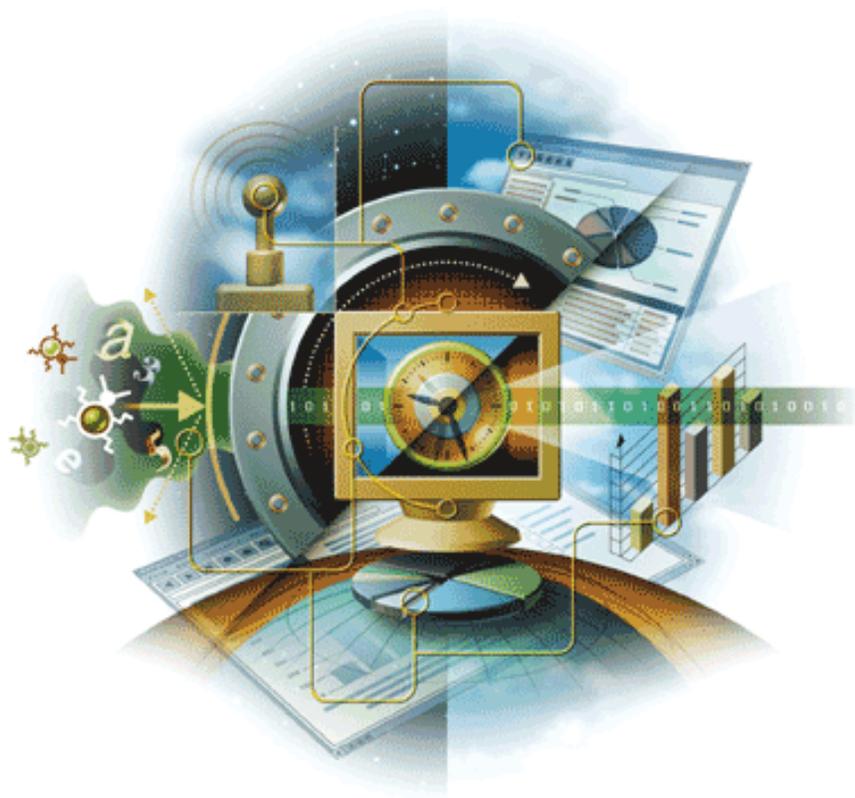


# ePolicy Orchestrator®

version 3.6



**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

**McAfee®**



# ePolicy Orchestrator®

version 3.6

**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

---

**McAfee®**

## COPYRIGHT

Copyright © 2005 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, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE 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 WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

### 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](http://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](http://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](mailto: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](mailto: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](mailto: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](mailto: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.

# Contents

<b>Troubleshooting with Log Files</b>	<b>6</b>
Log files quick reference	7
When to analyze each log file	8
Troubleshooting policy update issue	9
Adjusting the level of the Tomcat log	9
Debug logs	10
About the debug logs	10
About the backup debug logs	10
What is in the debug logs	11
Controlling the level of logging in debug logs	11
Turning detailed logging on for MSCRIPT.LOG	12
Controlling the maximum size of the debug logs	12
When does a change in logging take effect?	12
About the relationship between the agent debug log and the agent activity log	13
About the relationship between debug logs and the VirusScan Enterprise 8.0i UPDATE.TXT file	13
Troubleshooting issues using the debug logs	13

# Troubleshooting with Log Files

This document describes how to troubleshoot ePolicy Orchestrator 3.6 using log files, and provides the following information:

- Name and location of each log file.
- Types of issues recorded in each log file and when to analyze them.
- Format of the debug logs.
- Controlling the level of logging in the debug and other log files.
- Setting the maximum size of the debug log files.
- How the debug logs relate to other log files.
- A recommended process for troubleshooting issues using the debug logs.

## Log files quick reference

This table lists the name and location of each ePolicy Orchestrator 3.6 log file.

Log file name	Location
AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG	<AGENT DATA PATH>\DB
EPO.LOG	PROGRAM FILES\COMMON FILES\MCAFFEE\TOMCAT\LOGS
EPOAUDITLOG.CSV	<INSTALLATION PATH>:\DB\AUDIT LOGS
EpoApSvr.LOG	<INSTALLATION PATH>\DB\LOGS
ERRORLOG.<CURRENT_DATETIME>	<INSTALLATION PATH>\MCAFFEE\APACHE2\LOGS
CLEANUP_<COMPUTER>.LOG, CLEANUP_<COMPUTER>_BACKUP.LOG	<CURRENT USER'S TEMP DIRECTORY>\NAI LOGS
CONSOLE.LOG, CONSOLE_BACKUP.LOG	<INSTALLATION PATH>
DBINIT.LOG	<CURRENT USER'S TEMP DIRECTORY>\NAI LOGS
EVENTPARSER.LOG, EVENTPARSER_BACKUP.LOG	<INSTALLATION PATH>\DB\LOGS
FRMINST_<COMPUTER>.LOG, FRMINST_<COMPUTER>_BACKUP.LOG	<CURRENT USER'S TEMP DIRECTORY>\NAI LOGS
LICENSING.LOG	<CURRENT USER'S TEMP DIRECTORY>\NAI LOGS
LOCALHOST.<CURRENT DATE>.TXT	<INSTALLATION PATH>\TOMCAT\LOGS
MCSCRIPT.LOG	<AGENT DATA PATH>
NOTIFICATIONS.LOG	<INSTALLATION PATH>\TOMCAT\LOGS
PRDMGR_<COMPUTER>.LOG, PRDMGR_<COMPUTER>_BACKUP.LOG	<AGENT DATA PATH>\DB
REPLICATION.LOG	<INSTALLATION PATH>\DB\LOGS
SERVER.LOG, SERVER_BACKUP.LOG	<INSTALLATION PATH>\DB\LOGS
SERVERTASK.LOGS	<INSTALLATION PATH>\DB\LOG
TRACE.LOG S	<CURRENT USER'S TEMP DIRECTORY>\NAI LOG

### <AGENT DATA PATH>

The default location of the agent data files is:

```
<DOCUMENTS AND SETTINGS>\ALL USERS\APPLICATION DATA\MCAFFEE\COMMON  
FRAMEWORK
```

- Where <DOCUMENTS AND SETTINGS> is the location of the DOCUMENTS AND SETTINGS folder, which varies depending on the operating system.
- If the operating system does not use a DOCUMENTS AND SETTINGS folder, the default location is as follows:

```
<AGENT INSTALLATION PATH>\DATA
```

For more information, see *Agent installation directory* in the *ePolicy Orchestrator 3.6 Product Guide* or Help.

To determine the actual location of the agent data files, view this registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\MCAFFEE\TVD\SHARED COMPONENTS\FRAMEWORK\DATA  
PATH
```

### <CURRENT USER'S TEMP DIRECTORY>

This is the currently logged in user's temp folder. To access this folder:

- 1 Select **Start | Run** from the taskbar.
- 2 Type `%temp%` in the **Open** text box, then click **OK**.

### <INSTALLATION PATH>

The default location of the ePolicy Orchestrator 3.6 server and console software is:

`C:\PROGRAM FILES\COMMON FILES\MCAFFEE\EPO\3.6.0`

If you upgraded the software from 3.0.2 or 3.5, the default location is:

`C:\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FILES\EPO\3.6.0`

## When to analyze each log file

This table identifies the types of issues recorded in each ePolicy Orchestrator 3.6 log file, to help you determine when to analyze each log file.

For issues with...	See these log files...
Agent (general issues)	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG
Agent-server communication	SERVER.LOG
Agent installation	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG, FRMINST_<COMPUTER>.LOG, FRMINST_<COMPUTER>_BACKUP.LOG
Agent uninstallation	CLEANUP_<COMPUTER>.LOG, CLEANUP_<COMPUTER>_BACKUP.LOG FRMINST_<COMPUTER>.LOG, FRMINST_<COMPUTER>_BACKUP.LOG
Client tasks (communication issues)	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG PRDMGR_<COMPUTER>.LOG, PRDMGR_<COMPUTER>_BACKUP.LOG
Client tasks (script issues)	PRDMGR_<COMPUTER>.LOG, PRDMGR_<COMPUTER>_BACKUP.LOG  MCSCRIPT.LOG
Console	CONSOLE.LOG, CONSOLE_BACKUP.LOG, EPO.LOG
Console setup	TRACE.LOG
Events, event update	EVENTPARSER.LOG, EVENTPARSER_BACKUP.LOG
Licensing	LICENSING.LOG
Notifications	NOTIFICATIONS.LOG, LOCALHOST_LOG.<CURRENT DATE>
Package check-in during installation	DBINIT.LOG
Plug-in files	PRDMGR_<COMPUTER>.LOG, PRDMGR_<COMPUTER>_BACKUP.LOG
Policies	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG, SERVER.LOG
Product property update	EVENTPARSER.LOG, EVENTPARSER_BACKUP.LOG
Pull now	EPOAPSVR.LOG, EPO.LOG, REPLICATION.LOG
Replicate now	EPOAPSVR.LOG, EPO.LOG, REPLICATION.LOG
Repository pull	EPOAPSVR.LOG, EPO.LOG, REPLICATION.LOG
Repository replication	EPOAPSVR.LOG, EPO.LOG, REPLICATION.LOG
Rogue system detection	ROGUE.LOG, LOCALHOST_LOG.TXT

For issues with...	See these log files...
Script engine, script messages	MCSCRIPT.LOG
Server (general issues)	SERVER.LOG, SERVER_BACKUP.LOG
Server installation	DBINIT.LOG, TRACE.LOG
Server setup	TRACE.LOG
Server tasks	SERVERTASK.LOG, EPO.LOG
Updating	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG

## Troubleshooting policy update issue

To troubleshoot incremental policy update issues, set the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY
ORCHESTRATOR\SAVEAGENTPOLICY DWORD 1
```

