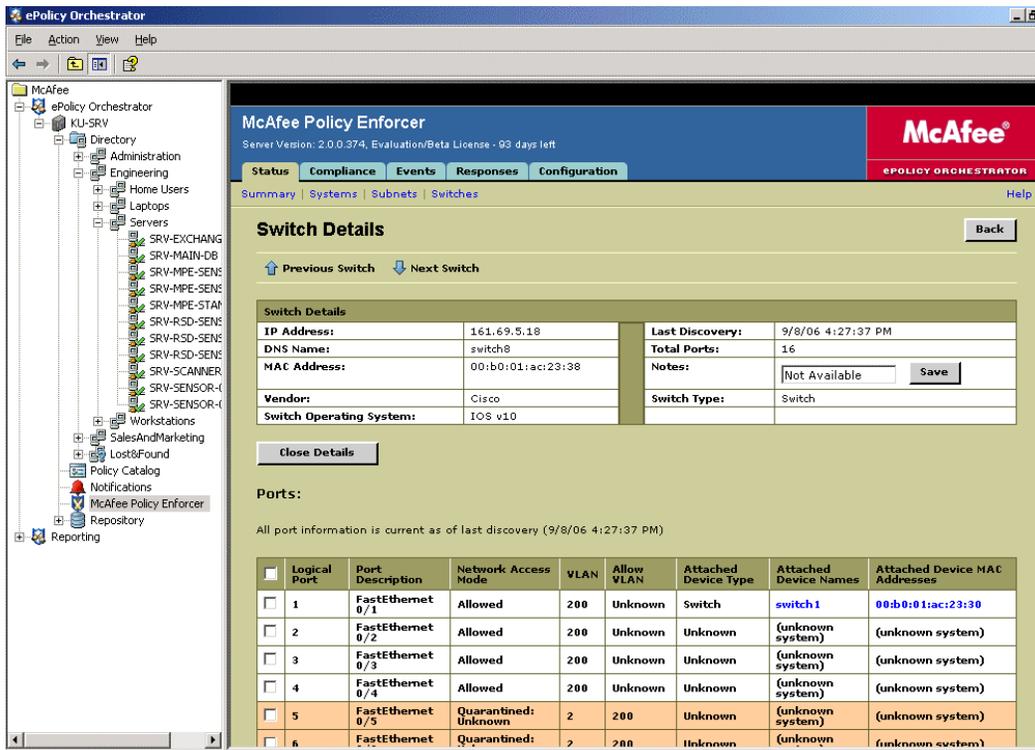


Figure 2-6 McAfee Policy Enforcer | Status tab | Switches tab



How MPE sensors work

The MPE sensor gathers network information by listening to network traffic and querying network access devices. The sensor can detect and map the topology of the network by locating network access devices, host systems, printers, etc., and can dynamically move switch ports onto different VLANs.

The MPE sensor performs these functions:

- **Detection** — Sensors that perform detection identify systems on the network by passively listening to messages from hosts when they request network access. Detection can be based on broadcast messages, DHCP messages, or both.
- **Topology discovery and mapping** — Sensors that perform discovery and mapping identify all switches and routers on the LAN and their relationship to each other. These sensors also find the network location of systems — using network topology data — each time they are detected.
- **Switch enforcement** — Sensors that perform enforcement only affect systems *being scanned remotely*. If a remote scan produces a noncompliant result, the switch port the system uses to access the network is blocked or redirected to a VLAN enforcement zone. The network access mode (allow, quarantine, or drop) of a switch port can be handled manually or automatically in response to an event.

Deploying MPE sensors

MPE sensors can be deployed only to managed systems. Where you deploy a sensor depends on the functions it performs, and to some degree, the topology of your network.

Sensors should be deployed on a server if possible. A sensor always should be available; deploying sensors on non-server machines risks the possibility of no coverage.

When a sensor is first deployed to a system, it has the default sensor policy assigned to it. You can assign sensor policies to each sensor host system from the ePO directory tree.

To deploy sensors, you can use an ePO deployment task, or you can use the Deploy Sensors option of the **Subnet List** screen in the McAfee Policy Enforcer interface. From the **Subnet List**, you can elect sensor host systems manually or automatically, based on specific criteria.

Topics included in this section

- [Associating MPE sensors with standalone MPE servers on page 36](#)
- [MPE sensors vs. rogue system sensors on page 36](#)
- [Primary and secondary sensors on page 36](#)
- [Topology discovery and mapping on page 37](#)
- [Switch enforcement on page 41](#)
- [How detection works on page 41](#)

Associating MPE sensors with standalone MPE servers

You can configure a sensor to report its data to, and be managed by, a specific MPE server. The default sensor Global policy page specifies that sensors using that policy report to the integrated MPE server. To have a sensor report to a standalone MPE server, you must create a new Global policy page that specifies the NetBIOS name or IP address of the standalone MPE server machine, and the port number to use for scanner-to-server and sensor-to-server communication.

Although you can associate both MPE and rogue system sensors with a standalone MPE server, McAfee strongly recommends upgrading all sensors to MPE sensors.

You create, edit, and manage sensor policies by selecting **Policy Enforcer Sensor 2.0.0** under **Policy Catalog** in the ePO console tree.

MPE sensors vs. rogue system sensors

If you are currently using ePolicy Orchestrator Rogue System Detection sensors, you should upgrade these to MPE sensors. All new sensors you deploy should be MPE sensors.

You can continue using existing rogue system sensors for broadcast detection until you want to upgrade them to MPE sensors. However, rogue system sensors only support broadcast detection; they do not support DHCP detection.

After you install the McAfee Policy Enforcer software:

- You can no longer deploy (send and install) rogue system sensors from the ePO console. The **Rogue System Sensor Install** client task along with the rest of the Rogue System Detection interface is removed during the installation.
- You can upgrade rogue system sensors to MPE sensors.
- You can uninstall rogue system sensors from the **Subnet Details** page or manually.

Primary and secondary sensors

If multiple sensors are installed in a subnet, you can enable primary and secondary sensors for redundancy. When enabled, the server switches between sensors actively gathering and reporting data, called primary sensors, and others that serve as secondary sensors.

There are three sensor parameters that establish primary and non-primary sensors. These are accessed on the **Configuration tab**, then select the **Basic Configuration** page, then scroll to the **Sensor Parameters** section. You select the checkbox to enable, then set the maximum number of sensors that can be primary sensors.

For example, if you set the **Maximum number of primary sensors per subnet** value to 3, and deploy 5 sensors into the subnet, 3 are primary, and the other two secondary. Alternately, if you deploy one sensor to a subnet, and **Maximum number of primary sensors per subnet** is 2, then you only have one primary sensor and no secondary (backup) sensors.

Using the default setup on the **Basic Configuration** tab, the server ensures that, at most, there are no more than two primary sensors in each subnet (the default value of **Maximum number of primary sensors per subnet**). Every 12 hours, primary sensors are replaced by non-primary sensors. If a primary sensor fails to contact the server within the 90 minute sensor timeout (default), the server promotes a non-primary sensor to primary status. In addition, non-primary sensors contact the server every hour to check whether a primary sensor needs to be replaced.

All sensors deployed in a subnet are deployed to separate systems. If you deploy more than the maximum number of primary sensors, which ones become primary initially is decided by the MPE server (based on which sensors report to the server first).

Topology discovery and mapping

Topology discovery identifies all switches and routers on the LAN and their relationship to each other. Topology mapping finds the network location of systems — using network topology data — each time they are detected.

Sensors perform these functions by communicating with network access devices (NADs) using SNMP to determine which systems or devices are connected to each NAD.

Topology discovery identifies all OSI layer 2 network access devices, such as switches on a local area network (LAN), and their relationship to each other. Network topology data is used by topology mapping to quickly find systems. Topology discovery and topology mapping use SNMP to gather data from the network.

The concepts associated with topology discovery and topology mapping are:

- [How topology discovery works.](#)
- [How overlaps are prevented during topology discovery.](#)
- [How often topology discovery runs.](#)
- [How topology mapping works and how often it runs.](#)
- [The boundaries of topology discovery and switch enforcement.](#)

How topology discovery works

To start topology discovery, an IP address of a switch from which to start the process is needed. The sensor can automatically retrieve the IP address of its closest switch using Cisco Discovery Protocol (CDP) or Spanning-Tree Protocol (STP). If CDP or STP is not enabled on switches on the LAN or if you want to manually specify the starting switch, you must provide its IP address. To find a starting Cisco switch automatically, we recommend that CDP is enabled.

In addition, the IP address of the local router (IP default gateway) on the same subnet as the topology discovery and mapping sensor host computer is needed. The sensor uses the ARP cache on the starting router in the discovery process. The sensor can automatically retrieve the IP address of the local router from the default gateway. If no default router is enabled or if you want to manually specify the starting router, you must provide its IP address.

Because topology discovery uses SNMP to gather data from the network, SNMP communities are also needed. At a minimum, you need to provide one read-only community string for all switches and one read-only community string for all routers on the LAN.

Table 2-1 Data needed for topology discovery

Data discovery needs	How data is provided
IP address of starting switch	<ul style="list-style-type: none"> ■ By default, this is automatically retrieved. We recommend that CDP is enabled to find a starting Cisco switch. ■ If CDP or STP is not enabled or if you want to manually specify the starting switch, you must provide its IP address.
IP address of starting router	<ul style="list-style-type: none"> ■ By default, this is automatically retrieved. ■ If no default route is enabled or if you want to manually specify the starting router, you must provide its IP address.
SNMP community for all switches and routers	<p>You must provide this data:</p> <ul style="list-style-type: none"> ■ One read-only community string for all switches on LAN ■ One read-only community string for all routers on LAN

Once the IP address of the starting switch and router are known, the sensor uses a variety of techniques to find the IP address of the next switch. If none of the MAC addresses on a switch port belong to a managed switch or router, topology discovery does not continue beyond this switch port. It is assumed that the port is either connected to a hub, unmanaged switch, or wireless access point, or that the sensor cannot access the switch for some reason, such as an invalid SNMP community. The sensor continues looking for switches in this way until it reaches an OSI layer 3 network access device that connects to non-Ethernet, dial-up, or token ring interfaces.

In addition to finding all layer 2 network access devices, such as switches on the LAN and their relationship to each other, the sensor gathers other pertinent data and sends it during the sensor-to-server communication interval. This data includes the following:

- IP address and MAC address of each switch.
- Network access mode of each switch port (allowed, quarantined, or dropped).
- Current VLAN value assigned to each switch port.
- MAC address of each system connected to these switches.
- All subnets known to the local router.

How overlaps are prevented during topology discovery

Topology discovery is performed concurrently by — at most — one sensor on each subnet. If all switches and routers on the LAN use common SNMP communities, you need only one discovery and enforcement sensor per physical site.

If switches and routers on the LAN use multiple SNMP communities, you need one discovery and enforcement sensor for each set of unique community strings. In this case, McAfee recommends a maximum of one sensor per subnet to reduce network traffic and prevent the possibility of multiple sensors performing discovery on the same subnet. However, it is strongly recommended that you change the SNMP community on switches and routers to use common strings.

The MPE server prevents sensors from discovery on the same subnet. It does this by using data that the sensor sends when it starts discovery and when it reaches a layer 3 network access device that connects to non-Ethernet, dial-up, or token ring interfaces.

How often topology discovery runs

By default, topology discovery begins immediately following sensor installation. It then repeats every 24 hours. You can change this frequency at which it runs. See [Configure an MPE sensor policy on page 31](#).

How topology mapping works and how often it runs

Topology mapping uses the network topology data in the ePO/MPE database to find systems quickly. Mapping runs every time a new system is detected or whenever an action is taken on a system. The MPE server provides hints to the sensor on the most likely places to look for the system. These mapping hints are the IP addresses of switches:

- Switch where the system was last seen (if it was previously detected).
- Root switch on the LAN.

The sensor uses SNMP queries to find a port on these switches where the MAC address of the newly detected system is the only MAC address assigned to the port.

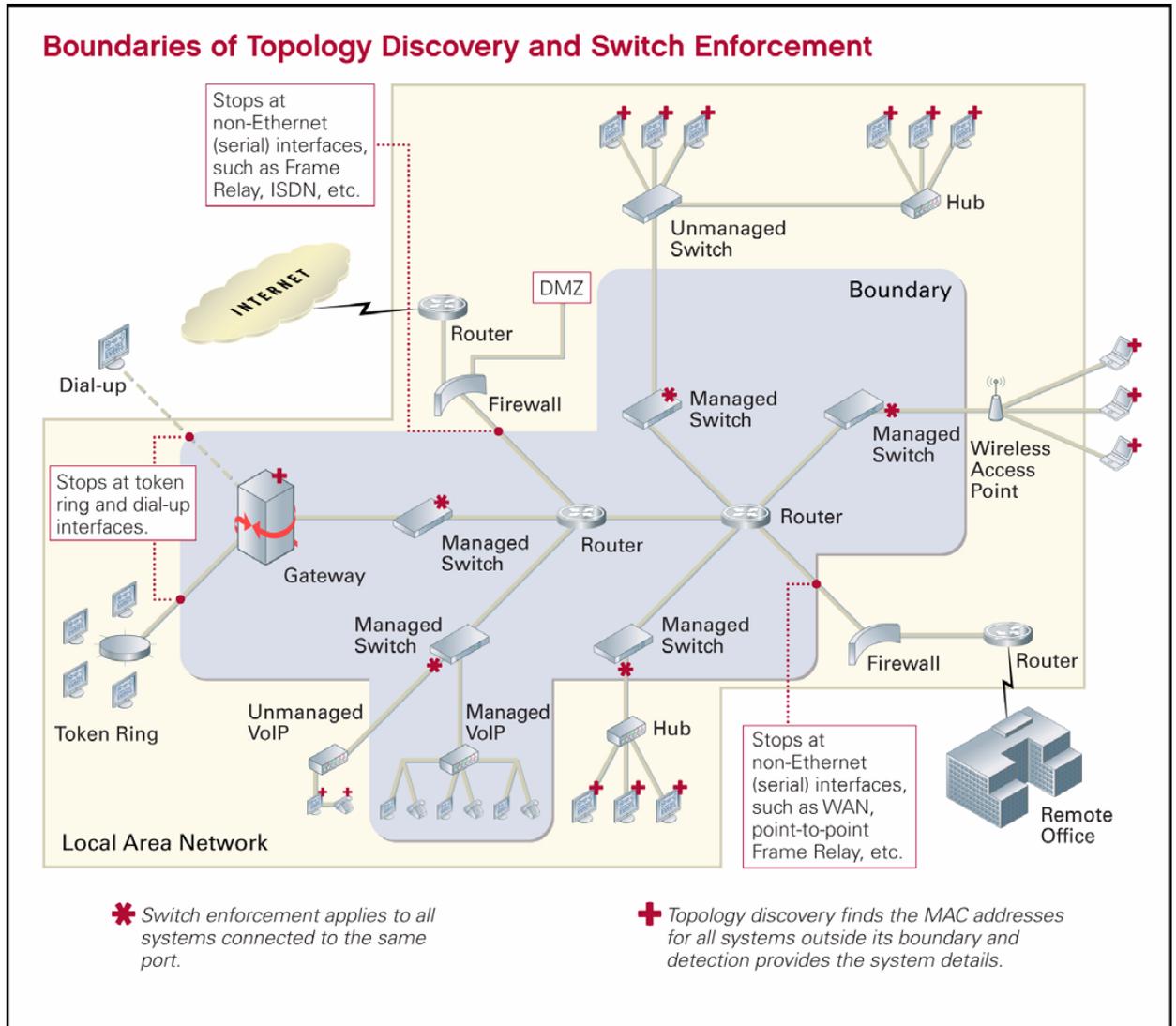
If the system cannot be found, the sensor uses network topology data to systematically find the system, starting with the nearest switch. The sensor queries each switch until it finds a port where the MAC address of the newly detected system is the only one assigned to the port, or when the discovery process is exhausted. The sensor then sends updated topology discovery data to the server.

The boundaries of topology discovery and switch enforcement

Although topology discovery has the same boundaries as switch enforcement, it finds the MAC addresses of systems outside its boundary. Detection provides the remaining system details.

Because switch enforcement applies to the port, changing the network access mode (allow, quarantine, or drop) affects all systems connected to the same port regardless of their compliance status. By default, network access mode is changed only when one system is connected to a switch port.

Figure 2-7 Boundaries of topology discovery and switch enforcement



How topology and mapping data is used

Once topology discovery and mapping runs initially, the **Switch List** page displays all the switches that were found. See [Figure 2-6 on page 34](#). Using the **Switch Details** page, you can get details about a switch and see all the systems connected to it. You can then quarantine or allow (or drop) systems directly by using the options on this page. This can be done at any time, but is useful if you are not yet ready to enforce a compliance policy on your network.

Switch enforcement

The MPE sensor switch enforcement functionality must, at a minimum, be combined with a sensor that performs topology discovery and mapping. The enforcement function of an MPE sensor is responsible for configuring the network connectivity of unmanaged systems. Its primary function is to move host systems to new or different VLANs by controlling the VLAN assignments of individual switch ports.

For sensors that perform enforcement, you need to have the read-write community string for all switches on the LAN. For more information, see [Topology discovery and mapping on page 37](#).

How detection works

Sensors perform host detection by listening to ARP broadcasts and DHCP requests. The information in these messages is used to associate a system's MAC address with an IP address. You can configure detection using broadcast only, DHCP only, or both broadcast and DHCP. Because there is no overhead associated with using both detection methods, McAfee recommends that you enable both broadcast and DHCP detection for all sensors that are performing host detection.

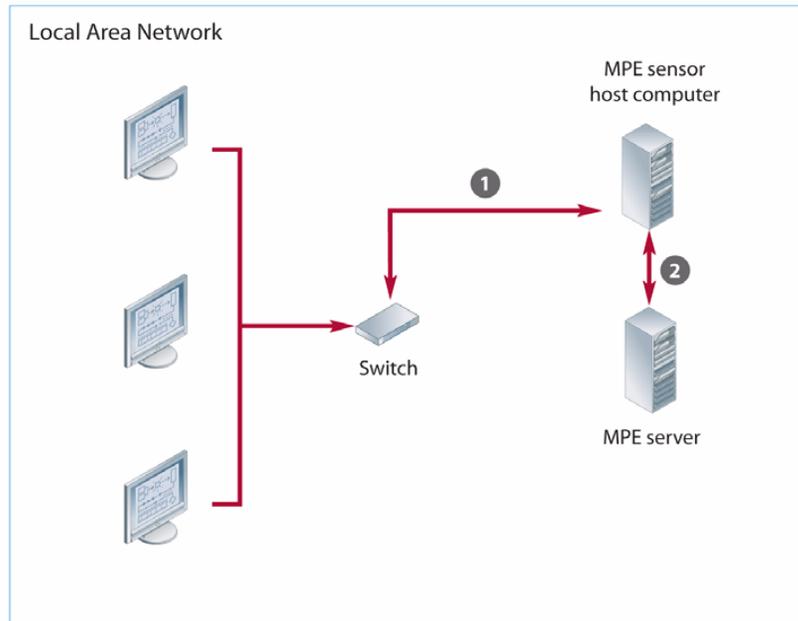
This section describes:

- [Broadcast detection](#)
- [DHCP detection](#) using Windows and non-Windows servers.

Broadcast detection

Broadcast detection finds systems with static or dynamic IP addresses within one subnet. The sensor detects new systems when they request access to or communicate on the network by capturing broadcast packets. The ePO RSD sensor can only detect systems using broadcast detection.

Figure 2-8 Broadcast detection



- 1** The sensor captures broadcast packets to detect new systems.
- 2** The sensor sends the detection message to report new systems.

MPE server

- Can be integrated or standalone.

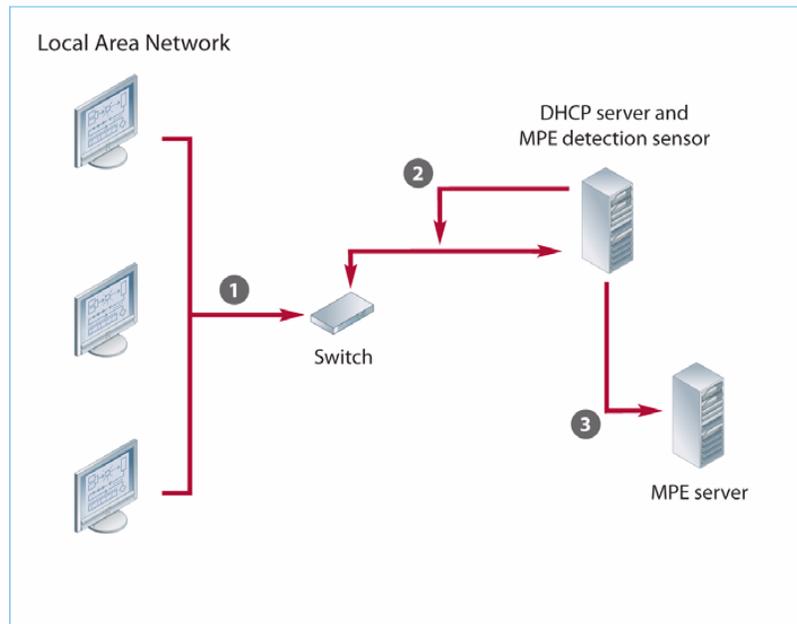
MPE sensor

- Sensor configured for broadcast detection.
- One per subnet (required).
- Managed system (required).
- Server (recommended).

DHCP detection

DHCP detection finds systems with dynamic IP addresses assigned by the DHCP server. The sensor detects new systems when they request access to or communicate on the network by capturing DHCP responses. DHCP detection requires only one sensor per physical site or DHCP server. The ePO RSD sensor can only detect systems using broadcast detection.

Figure 2-9 DHCP detection using a Windows DHCP server



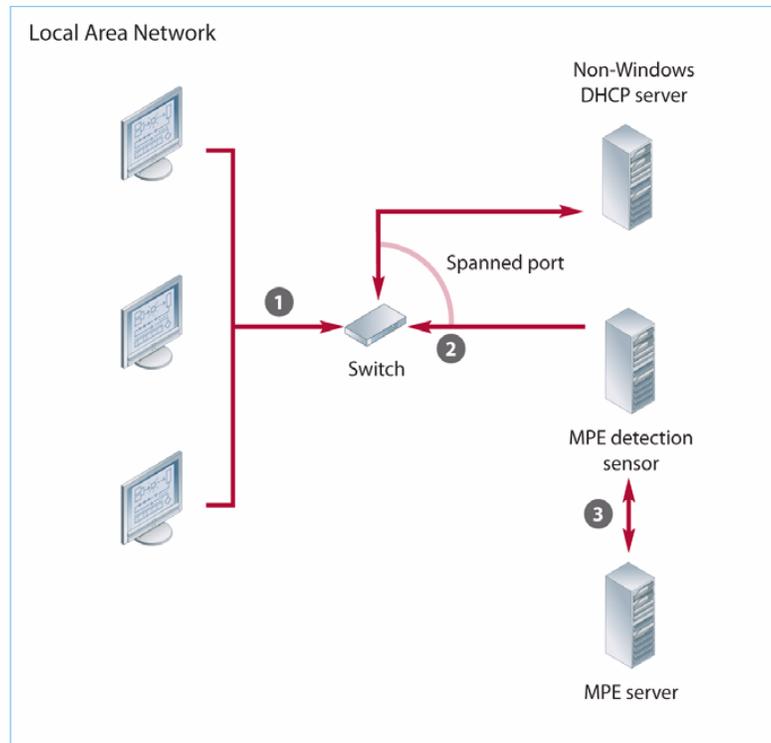
- 1 Requests network access to obtain an IP address.
- 2 Sensor captures DHCP response to identify new systems.
- 3 Sensor sends detection message to report new systems.

MPE server

- Can be integrated or standalone.

MPE sensor

- Sensor configured for DHCP detection.
- One per physical site or DHCP server.
- Managed system (required).
- Co-locate with topology discovery and mapping sensor (recommended).

Figure 2-10 DHCP detection using a non-Windows DHCP server

- 1 Requests network access to obtain an IP address.
- 2 The sensor captures DHCP response from the spanned port to identify new systems.
- 3 The sensor sends the detection message to report new systems.

MPE server

- Can be integrated or standalone.

MPE sensor

- Sensor configured for DHCP detection.
- One per physical site or DHCP server.
- Managed system (required).
- Co-locate with topology discovery and mapping sensor (recommended).
- Server (recommended).

Configuring and managing scanners

Configuring a scanner means to configure a scanner policy to enable the functions you want the scanner to perform. Managing a scanner means to control its installation and performance.

Configure a scanner policy

Scanners are configured by a scanner policy. Before deploying scanners throughout your network, you must configure their attributes by creating one or more scanner policies.

- 1 In the console tree under **ePolicy Orchestrator** | <SERVER> | **Policy Catalog**, select the **Policy Enforcer Scanner** policy. See [Figure 2-11](#).
- 2 Select **Scan Policies** and configure scanner functionality. See table below for descriptions of policy settings. See [Figure 2-12](#).

Scanner configuration tasks

Task	Description
Configuring a scanner policy	Scanner policy configuration includes: <ul style="list-style-type: none"> ■ Associating a scanner with a standalone MPE server. ■ Enabling or disabling remote scanning. ■ Specifying the administrator credentials to use for remote scanning. ■ Enabling or disabling continuous compliance scanning. ■ Specifying the time interval for continuous compliance scanning. ■ Enabling or disabling self-enforcement. ■ Designating the list of servers that can be accessed by a quarantined system for remediation.
Creating a custom scanner policy	Creating a custom scanner policy involves saving a default policy page with a new name and description, and modifying the option settings. You can create as many custom policy pages as you require.

There is also a scanner parameter that is part of the MPE server configuration. This parameter specifies how many days to wait before purging scan results (local and remote) from the ePO database. See the Basic Configuration page information in [Configure MPE servers on page 27](#).

Figure 2-11 ePolicy Orchestrator | <server> | Policy Catalog | Policy Enforcer Scanner | Scan Policies

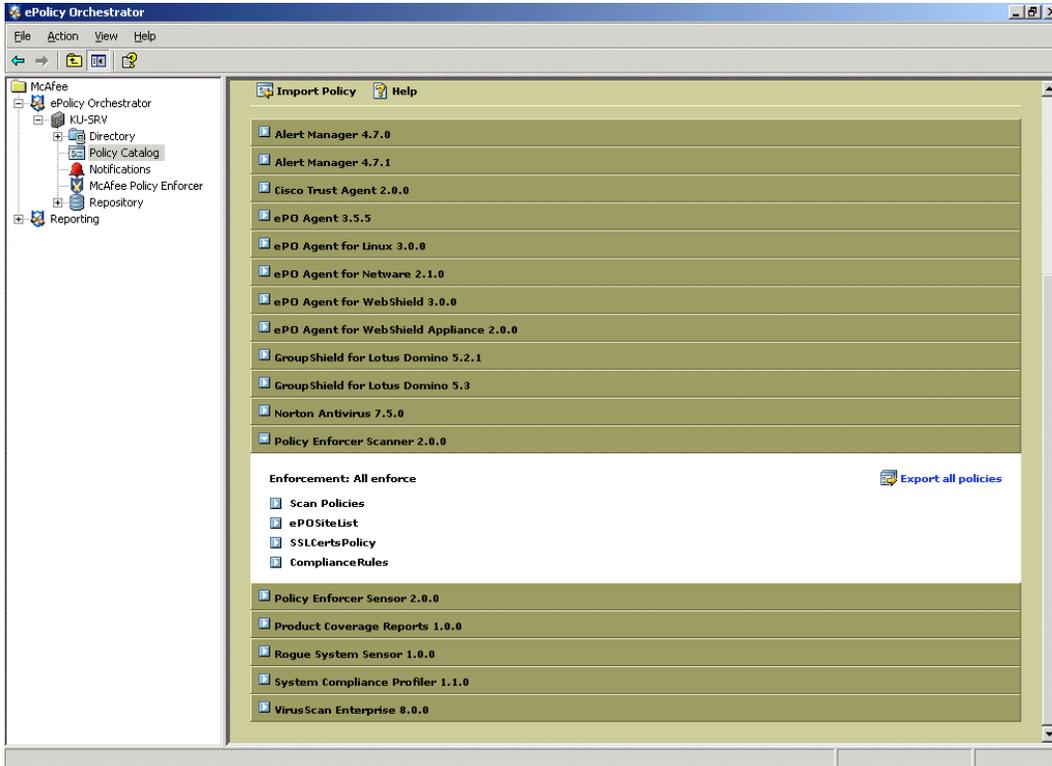
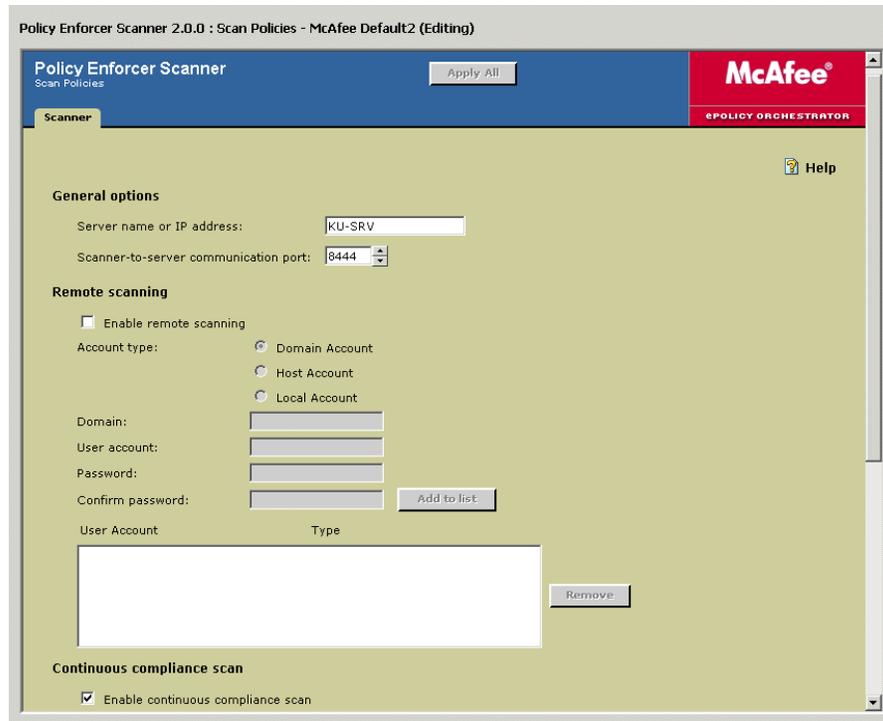


Figure 2-12 Policy Enforcer Scanner Scan Policies page



The default scanner policy

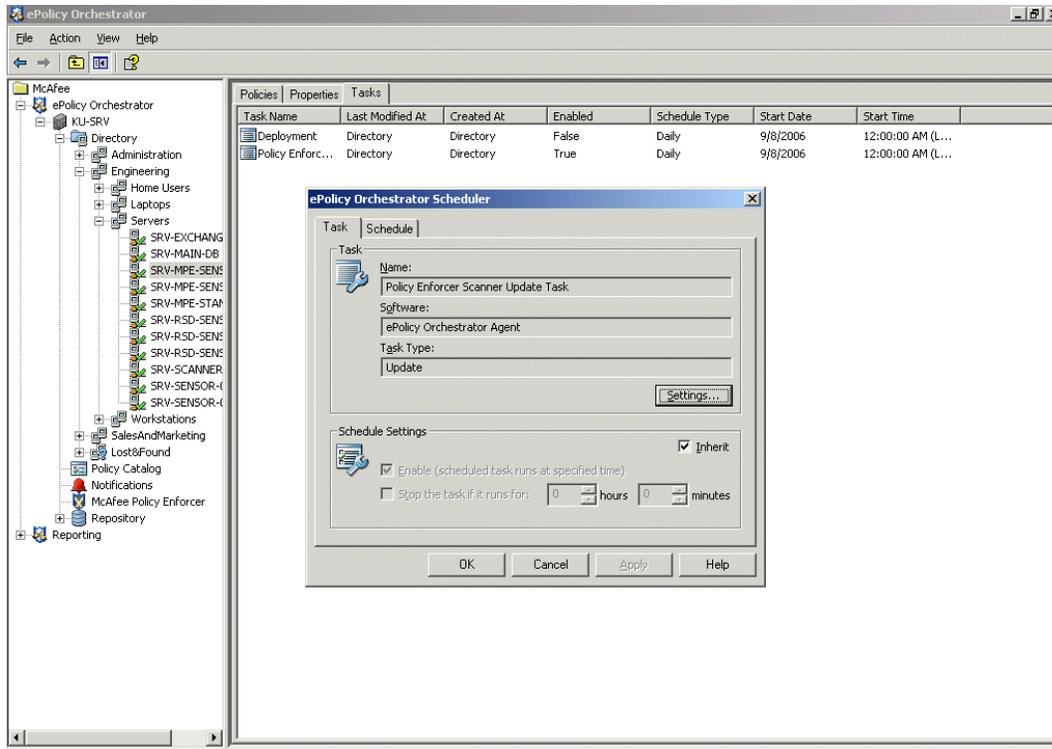
McAfee Policy Enforcer software includes a default scanner policy you can use “as is” or use as the basis for creating your own scanner policies. The default scanner policy enables the following functionality:

Enabled by default	Description
Self-enforcement	Noncompliant systems with an MPE scanner installed use self-enforcement.
Continuous compliance	The scanner rescan its host system once per day.
MPE server	The scanner reports data to the integrated MPE server.

Scanner management tasks

Scanner management tasks and where to go to do them are listed below. The online Help provides step-by-step procedures and field definitions.

Task	Description	Where to do task
<i>Deploying a scanner</i>	Deploy scanner using the ePO deployment task, command-line options, or using the scanner Setup program.	ePolicy Orchestrator Directory <select a computer hosting an MPE scanner> Tasks tab, then double-click Deployment and click the Settings button. See Figure 2-13 .
<i>Assign a scanner policy</i>	Once you have created one or more scanner policies, you need to assign them to deployed sensors.	ePolicy Orchestrator Directory <select a computer hosting an MPE scanner> Policies tab Policy Enforcer Scanner <select the scanner policy to assign>, then click Edit .
<i>Change the default scanner update client task</i>	The Policy Enforcer Scanner Update Task is created by default to ensure that you always have the most current McAfee Policy Enforcer content. This task updates all check packages on managed computers daily at 12 A.M.	ePolicy Orchestrator Directory <select a computer hosting an MPE scanner> Tasks tab, then double-click Policy Enforcer Scanner Update Task and make changes.
<i>Optimizing scanning</i>	You can optimize scanner performance on systems running older operating systems and when scanning a large number of remote systems.	Change specific registry settings on the scanner host computer. See online Help.
<i>Uninstall a scanner</i>	Regardless of how they were installed, you can uninstall scanners using the ePO Deployment task.	ePolicy Orchestrator Directory <select a computer hosting an MPE scanner> Tasks tab, then double-click Deployment and remove the scanner.

Figure 2-13 ePolicy Orchestrator | Directory | <select a computer> | Tasks tab | Deployment

How MPE scanners work

MPE scanners are responsible for assessing the compliance of systems on the network, both locally and remotely. The MPE scanner can be installed only on managed systems. Whether a system has the MPE scanner installed determines how it is scanned (local or remote) and the type of LAN enforcement used (self or switch). Scanners can be configured to perform local scans only or local and remote scans.

McAfee recommends installing the MPE scanner on every managed system. Managed systems with an MPE scanner can perform local scans, which are faster than remote scans and more thorough (they can perform all checks without needing credentials), and can perform self-enforcement. Local scanners also change the network access mode of managed systems based on scan results.

However, not all systems can host an MPE scanner and be scanned locally. Systems running older Windows or non-Windows operating systems, and unmanaged systems must be scanned remotely.

If a managed system does not have the MPE scanner, it cannot conduct a local scan, and cannot initiate self-enforcement. A nearby system with an MPE scanner must perform a remote scan. A remote scan requires credentials to perform certain checks, and uses switch enforcement.

Scanners need to be:

- Configured to perform specific tasks and functions in the scanner policy.
- Deployed to systems throughout your network.

MPE scanner deployment and removal

You can automate the deployment of MPE scanners to managed systems using the ePolicy Orchestrator **Deployment** client task. You can also deploy MPE scanners manually on managed computers from a command prompt or login script using command-line options, or by running the Setup program for the scanner.

If you deploy scanners manually, you must be logged on to the host computer as a local administrator or a member of the **Administrators** group.



If you are deploying scanners to VPN-connected computers using Check Point IPSec VPN, users must restart their computers to complete the scanner installation.

You can uninstall MPE scanners using the ePolicy Orchestrator **Deployment** client task, regardless of the method used to install them.

When are scans initiated?

When?	Description
At system startup.	Applies to local scanners only.
When the scanner service is restarted.	Applies to local scanners only.
When the continuous compliance scan interval is reached.	Applies to both local and remote scanners.
When a system is reconnected to the network or its network adapter changes.	Applies to local scanners only.
When a system is assigned a new IP address.	Applies to local scanners only.
When the MPE server prompts for a scan or rescan.	Applies to both local and remote scanners.
When a scanner receives a new or updated compliance policy.	Applies to both local and remote scanners.
When a system (host) is detected on the network by a sensor.	Applies to both local and remote scanners.

If a scan doesn't complete within 30 minutes, it is cancelled.

Associating scanners with standalone servers

You can configure a scanner to report its data to, and be managed by, a specific MPE server. The default scanner policy page specifies that scanners using that policy report to the integrated MPE server. To have a scanner report to a standalone MPE server, you must create a custom policy page that specifies the NetBIOS name or IP address of the standalone MPE server machine, and the port number to use for scanner-to-server and sensor-to-server communication.

Local scanners

A local scanner is one that scans and assesses the compliance of the system on which it is installed. All scanners you deploy perform local scanning. Scanners that perform local scanning only are typically deployed to all workstations on the network.

Local scanners perform self (host) enforcement if the system is noncompliant. The enforcement decision is made by the scanner and enforced immediately if the system is noncompliant. Self-enforcement is performed through a TDI driver that blocks (and allows) outgoing TCP and UDP connections.

Scan results are sent to the MPE server, which can then initiate a new scan request if there is a new or updated compliance policy.

A local scan is triggered when a machine on the network is turned on, a new compliance policy is received, and/or it requests a network connection. Once the scan is performed, the scanner does not scan that machine again until:

- The network connection changes.
- The next continuous compliance scan interval.
- A “Scan of a System for Compliance” action is requested.
- A new compliance policy is received.

Remote scanners

A remote scanner is one that scans both its own host system (managed) and other systems the MPE server has identified as:

- Being unmanaged (having no ePO agent installed).
- Not having a local MPE scanner installed or functioning properly.

A remote scanner makes no decisions on its own. When an MPE sensor detects a system on the network, that system's information is sent to the MPE server, which determines whether the system is known or doesn't have a local scanner. If the system has a local scanner installed, the server sends a scan request to the system. If the system does not respond, or if no local scanner is installed on that system, the server sends a scan request to the nearest remote scanner.

The remote scanner performs the scan and sends the results to the MPE server. The server then makes any necessary enforcement decisions (Yes or No), and sends that decision to the sensor that discovered the switch.

A remote scanner must be located where it can connect (or have an IP path) to all systems it needs to scan. You also need to have a remote scanner that can access your enforcement zones (VLANs). How many remote scanners you need to deploy depends on:

- The size and configuration of your network.
- How many unmanaged systems need to be scanned.

If there is the possibility of an unmanaged system accessing your network, you should deploy at least one remote scanner. If you are going to quarantine noncompliant systems, you need at least one remote scanner, deployed to a system that can be accessed from your enforcement zones (or quarantine VLANs), to handle rescan requests.

Remote scanners typically are deployed to servers. Although a remote scanner can be deployed to a workstation class system and to a non-server operating system, McAfee recommends following the guidelines specified in the *McAfee Policy Enforcer Installation Guide*.

Using credentials for remote scans

For a remote scanner to access a system, it needs to present administrator level credentials. The credentials you want to use for authenticating a remote scanner are specified in the scanner policy. If you have systems on the network that use different administrator credentials, such as systems in different Windows domains, you can specify multiple sets of credentials in the scanner policy to cover all potential domain situations.

The credentials specified in the scanner policy simply form a list. The scanner tries each set of credentials in turn until it finds one that is valid for any particular system. If a valid set of credentials is not found, a `Scan Failed - credentials error` is returned and reported in the Scan Results column of the Status table.

For information about specifying the credentials for remote scanning, see [Configure a scanner policy on page 45](#).

Using continuous compliance scanning

The continuous compliance scanning feature can be used to ensure that all systems (managed and unmanaged) are scanned at regular intervals. This feature is enabled and the time interval set in the scanner policy.

When a system first requests access to the network, it is scanned for adherence to the compliance policy. If continuous compliance scanning is disabled, once a system has been scanned initially it is only rescanned:

- The next time the system is turned on.
- If the system's network connection changes.

Because users might uninstall required software, install unsupported software, inadvertently infect their systems, or otherwise cause their system to deviate from the compliance policy, you can use the continuous compliance scan interval to ensure that systems are scanned periodically. By default, continuous compliance scanning is enabled and runs every hour.

Continuous compliance scans occur only while systems are connected to the network. When scanning the local computer, a scan is initiated immediately once a network connection is made. When scanning remote systems, a scan is initiated on target systems during the next continuous compliance scan interval.



Continuous compliance scanning applies only to systems on the LAN.

3

Compliance Policy Enforcement

It is necessary to understand how enforcement works before defining your compliance policy.

Topics in this section:

- [How compliance policy enforcement works](#)
- [Enforcement methods](#)
- [Enforcement types](#)
- [Enforcement modes](#)
- [Policy enforcement and enforcement zones](#)

How compliance policy enforcement works

You can enforce a compliance policy for all systems connected to your network (LAN wired and wireless connections, VPN connections, and Cisco NAC connections). Policy Enforcer uses the following enforcement concepts:

- **Enforcement method** — Specifies the physical method for how a system is allowed, restricted, or denied network access. For managed systems with the MPE scanner installed, Policy Enforcer uses a method called self-enforcement (host-based). Self-enforcement is a function of the MPE scanner. Unmanaged systems use a method called switch enforcement. Switch enforcement is a function of the MPE sensor (when the sensor's **Enforcement** option is enabled).
- **Enforcement type** — Specifies the network connection type (LAN, VPN, NAC, etc.) used by a particular system. A compliance policy consists of one or more rule sets (see [Chapter 4, Compliance Policy Definition](#)). Each rule set can designate one or more enforcement types to which it applies. For example, you could define an anti-virus rule set and have it apply only to the LAN and VPN enforcement types, or you could create two anti-virus rule sets and apply one to LAN enforcement and one to VPN enforcement.
- **Enforcement mode** — Specifies how a particular compliance rule set is applied to a noncompliant system. The enforcement modes are Enforce, Audit, or Ignore.

If Policy Enforcer is being used within a Cisco Network Access Control (NAC) enforcement framework, different enforcement methods are employed, and are configured using Cisco's software and components.

Enforcement methods

Policy Enforcer uses two enforcement methods: self-enforcement and network-based enforcement. Whether a system has the ePO agent and MPE scanner installed determines how it is scanned and the enforcement method used. Self- and switch enforcement apply to systems that connect via LAN.

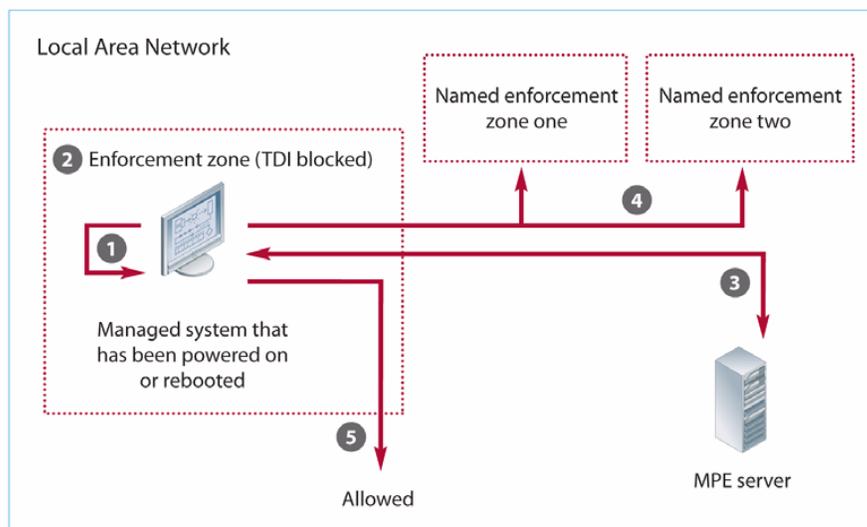
Systems that connect to your network via VPN must be managed systems, and enforcement is performed by the VPN vendor's software and hardware. Policy Enforcer assesses the compliance of VPN connected systems, and can either allow or drop the system. For details, see [VPN enforcement on page 59](#).

For systems that are controlled by the Cisco NAC enforcement framework, enforcement is performed by the Cisco NAC components. Policy Enforcer can be used to assess compliance, but the NAC components control access enforcement decisions. For details, see [Cisco NAC enforcement on page 60](#).

Self-enforcement

Self-enforcement (sometimes called host enforcement) is used on systems that have the ePO agent and the MPE scanner installed. These are called *managed systems*. The MPE scanner always scans the system it is installed on, which is called *local scanning* or *assessment*.

Local scanners perform self-enforcement if the system is noncompliant. The enforcement decision is made by the scanner and enforced immediately. Self-enforcement is performed through a TDI driver that blocks (and allows) outgoing TCP and UDP connections. [Figure 3-1](#) shows the self-enforcement process.

Figure 3-1 Local scanning and self-enforcement

- 1 When a network connection is requested, the local scanner initiates a scan.
- 2 During a boot of the system and until compliance has been determined, the managed system is placed in the default enforcement zone. If a system is already connected to the LAN, the system is not placed in an enforcement zone until it is scanned and found noncompliant.
- 3 Scan results are assessed. If a newer compliance policy is available, the scanner receives a rescan request.
- 4 If the managed system is noncompliant, it is quarantined to the appropriate enforcement zone as defined by the remediation list.
- 5 If the managed system is compliant, it is given full network access.

When self-enforcement occurs on a non-compliant system, the noncompliance message of the failed rule is displayed. The noncompliance message provides information about the failed checks, and any information you decide to include, such as a URL to the remediation portal.

If a managed system is quarantined, the resources it can access while in quarantine are determined by the combined remediation lists of the scanner policy and the enforcement zone. For details, see [Quarantining managed systems on page 65](#) and [The remediation list on page 81](#).

There are two possible scenarios when a scanner assesses a managed system:

- A system that has been turned off then turned on is immediately restricted to the network resources defined by the remediation list of the scanner policy. The scan occurs and allows the system access or puts it in an enforcement zone.
- A system that has been logged off (not turned off) is in the same state as it was based on the last scan. When the next scan happens, the system's state is not changed just because it is being scanned. If it fails the next scan, it is quarantined appropriately.

Overriding self-enforcement

The scanner policy has a “Self-enforcement” section. If you disable self-enforcement, the scanner sends its compliance assessment to the MPE server, and the server carries out the actions for switch enforcement. The behavior is exactly as if the system had been scanned remotely.