After changing this, restart all ePolicy services and shutdown and restart any running consoles. Detailed descriptions of which failures are occurring, including source files and line numbers, appear in the application log for the specific component experiencing issues. The ePolicy Orchestrator server creates a DB\Debug folder, and for every agent connection, the server generates a policy XML file named <AGENTGUID>-TIMESTAMP.XML that displays the content that the server sends to agent.

## Adjusting the level of the Tomcat log

To adjust the tomcat log level:

- 1 Open the LOG-CONFIG.XML file, located at:

```
<PROGRAM_FILES>\<COMMON_FILES>\McAfee\Tomcat\conf\epo
```

- 2 Modify the following lines:

```
<category name="com.mcafee.epo.core.servlet">
  <priority value="warn"/>
</category>

<root>
  <priority value ="warn" />
  <appender-ref ref="ROLLING" />
  <appender-ref ref="STDOUT" />
</root>
```



Tomcat automatically picks up the log level changes; it's not necessary to restart tomcat service.

---

## Debug logs

Except where noted, the subsequent topics only apply to these log files:

- AGENT\_<COMPUTER>.LOG
- CLEANUP\_<COMPUTER>.LOG
- CONSOLE.LOG
- DBINIT.LOG
- EVENTPARSER.LOG
- FRMINST\_<COMPUTER>.LOG
- PRDMGR\_<COMPUTER>.LOG
- SERVER.LOG
- EPOAPSVR.LOG

### About the debug logs

- Debug log files are for the use of development and support, not users.
- Debug logs contain both translated user messages and English-only debug messages.
- Debug logs usually contain short messages that can be helpful to programmers with access to the source code.

### About the backup debug logs

- When most log (<LOG NAME>.LOG) files reach their maximum size (default is 1MB), they are renamed to (<LOG NAME>\_BACKUP.LOG) and a new log file is created.
- If a backup copy of a log file already exists, it is overwritten.
- Be sure to check both logs; if the log file was recently renamed it might not have many messages in it.

## What is in the debug logs

Here is part of an example agent log file. Each column is described below the example.

**Figure 1-1 Example of the AGENT\_<COMPUTER>.LOG file**

```

20021231113407 i Management Enforcing Policies for ePolicy
Orchestrator Agent
20021231113407 I Agent Enforcing policies
20021231113407 x InetMgr Enforcing policies
20021231113407 I Logging Enforcing policies
20021231113407 I Management Enforcing policies
20021231113407 I Scheduler (564)>>--CSchedule::EnforcePolicy
20021231113407 x Management Enforcing Policies
20021231113407 E Scheduler (564)<<--CEnumTask::GetFirst
hr=0x8000002a
20021231113407 I Scheduler (564)<<--CSchedule::EnforcePolicy
20021231113407 I Script Enforcing policies
20021231113407 I Updater Enforcing policies
20021231113407 I UserSpecCont Enforcing policies
20021231113407 i Agent Agent finished Enforcing policies
20021231113407 i Agent Next policy enforcement in 5 minutes

```

### Column 1 — Date and time

Displays the date and time in YYYYMMDDHHMMSS format. For example, 20021231113407 is December 31, 2002 at 11:34:07 AM. Time uses the 24-hour format.

### Column 2 — Component

Displays the type of message. The table below describes message types and the logging level in which they are recorded.

Message type	Message description	Logging level
e	Translated user error message	1
w	Translated user warning message	2
i	Translated user information message	3
x	Translated user extended information message	4
E	Debug error message in English only	5
W	Debug warning message in English only	6
I	Debug information message in English only	7
X	Debug extended information message in English only	8

### Column 3 — Component

The agent, server, or console component. For example, "Scheduler," "DOMSYNCH."

### Column 4 — Message

Displays the message itself. For example, "Enforcing policies."

## Controlling the level of logging in debug logs

- This DWORD registry value controls logging:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY
ORCHESTRATOR\LOGLEVEL
```

- The values are the numbers 1 through 8.

- The larger the number, the more messages are logged. For example, level 5 logs the first 5 levels (message types e, w, i, x, and E).
- If there is no LOGLEVEL, the default is 7.
- Log level 7 (message types e, w, i, x, E, W, and I) is a good value for normal debugging.
- Log level 8 (message types e, w, i, x, E, W, I, and X) produces extensive output, including every SQL query, whether there is an error or not. Log level 8 also provides all communication details needed to troubleshoot issues related to the network and proxy servers.

## Turning detailed logging on for MSCRIPT.LOG

To turn on the logging of all script commands used during updating and deployment, add this registry key and value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED
COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2
```

We recommend that you delete this key once you are done troubleshooting.

## Controlling the maximum size of the debug logs

- This DWORD registry value controls log size:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY
ORCHESTRATOR\LOGSIZE
```

- The value is the size of the log file in megabytes. For example, 1 = 1MB, or 2 = 2MB.
- The default size is 1MB.
- For information on what happens when the maximum size is reached, see [About the backup debug logs](#).

## When does a change in logging take effect?

Log file	Change in logging takes effect...
AGENT_<COMPUTER>.LOG	Once per minute
CLEANUP.LOG	Always level 7, 1MB
CONSOLE.LOG	On startup
DBINIT.LOG	On startup
EPOAPSVR.LOG	On startup of the McAfee ePolicy Orchestrator services, once per minute.
EVENTPARSER.LOG	Once per minute
FRMINST.LOG	Always level 7, 1MB
PRDMGR_<COMPUTER>.LOG	Once per minute
SERVER.LOG	On startup of the McAfee ePolicy Orchestrator services

## About the relationship between the agent debug log and the agent activity log

The agent activity log (AGENT\_<COMPUTER>.XML) file is a subset of the agent activity debug log (AGENT\_<COMPUTER>.LOG) file. By default, the agent activity log file includes the translated user messages (message types e, w, and i), which is logging activity at levels 1 – 3. If you enable detailed logging of agent activity, the translated user messages (message type x) logged at level 4 are also recorded in the agent activity log file. In addition, the agent activity log and the **ePolicy Orchestrator Agent Monitor** dialog box include the same messages.

If you enable remote access to the agent activity log file, you can also view the agent debug log files remotely by clicking **View debugging log** and **View backup debugging log** in the agent activity log file. For instructions, see *Enabling or disabling the logging of agent activity and remote access to log files* and *Viewing the agent activity log files remotely* in the *ePolicy Orchestrator 3.6 Product Guide* or Help.

## About the relationship between debug logs and the VirusScan Enterprise 8.0i UPDATE.TXT file

- The McAfee VirusScan Enterprise 8.0i UPDATELOG.TXT file does not contain significant additional information from the agent activity log (AGENT\_<COMPUTER>.LOG) file.
- The agent allows other programs to intercept agent log messages. The other programs can filter out messages they don't want, and can reformat them and print them to files any way they like. This is how the UPDATELOG.TXT file is created.
- VirusScan Enterprise 8.0i creates the file for compatibility with previous versions of VirusScan software. Existing users might want to use the VirusScan interface to control the content and location of this log file.

---

## Troubleshooting issues using the debug logs

Here are some recommended guidelines for using the debug log files to troubleshoot issues:

- 1 Look for the time of the problem activity, if known.
- 2 Look for message types e and E.
- 3 Look for Windows error codes.

At press time, the list of Windows system error codes was available on the following MSDE web site.

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system\\_error\\_codes.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp)

You can also use the ERRLOOK.EXE utility to determine the cause of these error codes. This utility is distributed with Microsoft Visual Studio.

For example, here's a log message with error code 1326:

```
20030102182201    I   Srv   EPOServer   Processing Console Request...
20030102182201    I   Srv   EPOServer   Console Request processed.
20030102182201    E   Srv   EPOServer   Failed to authenticate to
                \\2KADV, err=1326
20030102182201    E   Srv   EPOServer   Push Agent Installation Program
                to 2KADV Fail!
```

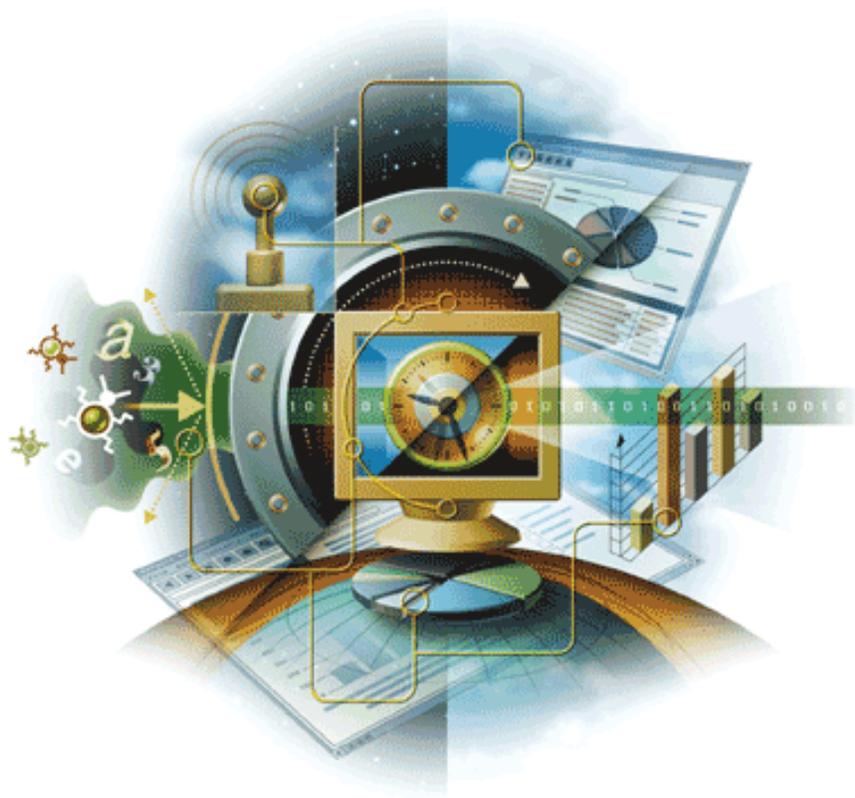
When you look up the error code, you find a literal description of the issue, which gives you more detailed information about the cause of the issue. For example:

Logon failure: unknown user name or bad password.

# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6



**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

**McAfee®**



# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6

**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

---

**McAfee®**

## COPYRIGHT

Copyright © 2005 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, MCAFE, MCAFE (AND IN KATAKANA), MCAFE AND DESIGN, MCAFE.COM, MCAFE 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 WEB SITE 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 MCAFE 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 pro+34vide 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](http://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/Æ Optimizer/Æ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In/Æ Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In/Æ 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](http://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](mailto: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 ([gregor@cs.rpi.edu](mailto:gregor@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](mailto: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](mailto: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.

## PATENT INFORMATION

Protected by US Patents 6,470,384; 6,493,756; 6,496,875; 6,553,377; 6,553,378.

# Contents

<b>1</b>	<b>Hardware Sizing Recommendations</b>	<b>6</b>
	Summary . . . . .	6
	Outbreak response requirements . . . . .	7
	The test bed . . . . .	7
	Database servers . . . . .	8
	Network environment . . . . .	8
	Recommendations . . . . .	9
	Four-processor (700MHz) system . . . . .	9
	Two-processor (2.7GHz) system . . . . .	10
	Four-processor (2.7GHz) system . . . . .	11
	Eight-processor (2.7GHz) system . . . . .	12
	Repository replication . . . . .	13
<b>2</b>	<b>Bandwidth Usage</b>	<b>15</b>
	Initial deployment . . . . .	15
	Deploying agents . . . . .	15
	Deploying VirusScan Enterprise and other products . . . . .	17
	Deploying rogue system sensors . . . . .	19
	Initial repository replication . . . . .	19
	Normal operations . . . . .	20
	Updating DAT and engine files . . . . .	20
	Policy updates . . . . .	22
	Agent-server communication . . . . .	23
	Rogue system sensor communication . . . . .	24
	Incremental repository replication . . . . .	25
	Outbreaks . . . . .	25
	Event files . . . . .	25
	Updating DAT files . . . . .	26

# 1

## Hardware Sizing Recommendations

### What type of server do you need?

McAfee provides hardware recommendations for the server-based components of your ePolicy Orchestrator 3.6 deployment. Use these recommendations when allocating server hardware to host the ePolicy Orchestrator server.

- [Summary.](#)
- [The test bed.](#)
- [Recommendations.](#)
- [Repository replication.](#)

---

### Summary

McAfee, Inc. conducted extensive tests on four server-class systems to assess and recommend the hardware needed to support and manage environments of different sizes.

The tests measured the number of agent communication transactions processed over a period of time. The measurements determine the peak transaction rates for each server configuration.

Once these measurements were collected, the throughput the server can sustain was determined. The throughput data allows McAfee, Inc. to recommend a number range of systems a given server can manage.

Information is provided for ePolicy Orchestrator 3.5 (with patch 4) and ePolicy Orchestrator 3.6.

When considering these recommendations, you must factor in your organization's outbreak response requirements.

Additionally, McAfee measured repository replication performance for ePolicy Orchestrator 3.6, and provides this data here.

## Outbreak response requirements

When applying this data to your own environment, you must consider your outbreak response requirements.

### Response time

The time period during which all systems must check into the ePolicy Orchestrator server. Three factors that define the response time in ePolicy Orchestrator 3.6 are:

- **Agent-to-server communication interval** — You can configure the response time when setting the agent-to-server communication interval (ASCI) on the **ePO Agent 3.5.0 | Configuration** policy pages.
- **Agent wakeup call** — The agent wakeup call is initiated manually, but you can determine the response time by setting this period as the **Agent randomization** interval on the **Agent Wakeup Call** dialog box that appears when the agent wakeup call is initiated.
- **Global updating** — Once configured, global updating initiates updating automatically when packages are checked in. You can configure the response time by setting the **randomization interval** on the **Settings** tab, available when you select the ePolicy Orchestrator server in the console tree.



Although we provide data regarding one-to-eight hour response times, McAfee recommends a response time no greater than six hours.

### Number of systems

The number of managed systems required to check in within the response time.

---

## The test bed

These tests were performed on four server-class systems:

- *Four-processor (700MHz) system.*
- *Two-processor (2.7GHz) system.*
- *Four-processor (2.7GHz) system.*
- *Eight-processor (2.7GHz) system.*

**Four-processor (700MHz) system**

This server has the following hardware configuration:

Component	Description
Random access memory (RAM)	2GB
Hard drive	RAID array 5
Network interface card (NIC)	1GB

**Two-processor (2.7GHz) system**

This server has the following hardware configuration:

Component	Description
Random access memory (RAM)	2GB
Hard drive	RAID array 5
Network interface card (NIC)	1GB

**Four-processor (2.7GHz) system**

This server has the following hardware configuration:

Component	Description
Random access memory (RAM)	2GB
Hard drive	RAID array 5
Network interface card (NIC)	1GB

**Eight-processor (2.7GHz) system**

This server has the following hardware configuration:

Component	Description
Random access memory (RAM)	2GB
Hard drive	RAID array 5
Network interface card (NIC)	1GB

**Database servers**

Each test used a dedicated server to host Microsoft SQL Server 2000 with Service Pack 3a. For each test, the database server system was identical to the system that hosted the ePolicy Orchestrator server.

**Network environment**

All tests were conducted in a fast Ethernet network (100Mbps).

## Recommendations

For each server, McAfee recommends a limit for the number of client systems the server should support. A graph shows recommended response times (in hours) for the number of supported systems.

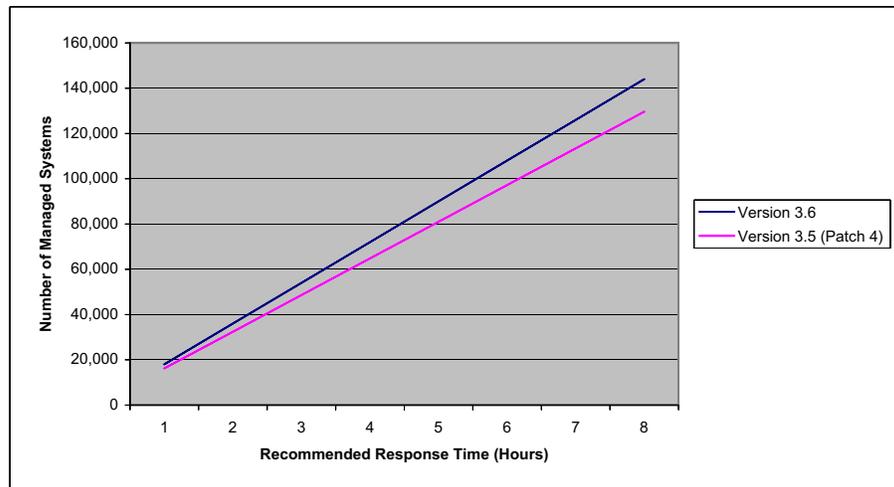


The recommendations are conservative, based on test results that were significantly higher, in order to accommodate instances of increased load.

Although we provide data for one to eight hour response requirements, McAfee recommends a response time no longer than six hours.

### Four-processor (700MHz) system

The graph and table show the recommended response times for numbers of managed systems when using a four-processor (700MHz) system to host ePolicy Orchestrator versions 3.5 (with patch 4) and 3.6.