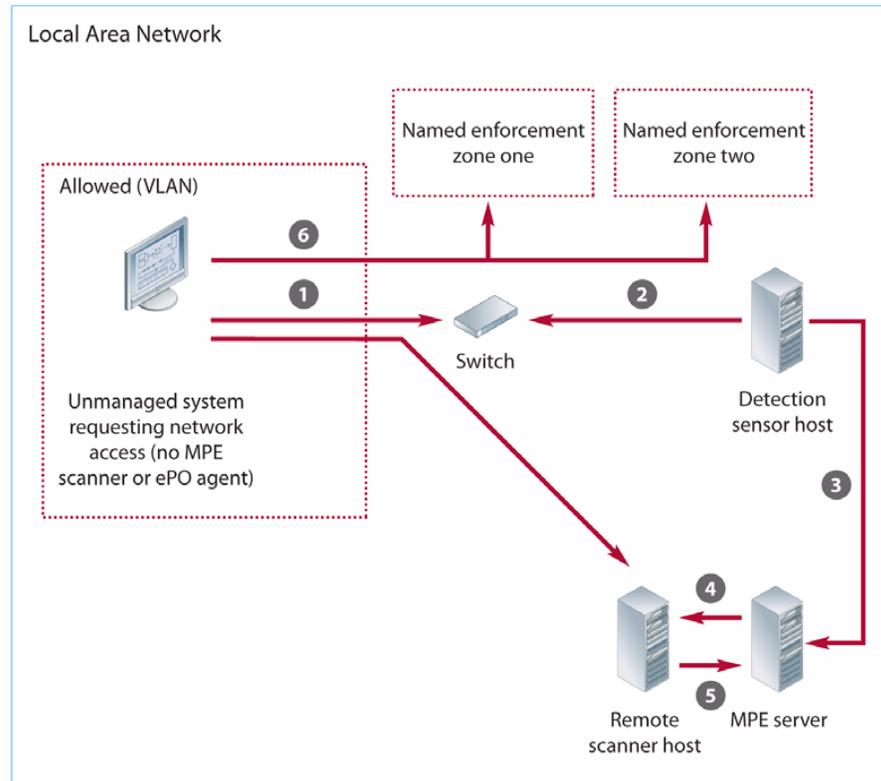
The self-enforcement override is part of the scanner policy, so it is imported and exported using the **Import/Export** buttons in the policy catalog.

Switch enforcement

Switch enforcement is used on systems where self-enforcement has been turned off. These are called unmanaged systems. An unmanaged system must be scanned by a remote scanner, or alternately, the user can download the on-demand ActiveX scanner.

When an unmanaged system is determined to be noncompliant, enforcement of the compliance policy is performed at the switch. When you configure an enforcement zone, you designate the VLAN used for switch enforcement.

When switch enforcement occurs on an unmanaged system that is noncompliant, the noncompliance message of the failed rule is not displayed unless the ActiveX scanner is used. If the unmanaged system is quarantined, it only has access to the remediation resources defined for the enforcement zone (see [Quarantining unmanaged systems on page 66](#)). Users of noncompliant unmanaged systems must be redirected to the remediation portal (see [Accessing the remediation portal on page 81](#)).

Figure 3-2 Remote scanning and switch enforcement

- 1 Unmanaged system requests network access.
- 2 The MPE sensor detects the system either by broadcast or DHCP detection.
- 3 The detection sensor reports the new system to the MPE server.
- 4 The MPE server requests a nearby scanner to scan the unmanaged system.
- 5 The remote scanner scans the unmanaged system and reports the results to the MPE server.
- 6 If the system is noncompliant, it is quarantined to the appropriate enforcement zone.

Enforcement types

Every rule set you define for your compliance policy can be associated with one or more of the available enforcement types:

- [LAN enforcement](#)
- [VPN enforcement](#)
- [Cisco NAC enforcement](#)

This means that you can create separate rule sets for LAN, VPN, and Cisco NAC enforcement, or create a single rule set for all enforcement types.

LAN enforcement

The LAN enforcement type uses the self-enforcement and switch enforcement methods described in [Enforcement methods on page 54](#). Self-enforcement is a function of the MPE scanner. Since any deployed scanner must have local scanning enabled, the scanner always performs self-enforcement on its host system unless the system has been marked as a trusted or exception system or local enforcement has been disabled in the scanner policy.

For each rule set, you specify whether you want it enforced for LAN connections by enabling the LAN enforcement type and setting it as a “selected” enforcement type. In the definition of each enforcement zone, you specify the resources that can be accessed from the enforcement zone for self-enforcement, and the VLAN to use for switch enforcement.

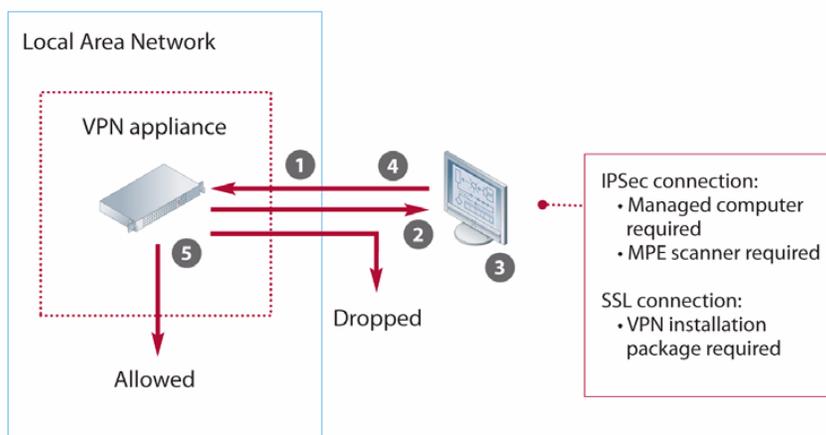
The LAN enforcement type definition also specifies a policy-wide setting for quarantining switch ports when more than one system would be affected. For example, if several systems all gain network access through one switch port and some of them are noncompliant, you have the option of designating whether all of the systems are put into an enforcement zone or not.

VPN enforcement

For VPN-connected systems, the enforcement process is similar to the LAN method except for remediation. Compliance enforcement for VPN-connected systems is jointly controlled by the VPN and Policy Enforcer components. Enforcing compliance is only supported on systems accessing the network using supported VPN vendors.

Figure 3-3 shows the enforcement process for VPN connections. No communication between the client system and the MPE server occurs until after the client is allowed network access. Also, VPN-connected systems are never quarantined by Policy Enforcer. Once a system has been allowed network access through a VPN connection, it is treated like any other managed system. It is scanned and receives policy and content updates at defined intervals.

Figure 3-3 Enforcement for VPN connections



- 1 A VPN client requests network access through a VPN appliance.
- 2 The VPN appliance tells the VPN client to get compliance status.
- 3 The VPN client tells the MPE scanner to scan the system.
- 4 Scan results are sent to the VPN appliance by the VPN client.
- 5 The VPN appliance either allows or drops the connection.

For each rule set, you specify whether you want it enforced for VPN connections by enabling the VPN enforcement type and setting it as a “selected” enforcement type. In the definition of each enforcement zone, you specify a network access mode of Allow or Drop for VPN connections.

Since enforcement zones are associated with rules, if a rule fails and its noncompliance action is set to an enforcement zone, the rule with the most restrictive network access is applied. For more information, see [Configuring and managing remediation on page 77](#).

When you configure the VPN enforcement type, you can specify whether you want Policy Enforcer to build an installation package for the Juniper SSL VPN product. For details, see [Configuring SSL VPN Products on page 110](#).

Cisco NAC enforcement

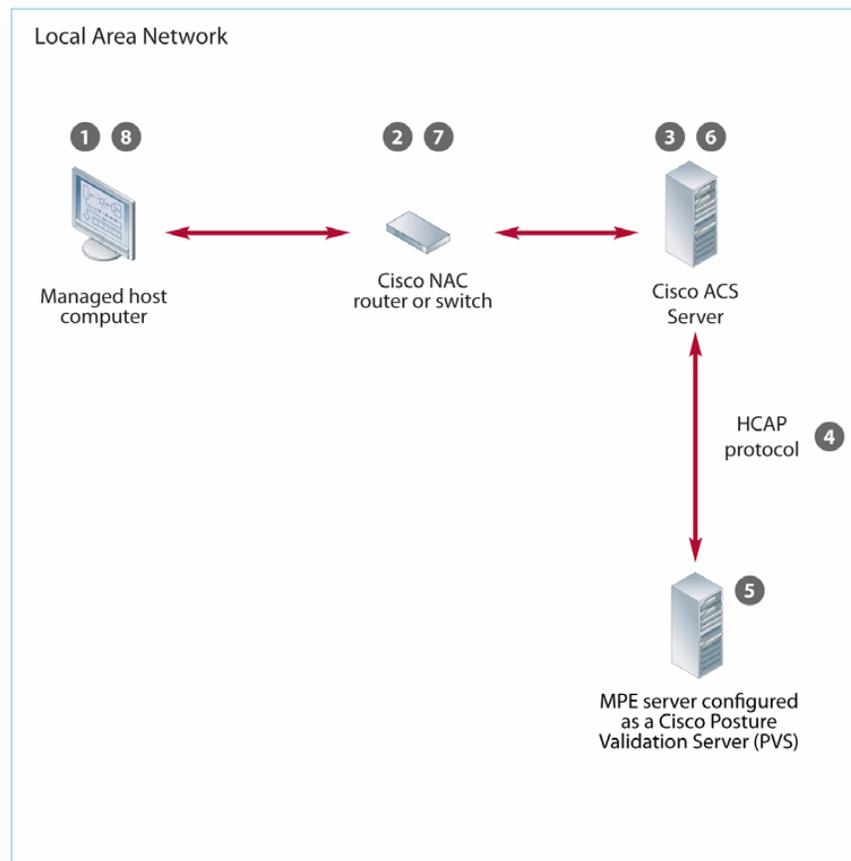
For systems that connect to a network that employs Cisco NAC components, compliance assessment is jointly controlled by both the Cisco NAC and Policy Enforcer components. However, all network access states (enforcement modes) are specified and controlled by the Cisco NAC components (the ACS server). The role of Policy Enforcer is to assess the scan results and send a health level token to the Cisco ACS server.

For each rule set, you specify whether you want it enforced for NAC connections by enabling the NAC enforcement type and setting it as a “selected” enforcement type. In the definition of each enforcement zone, you specify a health level token to send to the Cisco ACS server. If a system in a NAC environment fails a rule, the health level token from the enforcement zone associated with the rule is sent. When you configure the NAC enforcement type, you must provide authentication credentials for the HCAP and GAME protocols.

Managed systems and NAC

The steps in the following list correspond to the numbers in [Figure 3-4](#), and describe the events that occur in the policy enforcement process for managed systems in a Cisco NAC network environment.

Figure 3-4 Managed systems with Cisco NAC connections



- 1 Unmanaged system requests network access.
- 2 The NAD forwards the scan results sent by CTA to the Cisco ACS server.
- 3 The Cisco ACS server communicates the scan results to the MPE server.
- 4 The HCAP protocol is used for communication between the ACS server and the MPE server. The MPE server hosts an HCAP servlet.
- 5 The MPE server, configured as a Cisco Posture Validation Server (PVS), assesses the scan results.
 - If the scan passes, a Cisco NAC health level token of “Healthy” is sent to the ACS server.
 - If the scan fails, the Cisco NAC health level token specified by the enforcement zone associated with the failed rule is sent to the ACS server.
 - For information, see [Policy enforcement and enforcement zones on page 64](#) and [Defining a compliance policy on page 67](#).
- 6 The ACS server accepts the health level token from the MPE server and passes it to the NAD.
- 7 The ACS server sets the access policy for the managed system based on the health level token returned by the MPE server. The NAD applies this policy and passes the token to CTA, which forwards it to the MPE scanner.
- 8 The ACS server sets the access policy for the managed system based on the health level token returned by the MPE server. The NAD applies this policy and passes the token to CTA, which forwards it to the MPE scanner.

If the health level token allows network access or quarantines the managed system, the MPE scanner communicates this state to the MPE server. If the managed system is dropped from the network, the MPE scanner cannot communicate that state to the MPE server.

If the MPE server determines that a managed system in a Cisco NAC environment is not compliant with the MPE compliance policy, the health level token corresponding to the most restrictive access type of any failed rule is returned to the ACS server. For example:

- If the noncompliance action of a failed rule is “Allow,” a Cisco NAC health level token of “Healthy” is sent to the ACS server.
- If the noncompliance action of a failed rule is “Quarantine:Zone XYZ,” the Cisco NAC health level token specified by enforcement zone XYZ is sent to the ACS server.

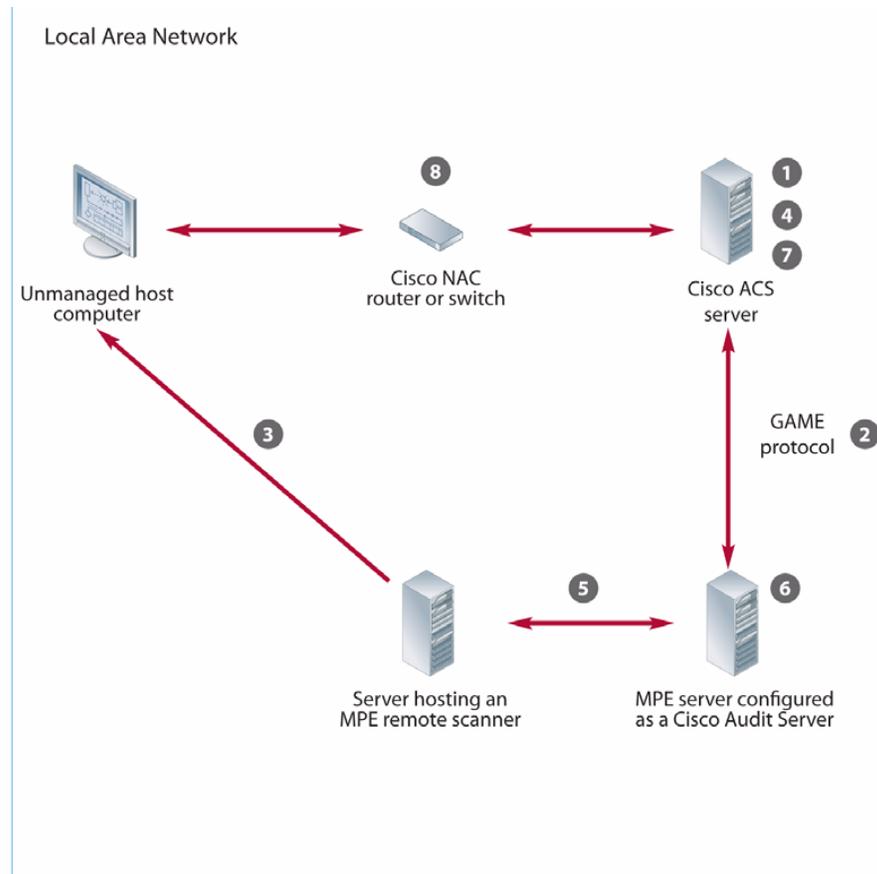
Systems that connect to the network in a Cisco NAC environment are never quarantined by Policy Enforcer. Cisco NAC has its own quarantine mechanism and is based on the ACS server configuration.

For more information about how Policy Enforcer integrates with a Cisco NAC network, see [Chapter 7, Cisco NAC Integration](#).

Unmanaged systems and NAC

The steps in the following list correspond to the numbers in [Figure 3-5](#), and describe the events that occur in the policy enforcement process for unmanaged systems in a Cisco NAC network environment.

Figure 3-5 Unmanaged systems with Cisco NAC connections



- 1** When the Cisco ACS server identifies an unmanaged host system, it requests the MPE server (configured as a Cisco audit server) to perform a compliance check.
- 2** The GAME protocol is used for communication between the ACS server and the MPE server. The MPE server hosts a GAME servlet.
- 3** The MPE server initiates a remote scan of the unmanaged system by sending a scan request to a remote scanner. It also provides the ACS server with an estimate of when it expects to have a compliance decision.
- 4** The ACS server continues to poll the MPE server for a compliance result.
- 5** The remote scanner returns scan results to the MPE server.
- 6** The MPE server sends a Cisco NAC health level token to the ACS server based on the scan results.

- 7 The ACS server accepts the health level token from the MPE server and passes it to the NAD.
- 8 The ACS server sets the access policy for the unmanaged system based on the health level token returned by the MPE server. The NAD then applies this policy.

Enforcement modes

Each compliance rule set you define has an associated enforcement mode. If a system, assessed by a scanner, fails one or more rules that comprise a rule set, the system is considered “noncompliant”. If a system is noncompliant, the enforcement mode specifies whether Policy Enforcer should enforce the rule set, audit the rule set, or ignore the rule set.

When a system is noncompliant, the enforcement modes are applied as follows:

Enforcement mode	Description
Enforce	Policy Enforcer enforces the Network Access Mode specified as the “noncompliance action” of the failed rule or rules. The Network Access mode can either allow the system, quarantine the system to a specific enforcement zone, or drop the system. The Enforce mode should be used after a rule set has been tested (usually in Audit mode) and determined to be ready for your production environment.
Audit	Policy Enforcer does not enforce the Network Access Mode specified as the “noncompliance action” of the failed rule or rules. Compliance violations are reported in the Status information (McAfee Policy Enforcer Status tab in the user interface).
Ignore	Policy Enforcer does not enforce the Network Access Mode specified as the “noncompliance action” of the failed rule or rules, and does not report the status of systems that are not in compliance with the rule set. This rule set is not scanned when this enforcement mode is active.

Policy enforcement and enforcement zones

Enforcement zones provide a means of applying multiple levels of network access for noncompliant systems, based on the degree to which a system does not comply with your network access policy. Enforcement zones are defined from the Enforcement Zones page of the Compliance tab as part of your compliance policy definition. A particular enforcement zone then can be specified as the Network Access Mode assigned to a system that fails a particular rule within your compliance policy.

The way enforcement zones are used by Policy Enforcer depends on the connection type (LAN, VPN, or Cisco NAC).

- Managed systems on the LAN can be quarantined by having their network access restricted to the whitelists of servers defined by the scanner policy and the enforcement zone to which they are confined.
- Unmanaged systems on the LAN can be quarantined at the switch port, and are transferred to a designated VLAN. These systems have access only to the resources available within the particular VLAN.
- Managed and unmanaged systems connecting through a VPN are not quarantined by Policy Enforcer unless LAN enforcement is enabled. In this case, a managed system acts as a client attached to the local LAN. In this instance, the local scanner uses the TDI driver to quarantine itself if it determines that it is noncompliant. For each enforcement zone defined, you specify the VPN access mode (Allow or Drop) for that zone. For details, see [VPN enforcement on page 59](#).
- Managed and unmanaged systems that connect through a Cisco NAC controlled connection are never quarantined by Policy Enforcer. For each enforcement zone defined, you specify a NAC health level for that zone. For details, see [Cisco NAC enforcement on page 60](#).

Enforcement zones are associated with the compliance policy; therefore, the enforcement zone definitions are imported and exported with the compliance policy.

Quarantining managed systems

When a managed system on the LAN is quarantined, that machine is allowed access to:

- The servers specified by the particular enforcement zone to which the machine is restricted.
- The list of servers specified by the MPE scanner policy that has been applied or inherited by that node on the ePO Directory tree. For details, see [The remediation list on page 81](#).

Each rule in a rule set can specify an enforcement zone to apply when a system fails the rule's checks. If a rule checks for specific viruses, the enforcement zone for the rule should be more restrictive (for example, provide access to a single read-only file server and the web server). If a rule checks for patch management products, the enforcement zone for the rule might be less restrictive. For details, see [Defining a compliance policy on page 67](#).

When a managed system is quarantined, that status and the specific enforcement zone is displayed on:

- The Compliance Summary page when the table displays systems using the **By Network Access Mode** filter.
- The System List page.
- The System Details page.

In addition, each named enforcement zone is available as an action when you define an automatic response to an event. For more information, see [Configuring automatic responses](#) in the ePolicy Orchestrator online Help.

Managed systems start in quarantine

When a managed system is rebooted (hard or soft), it starts in a built-in restrictive quarantine that only uses the list of allowed resources from the scanner policy. None of your configured enforcement zones are used until after the first scan of the system has completed.

Quarantining unmanaged systems

Unmanaged systems on the LAN that fail the compliance policy are quarantined at the network switch and transferred to a VLAN. Each enforcement zone definition contains a section where you specify the VLAN number to use for switch enforcement. This applies to LAN enforcement and not for NAC-enforced connections.

This VLAN is used for:

- Noncompliant managed systems whose scanner policy has self-enforcement disabled, and that fail any rule that specifies an enforcement zone as its noncompliance action.
- Noncompliant managed systems with a scanner that fails. These systems are scanned remotely and considered as rogues.
- Noncompliant unmanaged systems that fail any rule that specifies an enforcement zone as its noncompliance action. Unmanaged systems then have access only to the network resources available from the VLAN.

If an unmanaged system fails multiple rules, it is redirected to the VLAN designated by the enforcement zone with the highest priority.

For details, see [Enforcement zone priority on page 66](#).

Enforcement zone priority

Enforcement zones also have a priority, which is used to decide which zone to apply when a system fails multiple rules, and the failed rules encompass more than one enforcement zone. In such cases, the noncompliant system is quarantined to the zone with the highest priority.

Enforcement zone priority is designated by the order they are listed in the Enforcement Zone Priority table on the **Compliance | Enforcement Zones** page. Enforcement zone order goes from most restrictive (first table entry) to least restrictive (last table entry).

Manually quarantining a system or switch port

You can manually quarantine a system or a switch port to a specific enforcement zone from the Systems Details page, the System List table, and the Switch Details table.

To manually quarantine a system:

- 1 Click **Status**, then **Systems** to open the **System List** page.
- 2 In the table, select the systems you want to quarantine.
- 3 In the **Checked Systems** field, select the enforcement zone to use, then click **Apply**.

To manually quarantine a switch port:

- 1 Click **Status**, then **Switches** to open the **Switch List** page.
- 2 In the **Switches** table, click the switch with the port you want to quarantine. The **Switch Details** page is displayed. See [Figure 2-6 on page 34](#).
- 3 In the table, check the port or ports you want to quarantine.
- 4 In the **Checked Ports** field, select the enforcement zone to use, then click **Apply**.

4

Compliance Policy Definition

Topics in this section:

- [Defining a compliance policy](#)
- [How compliance policy definition works](#)
- [How rule sets work](#)
- [Comparing exception systems and trusted systems](#)

Defining a compliance policy

Rule definitions, which are part of each rule set, might require that you have your enforcement zones defined (if you plan on quarantining systems). McAfee recommends that you define your enforcement zones before defining your rule sets.

Follow these tasks to define a compliance policy.

Task	Where to do task
<i>Define enforcement zones</i>	Compliance tab Enforcement Zones , then Add Enforcement Zone or click an existing enforcement zone.
<i>Set enforcement zone priority</i>	Compliance tab Enforcement Zones , then Reorder Enforcement Zones .
<i>Define rule sets</i>	Compliance tab Rule Sets , then Add Rule Set or click a rule set name. See Figure 4-1
<i>Define rules</i>	Compliance tab Rule Sets , click to add or edit a Rule set, then click Add Rule or click a rule name.
<i>Define computer conditions</i>	Compliance tab Rule Sets , then click Add Trusted System rule or click a trusted system rule. See Figure 4-2 .
<i>Define trusted systems</i>	Compliance tab Rule sets page, then click to add or edit a Rule set, then click Add Condition , or change the settings of an existing condition.
<i>Configure enforcement types</i>	Compliance tab Enforcement Types page, then select the enforcement type to configure.