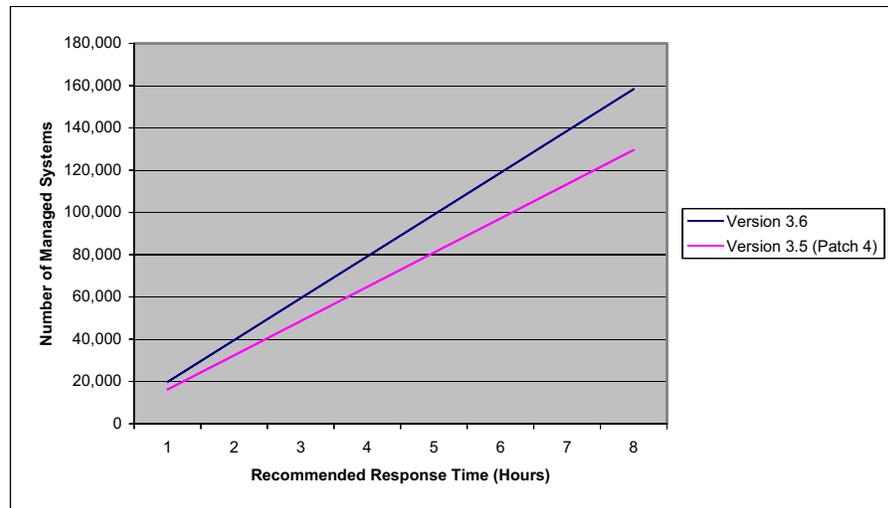
Recommended response time (hours)	Number of systems managed by ePolicy Orchestrator 3.5	Number of systems managed by ePolicy Orchestrator 3.6
1	16,200	18,000
2	32,400	36,000
3	48,600	54,000
4	64,800	72,000
5	81,000	90,000
6	97,200	108,000
7	113,400	126,000
8	129,600	144,000

#### Recommendation

Use ePolicy Orchestrator 3.6 on such a system to manage up to 108,000 systems.

## Two-processor (2.7GHz) system

The graph and table show the recommended response times for numbers of managed systems when using a two-processor (2.7GHz) system to host ePolicy Orchestrator versions 3.5 (with patch 4) and 3.6.



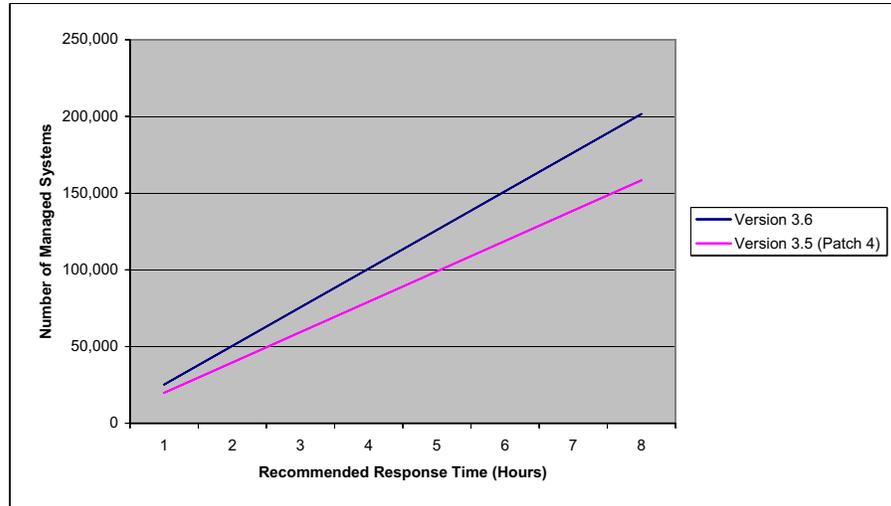
Recommended response time (hours)	Number of systems managed by ePolicy Orchestrator 3.5	Number of systems managed by ePolicy Orchestrator 3.6
1	16,200	19,800
2	32,400	39,600
3	48,600	59,400
4	64,800	79,200
5	81,000	99,000
6	97,200	118,800
7	113,400	138,600
8	129,600	158,400

### Recommendation

Use ePolicy Orchestrator 3.6 on such a system to manage up to 118,800 systems.

## Four-processor (2.7GHz) system

The graph and table show the recommended response times for numbers of managed systems when using a four-processor (2.7GHz) system to host ePolicy Orchestrator versions 3.5 (with patch 4) and 3.6.



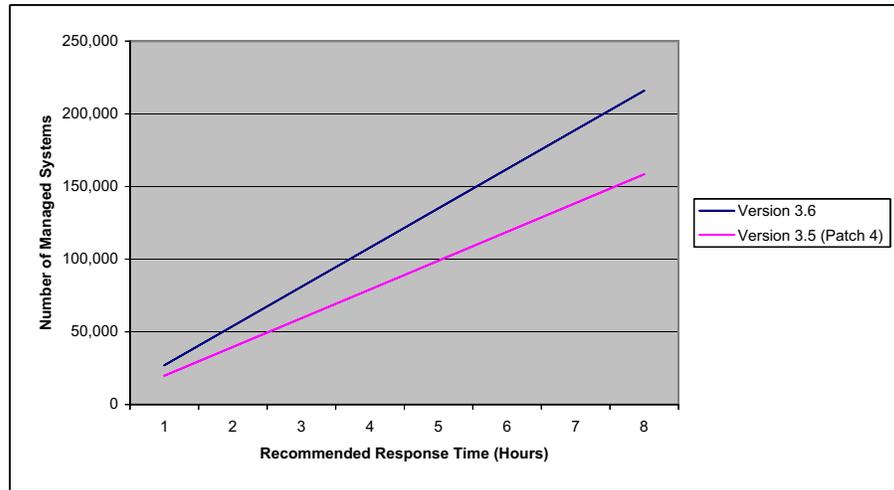
<b>Recommended response time (hours)</b>	<b>Number of systems managed by ePolicy Orchestrator 3.5</b>	<b>Number of systems managed by ePolicy Orchestrator 3.6</b>
1	19,800	25,200
2	39,600	50,400
3	59,400	75,600
4	79,200	100,800
5	99,000	126,000
6	118,800	151,200
7	138,600	176,400
8	158,400	201,600

### Recommendation

Use ePolicy Orchestrator 3.6 on such a system to manage up to 151,200 systems.

## Eight-processor (2.7GHz) system

The graph and table show the recommended response times for numbers of managed systems when using a eight-processor (2.7GHz) system to host ePolicy Orchestrator versions 3.5 (with patch 4) and 3.6.



<b>Recommended response time (hours)</b>	<b>Number of systems managed by ePolicy Orchestrator 3.5</b>	<b>Number of systems managed by ePolicy Orchestrator 3.6</b>
1	19,800	27,000
2	39,600	54,000
3	59,400	81,000
4	79,200	108,000
5	99,000	135,000
6	118,800	162,000
7	138,600	189,000
8	158,400	216,000

### Recommendation

Use ePolicy Orchestrator 3.6 on such a system to manage up to 162,000 systems.

## Repository replication

ePolicy Orchestrator 3.6 provides significant improvement in replication performance. All replication, regardless of how it is initiated, has the same impact and is now always performed on the ePolicy Orchestrator server.

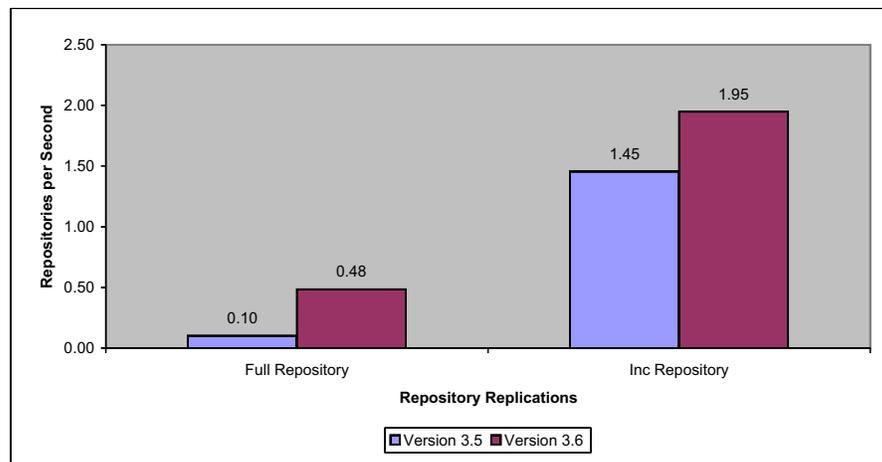
The tests were conducted using a:

- Four-processor (2.7GHz) system.
- Repository size of 21MB.
- 100Mbps environment.
- Replicate now task.

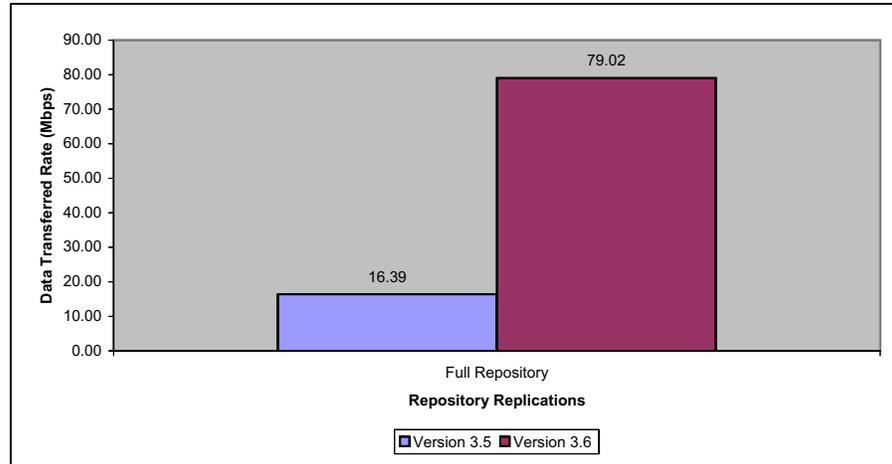
The graphs and tables show the performance of replication in these categories:

- *Repositories replicated to per second.*
- *Replication data transfer rate.*
- *CPU usage during replication.*

### Repositories replicated to per second



**Replication data transfer rate**



**CPU usage during replication**

Replication type	Version 3.5	Version 3.6
Full	22.73%	45.33%
Incremental	56.34%	67.25%

# 2

## Bandwidth Usage

### Network traffic generated by ePolicy Orchestrator 3.6

This section identifies and describes the network traffic generated by ePolicy Orchestrator and its components in a managed environment. This section also covers product tuning information to help you balance bandwidth resources with your requirements of the product.

This information can help customize your deployment strategies and policy settings to maximize network efficiency and ensure that your bandwidth limitations are not exceeded.

This section covers what to expect during:

- *Initial deployment.*
- *Normal operations.*
- *Outbreaks.*

---

### Initial deployment

When implementing ePolicy Orchestrator in your environment, you must distribute agents, components, and security products to manage and protect the systems on the network.

This section provides bandwidth usage information for:

- *Deploying agents.*
- *Deploying VirusScan Enterprise and other products.*
- *Deploying rogue system sensors.*
- *Initial repository replication.*

### Deploying agents

Deploying the agent from the ePolicy Orchestrator console when initially setting up the managed environment generates enough network traffic quickly to require planning. Although the agent installation package is smaller than those of other products, the agent must be deployed to each system you want to manage, regardless of which product you install on the system.

**Table 2-1 Agent deployment**

Action	Total bytes	Server-to-client	Client-to-server	Comments
Actual deployment	1.67MB	1.63MB	44KB	Agent deployment includes the 1.61MB agent installation package and network message overhead used to copy and run the agent installer.
Initial agent-server communication	13KB	7.5KB	5.7KB	When the agent calls into the server for the first time, it sends all system properties and downloads all policies. The server then populates the database with the system's properties.

Bandwidth used by agent deployment is divided between two actions:

- *Actual deployment.*
- *Initial agent-server communication.*

## Actual deployment

The first and most expensive use of bandwidth occurs when the 1.61MB agent installation package is deployed to client systems. You can deploy the agent installation package from the ePolicy Orchestrator console to sites, groups, or systems in the Directory using the **Install Agent** command, a network login script, or a third-party software deployment tool. Regardless of the method, deploying the agent installation package over the network generates 1.67MB of traffic to each system.

Base the agent deployment on the number of client systems you plan to manage, their location in the network topology, and the amount of bandwidth you have available between the ePolicy Orchestrator server and these systems.

McAfee recommends deploying agents:

- In stages that won't push network utilization over 80% at any time for any segment of resources.
- To individual sites or groups, especially if you have more bandwidth-limiting factors, such as slower connections between geographic locations.

## Location of network impact

Agent-deployment traffic occurs directly between the ePolicy Orchestrator server and database and between the ePolicy Orchestrator server and the systems to which the agent is deployed.

## Initial agent-server communication

After the installation completes, the agent calls into the server. The agent sends computer properties, such as operating system, RAM, and IP address to the server, then downloads policy settings and client tasks configured for the host system.

The size of this initial agent-server communication is a combination of three factors:

- *Number of NAP files checked into the repository.*

- *Custom policies.*
- *Client tasks.*

With no additional NAP files checked into the repository, with no policy customizations, and with no client tasks configured, the initial agent-server communication generates 13KB of traffic for each agent, or each managed system. Modifying NAP files in the repository, policies, or tasks affects the total.

### Number of NAP files checked into the repository

Each NAP file that is checked into the repository adds 10–20KB for each initial agent-server communication.

### Custom policies

You may need to customize agent or product policies. If you do so before the deployment (so that the custom policy settings are applied as soon as possible), the bandwidth requirements increase slightly per system. Individual policy changes add 3–5KB to the next communication.