Figure 4-1 McAfee Policy Enforcer | Compliance tab | Rule Sets | Add Rule Set

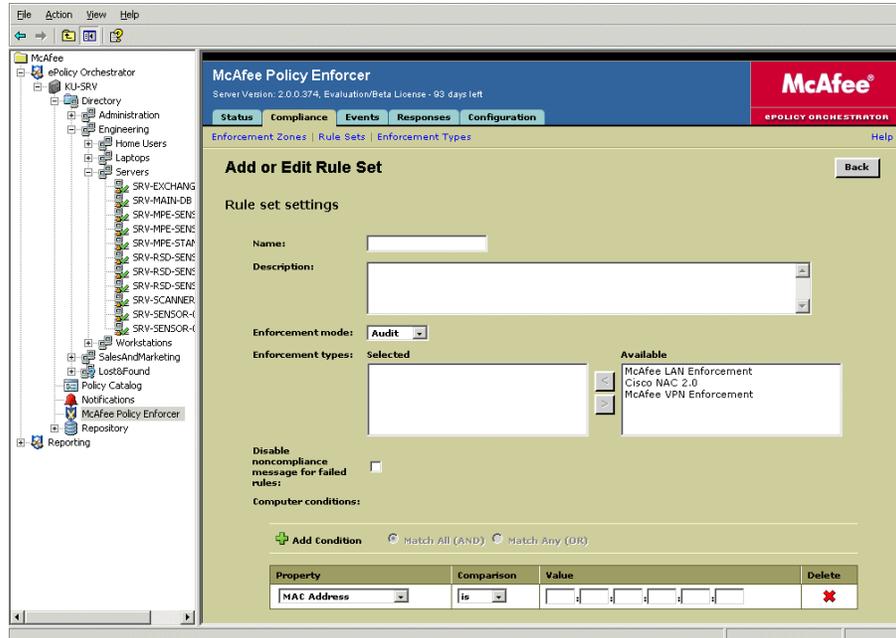
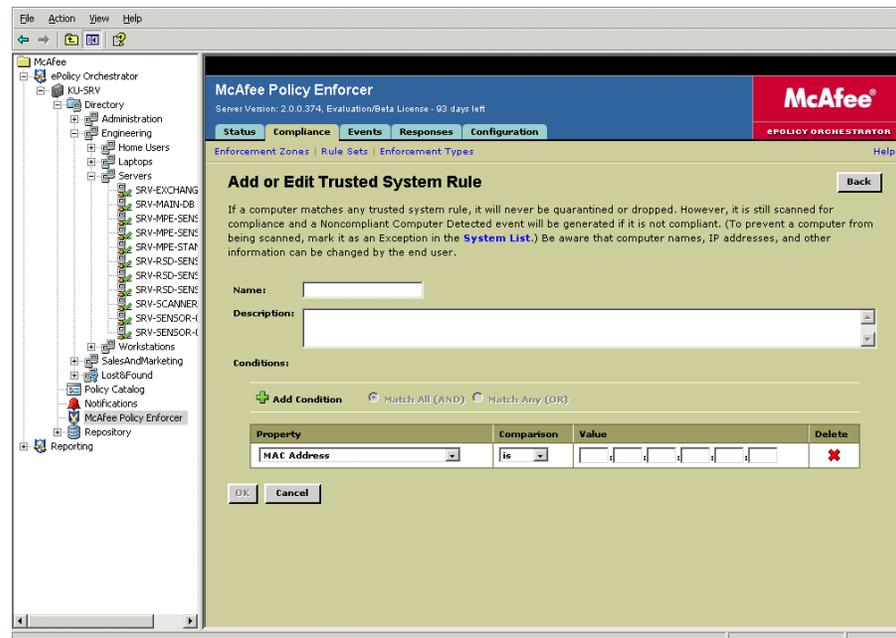


Figure 4-2 McAfee Policy Enforcer | Compliance tab | Rule Sets | Add Trusted System



How compliance policy definition works

The protection of your network is only as good as your definition of compliance. It is important to understand how the compliance policy works before you define it. A compliance policy defines the minimum requirements that systems that must meet to permit full network access.

You define a compliance policy from the **Compliance** tab in the Policy Enforcer interface. Before you begin defining your compliance policy, create one or more enforcement zones, because you will likely specify a quarantine action as a noncompliance response in one or more compliance rules.

A compliance policy is defined by:

Rule sets	An MPE compliance policy is defined by one or more rule sets, each consisting of one or more rules. Each rule specifies which checks are assessed, which operating systems the host system is running, and what do to if a system is not compliant with the rule. Rule sets can be further limited to apply only to specific systems based on various conditions.
Trusted systems	Trusted systems are ones that host critical applications or data that you would not want to have quarantined or dropped by Policy Enforcer. After rule sets are defined, you can designate which systems on your network are trusted. These systems are scanned and the results reported, but the compliance policy is never enforced. This determines, through the interface, whether your critical systems are out of compliance, but not affect their network availability.
Settings for enforcement zones and SSL VPN packages	A compliance policy includes the following settings: <ul style="list-style-type: none"> ■ Define one or more enforcement zones for noncompliant systems. Enforcement zones are associated with the rules in your rule sets, and can be given a priority in case a system fails more than one rule. ■ Designate whether Policy Enforcer should create a build package for any supported SSL VPN products. This package is required and must be installed (uploaded) to the SSL VPN appliance.

How rule sets work

Rule sets are the building blocks of a compliance policy. They are built using the following elements:

- Rules and checks
- Computer conditions

A valid compliance policy must have at least one rule set, but most compliance policies consist of multiple rule sets. For example, you may want a compliance policy to have an anti-virus rule set, a Microsoft Service pack rule set, a firewall rule set, and a threat (infection) rule set. You may also want multiple rule sets of each type that can be applied to specific systems, or have different enforcement types or enforcement modes. Rule sets consist of one or more rules, and rules consist of one or more checks.

A rule set also can be restricted to specific systems or users based on conditions such as an IP Address, MAC Address, DNS Name, user name, etc. For more information, see [Rule set computer conditions on page 71](#).

In addition to rules and computer conditions, a rule set is defined by the following items. See [Figure 4-1 on page 68](#).

- **A name.**
A unique descriptive name that typically specifies the category of rules that comprise the rule set; for example, anti-virus products.
- **A description.**
A descriptive sentence or two that typically identifies the purpose and content of the rule set.
- **An enforcement mode** (Enforce, Audit, Ignore).
A field that specifies whether to enforce the rule set (any failed rules are enforced), audit the rule set (failed rules are reported but not enforced), or ignore the rule set (failed rules are not reported or enforced).
- **An enforcement type** (LAN, VPN, and Cisco NAC).
A field that specifies whether the rule set applies to LAN connections, VPN connections, or Cisco NAC connections. Any combination of these are allowed. For example, a policy defines an anti-virus rule set consisting of separate rules for different anti-virus products, and a rule set of potentially unwanted programs (PUP). Each rule set can be associated with one or more enforcement types. You can apply the anti-virus rule set to all enforcement types, but the potentially unwanted programs rule set applies only to the LAN and Cisco NAC enforcement types.

The rules within a rule set are evaluated independently of one another. If one rule fails, the system is marked noncompliant. If more than one rule fails, the most restrictive access mode of any failed rule is applied.

Rule set computer conditions

In each rule set, you can designate specific computer conditions that restrict the assessment of the rule set. For instance, you can use IP address ranges or DNS names to include or exclude systems from having the rule set evaluated.

One example is assessing compliance on systems operating in a coffee shop or hotel. You can create separate rule sets for conditions when systems are inside or outside the LAN. If the condition is the IP address range, the inside LAN rule set includes the range, and the outside LAN rule set excludes the same range.



The resolution of DNS client names can be intermittent in a Cisco NAC environment. If you need to set computer conditions in a NAC environment, McAfee suggests you use the "Friendly Name" or "NetBIOS Name" of systems rather than the "DNS Name."

How rules work

Rules define a single compliance requirement, consisting of one or more checks from a single check category. Rules consist of:

- A name and description.
- A set of operating systems to which the rule applies.
- The checks that comprise the rule.
- The network access mode to apply to systems that fail the rule.
- A noncompliance message providing remediation instructions that displays on managed systems (this message is displayed when the rule set enforcement mode is set to Enforce or Audit).
- A few miscellaneous option settings.

All checks in a rule must be from the same category. Checks fail if an undesirable condition is found. For example, the minimum release is not installed or the level of the engine or DAT file are not supported.

McAfee recommends that you define your rule set options before defining the rules that comprise the rule set.

As an example, an anti-virus rule set might include an anti-virus products rule for server operating systems and an anti-virus products rule for non-server operating systems.

Server rule definition	Non-server rule definition
McAfee VirusScan Enterprise 8.0i or later.	McAfee VirusScan Professional 7.1 or later.
Detection definition (DAT) files no older than 48 hours.	Detection definition (DAT) files no older than 5 days.
Scanning engine version 4400 or later.	Scanning engine version 4.2 or later.
Applies to systems running Windows NT Server, Windows 2000 Server, or Windows Server 2003.	Applies to systems running Windows NT Workstation, Windows 2000 Professional, Windows XP, Windows Me, and Windows 9x.
Noncompliance action set to Allow.	Noncompliance action set to Quarantine.
Noncompliance message is blank.	Noncompliance message contains details on how to make the system compliant.

Systems running server operating systems that fail the rule are allowed full access because they are servers. If any of these systems are noncompliant, you are notified when you view the Summary and Systems pages on the Status tab. You can then update these systems so they are compliant, and also decide whether to designate these systems as “trusted.”

Systems running non-server operating systems that fail the rule are quarantined to the appropriate enforcement zone until they have been made compliant.

Rules are evaluated independently of one another. If more than rule within a rule set fails, the rule with the most restrictive network access mode is applied.

McAfee default rules

Policy Enforcer includes default rules, which are designed to serve as both examples of how to define rules and as a starting point for your own compliance policy. For a description of the McAfee default rules, go to solution ID [KB46370](#) on the McAfee KnowledgeBase.

Checks

Checks detect the presence of:

- Anti-virus products.
- Firewall products.
- Host Intrusion Prevention products.
- Infections.
- McAfee Management Agent.
- Microsoft service packs.
- Patch management products.
- Potentially unwanted programs.
- Security bulletins: Applications.
- Security bulletins: Internet Explorer.
- Security bulletins: operating systems.
- Third-party products.

Checks are grouped into categories. All checks in a rule must be from the same check category. Checks fail if an undesirable condition is found, such as a missing patch release, a virus is present, a product is missing or the minimum version isn't installed.

Some check categories, such as anti-virus products and firewall products, have subcategories for specific products, such as McAfee VirusScan Enterprise and McAfee VirusScan Professional. You can identify check subcategories because they do not have an ID number and they are displayed in **bold** font. Each check subcategory (once checked) lists the specific checks it supports, such as minimum and maximum product versions, DAT file age requirements, etc.

Checks with subcategories are evaluated differently than those without subcategories. For more information, see [How are checks evaluated? on page 74](#).

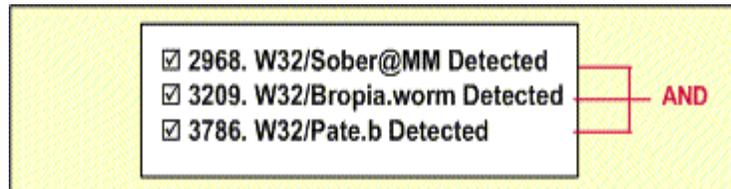
Each check category contains one or more individual checks. An individual check is identified by an ID number. All checks begin with an ID, which distinguish them from subcategories. For example, threat checks do not include subcategories, only the checks themselves, like **2968. W32/Sober@MM Detected**. A check that includes an asterisk (*) before the ID number does not require credentials to run. All other checks require appropriate administrative level credentials to be run.

How are checks evaluated?

All checks in any given rule are evaluated together as a part of determining the success or failure of the entire rule. All checks are grouped into categories. Some categories contain subcategories into which checks are grouped.

Figure 4-3 shows a check category with no subcategories. If a check category has no subcategories, all selected checks must pass for the rule to pass. This constitutes a logical AND test.

Figure 4-3 Evaluation of checks without subcategories

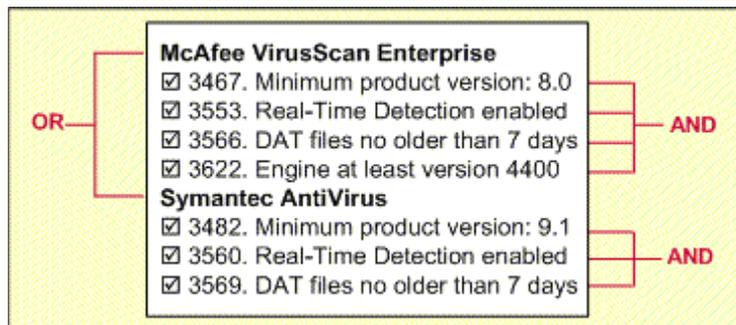


If a check category has subcategories:

- All selected checks within a subcategory must pass for the subcategory to pass (a logical AND test).
- If checks within multiple subcategories are selected, at least one subcategory must pass all its checks for the rule to pass (a logical OR test).

In Figure 4-4, all McAfee VirusScan Enterprise checks must pass or all Symantec AntiVirus checks must pass for the rule to pass. The failure of any selected check causes the rule to fail and results in the system being marked noncompliant.

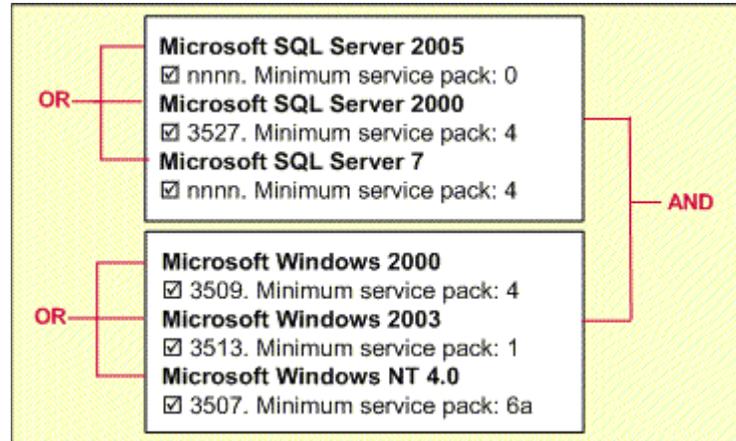
Figure 4-4 Evaluation of checks with subcategories



The Microsoft service pack releases check category is an exception because it covers multiple products. If you need multiple products from the same check category present at the same time, create a separate rule for each product.

For example, if you create a rule for Windows XP service pack 2, and you also want to check for Microsoft SQL Server 2000 service pack 4, you need to create a separate rule for each check.

Figure 4-5 Evaluation of multiple rules with checks from same check category



Comparing exception systems and trusted systems

Table 4-1 A comparison — Exception systems versus trusted systems

System type	Detect	Assess	Enforce	Report
Exception	Yes	Never scanned	Always allowed full access	No
Trusted	Yes	Always scanned	Always allowed full access	Yes

To prevent systems from being scanned, mark them as exceptions. Exception systems are never scanned and are always allowed full access to the network. Exception systems are those for which the compliance policy does not apply, such as printers, routers, switches, VOIP phone adapters, and VPN appliances. MPE sensors detect and report on any system with a MAC address.

Exception systems are never scanned and always allowed full access to the network. Once systems have been detected and scanned, you can mark them as exceptions manually or automatically based on specific conditions, such as IP address range, MAC address, OUI family, network access device (NAD) type (router or switch), operating system, or scan result.

Trusted systems are those that always need full access to the network regardless of their adherence to the compliance policy, such as mission-critical servers or a specific individual's system. Trusted systems are always scanned and reported on, but never quarantined or dropped from the network. You can be notified when trusted systems fail to adhere to the compliance policy, so you can take action to update them. As part of the compliance policy, you can define the conditions, such as computer name, that systems must meet to be classified as trusted.

For example, you probably want to have systems hosting MPE sensors that are performing switch enforcement and MPE scanners that are scanning remote systems automatically added as trusted systems.

When defining trusted system rules, it is important to consider that users can change computer names, IP addresses, and other data used to define trusted system rules.

5

Remediation

Topics in this section:

- [What is needed to perform remediation?](#)
- [Configuring and managing remediation](#)
- [How does remediation work?](#)
- [The remediation portal](#)
- [The remediation list](#)
- [Automatic remediation](#)
- [Rescanning a system in an enforcement zone](#)
- [Remediation of managed systems](#)
- [Remediation of unmanaged systems](#)
- [Remediation for VPN enforcement](#)

What is needed to perform remediation?

The following table lists the elements needed to perform remediation.

Element	Description
Remediation portal	A web server that provides instructions to users. The default page explains the user's situation.
Remediation web pages	A set of web pages that provide instructions and links so that users both understand their noncompliance and can access the resources needed to remedy their systems.
McAfee Policy Enforcer automatic remediation	Automatic remediation allows administrators to specify actions or programs that run automatically if a user's system fails a compliance rule. For managed systems only.
Remediation list	A list of systems that noncompliant systems can access when moved to an enforcement zone. The remediation list is specified in the MPE scanner policy and for each enforcement zone.
Noncompliance message of compliance rules	Each compliance rule allows administrators to include a message that is displayed to users when their system fails the rule. This message should include instructions on how to make their system compliant. This feature is available for managed systems only.
Rescanning a system in an enforcement zone	Allows users to reassess their systems for compliance once they have taken steps to remediate their systems. This can be done with a remote scanner that is accessible to systems in an enforcement zone, or with the downloadable ActiveX scanner included with Policy Enforcer.

To ensure that users can remediate their noncompliant systems (make them compliant), you must provide:

- **Remediation instructions** — Specify how the user’s system is noncompliant and the steps necessary to correct the problem. Provide a link or URL to your remediation portal’s home page. For unmanaged systems you need to set up browser redirection that forces users to your remediation portal. It is also recommended that you provide information to users about the remediation process prior to enforcing your compliance policy.
- **Remediation resources access** — Identify and set up all resources that users need to remediate their systems. All servers that users need to access, including the server hosting your remediation portal, must be specified in your remediation list, and must be accessible from your enforcement zones or VLANs.

Configuring and managing remediation

Remediation tasks and where to go in the GUI to do them are listed below. The online Help provides step-by-step procedures and field definitions.

Task	Where to do this task
<i>Remediation of managed systems</i>	ePolicy Orchestrator <SERVER> Policy Catalog Policy Enforcer Scanner , and select Scan Policies . Click Define new policy , and type a name such as Remediation List.
<i>Set automatic remediation options</i>	ePolicy Orchestrator <SERVER> select McAfee Policy Enforcer Compliance tab Rule Sets tab then click Add Rule and select Set Noncompliance Actions page.
<i>Use a remote scanner for rescan requests</i>	Through your remediation portal.
<i>Use the ActiveX scanner for rescan requests</i>	Through your remediation portal.
<i>Set the quarantine VLAN for switch enforcement</i>	McAfee Policy Enforcer Compliance tab Enforcement Zones tab.
<i>Re-enable dropped or enforced ports</i>	System to allow: McAfee Policy Enforcer Status tab Systems tab, then select system and select Allow System .

How does remediation work?

Remediation is the process of updating systems to bring them into compliance with your Policy Enforcer policies. In most cases, a noncompliant system is moved to an enforcement zone if it fails one or more compliance checks.

Once moved to the enforcement zone, the noncompliant system should be permitted access only to systems that contain resources for remediation, such as a web server and specific file servers.

Once a user has taken steps to remediate a noncompliant system, a rescan can be requested through the portal resources. If the rescan assesses the system as compliant, the system is removed from enforcement zone and allowed full network access again.

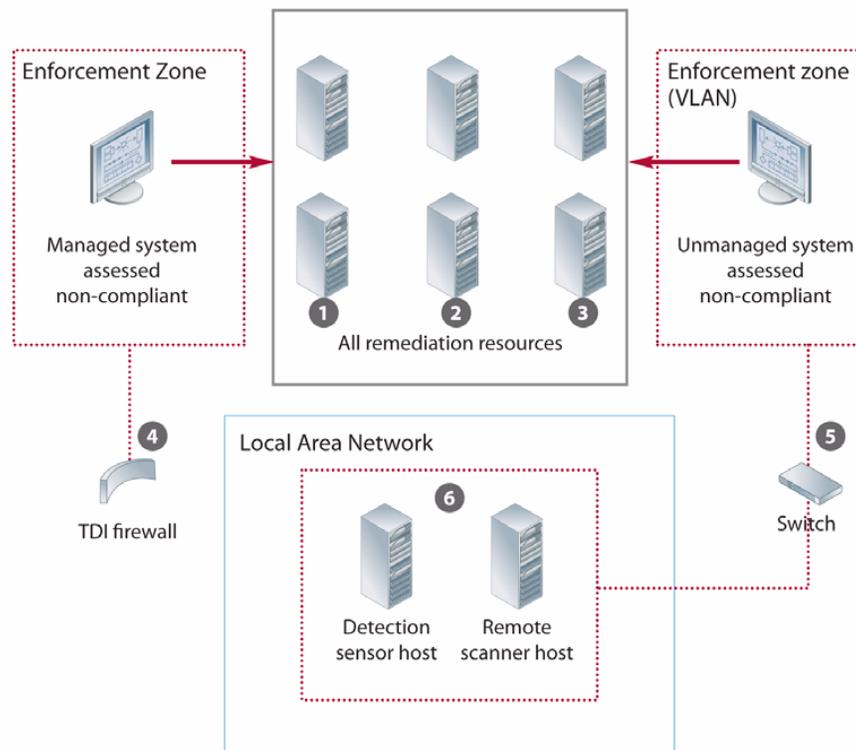
Managed and unmanaged systems that use the LAN or NAC enforcement type can be remediated using the remediation portal. Systems to which the VPN enforcement type applies cannot be remediated in the same way because they cannot be enforced. Noncompliant VPN systems can be either allowed or dropped.

Figure 5-1 shows how remediation resources are situated once a system (managed or unmanaged) is moved to an enforcement zone. For managed systems, network access is blocked by the switch enforcement configured in the scanner NAP or by the MPE scanner's TDI firewall. Managed systems are moved to one of the enforcement zones you defined under the **Compliance** tab. For unmanaged systems, network access is blocked by an enforcement sensor that forces the switch port to an enforcement zone VLAN, which is set up by a network administrator.

All managed systems have access to the resources represented by Item 1 in the diagram. The resources comprising Items 2 and 3 are designated by the McAfee Policy Enforcer administrator in the scanner policy and in the definition of each enforcement zone. These are also available to managed systems, depending on which scanner policy they use, and to which enforcement zone they are restricted.

For unmanaged systems, the network administrator has to make all remediation resources, including the remediation portal, available to the enforcement zone VLAN. A detection sensor and a remote scanner also must be accessible from the enforcement zone VLAN. The detection sensor is required because once the unmanaged system is transferred to the enforcement zone VLAN, it gets a new IP address. The remote scanner is needed for rescan requests from systems in the enforcement zone VLAN.

Figure 5-1 Remediation resources from the enforcement zone



- 1 The systems McAfee Policy Enforcer automatically includes as remediation resources: the ePO/MPE server, all ePO managed repositories, the default IP gateway, and all DNS servers assigned to the system statically or dynamically.
- 2 The systems specified for the remediation list in the MPE scanner policy. Available only to managed systems.
- 3 The systems specified for the remediation list of the MPE enforcement zone. Available only to managed systems.
- 4 Noncompliant managed systems are blocked from network access by a TDI firewall. The local scanner provides this.
- 5 Noncompliant unmanaged systems are blocked from network access by an enforcement sensor, which changes the system's switch port to the enforcement zone VLAN.
- 6 The network administrator must ensure that both a detection sensor and a remote scanner can access systems in an enforcement zone VLAN.

The remediation portal

The remediation portal is a web portal that provides manual remediation steps to bring systems into compliance. It also allows users to initiate a rescan after updating their systems. Typically, the portal should provide access to installation and update packages that noncompliant systems need for remediation.

The remediation portal should always present users with the following information:

- A description of the corporate compliance policy.
- A list or description of the resources, patches, applications, etc., that must be installed and applied for the system to be compliant.
- Instructions for rescanning a noncompliant system so it can be removed from an enforcement zone.