### Client tasks

You should create and schedule any desired client tasks for each of your client systems. Common client tasks include update and scan tasks, but vary according to the managed product. Each task you create or modify adds 2–4KB per communication.

### Location of network impact

The traffic occurs between the ePolicy Orchestrator server and each system hosting an agent.

### Methods to minimize impact

To minimize bandwidth usage caused by the initial agent-server communication, leave only the NAP files of products and components you will manage. Each NAP file that is checked into the repository adds 10–20KB per communication.



The agent selects which policies to download from the server based on the operating system of the client system. The agent downloads policies for all products that could be installed on such an operating system, even if those products aren't actually installed on the client system. For example, an agent installed on a computer running Windows 2000 Server downloads the GroupShield policies, even though that server may not be a mail server.

## Deploying VirusScan Enterprise and other products

Deploying security products (like VirusScan Enterprise) to client systems can be the most bandwidth-intensive phase of setting up of a managed environment. Like the agent, anti-virus and other security software must be installed on each system you plan to manage.

## Deploying VirusScan Enterprise

McAfee releases VirusScan Enterprise with the latest DAT file available at the time of release, and is out-of-date quickly. Because of this, VirusScan Enterprise performs an immediate and automatic DAT file update after the installation completes on the client system. Therefore, if you deploy VirusScan Enterprise using the DAT file included in the default deployment package, add 5.6MB to the required bandwidth for each agent.

**Table 2-2 VirusScan Enterprise 8.0i deployments**

Action	Total bytes	Server-to-client	Client-to-server	Comments
VirusScan Enterprise deployment	10.53MB	10.28MB	253KB	Use the deployment task to download and run the VirusScan Enterprise installation package onto the client system.  Create a custom deployment package with the latest DAT files to avoid having to add a 5.6MB DAT file update.
VirusScan Enterprise re-deployment	7.3KB	3.5KB	3.8KB	During the initial deployment, the installation application is copied to the client system and launched from there. If VirusScan Enterprise is deleted for any reason, the agent can re-install it without having to download the installer again.  This amount does not include the automatic DAT file update that occurs after VirusScan Enterprise installs.

## Deploying other managed products

Deploying managed products to client systems requires bandwidth proportional to the size of the deployment installation package plus another 30-40KB for network overhead.

You can estimate the network traffic other product deployments generate by checking the size of the folder containing the product installation files. These are located on your ePolicy Orchestrator server system in the temporary folders to which you extracted installation files. Be sure to consider all the contents of the installation folder, not just the PKGCATALOG.Z file.

## Impacted connections

The VirusScan Enterprise deployment generates about 10MB of traffic between:

- The master repository and each distributed repository.
- Each client system and its repository.

## Methods to minimize impact

To minimize traffic generated by deploying products:

- Deploy the product to segments of the Directory, instead of all systems at once. Schedule the deployment task to run one site or group at a time.

- Use randomization intervals to distribute the deployment to a site or group over a period of time.
- Schedule the deployment task to run at local time (the default). This is helpful if you have office locations in different time zones.
- Use McAfee Installation Designer to create a custom deployment package that includes the latest DAT and engine file updates. Creating and deploying such a package reduces the required bandwidth by up to 5.6MB per client system because VirusScan Enterprise will not require updating after installation.
- Create and configure distributed repositories to localize network traffic during product deployments. Before running the deployment task, replicate the deployment package from the master repository to the distributed repositories. The deployment task generates traffic between the agent and the nearest repository only. However, after an installation, the agent sends properties to the server. Updating from the closest distributed repository localizes product deployment traffic.

## Deploying rogue system sensors

Sensor deployments require 3.9MB of bandwidth between the server and each client system to which you deploy the sensor. However, only one sensor is required per broadcast segment. McAfee recommends deploying at least three sensors to each broadcast segment to ensure continuous coverage.

The sensor is installed in a disabled state, becoming enabled and sending information to the server after the first agent-server communication. The length of time the sensor requires to start depends on your agent-server communication policy settings (up to an hour, if you use the default ASCII).



Properties and policies are exchanged during the first agent-server communication after sensor deployment. These add 1–2KB to the traffic between these systems and the ePolicy Orchestrator server.

**Table 2-3 Rogue system sensor deployment**

Action	Total size	Server-to-client	Client-to-server	Comments
Sensor deployment to any system	3.9MB	3.8MB	94KB	McAfee recommends deploying at least three sensors to each broadcast segment. If possible, deploy these sensors to server systems.

## Location of network impact

The sensor deployment requires 3.9MB of bandwidth between the ePolicy Orchestrator server and each system to which you deploy the sensor. (McAfee recommends deploying at least three per subnet.)

## Initial repository replication

The following measurements were taken during replication to a SuperAgent repository. The traffic generated is similar when using other distributed repository types, such as UNC shares, HTTP or FTP servers.

The initial replication is the largest. All subsequent replications copy only the new files to the distributed repositories.

**Table 2-4 Initial replication to distributed repositories**

Action	Total size	Server-to-client	Client-to-server	Comments
Repository replication (initial)	34.4MB	33.6MB	867KB	This example includes all default packages, plus VirusScan Enterprise 8.0i, and full DAT and engine files. The size of the replication depends on which packages and files are replicating.

## Normal operations

Although not as large as the initial deployment of the agent, sensor, and products, there is significant bandwidth usage during your normal day-to-day operations. Updates must be distributed throughout the network, policies must be enforced, and the agent must communicate with the server for your systems to be managed and secure.

The following topics are covered in this section:

- [Updating DAT and engine files.](#)
- [Policy updates.](#)
- [Agent-server communication.](#)
- [Rogue system sensor communication.](#)
- [Incremental repository replication.](#)

## Updating DAT and engine files

Keeping DAT and engine files up-to-date is critical to your anti-virus protection. Deciding how often to update these files requires balancing protection and network performance. Update too infrequently, and the network becomes vulnerable to new viruses. Update too frequently, and generate unnecessary network traffic for little benefit.

McAfee releases DAT files daily. Engine updates are released once or twice per year.

**Table 2-5 DAT and engine file deployment**

Action	Total size	Server-to-client	Client-to-server	Comments
Full DAT file	5.6MB	5.5MB	128KB	This involves downloading the DAT file package, plus network overhead.
Incremental DAT file increase	16.2KB per update	10.8KB	5.4KB	Incremental updates can vary in size.

**Table 2-5 DAT and engine file deployment**

Action	Total size	Server-to-client	Client-to-server	Comments
Engine (4400)	3.3MB	3.2MB	76.6KB	Engine package is 2.9MB, plus network overhead.
Update task, DAT files and engine only (no changes)	8.7KB	4.5KB	4.2KB	Client system already has the most up-to-date DAT and engine files — this traffic is generated by the task only.

## Incremental and full DAT file updates

Distributing a full DAT file at each release would generate significant network traffic, especially in very large networks. To ease this impact, each full DAT file released includes separate incremental updates for each update, up to the 15 previously released DAT files.

Each of these incremental updates is a separate UPD file saved in the repository along with the full SCAN.DAT file. These UPD files vary in size depending on how many signatures have been added since the last release.

When an update task runs, the agent compares the version on the client system with the version in the repository. If the client version is within 15 versions of the latest DAT file, the agent only downloads the specific incremental updates required. If the version on the client system is more than 15 versions out-of-date, then the agent downloads the full DAT file. The agent determines this automatically.

## Location of network impact

Updating generates traffic between:

- The master repository and the distributed repository.
- Each client system and its repository.

## Methods to minimize impact

To minimize traffic generated by updating DAT and engine files:

- Use distributed repositories. During update tasks, the agent communicates only with a repository, not the ePolicy Orchestrator server. Updating from the closest distributed repository localizes network traffic over faster LAN connections. This is much more efficient than updating over WAN or VPN connections that can exist between geographic locations.
- Use global updating and configure it to run only when new DAT or engine files are checked into the master repository. This minimizes the impact by only running repository replication and client update tasks when there is a new DAT or engine file update available. If you use global updating, and especially if your network is large, enable randomization to spread the network load out over time.
- Schedule your pull tasks to run when network use is low, especially when using global updating.

- Create a separate client update task for DAT and engine files, and schedule the task to run often.
- Ensure your DAT files are up-to-date. Keeping DAT files current ensures that only incremental updates are required.

## Policy updates

At each policy enforcement interval, the agent checks the client system on which it is installed to ensure that the current policy settings are in effect. The agent uses the most recent policies downloaded from the server at the last agent-server communication. By default, the agent enforces policies on the client system every five minutes.

**Table 2-6 Policy enforcement interval**

Action	Total size	Server-to-client	Client-to-server	Comments
Policy update, with the deployment task configured to install products at the interval	4.3KB	2.7KB	1.6KB	When the deployment task is set to install a product, the agent contacts the distributed repository at each enforcement interval to confirm the installed versions of selected products are the same as those in the repository.
Policy update, with the deployment task configured not to install products at the interval	4.1KB	2.5KB	1.6KB	

If a product is not installed but should be, for example if a user uninstalls VirusScan Enterprise, the agent re-installs the product at the next policy enforcement interval. This installation does not create additional traffic to the repositories because the installation files are already on the client system.

## Methods to minimize impact

To minimize traffic generated by policy enforcement:

- Use distributed repositories to localize network traffic during enforcement intervals and when running deployment tasks.
- Deselect **Run this task at every policy enforcement interval** in the Deployment task settings. If you do this, schedule the Deployment task to run at regular times to ensure the desired products are installed.
- McAfee does *not* recommend setting the Deployment task actions to **ignore** for critical products. Ensuring that the right version of a product is installed and running on each client system is one of the most important things that ePolicy Orchestrator does.

## Agent-server communication

The agent-server communication can refer to the agent-to-server communication interval (ASCI) or an agent wakeup call. The ASCI setting determines how often the agent communicates with the ePolicy Orchestrator server to send any changed properties and check for new policies. Unless you plan to use agent wakeup calls from the server, the ASCI is the primary means to initiate communication between agent and server.

**Table 2-7 Agent-to-server communication**

Action	Total size	Server-to-client	Client-to-server	Comments
Agent wakeup call	8.2KB	4.1KB	4.1KB	
Agent wakeup call with full properties	25KB	20KB	5KB	The only way to force the agent to resend all properties to the server is to send an agent wakeup call with the <b>Get full product properties</b> option selected.  This example uses a client system with the agent, VirusScan Enterprise, and System Compliance Profiler installed.
ASCI (no changes)	1.53KB	801 bytes	732 bytes	The amount of bandwidth used during the ASCI depends on the number of policies have changed since the previous ASCI, and how many products are installed on the client system. This example measures an ASCI with no policy or task changes.
ASCI (one policy change)	1.9KB	958 bytes	986 bytes	This example measures an ASCI with one policy change.

### Location of network impact

Agent-server communication traffic occurs between the ePolicy Orchestrator server and managed systems.

### Methods to minimize impact

Configure the ASCI to occur frequently enough to ensure your products are updated as often as you require, but not so frequently that your resources are impacted.

By default, the ASCI is set to 1 hour. McAfee recommends setting the ASCI to 6 hours or less.

## Rogue system sensor communication

The rogue system sensor generates and forwards detection messages to the ePolicy Orchestrator server.

**Table 2-8 Rogue system sensor communication**

Action	Total size	Client-to-server	Server-to-client	Comments
Sensor reports detected rogue systems	5.1KB	1KB	4.1KB	Nearly all systems on the subnet are detected and reported within the first two primary sensor communication intervals (PSCI).  The sensor re-sends detection events to the server at the PSCI, as specified in the <b>Minimum reporting interval for each detected host</b> policy setting (default is one hour).
Non-primary sensor communication interval	2KB	.5KB	1.5KB	Non-primary sensors are backups that are not actively reporting detections to the server. They do, however, call in periodically to the server to see if they should become active.