Policy Enforcer provides all the elements necessary for setting up a remediation portal, and supports eight languages. To set up a remediation portal, you can:

- Use the template files supplied with the product and modify them as needed. For information, see *Installing and customizing the remediation portal* in the *McAfee Policy Enforcer 2.0 Installation Guide*.
- Set up your own remediation portal.
- Use an existing remediation portal.

Whether you setting up a remediation portal for the first time, or modifying an existing portal, you need to provide a way for users to rescan their systems. Code for this is provided in the McAfee Policy Enforcer template files.

Accessing the remediation portal

Noncompliant systems access the remediation portal differently depending on whether they are managed or unmanaged, and the enforcement type of the rule sets that contain the failed rule or rules.

Enforcement and system type	Method to access remediation portal
<ul style="list-style-type: none"> ■ LAN enforcement ■ Managed system (MPE scanner and ePO agent) 	The server hosting the remediation portal is specified in the remediation list of either the scanner policy or the enforcement zones. McAfee suggests including the remediation portal server in all scanner policy remediation lists. Also, provide a link to the portal home page in the noncompliance message for every rule.
<ul style="list-style-type: none"> ■ LAN enforcement ■ Unmanaged system (no MPE scanner and ePO agent) 	The remediation portal and all other remediation resources must be accessible from your enforcement zone VLANs. This is done with your Access Control Lists (ACLs), or specified in the routing information of your network access devices.
<ul style="list-style-type: none"> ■ NAC enforcement ■ Managed or unmanaged system (CTA, MPE scanner, and ePO agent) 	The remediation portal and all other remediation resources must be accessible from the ACLs you have specified as part of authorization for all your Network Access Profiles.
<ul style="list-style-type: none"> ■ VPN enforcement ■ Managed or unmanaged system 	Systems to which VPN enforcement applies cannot access the remediation portal. Some VPN vendors support remediation. For information, see the VPN vendor product documentation.

The remediation list

The resources (servers and other network systems) a noncompliant system can access once it has been moved to an enforcement zone is specified by the remediation list. The remediation list is a combination of:

- The systems Policy Enforcer automatically includes as remediation resources. These do not have to be listed in a scanner policy or enforcement zone.
- The systems you specify in your MPE scanner policy or policies.
- The systems you specify in your enforcement zones.

The list of remediation resources available to any individual noncompliant system depends on which MPE scanner policy it is assigned, and which enforcement zone it is placed in.

The systems that Policy Enforcer automatically includes as remediation resources are:

- The ePO server and the ePO managed repository site list.
- The MPE server, including any standalone MPE servers.
- The default IP gateway.
- All DNS servers assigned to a system either statically or dynamically.

You must manually add the server hosting the remediation portal, and any file servers or other systems linked to the portal to either the MPE scanner remediation list or enforcement zone remediation list. To add systems such as your primary and backup domain controllers, these also must be added manually.



If you are editing the remediation list of an existing MPE scanner policy, systems that are already assigned that policy receive an update during the next agent-server communication.

Automatic remediation

For managed systems, you can set some automatic remediation options as part of the “Noncompliance Response” for any of your compliance rules. When a managed system fails a rule, you can attempt to automatically remediate the system with these options:

- Execute ePO agent Update on failure.
- Execute command line on failure.

Executing an ePO agent Update is useful when your compliance rules have checks that require regular content updates for McAfee point products, such the detection definition (DAT) files for VirusScan Enterprise.

The command-line option allows administrators to attempt a single remediation action per failed rule without involving the user. The noncompliant system remains in an enforcement zone until a rescan determines whether the system is compliant.

The command-line option allows administrators to run installer packages, custom scripts that might install several applications, or any program that can be executed from the Windows command prompt as remediation action.

If you use these automatic remediation options, you can include information in the rule’s noncompliance message. This way users know what actions have been taken, whether they should attempt a rescan immediately or take further manual remediation steps.

Rescanning a system in an enforcement zone

Through your remediation portal, users can rescan their noncompliant system to determine if their remediation actions have made their system compliant. Users click the **Rescan** link on your portal web page. Optionally, you can require users to enter credentials.

The person responsible for the remediation portal, has two choices:

- Use a remote scanner for rescan requests. You can make an MPE remote scanner accessible to all your enforcement zones and enforcement VLANs.
- Use the ActiveX scanner for rescan requests. You can give systems in an enforcement zone access through your portal to the Policy Enforcer downloadable ActiveX scanner. This rescan method is particularly useful for systems that are running a firewall, or are otherwise inaccessible to a remote scanner.

The default remediation portal web page provided with McAfee Policy Enforcer includes links for using both a remote scanner and the downloadable ActiveX scanner. To allow use of either scanner, make sure the link on the web page is correct.

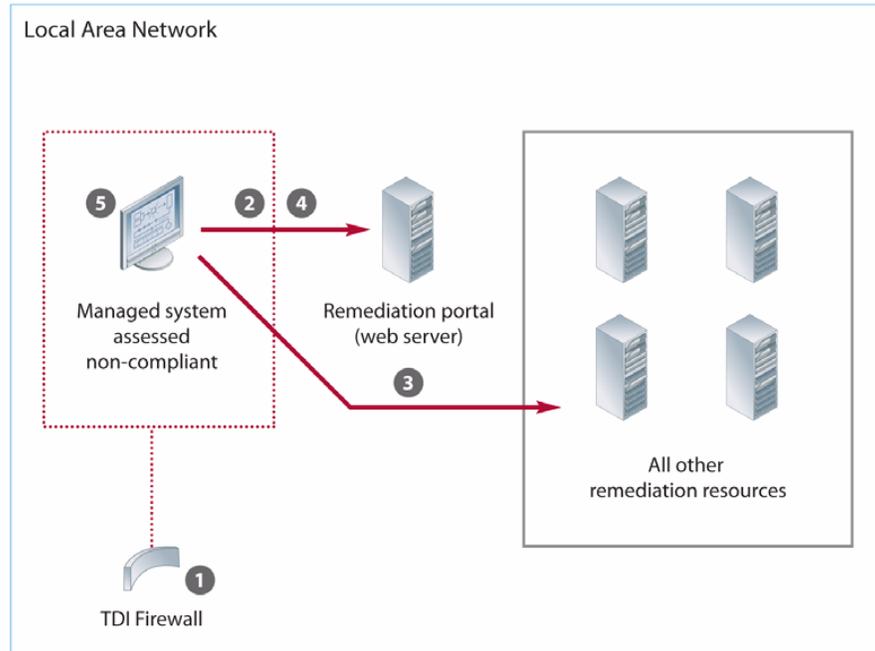
The ActiveX scanner may take several minutes to download and complete the scan. The user is provided with an explanation of the scan results, then the scanner is uninstalled.

Remediation of managed systems

If a system is managed, the MPE scanner performs enforcement through a TDI firewall that blocks outgoing TCP and UDP connections on the scanner host. Because the scanner provides this type of self-enforcement, managed systems have more options for how remediation is handled than an unmanaged system. Remediation functions that apply only to managed systems are:

- The noncompliance message is displayed when the system is found noncompliant. This message can include an active link to the remediation portal or other URLs. The ActiveX scanner displays the failed rules within the noncompliant web page.
- Automatic remediation options.
- Remediation resources can be specified in your MPE scanner policies and in each of your named enforcement zones.

Figure 5-2 shows how the remediation process works for managed systems.

Figure 5-2 Remediation process on managed systems

- 1** The local scanner determines the system is noncompliant. The TDI firewall is activated, the system is placed in the enforcement zone designated by the failed rule, and the noncompliance message is displayed.
- 2** The user clicks links from the noncompliance message to access the remediation portal.
- 3** The user updates the system to be compliant by accessing the remediation resources made available by the scanner policy and the enforcement zone.
- 4** The user requests a rescan of the system from the remediation portal webpage.
- 5** The rescan assesses whether the system is now compliant. If it is, the TDI firewall is removed and network access is restored.

To remediate managed systems that use the LAN enforcement type, users need the following information when their systems are noncompliant.

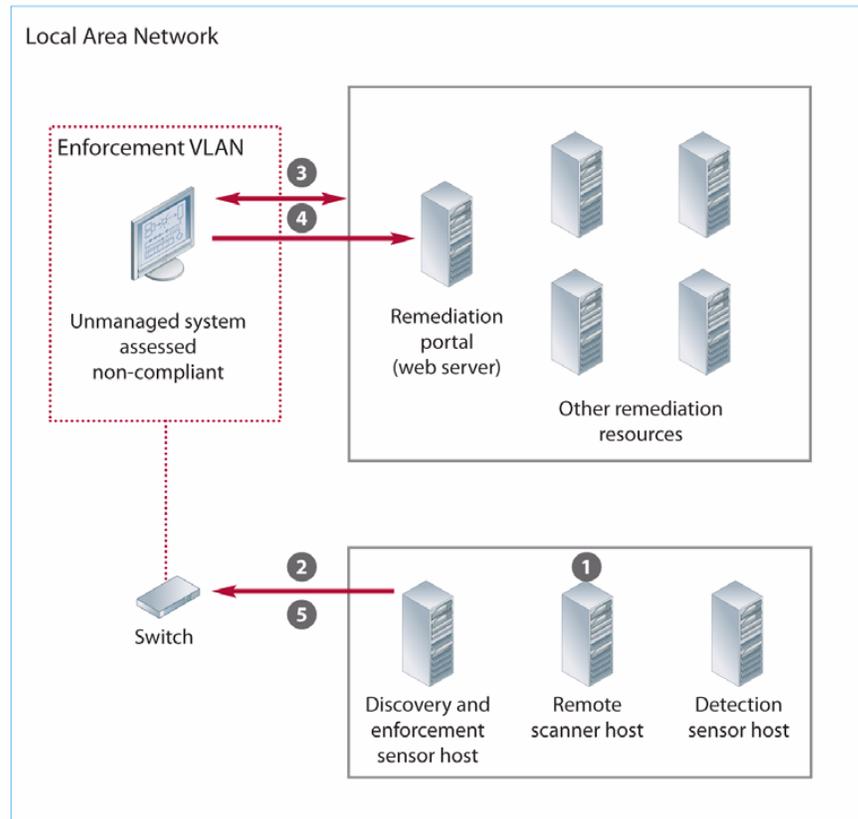
Information required	Details
Remediation instructions	<p>The noncompliance message from a rule definition automatically displays the list of failed checks to users. Additionally, you can add text that provides more details about the problem and what users should do about it. To give users access to the remediation portal, you must include the portal's URL in this message. See Defining a compliance policy on page 67.</p> <p>You can also add remediation instructions to the web pages your remediation portal displays. For information, see <i>Installing and customizing the remediation portal</i> in the <i>McAfee Policy Enforcer 2.0 Installation Guide</i>.</p>
Remediation resources access	<p>Add all systems that provide remediation resources to the remediation list. This includes the system that hosts the remediation portal. The remediation list consists of the systems specified in the scanner policy, and in the enforcement zone.</p> <p>See Defining a compliance policy on page 67.</p>

Remediation of unmanaged systems

If a system is unmanaged, it has no local scanner and self-enforcement is not possible. In this case, switch enforcement is used, and noncompliant systems are moved to an enforcement zone VLAN. The network resources used for remediation must be given access to this VLAN.

Without a local scanner, the noncompliance message cannot be displayed on an unmanaged system. You must set up a browser redirection that sends users of noncompliant systems to the remediation portal the next time they open a browser after being enforced. If you do not set up browser redirection, you may need to publish instructions telling users how to access your remediation portal.

[Figure 5-3](#) shows how the remediation process works for unmanaged systems. The Network Administrator must make all remediation resources available to the enforcement zone VLAN, and must assure that a detection sensor and a remote scanner can access the enforcement zone VLAN.

Figure 5-3 Remediation process on unmanaged systems

- 1 A remote scanner determines an unmanaged system is noncompliant.
- 2 A sensor that performs enforcement changes the system's switch port to the designated enforcement zone VLAN. The user does not receive the noncompliance message of the failed rule.
- 3 The user updates the system to be compliant by accessing the remediation resources made available by the network administrator.
- 4 The user requests a rescan of the system from the remediation portal webpage. The rescan can be performed by a remote scanner, or by a downloadable ActiveX scanner.
- 5 If the rescan determines the system is now compliant, the sensor performing enforcement changes the switch port back to the Allow VLAN, and network access is restored.

To set up remediation for unmanaged systems using a LAN connection, you must provide the following:

Information required	Details
Remediation instructions	Add remediation instructions on the web pages your remediation portal displays. For instructions, see <i>Installing and customizing the remediation portal</i> in the <i>McAfee Policy Enforcer 2.0 Installation Guide</i> .
Remediation resources access	Ensure that the remediation VLAN has access to the server hosting the remediation portal, and any servers hosting the applications, patches, content updates, etc. required for remediation.
Provide portal URL to users	Set up a browser redirection on the remediation portal web server; go to KB46354 on the McAfee KnowledgeBase for example methods.

Remediation for VPN enforcement

If a system is noncompliant and uses a VPN connection to access your network, the only enforcement options through Policy Enforcer are allow and drop. Because VPN systems cannot be enforced by Policy Enforcer, they cannot access the remediation portal.

However, some VPN vendors support remediation. For information, see the VPN vendor's product documentation. Additionally, the noncompliance message for any failed rule displays on VPN-connected systems if they are managed. For information about the noncompliance message, see [How rules work on page 71](#).

6

Actions, Notifications, Troubleshooting

The Policy Enforcer interface provides data for all known systems, subnets, and switches on the network. Examples of events include changes in the status of systems or processes, or new systems added to the network. An action is a response to an event that you can initiate automatically or manually. Notifications are alerts sent to specified personnel after an event occurs.

You can set the network access mode manually or automatically in response to an event. You can send notifications whenever systems are moved to an enforcement zone with limited access or dropped from the network.

These topics for viewing and taking action on real-time data are covered in this section:

- [Status of systems compliance summary.](#)
- [Status of subnets.](#)
- [Custom filter.](#)
- [Automatic responses.](#)
- [Actions.](#)
- [Reports](#)
- [Troubleshooting tools.](#)

Status of systems compliance summary

Every known system on the network has a status:

- **Noncompliant Systems** — Systems that did not meet the minimum requirements of the compliance policy during the most recent scan.
- **Inactive Systems** — Systems that have not been detected by the sensor within the minimum reporting interval (default is three days); typically computers that have been turned off or disconnected from the network.
- **Compliant Systems** — Systems that met the minimum requirements of the compliance policy during the most recent scan.
- **Exception Systems** — Systems to which the compliance policy does not apply, such as printers, routers, switches, VoIP phone adapters, and VPN appliances.

- **Indeterminate Systems** — Systems that match a rule set in the compliance policy, but don't match any of the operating systems in the rules, or systems on which the scan could not be completed for some reason, such as missing credentials.

Status of systems

Every detected system has one of these status types. See online help for definitions.

- Indeterminate
- Managed
- Rogues
- Noncompliant
- Inactive
- Compliant
- Exceptions
- Enforcement zone (default zone)
- Allowed
- Dropped

Status of subnets

Every known subnet on the LAN has a status:

- **Covered** — Subnets with an active detection sensor.
- **Uncovered** — Subnets without an active detection sensor.

Status of switches

Every known switch on the LAN has a status:

Any Ports Dropped — Switch ports dropped from the system.

Any Ports Quarantined: Default Zone — Switch ports placed in an enforcement zone.

Any Ports Allowed — Switch ports with full access to the network.

Custom filter

A custom filter defines a set of conditions you can use to limit data in tables, such as on the **Subnet List** and **System List**. Use a custom filter to use criteria other than the predefined filters to limit data. This quickly find systems that meet a specific criteria, such as those that fall within a specific IP address range, or to combine such criteria with the predefined filters, such as the list of system statuses. For example, you could use a custom filter to find all noncompliant computers that are running Windows 95.

Automatic responses

Automatic responses combine a triggering event, additional conditions systems must meet, and a set of predefined actions or external commands. When the selected event occurs on systems meeting these conditions, the specified action is taken. Actions are taken in the order they appear in the interface and run concurrently. In other words, each action begins without waiting for the previous action to complete.

Events that trigger automatic responses are system-generated events that indicate a state change:

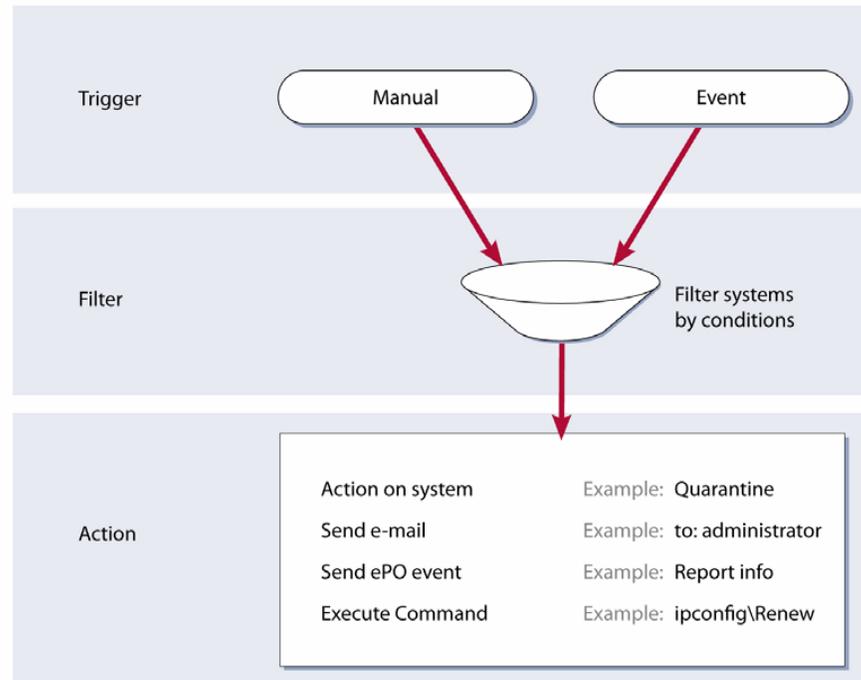
- **Noncompliant System Detected** — When the status of a system changes from compliant to noncompliant.
- **Subnet Uncovered** When a subnet is found that doesn't have an active detection sensor on it.
- **Enforcement Failed** — When an attempt to change the network access mode for a system or switch port cannot be completed for some reason.
- **Any Event** — When any ePO or MPE event occurs.
- **Enforcement Failed** — When an attempt to change the network access mode for a system or switch port cannot be completed for some reason.

When selected events occur (for example, when a system is marked as noncompliant), you can define a specific action be taken automatically in response to that event (for example, send an email message). The actions that can be taken include sending email messages, taking a predefined action, or running a program (external command) on the system. Although the event triggers the automatic response, you can further restrict the response to systems meeting specified conditions, such as having an IP address within a certain range. Automatic responses begin after receiving the triggering event.

Actions

You can take actions manually or automatically in response to events. Actions include a set of predefined actions on systems, sending email or events, and executing external commands. Actions are taken as part of automatic responses on systems that meet the specified conditions when the selected event occurs.

Figure 6-1 Manual actions and automatic responses



Reports

You can run reports to view trends of compliance over time.

These topics for viewing historical data are covered in this section:

- Accessing reports for the first time.
- McAfee Policy Enforcer report templates.

Accessing reports for the first time

The first time you access the McAfee Policy Enforcer reports, you must log on to the database server using ePO authentication. You can then use any authentication method (ePO, SQL, or Windows NT) to access these reports.

- 1 In the console tree, select the desired database server under **ePO Databases** to open the **ePO Database Login** dialog box.
- 2 Type an ePO global administrator user account in **User name** and **Password**, then click **OK**.
- 3 Answer yes when asked whether you want to download the new reports.

McAfee Policy Enforcer report templates

The McAfee Policy Enforcer software includes these predefined reports:

Name	Usage
Top 10 Failed Checks	Use to view the top ten checks that systems have failed to adhere to over time.
Daily Enforcement Summary	Use to view network access mode changes made on systems by day.
Noncompliance Summary	Use to view noncompliant systems over time.
Top 10 Noncompliant Systems	Use to view the top ten noncompliant systems over time.
Percentage of Noncompliant Systems	Use to view the percentage of noncompliant versus compliant systems over time.
Top 10 Failed Rules	Use to view the top ten rules that systems have failed to adhere to over time.

Troubleshooting tools

Depending on whether you encounter any issues, we might ask you to gather additional information using one or more of the following:

- [Scanner log files](#),
- [Sensor log files](#).
- [Packet capture of network traffic](#).

Scanner log files

The scanner log configuration (MPEScanner_Log.cfg) file controls the level of logging in the scanner log (MPEScanner_Out.log) file. Their default location is:

C:\Program Files\McAfee\MPE Scanner

The MPEScanner_Out.log file includes entries related to scan results, rule evaluation, and scanner-to-server communication.

The logging levels from most to least verbose are DEBUG, INFO, and WARN. The level that is set in the log configuration file includes entries at that level and lower; for example, the INFO level includes entries for both the INFO and WARN levels. For instructions, see [Changing the logging level of the scanner log files](#).

Changing the logging level of the scanner log files

- 1 On the scanner host computer, open the scanner log configuration (MPEScanner_Log.cfg) file in a text editor, such as Notepad. The default location is:

C:\Program Files\McAfee\MPE Scanner

- 2 Locate the following text near the top of the file:

```
log4cplus.rootLogger=WARN

#The following controls which categories go into which output files
log4cplus.logger.MPEScanner=DEBUG, STDOUT, SCANNERLOG

#The following is a list of categories supported by the
#McAfee Policy Enforcer Scanner
#Categories related to scanner communication and server communication
#in the scanner.
log4cplus.logger.MPEScanner.ServerCom=INFO
log4cplus.logger.MPEScanner.ScannerComm=INFO
log4cplus.logger.MPEScanner.ScannerComm.ScannerCommWorkerThread=INFO
log4cplus.additivity.MPEScanner=FALSE
```

- 3 Change the logging levels (DEBUG, INFO, or WARN) as needed.
- 4 Save and close the log configuration file. Changes take effect immediately.

Sensor log files

The sensor log configuration (MPESensor_Log.cfg) file controls the level of logging in the sensor log (RS_Sensor_Out.log) and the discovery and mapping log (Topology_Out.log) files. Their default location is:

C:\Program Files\McAfee\MPE Sensor

The sensor log includes entries related to detection of new systems and sensor-to-server communication. The discovery and mapping log includes entries related to topology discovery and topology mapping.

The logging levels from most to least verbose are DEBUG, INFO, and WARN. The level that is set in the log configuration file includes entries at that level and lower; for example, the INFO level includes entries for both the INFO and WARN levels. For instructions, see [Changing the logging level of the sensor log files on page 94](#).

Changing the logging level of the sensor log files

- 1 On the sensor host computer, open the sensor log configuration (MPESensor_Log.cfg) file in a text editor, such as Notepad. Their default location is:

C:\Program Files\McAfee\MPE Sensor

- 2 Locate the following text near the top of the file:

```
#The following is a list of categories supported by the
#McAfee Rogue System Sensor

#Categories related to detection and server communication in
#the sensor.

log4cplus.logger.MPESensor.NetListener=INFO
log4cplus.logger.MPESensor.Resolver=INFO
log4cplus.logger.MPESensor.ServerCom=INFO
log4cplus.additivity.MPESensor=FALSE

#Categories related to topology discovery and mapping
log4cplus.logger.Topology.TopologyMapper=INFO
log4cplus.logger.Topology.NetworkTopology=INFO
log4cplus.logger.Topology.NetTopoDiscovery=INFO
log4cplus.logger.Topology.NetTopoDiscovery.NetDiscoveryEngine=INFO
log4cplus.additivity.Topology=FALSE
```

- 3 Change the logging levels (DEBUG, INFO, or WARN) as needed.
- 4 Save and close the log configuration file. Changes take effect immediately.

Packet capture of network traffic

If you are asked to do so, use a network performance tool, such as Network General Sniffer Distributed, Network Monitor, or Ethereal to perform a packet capture.