### Regular primary sensor communication interval

You can configure how often the sensor sends detection events to the ePolicy Orchestrator server. For primary sensors is the primary sensor-to-server communication interval (PSCI). The default is five minutes.

When the PSCI is 0, each event is forwarded immediately and separately. Each detection message requires an SSL socket connection, whether that message contains one or 100 events. In large deployments, this can cause issues if there are not enough SSL connections on the ePolicy Orchestrator server

If you use the default PSCI (five minutes), the sensor sends its first detections on the local network subnet five minutes after that initial PSCI. The sensor sends additional detections every five minutes until all systems in the subnet have been detected.

### Minimum reporting interval

Detection events are sent once for each system, and then resent at the interval specified in the **Minimum reporting interval for each detected host** setting. By default, this is one hour.

### Non-primary sensor communication interval

If you deployed additional sensors to your broadcast segments, these are non-primary sensors. Non-primary sensors do not forward detection events to the server. The non-primary sensors communicate with the ePolicy Orchestrator server at the non-primary sensor communication interval (NPSCI) to determine whether they continue as non-primary sensors, or become primary sensors.

## Location of network impact

The traffic generated by the sensor takes place between the systems on which they reside and the ePolicy Orchestrator server.

## Incremental repository replication

The following measurements were taken using a SuperAgent distributed repository. The amount of traffic generated is similar when using other distributed repository types.

**Table 2-9 Incremental repository replication**

Action	Total size	Server-to-client	Client-to-server	Comments
Repository replication (incremental) with one DAT file	5.65MB	5.49MB	162KB	Replication includes one full DAT file, no other changes. Updating repositories with DAT files is the most frequent type of replication.
Repository replication (incremental) with no changes	54KB	21KB	33KB	The distributed repository is already up-to-date, so no packages are transferred. If you schedule regular replication tasks, it is better to schedule them too frequently than not frequently enough. Each time a replication runs and the repository is already current, only 54KB in traffic is generated between the ePolicy Orchestrator server and each distributed repository.

## Outbreaks

During an outbreak, most traffic is generated by the outbreak itself, but the traffic generated by your security products increases as well. During such a situation, a large number of event files are sent from affected systems to the ePolicy Orchestrator server. During this time you must update your DAT files as soon as possible on all client systems, and during the same time not overloading an already stressed network.

## Event files

Event files allow the server to know what is happening on managed systems. During an outbreak, this flow of event files is increased from all affected systems. There are many types of event files from security products. However, the size does not differ greatly. Some typical ones during an outbreak are represented in the table below.

**Table 2-10 Event files**

Action	Total size	Server-to-client	Client-to-server	Comments
Virus detected events	3.4KB	.7KB	2.7KB	
Buffer overflow	2KB		2KB	

Although individual event files are quite small, in large numbers they can significantly reduce the amount of available bandwidth and affect performance of the ePolicy Orchestrator server.

## Methods to minimize impact

Ensuring bandwidth is not exhausted during an outbreak allows ePolicy Orchestrator to distribute critical updates more quickly to remediate the outbreak. There are several configurations you can make to reduce the number of events the agent sends, lessening the bandwidth impact.

### Ensuring the agent forwards only critical events immediately

On the **Events** tab of the **ePO Agent 3.5.0 | Configuration** policy pages, ensure these options are selected:

- **Enable immediate uploading of events.**
- **Critical** from the **Report any events with severity value equal or greater than** drop-down list.

### Enabling event filtering to identify specific events that are forwarded immediately

You can narrow the subset of events that are forwarded immediately by enabling event filtering and selecting the specific events that you are interested in receiving as they occur.



If the agent is configured to send only critical events to the ePolicy Orchestrator server immediately, you only need to narrow the set of critical events with the event filtering feature.

- 1 In the console tree, select **Events** under the name of the database.
- 2 In the details pane, select the **Filtering** tab.
- 3 Select **Send only the selected events to ePO**.
- 4 Ensure only the essential critical level events are selected, then click **Apply**.

### Disabling any unnecessary notification rules

The speed by which ePolicy Orchestrator server processes events is affected by the number of enabled notification rules. During an outbreak, disable any unnecessary notification rules.

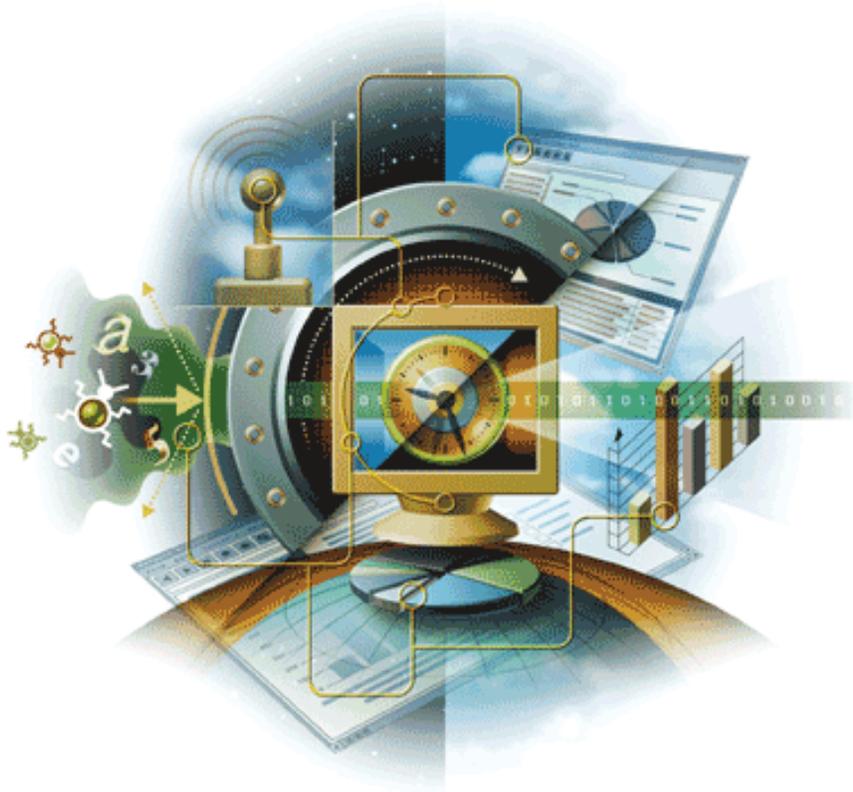
## Updating DAT files

To remediate an outbreak, you must update your anti-virus products on all of the systems in your environment as quickly as possible without overloading the resources. To improve the bandwidth usage of updating, McAfee recommends using global updating and SuperAgents. See the *ePolicy Orchestrator 3.6 Product Guide* for more information.

# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6



**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

**McAfee®**



# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6

**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

---

**McAfee®**

## COPYRIGHT

Copyright © 2005 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 WEB SITE 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 pro+34vide 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](http://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/Æ Optimizer/Æ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In/Æ Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In/Æ 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](http://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](mailto: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 ([gregor@cs.rpi.edu](mailto:gregor@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](mailto: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](mailto: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.

## PATENT INFORMATION

Protected by US Patents 6,470,384; 6,493,756; 6,496,875; 6,553,377; 6,553,378.

# Contents

<b>1</b>	<b>Requirements and Recommendations</b>	<b>5</b>
	System requirements . . . . .	5
	Server and console requirements . . . . .	5
	Remote console requirements . . . . .	6
	Database requirements . . . . .	7
	Distributed repositories . . . . .	8
	Reporting requirements . . . . .	8
	Agent requirements . . . . .	8
	SuperAgent requirements . . . . .	9
	Non-Windows agent requirements . . . . .	10
	Operating systems language support . . . . .	11
	Supported products . . . . .	11
<b>2</b>	<b>Pre-Installation</b>	<b>13</b>
	Pre-installation guidelines and requirements . . . . .	13
	Installing or upgrading the database software . . . . .	13
	Installing MSDE 2000 (with Service Pack 3) for the first time . . . . .	14
	Upgrading MSDE to MSDE 2000 (with Service Pack 3) . . . . .	15