Network Monitor is a Windows component that captures, displays, and analyzes network packets. Network Monitor is available on computers running Windows server operating systems. For instructions on installing and using this tool, see the Windows Help file.

Ethereal is free, open source software. At press time, this program and instructions for its installation and use were available on the Ethereal website:

<http://www.ethereal.com/download.html>



Ethereal and the MPE sensor cannot be installed on the same computer because they use different versions of WinPcap (Windows Packet Capture Library).

NAC-related troubleshooting

When configuring an ACS server, if the server cannot detect a NAC agentless host, check the switch/router configuration for the following Cisco IOS command statement:

```
eou allow clientless  
eou max-retry 2  
eou timeout retransmit 5
```

7

Cisco NAC Integration

Topics in this section:

- [MPE components in a NAC environment](#)
- [Setup requirements for Cisco NAC](#)
- [Cisco ACS server configuration](#)

Policy Enforcer supports and integrates with a Cisco NAC 2.0 network environment by providing components that allow:

- MPE scanners to pass scan results to the Cisco Trust Agent (CTA) on managed systems.
- MPE remote scanners to assess unmanaged systems and communicate the results to an MPE server.
- MPE servers to communicate with Cisco ACS servers.

Integration

To integrate Policy Enforcer into a Cisco NAC network environment, you must:

- Setup Cisco NAC so its components and Policy Enforcer can communicate.
- Configure specific elements of the Cisco ACS server so that it recognizes Policy Enforcer data.
- Configure the MPE server to act as an external Posture Validation Server.
- Configure the MPE server to act as an external audit server.

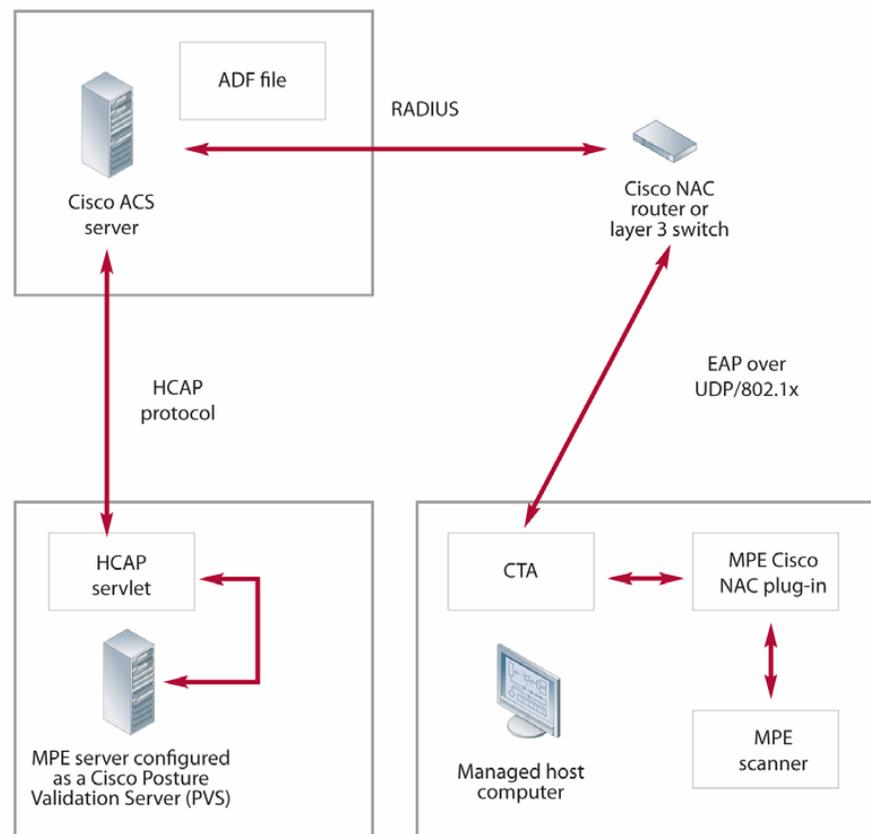
MPE components in a NAC environment

Figure 7-1 and Figure 7-2 show the components and the communication pathways for managed and unmanaged systems, respectively, in a Cisco NAC environment.

The HCAP service and HCAP protocol are used by Cisco NAC to gather posture data for hosts that are managed by Cisco NAC (that is, hosts that have the Cisco Trust Agent installed).

In Cisco NAC, when a host comes onto the network (and periodically thereafter), the network access device (switch) queries the Cisco Trust Agent (CTA) on that host for its posture data. If CTA is installed, the host is considered managed. A managed host's posture can be assessed either using Cisco ACS internal posture validation policies, or by configuring the MPE server to act as an external posture validation server, and setting a network access policy for managed systems.

Figure 7-1 Managed systems in a Cisco NAC environment



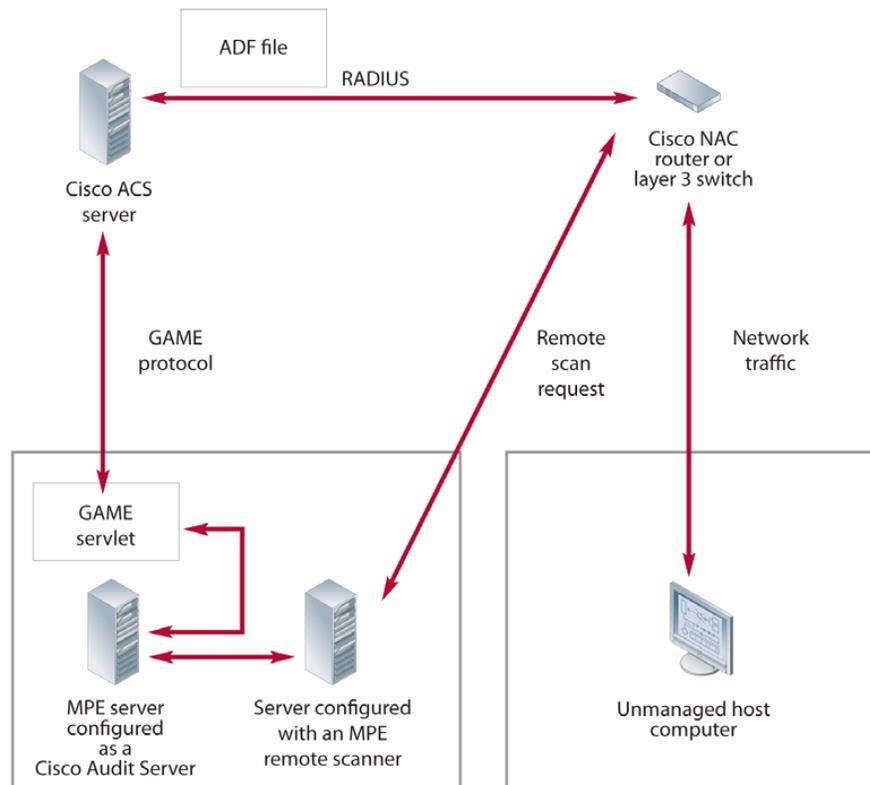
The Cisco ACS allows configuration of an external audit server to gather required posture data. The protocol that triggers these audits and gathers results is called GAME. Policy Enforcer includes a GAME service that handles these audit requests and sends posture data back to Cisco ACS.

The GAME service and GAME protocol are used by Cisco NAC to gather posture data for hosts that are unmanaged by Cisco NAC (that is, hosts that don't have the Cisco Trust Agent). A host that is unmanaged by NAC may or may not have an MPE scanner and ePO agent installed.

In Cisco NAC, when a host comes onto the network and periodically thereafter, the NAD (switch) queries the Cisco Trust Agent (CTA) on that host for its posture data. If CTA is not installed, the host is considered unmanaged and requires an external audit to determine its posture. This kind of host in NAC is sometimes called a NAC Agentless Host or NAH. To determine the posture of NAC Agentless Hosts, you configure the MPE server to act as an external audit server, and set a network access policy for these unmanaged systems.

When the host is first connected or the network changes because of an ipconfig renew command, the MPE scanner cannot detect that it should not be enforced at the Cisco device when a local scanner is installed on the NAH system. In this case, the scanner uses the configured LAN policy. All routine scans that are requested from MPE through ACS health requests use NAC enforcement and the NAC policy. To prevent this behavior, we recommend installing CTA if the system has a local scanner.

Figure 7-2 Unmanaged systems in a Cisco NAC environment



Setup requirements for Cisco NAC

You must completely configure the Cisco NAC network environment before the integration between Policy Enforcer and NAC components is functional. At a minimum, you must:

- Follow the instructions in Cisco's *NAC Framework Configuration Guide*, including all relevant switch configuration.
- Make sure the hardware used for network protection is Cisco NAC 2.0 compatible (for instance, Layer 3 switches).
- Deploy the Cisco Trust Agent (CTA) 2.0.x to managed systems.
- In Policy Enforcer, set the credentials that the ACS server uses for authentication when communicating with the MPE server. Credentials must match what is in the ACS.
- ACS certificate file must be accessible by your clients from a file share.
- Add all MPE servers, sensors, and remote scanners to both your static and downloadable Access Control Lists (ACLs).
- Make sure the ePO and MPE servers are accessible to all managed systems that are placed in a quarantine state.

Deploy the Cisco Trust Agent

You can deploy the Cisco Trust Agent (CTA) to managed systems automatically from ePolicy Orchestrator, or manually.

Policy Enforcer includes a default Cisco Trust Agent 2.0.0 policy (go to the Policy Catalog section in the ePO console). This default policy must be copied, renamed as a new policy, and modified before you can deploy CTA (see *Creating a Cisco Trust Agent policy* in online Help). For option descriptions, click **Help** on the Cisco Trust Agent 2.0.0 policy page.

The Cisco Trust Agent 2.0.0 policy has four sections: General Options, Credentials Settings, Certificate Settings, and Configuration Settings. In General Options, You accept the EULA, then can select to enable optional features. By default, the Cisco Trust Agent only supports EAP over UDP communications.

CTA policy page sections	Purpose
General Options	<p>Required: Accept the EULA.</p> <p>Optional: Enable installation of additional CTA features/components.</p> <p>Support for communications using 802.1x is enabled by default.</p> <p>You can install the CTA scripting interface (disabled by default).</p> <p>You can designate a custom installation path.</p>
Credentials Settings	<p>Required. Enter the authentication credentials needed to access the system where you have stored the CTA certificate.</p>
Certificate Settings	<p>Required. Use the same CA certificate that was used during the setup of your Cisco ACS server for NAC. McAfee recommends placing the CTA certificate on the ePO server.</p>
Configuration Settings	<p>Optional. You can provide the path to the CTA configuration file (ctad.ini by default).</p>

For information about credentials, the CTA configuration file, and using the CTA scripting interface, refer to Cisco's *CTA Administration Guide*.

To deploy the Cisco Trust Agent (CTA) using ePolicy Orchestrator:

- 1 In the console tree, double-click a site, group, or individual system.
- 2 Select the **Policies** tab, open the Cisco Trust Agent 2.0.0 policy section, and select one of the custom policies you created (the McAfee default policy does not work).
- 3 Select the **Tasks** tab, and double-click **s**.
- 4 In the Deployment window, select **Settings**.
- 5 Locate the entry for Cisco Trust Agent Deployment package, and select **Install** from the drop-down list.
- 6 Click **OK**, then click **Apply**. To schedule this task, you need to enable the task in the Schedule Settings section, then set the appropriate scheduling options.

At the next ePO agent wakeup call, the CTA deployment package is copied to the following location on the systems you selected:

C:\Program Files\McAfee\MPE CTA Deployment

The first ePO agent wakeup call only copies the deployment package, it does not install CTA. For information about initiating ePO agent wakeup calls, see the ePolicy Orchestrator online Help.

To deploy the Cisco Trust Agent (CTA) manually:

- 1 Download the CTA 2.0 installation from Cisco and run Setup on the client systems.
- 2 Generate a certificate on the ACS server if you haven't done so already, using the instructions in the *User Guide for Cisco Secure ACS*.
- 3 Import the certificate from the ACS server, using the instructions for the ctacert utility in the *Cisco Trust Agent Administrator Guide*.
- 4 Enable CTA logging on client systems. For information, refer to Logging Notifications in the *Cisco Trust Agent Administrator Guide*.

Set credentials for ACS authentication

For the ACS server to communicate with Policy Enforcer during posture validation, you need to set a user name and password in the MPE server configuration.

- 1 Select the **Compliance** tab, then the **Enforcement Types** page.
- 2 In the **Enforcement Types** table, click the Cisco NAC enforcement type entry.
- 3 Type a user name and password in the **Name** and **Password** fields. This must be the same user name and password you use when setting up the MPE server to act as an external posture validation server and as an external audit server in the ACS server.
- 4 Click **Apply**.

Cisco ACS server configuration

To configure the ACS server to work with McAfee Policy Enforcer, you must:

- Import the McAfee Policy Enforcer ADF file to the Cisco ACS server.
- Set the configuration for handling NAC managed hosts. You can either:
 - Change or create internal Posture Validation Policies in the ACS configuration interface.
 - Change or create an external Posture Validation Policy for the MPE server in the ACS configuration interface, and set the posture validation token to send from the MPE server to the ACS server.

For information, see the Internal Policies and External Policies sections in the *User Guide for Cisco Secure ACS* document from Cisco.

- Set the configuration for handling of NAC Agentless (unmanaged) hosts.

Import ADF file to ACS server

The Attribute Definition File (ADF) contains a list of attributes specific to each third-party product that integrates with Cisco NAC. The ADF must be imported before configuring ACS to work with McAfee Policy Enforcer.

McAfee Policy Enforcer includes an ADF that specifies the attributes sent from the MPE scanner to CTA, and then from CTA to the ACS server. This file is named MPE20.adf and is included in the McAfee Policy Enforcer installation package. To import the McAfee Policy Enforcer ADF, follow the instructions under Import Vendor Attribute-Value Pairs in Cisco's *User Guide for Cisco Secure ACS*.

Configuration for NAC managed systems

Systems that have the Cisco Trust Agent (CTA) installed are considered "NAC managed." To assess the posture of these systems, you can either create an internal Posture Validation Policy in the Cisco ACS, or set up the MPE server to act as an external Posture Validation Server. Whichever method you choose, you must also create a Network Access Profile for NAC managed systems in ACS.

Configure Internal Posture Validation Policies

For the ACS server to recognize data from the MPE scanner, you must change or create internal Posture Validation Policies in the ACS configuration interface. The internal policies are used only for systems that have the Cisco Trust Agent, the MPE scanner, and the ePO agent installed. Policy Enforcer provides the attribute "McAfee:McAfeePolicyEnforcer:HealthLevel" for use in the Posture Validation Policies. This attribute contains a value corresponding to the NAC health levels:

0 = Healthy	20 = Quarantine
10 = Checkup	30 = Infected
15 = Transition	100 = Unknown

To configure internal Posture Validation Policies for Policy Enforcer:

- 1 In the ACS navigation pane, click **Posture Validation**.
- 2 Click **Internal Posture Validation Setup**.
- 3 Under Posture Validation Policies, click **Add Policy**. Type a name and description.
- 4 Under Posture Validation Policy, add at least one posture validation rule.
- 5 Specify "McAfee:McafeePolicyEnforcer" as the posture token, and choose a health level.
- 6 Add a condition set, and specify the value of "McAfee:McAfeePolicyEnforcer:HealthLevel" that should correspond to the posture token. McAfee recommends that you add the following rules for the posture validation policies:

```
Condition: McAfee:McAfeePolicyEnforcer:HealthLevel = 0
```

```
Posture Token: McAfee:McAfeePolicyEnforcer:Healthy
```

```
Condition: McAfee:McAfeePolicyEnforcer:HealthLevel = 10
```

```
Posture Token: McAfee:McAfeePolicyEnforcer:Checkup
Condition: McAfee:McAfeePolicyEnforcer:HealthLevel = 15
Posture Token: McAfee:McAfeePolicyEnforcer:Transition
Condition: McAfee:McAfeePolicyEnforcer:HealthLevel = 20
Posture Token: McAfee:McAfeePolicyEnforcer:Quarantine
Condition: McAfee:McAfeePolicyEnforcer:HealthLevel = 30
Posture Token: McAfee:McAfeePolicyEnforcer:Infected
Condition: McAfee:McAfeePolicyEnforcer:HealthLevel = 100
Posture Token: McAfee:McAfeePolicyEnforcer:Unknown
```

Once the rules are added, they can be used as part of the Network Access Profiles (see [Configure Network Access Profile for NAC managed systems on page 104](#)). You must set up a Network Access Profile for NAC managed systems.

For additional information, see the sections on Posture Validation and Network Access Profiles in the *User Guide for Cisco Secure ACS*.

Configure MPE server as an external Posture Validation Server

To communicate with the ACS server using the HCAP protocol, the MPE server must be configured so that the ACS server recognizes it as an external Posture Validation Server.

The following steps must be performed on the ACS server:

- 1 Open Internet Explorer and go to `https://servername:8443/snowcap/start`, where `servername` is the name of your MPE server.
- 2 At the Security Alert dialog box, click the **Certificate Path** tab.
- 3 Double-click the root certificate. This is typically named `ePO_servernameCA`, where `servername` is the name of your MPE server.
- 4 Click **Install Certificate** to start the Certificate Import Wizard, then click **Next** to start the import process.
- 5 Select **Place all certificates in the following store** and click **Browse**.
- 6 Select **Show physical stores**, then expand the **Third-party Root Certification Authorities** node (Windows 2003 server) or the **Trusted Root Certification Authorities** node (Windows 2000 server) in the tree above. Select **Local Computer** and click **OK**.
- 7 Click **Next**, then **Finish** to import the Policy Enforcer root certificate.
- 8 At the Import Successful dialog box, click **OK**.
- 9 At the View Certificate dialog box, click **OK**.
- 10 At the Security Alert dialog box, click **Yes**, then close Internet Explorer.
- 11 Open the ACS administration web page and go to Posture Validation, then External Posture Validation Setup.

- 12 Click **Add Server**.
- 13 Type a server name and description. In Primary Server configuration, type `https://servername:8443/snowcap/hcap`, where `servername` is the name of your MPE server.
- 14 Type the user name and password that you set in Policy Enforcer for ACS server authentication (see [Set credentials for ACS authentication on page 101](#)). Leave the time-out field as the default value. For the **Trusted Root CA** field, click the drop-down list and select the MPE server's root certificate. This is usually named `ePO_servernameCA`, where `servername` is the name of your MPE server.
- 15 Deselect **Secondary Server configuration**.
- 16 In the Forwarding Credential Types section, select **McAfee:McAfeePolicyEnforcer** from the Available Credentials list, then click the right arrow to move it to the Selected Credentials list.
- 17 Click **Submit** when done.
- 18 Click **Apply and Restart** to save the configuration and restart the ACS server.

Configure Network Access Profile for NAC managed systems

The procedure for configuring Network Access Profiles for NAC managed hosts is beyond the scope of this document. Refer to the Network Access Profiles section in the *User Guide for Cisco Secure ACS*.

Configuration for NAC Agentless Hosts

Systems that do not have the Cisco Trust Agent (CTA) installed are considered "NAC Agentless Hosts." To assess the posture of these systems, you must set up the MPE server to act as an external audit server. You must also create a Network Access Profile for NAC Unmanaged Hosts in ACS.

Configuring an external audit server

For Cisco NAC agentless hosts (no CTA), an external audit server can be used to determine the host's overall health level. MPE supports this audit server configuration via the GAME protocol.

To configure the ACS server to use the MPE server as an external audit server:

- 1 In the ACS Navigation pane, click **Posture Validation**.
- 2 Click the External Posture Validation Audit Setup link to set up an audit server.
- 3 Click **Add Server** to add a new audit server.
- 4 Type a name and description (optional) for this audit server. This can be any name you choose.
- 5 Under **Which Hosts are Audited**, select any value from the list (**Audit All Hosts** is suggested).
- 6 Under **Use These Audit Servers**, set the **Audit Server Vendor** field to **McAfee**.

- 7 For URL, type `https://servername:8443/snowcap/game`, where `servername` is the name of your MPE server.
- 8 Type the user name and password that you set in Policy Enforcer for ACS server authentication (see [Set credentials for ACS authentication on page 101](#)).
- 9 Under Trusted Root CA, select the same ePO root certificate that you used for your external posture validation server.
- 10 Deselect the Validate Certificate Common Name field.
- 11 Deselect the Secondary Server Configuration field.
- 12 Under **Audit Flow Settings**, select a Posture token to use until the audit server results are available.
- 13 In the **Policy String to be sent to the Audit Server** field, type `default` for now (this typically would be a policy name). Leave all the other settings as they are.
- 14 Click **Submit**.
- 15 Click **Apply and Restart**.

Configure Network Access Profile for NAC Agentless Hosts

When using the MPE server as an external audit server to manage agentless systems, you must set up a Network Access Profile for Agentless Hosts in the Cisco ACS server.

- 1 In the ACS Navigation pane, click **Network Access Profiles**.
- 2 Click **Add Template Profile**.
- 3 Specify a name for the profile.
- 4 Select the Agentless Host template.
- 5 Select **Active**, then click **Submit**.
- 6 Click Authentication for your new profile, then click **Allow Posture Validation** under the EAP Configuration section.
- 7 Click **Submit**.
- 8 On the Posture Validation page, click **Posture Validation**, then click **Select Audit**.
- 9 Under **Select Audit Server**, select the name of the audit server you just configured. Under **Fail-open Configuration**, set any desired options, then click **Submit**.
- 10 Click **Done** to return to the Profiles page. Click **Authorization** to configure any authorization rules, as appropriate. For information about authorization rules, see the *User Guide for Cisco Secure ACS*.
- 11 In the ACS Navigation pane, click **System Configuration**.
- 12 Click Service Control.
- 13 Click **Restart** to restart the ACS server.

If you encounter any problems during this process, see [NAC-related troubleshooting on page 95](#).

8

VPN Integration

Topics in this section:

- [Configuring IPsec VPN products](#)
- [Configuring SSL VPN Products](#)
- [Allowing VPN-connected computers access to the VPN appliance](#)

McAfee Policy Enforcer supports the following VPN products:

- Check Point IPsec VPN
- Nortel IPsec VPN
- Cisco IPsec VPN
- Juniper SSL VPN

Configuring IPsec VPN products

To integrate IPsec VPN appliances for use with Policy Enforcer, you configure the appliance according to the instructions in the following sections. McAfee recommends that administrators also ensure that client systems are correctly configured. This may mean that you install an ePO agent and MPE scanner, or other software required by your network security policy.

Check Point

To use a Check Point IPsec VPN appliance for VPN enforcement, you must configure it to use Secure Configuration Verification (SCV), edit the SCV policy file (Local.scv), and install the desktop policy.

Configuring Secure Configuration Verification (SCV)

To configure Secure Configuration Verification (SCV): You must also edit the SCV policy (Local.scv) file and install the desktop policy. For instructions, see [Editing the SCV policy file on page 107](#) and [Installing the desktop policy on page 108](#).

- 1 Open SmartDashboard and log on. In the SmartDashboard console tree under **Network Objects | Check Point**, double-click the appropriate VPN appliance to open the **Check Point Gateway General Properties** dialog box.

- 2 Under **Check Point Products**, select **SecureClient Policy Server**. Close the **Check Point Gateway General Properties** dialog box.
- 3 From the menu, select **Policy | Global Properties**.
- 4 From the navigation pane in the **Global Properties** dialog box, select **Remote Access | Secure Configuration Verification (SCV)**.
- 5 Select **Apply Secure Verification Configurations on Simplified mode Security Policies**. This enables the SCV policy flag for all remote access rules in the simplified policy mode.
- 6 Under **Upon Verification Failure**, select the action to be performed when the client computer fails one or more SCV checks:
 - To drop network access for noncompliant computers, select **Block client's connection**.
 - To allow noncompliant computers access to the network, select **Accept and log client's connection**. Use this setting if you want to test the connections before enforcing the SCV checks.
- 7 Under **Basic configuration verification on client's machine**, select **Policy is installed on all interfaces** to assess the policy on all NICs on the VPN client.
- 8 Close the **Global Properties** dialog box.

Editing the SCV policy file

Edit the SCV policy file (Local.scv) so it refers to the McAfee Policy Enforcer VPN plug-in file (McCmplCk.dll). You must also configure it to use SCV and install the SCV policy. For instructions, see [Configuring Secure Configuration Verification \(SCV\) on page 106](#) and [Installing the desktop policy on page 108](#).



To edit the SCV policy file, you need local or secure shell (SSH) access to the VPN appliance.

- 1 Log on to the Check Point VPN appliance. After accessing the Check Point VPN server, type `Expert` at the command line. Use the same password you used to log on.
- 2 Use `vi` to edit the SCV policy file (Local.scv). The default location is:

```
opt/CPfw1-R55/conf
```



You must edit the file directly on the appliance using `vi`. You cannot edit the file using any other text editor or copy the file from another location to the appliance.

- 3 Locate these lines at the top of the file:

```
:SCVNames (
)
```

- 4 Add these lines (in bold):

```
:SCVNames (
  : (McCmplCk)
    :parameters (
    )
)
```

- 5 Locate these lines near the bottom of the file:

```
:SCVPolicy (
)
```

- 6 Add these lines (in bold):

```
:SCVPolicy (
  : (ckp_scv)
  : (McCmpLCK)
)
```

- 7 Save the file, then exit.

Installing the desktop policy

- 1 In SmartDashboard, select **Policy | Install**.
- 2 Select **Advanced Security** and **Desktop Security**, then click **OK** to install the new desktop policy.

Nortel

To use a Nortel IPSec VPN appliance for VPN enforcement, you must configure the appliance to use a Software and TunnelGuard rule set (SRS), then enable TunnelGuard. The TunnelGuard agent must be installed on the client system.

Configuring a Software and TunnelGuard rule set

To use a Nortel IPSec VPN appliance for VPN enforcement, you must configure the appliance to use SRS and the McAfee Policy Enforcer VPN plug-in file (TGCheck.dll). You must also enable TunnelGuard. For instructions, see [Enabling TunnelGuard on page 109](#). Perform the following steps from a computer that has the MPE scanner installed.

- 1 Point a browser to the IP address of the Contivity management interface.
- 2 Click **MANAGE SWITCH**, then log on as an administrator.
- 3 From the **Management** page in the left pane menu, select **Services | Firewall/NAT**.
- 4 Under **Rule Configuration**, click **Manage Policies** to open the **TunnelGuard Connectivity Manager** dialog box and another logon dialog box. Type the same user name and password you entered in [Step 2](#).
- 5 In the **TunnelGuard Software and Rule Definition Tool** dialog box, click **New Page**. Type a name for the new SRS definition, such as `McAfee`, then click **OK**.
- 6 Click **Folder Browse** to browse to the McAfee Policy Enforcer VPN plug-in file (TGCheck.dll). The default location is:

```
C:\Program Files\McAfee\MPE Scanner
```

You also can specify an alternate location from which to obtain the TGCheck.dll file.

- 7 In the left pane, select the SRS definition you created in [Step 5](#), then highlight it in the right pane to enable the row of buttons at the bottom of the pane.
- 8 Click **A** (the API option).

- 9 Select **File** | **Save**.

Enabling TunnelGuard

To use a Nortel IPSec VPN appliance for VPN enforcement, you must enable TunnelGuard. You must also configure the appliance to use a SRS. For instructions, see [Configuring a Software and TunnelGuard rule set on page 108](#).

- 1 Point a browser to the IP address of the Contivity management interface.
- 2 Click **MANAGE SWITCH**, then log on as an administrator.
- 3 From the **Management** page in the left pane menu, select **Profiles | Groups** to display the default and user-defined groups (\Base is the parent group).
- 4 Click **Edit** next to the parent group for which you want to enable TunnelGuard.
- 5 On the **Groups | Edit | Connectivity** page, click **Configure**. Under **TunnelGuard**, set the following:
 - **TunnelGuard** to **Enabled**.
 - **TunnelGuard: Restricted Filter** to **permit all**.
 - **TunnelGuard: Policy** to the SRS definition you created in [Step 5 on page 108](#).
 - **TunnelGuard: Initial Policy Failure Action** to **Leave Restricted**. Select the **Tear Down Tunnel** option only when you are ready to begin enforcing the VPN policy.
- 6 Click **OK** to save your changes. Before you enforce the McAfee VPN plug-in rule, be sure that the MPE scanner and the TGCheck.dll file are installed on client systems.
- 7 When prompted to verify that **TunnelGuard Filter** is selected in the Current Contivity Tunnel Filter set:
 - a Select the link to the **Profiles--Filters** page.
 - b Select **permit all** from the **Current Contivity Tunnel Filter** list, then click **Edit**.
 - c In the **Tunnel Filter Set** dialog box under **For these Remote Servers**, select **TunnelGuard**, then click **OK**.
- 8 Log off the VPN appliance.

Configuring SSL VPN Products

Policy Enforcer currently supports the Juniper SSL VPN product. To integrate with the Juniper VPN you must create an installation package when you configure the VPN Enforcement Type (see Enforcement Types).

Creating the Juniper SSL VPN installation package

If you are enforcing compliance on VPN-connected computers using Juniper SSL VPN, you need to create a VPN installation package (VPN.zip) and copy it to the VPN appliance. Do this every time you change the VPN policy, and when a new version of the scanner is released. The VPN installation package contains the MPE scanner, VPN plug-in, the VPN policy, and content packages.

- 1 In the console tree, select **McAfee Policy Enforcer**.
- 2 On the **Compliance** tab, select **Enforcement Types**.
- 3 Select the **Policy Enforcer VPN** enforcement type.
- 4 Under **Settings**, select **Juniper SSL**.
- 5 Click **Apply** to save the current entries. The VPN installation package is created when you exit the compliance policy page, or if no changes to the policy have been made for two minutes. The default location is:

C:\Program Files\Common Files\McAfee\Tomcat\webapps\snowcap\VPN\Juniper

Juniper

To use a Juniper Instant Virtual Extranet (IVE) SSL VPN appliance for VPN enforcement:

- 1 Upload the VPN installation package (VPN.zip).
- 2 Add Host Checker policies to the User Authentication Realm.
- 3 Add Host Checker policies to the User Roles.

Uploading the VPN installation package

The VPN installation package contains the MPE scanner, Juniper VPN plug-in, compliance policies, and content. Install the VPN.zip file on the Juniper VPN appliance. By default, the VPN.zip file is created in:

C:\Program Files\Common Files\McAfee\Tomcat\webapps\snowcap\VPN\Juniper

To upload the Host Checker policy file:

- 1 Open the Juniper IVE Administrator logon page, and log on using an IVE administrator account.
- 2 From the left column, open the System Host Checker configuration page (**System | Configuration | Security | Host Checker**).
- 3 Under **Policies**, click **New 3rd Party Policy**.
- 4 In the **Policy Name** field, type an appropriate Host Checker policy name, such as McAfee.

- 5 Click **Browse** next to the Policies File field, then locate the VPN.zip file. Make sure this field contains the full path to this file, including the file name.
- 6 Click **Save Changes**.

The Configuration page should list the new Host Checker policy name from Step 4. If changes are made to the VPN policy, you must regenerate and reload the VPN installation package to the VPN appliance.

Adding the Host Checker policy to the Authentication Realm

From the Juniper IVE Administrator interface:

- 1 In the correct User Authentication realm, open the User Authentication Host Checker page (**Users | Authentication | (Your User) | Authentication Policy | Host Checker**)
- 2 On the Host Checker Policy page, select the **Evaluate Policies** and **Require and Enforce** options for the McAfee and McAfee.FileCheck policies, then click **Save Changes**.

If VPN client users have not yet downloaded the MPE scanner, you may need to leave the **Require and Enforce** option disabled.

Adding the Host Checker policy to the User Roles

From the Juniper IVE Administrator interface:

- 1 Open the User Roles Host Checker Policy page (**Users | Roles | (Your User) | General | Restrictions | Host Checker**).
- 2 Select the **Allow users whose workstations meet the requirements specified by the Host Checker policies** option.
- 3 From the **Available Policies** list, select the two McAfee policies, then click **Add**. This places the McAfee policies in the **Selected Policies** list.
- 4 Click **Save Changes**.

Allowing VPN-connected computers access to the VPN appliance

To allow VPN-connected computers access to their VPN appliance, you must manually add the internal and external interface of the VPN appliance to the scanner configuration policy.

- 1** In the console tree under **Policy Catalog**, select **Policy Enforcer Scanner 2.0.0 | Scan Policies**.
- 2** To create a new named policy, click **Define new policy**, then type a descriptive name, such as `Allow VPN Access`.

To edit an existing named policy, click its name.

- 3** In **Protocol**, specify the protocol (TCP or UDP) to allow. If none is specified, both protocols are allowed.
- 4** In **System**, specify the IP address of the internal and external interfaces to the VPN appliance.
- 5** In **Port**, specify the communication port to allow. If none is specified, all ports are allowed.
- 6** Click **Apply All** to save the current entries.
- 7** If you created a new named policy or want to assign an existing named policy to a new computer:
 - a** Under **Directory** in the console tree, select a computer that is hosting an MPE scanner.
 - b** On the **Policies** tab, select **Policy Enforcer Scanner 2.0.0**.
 - c** In **Scan Policies**, click **Edit**, select the named policy in **Policy Name**, then click **Apply** to assign the named policy to the selected computer.

Changes take effect during the next agent-server communication. If you edited an existing named policy, computers that are already assigned that policy receive it during the next agent-server communication. To initiate communication immediately, send an agent wakeup call. For instructions, see [MPE server management tasks on page 27](#).

9

Frequently Asked Questions

This section answers these commonly asked questions:

- How does McAfee Policy Enforcer work with fast user switching?
- How do I deploy the discovery and enforcement sensor securely?
- What happens to laptops at a coffee shop or hotel? Are these systems quarantined?
- Does McAfee Policy Enforcer work with Cisco Network Admission Control?
- Does McAfee Policy Enforcer work with the 802.1x protocol?
- What happens to computers connected to the network via unsupported VPN software?
- What happens to VoIP phones on the network?
- What happens when multiple systems are connected to the same port of unmanaged switches, hubs, or WAPs?
- When should I deploy one sensor per subnet?
- Does McAfee Policy Enforcer work with multiple NICs?
- Where do I find bandwidth and performance data on McAfee Policy Enforcer?

How does McAfee Policy Enforcer work with fast user switching?

Scanning and enforcement take place on the system as a whole, independent of the logged on user. When scanning the local computer, the scanner logs on to the computer as a service under the Local System account. When scanning remote systems, the scanner uses the credentials provided in the **Policy Enforcer Scanner Scan Policies** page.

Enforcement affects the network access of all users. If one user session is noncompliant, the entire system is quarantined.

How do I deploy the discovery and enforcement sensor securely?

We recommend placing the discovery and enforcement sensor near switches in a secured area on the network. Although communication between the sensor and server is secure, SNMP communication is not. The sensor uses a read-write community string to change the network access mode (allow, quarantine, or drop) on switch ports.

If switches use IP address ranges different than computers (management network versus user network), you can also use an Access Control List (ACL) to secure the discovery and enforcement sensor. Give the sensor host computer access to the management network, then add the following data to the ACL:

- Sensor host computer's IP address.
- Read-only SNMP community for all switches.
- Read-only SNMP community for all routers.
- Read-write SNMP community for all switches.

In this case, we recommend using a dedicated server with a static IP address as the sensor host computer to ensure SNMP security. We recommend that this dedicated server use one NIC for the management network and another for the user network to retain security between networks.

What happens to laptops at a coffee shop or hotel? Are these systems quarantined?

This is only a concern if the scanner is installed on the computer. To prevent noncompliant computers from being quarantined when they operate outside the LAN, you must define computer conditions for each rule set in the compliance policy. Each rule in the rule set applies only to computers that match these conditions. For example, if you define a condition "IP address is in specified range," each rule applies only to computers with those IP addresses. In this way, you can apply the compliance policy to computers only when they are connected to the LAN.

To use a different definition of compliance (for example, a less stringent one) to assess computers operating outside the LAN, you must create separate rule sets with separate and, most likely, opposite conditions. For example, if you use IP address range as the condition, the stringent "on the LAN" rule sets apply only to computers assigned IP addresses within the specified range and the less stringent "outside the LAN" rule sets apply only to computers assigned IP addresses outside the same range.

Does McAfee Policy Enforcer work with Cisco Network Admission Control?

Yes. McAfee Policy Enforcer 2.0 supports Cisco Network Admission Control (NAC).

Does McAfee Policy Enforcer work with the 802.1x protocol?

The IEEE 802.1X protocol will be supported in a future version of McAfee Policy Enforcer.

What happens to computers connected to the network via unsupported VPN software?

Computers that are accessing the network remotely via unsupported VPN software are not supported by McAfee Policy Enforcer. In addition, unmanaged systems that are accessing the network remotely are not supported regardless of the VPN software in use.

What happens to VoIP phones on the network?

How phones or fax machines connected to Voice over Internet Protocol (VoIP) phone adapters, such as Cisco IP phones are affected by McAfee Policy Enforcer depends on these factors:

- Whether the phone adapter is SNMP-managed; for example, if it acts as a router or switch.
- Whether the phone and computer are connected to the same port.

If the adapter is SNMP-managed, the phone and computers connected to it are handled as individual systems. Because the operating systems running on VoIP phones fall outside the compliance policy, they are unaffected by McAfee Policy Enforcer.

If the phone and computer are connected to the same port on the VoIP phone adapter and the port is quarantined or dropped using switch enforcement, the network access mode of both systems can be affected. Switch enforcement applies to the port itself, so the network access mode (allow, quarantine, or drop) of all systems connected to the same port is changed regardless of their compliance status. By default, network access mode is changed only when one system is connected to a switch port. When the port is quarantined, phone service is unaffected as long as the phone adapter has access to the PBX from the remediation area. When the port is dropped, the phone service is disconnected. Once a switch port is dropped, you must manually allow or quarantine the same port to restore network access to the affected systems.

What happens when multiple systems are connected to the same port of unmanaged switches, hubs, or WAPs?

Quarantining noncompliant, unmanaged systems or dropping switch ports can affect all systems that are connected to the same port because these actions use switch enforcement. Switch enforcement applies to the port itself, so the network access mode (allow, quarantine, or drop) of all systems connected to the same port is changed regardless of their compliance status. By default, network access mode is changed only when one system is connected to a switch port. Once a switch port is dropped, you must manually allow or quarantine the same port to restore network access to the affected systems.

When should deploy one sensor per subnet?

To protect systems using static IP addresses, you need to deploy one broadcast detection sensor on each protected subnet. Broadcast detection finds rogue systems (unauthorized systems or systems that are not being managed by this ePO server) that are accessing the network locally (wired or wireless). IP spoofing is an example of one type of unauthorized access that broadcast detection protects against.

Does McAfee Policy Enforcer work with multiple NICs?

Yes, all functions of the MPE sensor and the MPE scanner work with multiple network interface cards (NICs).

A system with multiple NICs appears multiple times in the **System List** because the MAC address is used as the unique identifier. You can sort the list by system name to group multiple occurrences of the same system together.

Where do I find bandwidth and performance data on McAfee Policy Enforcer?

The *McAfee Policy Enforcer 2.0 Bandwidth and Performance Guide* provides data on how the software impacts network performance, system performance, and product scalability. This guide will be available after the product release.

Glossary

Product-specific and McAfee terms

For industry terms, see the McAfee Avert Labs website: http://www.mcafee.com/us/threat_center/glossary.html

agent	See <i>ePO agent</i> .
agent installation package	The Setup program and all files needed to install the ePO agent.
agent language packages	The set of files distributed to managed computers for viewing the ePO agent interface, Agent Monitor, in languages other than English.
Agent Monitor	The ePO agent interface, which appears optionally on managed computers, where you can immediately run tasks that are normally initiated by the agent, at predefined intervals.
agent wakeup call	Agent-server communication initiated from the ePO server. Compare to <i>SuperAgent wakeup call</i> .
agent-server communication	Any communication between ePO agents and the server where data is exchanged.
agent-to-server communications interval	ASCI; the time period between predefined agent-server communications.
allow	A network access mode in which systems are granted full access to the network. Compare to <i>drop</i> and <i>quarantine</i> .
ASCI	See <i>agent-to-server communications interval</i> .
assessment	The enforcement phase where the compliance status of systems is determined by running the checks in the compliance policy. Compare to <i>definition</i> , <i>detection</i> , <i>enforcement</i> , and <i>remediation</i> .
audit	An enforcement mode that assesses systems for adherence to the compliance policy, always allows them on the network regardless of the scan results, then reports the results. Compare to <i>enforce</i> and <i>ignore</i> .
Avert Labs	McAfee Avert Labs; a research center that supports the computing public and McAfee customers by researching the latest threats, and by uncovering threats that may arise in the future.
branch	Branches on the master repository for storing and distributing different versions (Current, Previous, Evaluation) of selected updates. See also <i>selective updating</i> .

broadcast detection	A type of detection where the sensor monitors broadcast packets to identify systems as they request access to the network. Compare to <i>DHCP detection</i> .
check	A script that detects the presence of security products, security patches, or virus infections.
check category	A collection of related checks.
check result	The result of a check is <i>true</i> if the condition specified for the check category is present. For example, the result of a security bulletin check is true if the vulnerability described in the bulletin is present (that is, if the security patch is not installed), and the result of a virus infection check is true if the specified virus is present and active.
checking in	The process of adding files to the master repository.
client tasks	Tasks that are executed on a managed computer.
community string	The password, such as "private" or "public," that is used to administer a device using SNMP; provides read-only or read-write permissions.
complete properties	The entire set of properties being exchanged during agent-server communication. Compare to <i>incremental properties</i> and <i>properties</i> .
compliance policy	The term that collectively refers to the LAN and VPN policies. See also <i>LAN policy</i> and <i>VPN policy</i> .
compliant	Adhering to the compliance policy. Compare to <i>noncompliant</i> , <i>inactive</i> , <i>exception</i> , and <i>indeterminate</i> .
computer	The term used to collectively refer to computers, such as a desktop, server, or laptop computer.
configuration policy	The settings that determine how each product that can be managed by ePolicy Orchestrator behaves on managed computers.
configuration settings	See <i>policy</i> .
console tree	The left pane of the ePO console that shows the items available in the console.
console tree item	An individual icon in the console tree.
content update	Policy Enforcer content that is periodically retrieved from the McAfee website. See also <i>infection checks</i> , <i>Microsoft security bulletin checks</i> , <i>product checks</i> , and <i>server update package</i> .
continuous compliance	The ability to schedule scans at more frequent intervals than during detection.
credentials	The user name and password required to perform scanning, installation, and other functions.
custom agent installation package	An agent installation package that performs the installation with the user credentials you provide, rather than credentials of the currently logged-on user.

DB Merge Tool	A program (avidb_merge_tool.exe) that combines data from multiple databases into a new or existing database. The resulting merged database is used for reporting purposes only.
definition	The enforcement phase where the definition of compliance is created. Compare to <i>assessment</i> , <i>detection</i> , <i>enforcement</i> , and <i>remediation</i> . A scheduled task that deploys all products currently checked in to the master repository at once. It enables you to schedule product installation and removal during off-peak hours or during the policy enforcement interval.
details pane	The right pane of the ePO console, which shows details of the currently selected console tree item.
detection	The enforcement phase where systems on the LAN are identified as they request access to the network. Compare to <i>assessment</i> , <i>definition</i> , <i>enforcement</i> , and <i>remediation</i> .
detection definition files	DAT files (signatures) that identify the characteristics of a threat, its detection, and the available actions to counter the threat.
DHCP detection	A type of detection where the MPE sensor monitors DHCP response packets to identify systems as they request access to the network. Compare to <i>broadcast detection</i> .
Directory	In the console tree, the list of all computers to be managed by ePolicy Orchestrator; the link to the primary interfaces for managing these computers.
distributed software repositories	A collection of websites or computers located across the network providing bandwidth-efficient access to managed systems. They store the files that managed systems need to install supported products and their updates. See also <i>fallback repository</i> , <i>master repository</i> , <i>source repository</i> , and <i>SuperAgent distributed repository</i> , and <i>unmanaged distributed repository</i> .
download site	The McAfee website for retrieving product, DAT, and engine updates.
drop	A network access mode in which systems are denied access to the network. Compare to <i>allow</i> and <i>quarantine</i> .
enforce (enforcement mode)	An enforcement mode that assesses systems for adherence to the rule set, enforces the network access mode based on the scan results, and reports the results. Compare to <i>audit</i> and <i>ignore</i> .
enforcement	The enforcement phase where the network access mode of systems is changed based on scan results, or is taken as an action. Compare to <i>assessment</i> , <i>definition</i> , <i>detection</i> , and <i>remediation</i> . See also <i>self-enforcement</i> , <i>switch enforcement</i> , and <i>VPN enforcement</i> .
enforcement mode	A setting in a rule set that determines how rules in the rule set are applied to systems. See also <i>audit</i> , <i>enforce (enforcement mode)</i> , and <i>ignore</i> .
ePO agent	A program that performs background tasks on managed computers, mediates all requests between the server and managed products on these computers, and reports back to the server on the status of these tasks.

ePO console	The interface of ePolicy Orchestrator software that is installed on the ePO server and remotely controls and monitors managed computers. Compare to <i>ePO remote console</i> .
ePO database	The database that stores all agent data received by the server and all settings made on the server itself. See also <i>ePO database server</i> .
ePO database server	The computer that hosts the database; can be the same computer where the ePO server is installed or a separate computer.
ePO remote console	The interface of ePolicy Orchestrator software that is installed on a computer other than the ePO server. Compare to <i>ePO console</i> .
ePO server	The back-end component of ePolicy Orchestrator software.
error reporting utility	A utility that tracks and logs failures in the McAfee software on your system. The information is used for troubleshooting.
event	During agent-server communication, data exchanged about each managed computer and its managed products (for example, policy settings and product version number).
exception	Systems to which the LAN or VPN policy does not apply, such as printers, routers, and switches. See also <i>trusted systems</i> . Compare to <i>inactive</i> , <i>compliant</i> , <i>noncompliant</i> , and <i>indeterminate</i> .
fallback repository	A type of distributed software repository used if managed computers cannot contact any of their predefined distributed repositories. See also <i>replication</i> .
framepkg.exe	See <i>agent installation package</i> .
full properties	All properties that can be exchanged during agent-server communication. Compare to <i>minimal properties</i> .
full replication	The act of copying all files from the master repository to distributed software repositories. Compare to <i>incremental replication</i> .
global administrator	A user account with read, write, and delete permissions, as well as rights to all operations; specifically, operations that affect the entire installation and are reserved for only the global administrator. Compare to <i>global reviewer</i> , <i>site administrator</i> , and <i>site reviewer</i> .
global reviewer	A user account with read-only permissions, that can view all settings in the software for an entire installation, but cannot change any settings. Compare to <i>global administrator</i> , <i>site administrator</i> , and <i>site reviewer</i> .
global updating	A method of deploying product updates as soon as the files are checked in to the master repository, without user intervention.
group	One or more managed systems defined by an administrator, used to manage security settings and analyze query data. Groups can be determined by any criteria.

host	A term used to refer to computers on which an MPE component is installed, such as sensor host computers.
ignore	An enforcement mode that disables the rule set. Compare to <i>audit</i> and <i>enforce (enforcement mode)</i> .
immediate event forwarding	The act of immediately sending events of a specific severity or higher to the ePO server once a predefined number of events is collected. This communication is separate from other agent-server communication.
inactive	The status of a system that has not been detected on the network within a defined time period. Compare to <i>compliant</i> , <i>noncompliant</i> , <i>exception</i> , and <i>indeterminate</i> .
inactive agent	Any agent that has not communicated with the server within a specified time.
incremental properties	Properties that have changed since the last agent-server communication. See also <i>complete properties</i> and <i>properties</i> .
incremental replication	The act of copying only files from the master repository that differ from the contents of the distributed software repository. Compare to <i>full replication</i> .
indeterminate	The status of a system that matches a rule set, but doesn't match any of the operation systems in the rules; or on which the scan could not be completed. Compare to <i>compliant</i> , <i>exception</i> , <i>inactive</i> , and <i>noncompliant</i> .
infection checks	A type of content update that contains checks for the presence of selected, active virus infections. Compare to <i>Microsoft security bulletin checks</i> , <i>product checks</i> , and <i>server update package</i> .
inheritance	Within a hierarchy, the application of settings defined for an item from the one above it.
integrated MPE server	The MPE server that is always installed with the ePO server. Compare to <i>standalone MPE server</i> .
LAN policy	The definition of compliance that is applied to systems that connect to the network from the LAN; includes a collection of rule sets, trusted system rules, and LAN-specific settings, such as the quarantine VLAN. Compare to <i>VPN policy</i> .
local message	The text that appears on managed computers when they are deemed noncompliant while attempting to access the network locally.
Lost&Found group	A group for temporarily storing computers whose appropriate location in the Directory cannot be determined.
managed computer	A system on which the ePO agent is installed.
managed products	Security products (McAfee and third-party) that are managed by ePolicy Orchestrator.

master repository	A type of distributed software repository whose contents is the standard for all distributed repositories. Typically, the contents of the master repository are defined from the source repository contents and additional files added manually. See also <i>pull</i> and <i>replication</i> .
MIB (Management Information Base)	A database of managed objects or variables that can be read or set using SNMP.
Microsoft security bulletin checks	A type of content update that contains checks for Microsoft application, operating system, and Internet Explorer security patches. Compare to <i>infection checks</i> , <i>product checks</i> , and <i>server update package</i> .
minimal properties	A subset of the full properties that can be exchanged during agent-server communication. Compare to <i>full properties</i> .
MPE scanner	A distributed component of Policy Enforcer, installed on host computers throughout the network and in the VPN environment. It determines whether computers meet the minimum requirements of the compliance policy.
MPE sensor	A distributed component of Policy Enforcer, installed on managed computers throughout the network. It performs broadcast detection, DHCP detection, topology discovery, topology mapping, and switch enforcement.
MPE server	See <i>integrated MPE server</i> or <i>standalone MPE server</i> .
named policy	A collection of policy settings that can be assigned independently of the Directory structure.
network access device (NAD)	Hardware devices that systems use to gain access to the network, such as routers, switches, or VPN appliances.
network access device support	Configuration information (OIDs in vendor-specific MIBs) within the server update package that extends support for enforcement, topology discovery, and topology mapping to additional network access devices, such as switches.
network access mode	The level of network access granted to systems based on scan results or taken as an action. See also <i>allow</i> , <i>drop</i> , and <i>quarantine</i> .
noncompliance actions	A setting in the rule that determines which network access mode is applied and the message that appears when a system is noncompliant.
noncompliance mode	A setting in the rule that determines how the results of checks (true or false) are interpreted when evaluating whether a system is compliant or noncompliant.
noncompliant	The status of a system that doesn't adhere to the LAN or VPN policy.
OID (object identifier)	Defines the location of variables in MIBs. Policy Enforcer software uses OIDs that set data on switches during enforcement, and that read data during topology discovery and topology mapping.
OUI (Organizational Unique Identifier)	Identity of the vendor network-connected systems, consisting of the first 24 bits of a system's MAC address.
policy	The configuration settings of a managed product that are defined and managed by ePolicy Orchestrator.

policy enforcement	The act of applying predefined settings on managed computers at predetermined intervals.
policy enforcement interval	The time period when the ePO agent enforces the settings it has received from the ePO server.
policy files	Policy settings for one or more products that are saved to the local drive of the ePO server, but cannot be accessed via a remote console.
policy pages	Part of the ePO console where you set policies and create scheduled tasks for managed products. Policy pages are stored on individual servers, not added to the master repository.
product checks	<p>A type of content update that contains checks for McAfee and third-party security products, including anti-virus, firewall, and intrusion prevention products.</p> <p>Compare to <i>infection checks</i>, <i>Microsoft security bulletin checks</i>, and <i>server update package</i>.</p>
production VLAN	<p>The VLAN value of a switch port that is saved when the system attached to it is quarantined, then restored when the system is allowed full access to the network, for example, when the system is deemed compliant.</p> <p>Compare to <i>quarantine VLAN</i>.</p>
properties	Data exchanged during agent-server communication that includes information about each managed computer, such as hardware and software, and its managed products, such as specific policy settings and product version number.
pull	The act of copying files from a source or fallback repository to the master repository. Because additional files can be added to the master repository manually, only those files on the source or fallback repository are overwritten.
quarantine	<p>A network access mode in which systems are redirected to the remediation area or only allowed access to network resources in the remediation list.</p> <p>Compare to <i>allow</i> and <i>drop</i>.</p>
quarantine VLAN	<p>The VLAN value that defines the remediation area.</p> <p>Compare to <i>production VLAN</i>.</p>
remediation	<p>The enforcement phase when systems are updated to bring them into compliance with the LAN or VPN policy.</p> <p>Compare to <i>assessment</i>, <i>definition</i>, <i>detection</i>, and <i>enforcement</i>.</p>
remediation area	A segregated part of the network, such as a VLAN, where noncompliant systems are redirected for the primary purpose of bringing them into compliance.
remediation list	The list of network resources to which a scanner host computer is allowed access when it is quarantined. This list always includes the computer's ePO server, standalone MPE server, DNS server, and ePO distributed repositories.
remediation portal	A web portal that provides instructions to users on bringing their systems into compliance, then allows them to rescan their systems.
remediation server	Computers, which noncompliant systems need to access for remediation, that contain update packages.
remote console	See <i>ePO remote console</i> .

replication	The act of copying files from the master repository to other distributed software repositories. See also <i>full replication</i> and <i>incremental replication</i> .
Repository	The location that stores policy pages used to manage products.
repository list	The sitelist.xml file, used by McAfee security products with the AutoUpdate program, that accesses distributed repositories and retrieves packages.
rogue system sensor	A distributed component of the Rogue System Detection feature in the ePolicy Orchestrator software, installed on managed computers throughout the network. It performs broadcast detection.
rogue system sensor	A distributed component of the Rogue System Detection feature in the ePolicy Orchestrator software, installed on managed computers throughout the network. It performs broadcast detection.
rule	A combination of checks, operating systems and other criteria, and network access mode that defines a single requirement of the compliance policy.
rule set	A collection of related rules with an associated enforcement mode.
scan	A close examination of a system to determine its adherence to the defined compliance policy.
scanner	See <i>MPE scanner</i> .
selective updating	The ability to specify which version of updates you want managed computers to retrieve from distributed software repositories. See also <i>branch</i> .
self-enforcement	The type of enforcement performed on scanner host computers on the LAN when the scanner examines the managed computer on which it is running. A noncompliant computer remains in the production VLAN, but is allowed access only to network resources in the remediation list. Compare to <i>switch enforcement</i> and <i>VPN enforcement</i> .
sensor	See <i>MPE sensor</i> or <i>rogue system sensor</i> .
Server Configuration program	The cfgnaims.exe program that changes the SQL Server user account information in ePolicy Orchestrator when you change that information in another program, such as SQL Server Enterprise Manager.
server events	Activity on the ePO server that is recorded by the Windows Event Viewer. This information is not stored in the database, so it is not available for reporting purposes.
server tasks	Tasks that are executed on the ePO server.
server update package	A type of content update that contains information, such as network access device support and check categories, that is stored on the MPE server. Compare to <i>infection checks</i> , <i>Microsoft security bulletin checks</i> , and <i>product checks</i> .
site	In the console tree, a logical collection of entities assembled for ease of management; can contain groups or computers, and can be organized by IP address range, IP subnet mask, location, department, and others.

site administrator	A user account with read, write, and delete permissions, as well as rights to all operations for the specified site (except those restricted to the global administrator), and for all groups and computers under it on the console tree. Compare to <i>global reviewer</i> , <i>global administrator</i> , and <i>site administrator</i> .
site reviewer	A user account with read-only permissions, that can view all settings in the software for the specified site, but cannot change any settings. Compare to <i>global administrator</i> , <i>global reviewer</i> , and <i>site administrator</i> .
sitelist.xml	See <i>repository list</i> .
source repository	A type of distributed software repository from which the master repository retrieves files. Typically, the source repository is the McAfee website or another master repository. See also <i>pull</i> .
spanned port	A switch port that monitors the port to which the DHCP server is connected.
standalone MPE server	The MPE server when it is installed on a separate computer from the ePO server computer. Compare to <i>integrated MPE server</i> .
starting router	The router on the LAN from which the MPE sensor starts topology discovery.
starting switch	The switch on the LAN from which the MPE sensor starts topology discovery.
SuperAgent	A type of agent for Windows, with the ability to send wakeup calls to all ePO agents in the same subnet. See also <i>global updating</i> , <i>SuperAgent wakeup call</i> , and <i>SuperAgent distributed repository</i> .
SuperAgent distributed repository	A type of distributed software repository that takes advantage of the HTTP capabilities of the SuperAgent to create a repository without a dedicated server to host it. See also <i>replication</i> .
SuperAgent wakeup call	The ability to prompt each SuperAgent and all ePO agents in the same subnet to contact the server when needed, rather than waiting for the next agent-server communication. Compare to <i>agent wakeup call</i> .
switch enforcement	A type of enforcement that is performed by the MPE sensor on switch ports. It occurs automatically based on the results of a scan, or is initiated manually from the software. A system is <i>allowed</i> , <i>quarantined</i> , or <i>dropped</i> by reconfiguring the switch port to which it is connected. Compare to <i>self-enforcement</i> and <i>VPN enforcement</i> .
system	A term used to refer to computers, printers, routers, and other hardware devices that sensors can detect.
topology discovery	The process of enumerating the network access devices on the LAN and their relationship to each other.
topology mapping	The process of using network topology data to quickly find newly detected systems.
trusted system rules	The conditions that define a trusted system.

trusted systems	<p>Systems, such as mission-critical servers, that always need full access to the network regardless of their adherence to the compliance policy. Trusted systems are always scanned and reported on, but are never quarantined or dropped from the network.</p> <p>See also <i>exception</i>.</p>
unmanaged distributed repository	<p>A type of distributed software repository whose content is updated manually, rather than by ePolicy Orchestrator.</p>
unmanaged products	<p>Installed security products that are not managed by ePolicy Orchestrator.</p>
unmanaged system	<p>A system without an ePO agent.</p>
updates	<p>Files from McAfee that provide more current information to a product. Updates can include upgraded software components and files containing revised information about existing threats and new information about recently identified threats.</p> <p>See also <i>detection definition files</i>.</p>
updating	<p>The process of installing updates to existing products or upgrading to new versions of products.</p>
VPN appliance	<p>The hardware device, such as an appliance or server, that provides the interface between the VPN and the network.</p>
VPN client software	<p>Software provided by the VPN vendor and installed on the managed computer that authenticates and provides VPN access to the network.</p>
VPN enforcement	<p>A type of enforcement that is performed by the VPN client or appliance. A computer is <i>allowed</i> or <i>dropped</i> by the vendor-specific VPN client software based on scan results.</p> <p>Compare to <i>self-enforcement</i> and <i>switch enforcement</i>.</p>
VPN installation package	<p>A collection of Policy Enforcer files, including the VPN policy, MPE scanner, and VPN plug-in file, that must be installed in the VPN environment to extend enforcement to VPN-connected computers.</p>
VPN plug-in file	<p>A McAfee application extension (.dll) file that communicates between the components in the VPN environment and the MPE scanner to determine whether to allow or deny computers access to the network.</p>
VPN policy	<p>The definition of compliance that is applied to computers connecting to the network through VPN; includes a collection of rule sets, trusted system rules, and VPN-specific settings.</p> <p>Compare to <i>LAN policy</i>.</p>
VPN portal	<p>Web portal provided by the VPN vendor that authenticates and provides VPN access to the network.</p>
VPN-connected computer	<p>A computer that is connected to the network through VPN.</p>

Index

A

- access permission, and ePO user roles [11](#)
- access to
 - network, broadcast detection [42](#)
 - network, DHCP detection [43](#)
 - Nortel IPSec VPN [112](#)
 - Policy Enforcer, for ePO user roles [11](#)
 - remediation portal [81](#)
 - resources, when quarantined [65](#)
 - VPN appliance [112](#)
- ActiveX scanner
 - new feature [19](#)
- agent wakeup call
 - enforce policy changes [112](#)
- allow access
 - to CheckPoint IPSec VPN [112](#)
- assessment, scanning
 - remote systems [58](#)
 - the local computer [58](#)
 - VPN-connected computers [59](#)
- audience for this guide [20](#)
- Audit, enforcement mode [63](#)
- automatic
 - remediation [18](#), [82](#)
- automatic responses
 - defined [90](#)
- Avert Labs Threat Center [22](#)

B

- beta program website [22](#)
- boundaries of
 - switch enforcement [40](#)
 - topology discovery [40](#)
- broadcast detection [42](#)
- browser redirection, setting up for remediation [87](#)
- build packages
 - compliance policy settings [69](#)

C

- check packages, types of [14](#)
- CheckPoint IPSec VPN, allowing access [112](#)
- Cisco NAC

- components [60](#), [96](#)
- CTA (Cisco Trust Agent) [96](#)
- enforcement framework
 - support, new feature [16](#)
- integration [96–105](#)
- setup requirements [99](#)
- compliance policy
 - creating VPN installation packages [110](#)
 - enforcement [53](#)
 - network access modes [71](#)
 - policy definition [67](#)
 - settings for enforcement zones [69](#)
- components
 - Cisco NAC [60](#)
 - Cisco NAC integration [96](#)
 - communication between [26](#)
 - for remediation [76](#)
 - MPE scanners [48](#)
 - MPE sensors [35](#)
 - MPE servers [28](#)
- components of Policy Enforcer [23](#)
 - scanners [48](#)
 - sensors [35](#)
 - servers [28](#)
- configuration
 - and managing sensors [48](#)
- contact information [22](#)
- continuous compliance scanning, about [52](#)
- CTA (Cisco Trust Agent) [96](#)
- custom filter, defined [90](#)
- custom policy
 - vs. default, for sensors [31](#)
- customer service, contacting [22](#)

D

- DAT files
 - Avert Labs notification service [22](#)
 - update website [22](#)
- default rules, defined [72](#)
- default sensor policy [31](#)
- definition of terms (See glossary)
- deploy MPE scanners, overview [24](#)

- deploying
 - MPE servers in a cluster [28](#)
- detection
 - broadcast [42](#)
 - DHCP [43](#)
 - host [41](#)
 - sensors [35](#)
- DHCP detection [43](#)
- download website [22](#)
- drop, network access mode [13](#)

E

- Enforce, enforcement mode [63](#)
- enforcement [58](#)
 - and enforcement zones [64](#)
 - assessment phase [58](#)
 - enforcement phases [58](#)
 - how it works through VPN [59](#)
 - methods [54](#)
 - modes [63](#)
 - self-enforcement phase [58](#)
 - switch enforcement phase [58](#)
 - VPN enforcement [59](#)
- enforcement types [58–62](#)
- enforcement zones
 - and policy enforcement [64](#)
 - compliance policy settings [69](#)
 - new feature [17](#)
 - priority, about [66](#)
 - settings for [69](#)
- engine updates [22](#)
- ePolicy Orchestrator
 - integration with [9](#)
 - roles and MPE access permission [11](#)
- ePolicy Orchestrator topics (See ePO online Help)
 - agent wakeup call
 - configuring automatic responses
 - distributing rogue system sensors
 - ePO server tasks
 - Rogue System Detection
 - evaluating McAfee products, download website [22](#)

- exception systems
 - vs. trusted systems [75](#)
- F**
- features, new [16–19](#)
- H**
- host detection
 - configuring and managing sensors [48](#)
- HotFix and Patch releases (for products and security vulnerabilities) [22](#)
- I**
- Ignore, enforcement mode [63](#)
- install VPN desktop policy [108](#)
- integrated server
 - defined [29](#)
 - deployment with [29](#)
- integration
 - Cisco NAC [96](#)
 - of policies [9](#)
 - support and vendors, overview [25](#)
 - with ePolicy Orchestrator [9](#)
- J**
- Juniper SSL VPN
 - allowing access [112](#)
 - installation package, creating [110](#)
- K**
- KnowledgeBase search
 - McAfee default rules (KB46370) [72](#)
 - setting up browser redirection, example (KB4654) [87](#)
 - website [22](#)
- L**
- local scanning [13](#)
- M**
- managed systems
 - assessed by local scanning [13](#)
 - automatic remediation [82](#)
 - defined [10](#)
 - in Cisco NAC environment [97](#)
 - remediation of [83](#)
- McAfee default rules, defined [72](#)
- McAfee Policy Enforcer
 - components [23](#)
 - process flow for using [23](#)
 - rogue system sensors and [36](#)
- MPE scanners [48](#)
- MPE sensors [35](#)
 - deploying [35](#)
- MPE servers [28–35](#)
- multiple enforcement zones, new feature [17](#)
- N**
- NAC, Cisco network [96](#)
- network access modes [38](#)
 - compliance requirements [71](#)
 - for VPN connections [59](#)
- network environment, Cisco NAC [96](#)
- network traffic, packet capture [95](#)
- new features [16–19](#)
 - automatic remediation [18](#)
 - Cisco NAC enforcement framework support [16](#)
 - multiple enforcement zones [17](#)
 - on-demand ActiveX scanner [19](#)
- noncompliant systems
 - accessing the remediation portal [81](#)
 - defined [88](#)
- Nortel IPSec VPN, allowing access [112](#)
- O**
- on-demand ActiveX scanner, new feature [19](#)
- P**
- packet capture of network traffic [95](#)
- permissions
 - access to Policy Enforcer [11](#)
- phases of enforcement [58](#)
- policy definition
 - compliance [67](#)
- policy enforcement (See enforcement)
- primary and non-primary sensors
 - about [36](#)
- product documentation
 - download site [22](#)
 - types and descriptions [21](#)
- product information, where to find [21](#)
- product permissions
 - ePO user roles [11](#)
- product upgrades [22](#)
- professional services, McAfee resources [22](#)
- Q**
- quarantine
 - for managed systems [65](#)
 - for system or switch port [66](#)
 - for unmanaged systems [66](#)
- quarantined systems
 - access to resources [65](#)
 - rescanning after remediation [83](#)
- R**
- remediation [76–77](#)
 - automatic [82](#)
 - components and elements for [76](#)
 - for VPN enforcement [87](#)
 - of managed systems [83](#)
 - of unmanaged systems [85](#)
 - rescanning quarantined systems [83](#)
 - setting up browser redirection [87](#)
- remediation list
 - specifying resources in [81](#)
- remediation portal
 - access for noncompliant systems [81](#)
 - defined [14](#)
 - overview [80](#)
- remote scanning [13](#)
 - for unmanaged systems [51](#)
- reports
 - accessing for the first time [92](#)
 - templates [92](#)
- rescanning a quarantined system [83](#)
- resources, for product information [21](#)
- rogue system sensors [36](#)
- rule sets [70–75](#)
- rules
 - default McAfee [72](#)
- S**
- scanner
 - associating with standalone servers [49](#)
 - uninstalling, about [49](#)
 - when scans are initiated [49](#)
- scanner log files
 - changing logging level [93](#)
 - defined [93](#)
 - location [93](#)
- scanner, installing
 - manually using Setup [49](#)
- scanning
 - continuous compliance [52](#)
 - local [13](#)
 - remote [13](#)
 - the local computer, defined [58](#)
 - VPN-connected computers, defined, illustrated [59](#)
 - when it is initiated [49](#)
- scanning remote systems
 - defined [58](#)
 - disabling continuous compliance scanning, about [52](#)

- illustrated [58](#)
 - Security Headquarters (See Avert Labs)
 - security updates, DAT files and engine [22](#)
 - self-enforcement
 - and network access mode [13](#)
 - defined [58](#)
 - defining the remediation list [81](#)
 - enforcement methods [54](#)
 - illustrated [58](#)
 - sensor log files
 - changing logging level [94](#)
 - defined [94](#)
 - location of [94](#)
 - sensor policies
 - custom vs default [31](#)
 - default policy [31](#)
 - defined [31](#)
 - sensors [35](#)
 - configuring and managing [48](#)
 - host detection [48](#)
 - primary and non-primary, about [36](#)
 - rogue system [36](#)
 - topology discovery and mapping [35](#)
 - server update package [14](#)
 - ServicePortal, technical support [22](#)
 - setup requirements for Cisco NAC [99](#)
 - standalone server
 - associating sensors with [36](#)
 - deploying with [30](#)
 - managing scanners [49](#)
 - submit a sample, Avert Labs [22](#)
 - subnet status, defined [89](#)
 - SuperAgent
 - defined [125](#)
 - switch enforcement
 - and network access modes [13](#)
 - boundaries [40](#)
 - defined [58](#)
 - enforcement methods [54](#)
 - illustrated [58](#)
 - sensors [35](#)
 - unmanaged systems [41](#)
 - switch ports
 - network access modes [38](#)
 - quarantining [66](#)
 - system status, defined [88](#)
- T**
- tasks
 - audit compliance policy, overview [25](#)
 - configure MPE server, overview [23](#)
 - define compliance policy [24](#)
 - define compliance policy, overview [24](#)
 - deploy MPE scanners, overview [24](#)
 - deploy MPE sensors, overview [24](#)
 - enforce compliance policy, overview [25](#)
 - set up remediation portal, overview [24](#)
 - set up support, vendor integration, overview [25](#)
 - technical support, contacting [22](#)
 - Threat Center (See Avert Labs)
 - threat library [22](#)
 - topology discovery
 - and switch enforcement [41](#)
 - boundaries [40](#)
 - data needed [37](#)
 - frequency [39](#)
 - how it works [37](#)
 - illustrated [40](#)
 - preventing overlaps [38](#)
 - sensors [35](#)
 - topology mapping
 - frequency [39](#)
 - how it works [39](#)
 - sensors [35](#)
 - training, McAfee resources [22](#)
 - trusted systems
 - defined [69](#)
 - vs. exception systems [75](#)
 - typeface conventions and symbols, using this guide [20](#)
- U**
- uninstalling
 - MPE scanners, ePO deployment task [49](#)
 - unmanaged systems
 - defined [10](#)
 - detection [26](#)
 - in Cisco NAC environment [98](#)
 - remediation of [85](#)
 - remote scanners and [51](#)
 - switch enforcement [41](#)
 - updates, DAT files and engine [22](#)
 - updating contents
 - check packages [14](#)
 - server update packages [14](#)
 - upgrade website [22](#)
 - using this guide [20](#)
- V**
- Virus Information Library (See Avert Labs Threat Library)
 - VPN appliances
 - allowing VPN-connected computers access [112](#)
 - VPN enforcement [59](#)
 - allowing VPN-connected computers access [112](#)
 - connections and enforcement modes [59](#)
 - creating VPN installation packages [110](#)
 - defined [59](#)
 - illustrated [59](#)
 - remediation [87](#)
 - VPN installation package, creating for Juniper SSL VPN [110](#)
 - VPN integration [106–112](#)
 - VPN-connected computers
 - allowing access [112](#)
 - CheckPoint IPSec VPN [112](#)
 - Juniper SSL VPN [112](#)
 - Nortel IPSec VPN [112](#)
 - scanning [59](#)
 - vulnerabilities, security releases [22](#)
- W**
- WebImmune, Avert Labs Threat Center [22](#)

700-1465-00

Copyright © 2006 McAfee, Inc. All Rights Reserved.

McAfee[®]

mcafee.com