	Installing SQL Server 2000 (with Service Pack 3) . . . . .	15
	Upgrading to SQL Server 2000 (with Service Pack 3) . . . . .	16
	Upgrading to MDAC 2.8 . . . . .	16
	Proxy settings . . . . .	17
<b>3</b>	<b>First-Time Installation</b>	<b>18</b>
	Before you begin . . . . .	18
	Installing the server and console . . . . .	18
	Installing remote consoles . . . . .	24
<b>4</b>	<b>Upgrading to ePolicy Orchestrator 3.6</b>	<b>25</b>
	Before you begin . . . . .	26
	Backing up ePolicy Orchestrator databases . . . . .	26
	Microsoft SQL Server . . . . .	26
	MSDE . . . . .	26
	Upgrading the server and console . . . . .	27
	Upgrading remote consoles . . . . .	30
	Migrating to a licensed version . . . . .	31
<b>5</b>	<b>Post-Installation Procedures</b>	<b>32</b>
	Completing a first-time installation . . . . .	32
	Completing an upgrade . . . . .	32
	Checking in files manually . . . . .	33
	Configuring the software for a server that has multiple NICs . . . . .	33
	Uninstalling the software . . . . .	34
<b>6</b>	<b>Troubleshooting</b>	<b>35</b>
<b>A</b>	<b>High Availability</b>	<b>39</b>
	Requirements . . . . .	39

Setting up and testing the ePolicy Orchestrator cluster . . . . .	39
Stopping the ePolicy Orchestrator services on all nodes . . . . .	39
Running the ePolicy Orchestrator Clustering Setup wizard . . . . .	40
Directing secondary nodes to a common database . . . . .	42
Creating and configuring the cluster group . . . . .	43
Creating the ePolicy Orchestrator group . . . . .	43
Creating the IP Address resource . . . . .	44
Creating the Network Name resource . . . . .	45
Moving the Quorum drive to the ePO group . . . . .	45
Creating the Generic Service resources . . . . .	46
Testing the ePolicy Orchestrator cluster . . . . .	47

<b>Index</b>	<b>48</b>
--------------	-----------

# 1

## Requirements and Recommendations

The minimum system requirements, minimum hardware configuration, and database software requirements are provided in these topics:

- [System requirements](#).
- [Supported products on page 11](#).

---

### System requirements

Before you begin the installation, verify that each component meets the minimum system requirements which are listed in these topics:

- [Server and console requirements on page 5](#).
- [Remote console requirements on page 6](#).
- [Database requirements on page 7](#).
- [Distributed repositories on page 8](#).
- [Reporting requirements on page 8](#).
- [Agent requirements on page 8](#).
- [SuperAgent requirements on page 9](#).
- [Non-Windows agent requirements on page 10](#).
- [Operating systems language support on page 11](#).

### Server and console requirements

Server and console requirements are divided into the following categories:

- [Hardware and network requirements on page 5](#).
- [Software requirements on page 6](#).

#### Hardware and network requirements

The hardware and network requirements for the server and console are:

- **Free disk space** — 500MB minimum (first-time installation); 1GB minimum (upgrade); 2 GB recommended.
- **Memory** — 512MB available RAM; 1 GB recommended.

- **Processor** — Intel Pentium II-class or higher; 450MHz or higher.
- **Monitor** — 1024x768, 256-color, VGA monitor.
- **NIC** — Network interface card; 100MB or higher.
- **Dedicated server** — If managing more than 250 client computers, we recommend using a dedicated server.
- **File system** — NTFS (NT file system) partition recommended.
- **IP address** — We recommend using static IP addresses for ePolicy Orchestrator servers.

### Software requirements

The software requirements for the server and console are:

- **Operating system** — Any of the following Microsoft Windows operating systems:
  - Windows 2000 Advanced Server with Service Pack 3 or later.
  - Windows 2000 Server with Service Pack 3 or later.
  - Windows Server 2003 Enterprise.
  - Windows Server 2003 Standard.
  - Windows Server 2003 Web.
- **Browser** — Microsoft Internet Explorer 6.0 or later.
- **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.

## Remote console requirements

Remote console requirements are divided into the following categories:

- Hardware and network requirements
- Software requirements

### Hardware and network requirements

The hardware and network requirements for the remote console are:

- **Free disk space** — 250MB.
- **Memory** — 128MB RAM.
- **Monitor** — 1024x768, 256-color, VGA monitor.
- **NIC** — Network interface card (NIC); 10MB or higher.
- **Processor** — Intel Pentium II-class or higher.
- **File system** — NTFS or FAT file system partition.

### Software requirements

The software requirements for the remote console are:

- **Operating system** — Any of the following Microsoft Windows operating systems:
  - Windows 2000 Advanced Server with Service Pack 3 or later.
  - Windows 2000 Professional with Service Pack 3 or later.
  - Windows 2000 Server with Service Pack 3 or later.
  - Windows 2000 Terminal Server.
  - Windows Server 2003 Enterprise.
  - Windows Server 2003 Standard.
  - Windows Server 2003 Web.
  - Windows XP Professional with Service Pack 1.
- **Browser** — Microsoft Internet Explorer 6.0 or later.

## Database requirements

The ePolicy Orchestrator database requirements are:

- **Database software** — Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) with Service Pack 3, or Microsoft SQL Server 2000 Standard or Enterprise Edition with Service Pack 3.



MSDE 2000 with Service Pack 3 cannot be installed on a backup domain controller (BDC).

- **Maintenance settings** — We recommend making specific maintenance settings to ePolicy Orchestrator databases. For instructions, see *Maintaining ePolicy Orchestrator databases* in the *ePolicy Orchestrator 3.6 Product Guide*.
- **Remote database server** — Microsoft Data Access Components (MDAC) 2.8.

### SQL Server

If you are using SQL Server, the following requirements apply:

- **Dedicated server and network connection** — Use a dedicated server and network connection if managing more than 5,000 client computers.
- **Local database server** — If using SQL Server on the same system as the ePolicy Orchestrator server, McAfee recommends using a fixed memory size in Enterprise Manager that is approximately two-thirds of the total memory for SQL Server. For example, if the computer has 1GB of RAM, set 660MB as the fixed memory size for SQL Server.
- **SQL Server licenses** — If using SQL Server, a SQL Server license is required for each processor on the computer where SQL Server is installed.



If the minimum number of SQL Server licenses is not available after you install the SQL Server software, you may have issues installing or starting the ePolicy Orchestrator software.

## Distributed repositories

Distributed repositories can be created on any of the following:

- HTTP-compliant (version 1.1) servers on Microsoft Windows, Linux, or Novell NetWare operating systems.
- Windows, Linux, or NetWare FTP servers.
- Windows, Linux, or UNIX Samba UNC shares.
- Computer with a SuperAgent installed on it. For more information, see [SuperAgent requirements on page 9](#).

## Reporting requirements

To create custom report templates, you must use Crystal Decisions Crystal Reports 8.0.

If you require reports in Chinese (Simplified or Traditional), Japanese, or Korean languages, you must install Crystal Reports 8.0 on computers equipped with the corresponding language version of the supported operating system and database software.

## Agent requirements

The agent requirements are divided into the following categories:

- Hardware and network requirements
- Software requirements

### Hardware and network requirements

The hardware and network requirements for the agent are:

- **Processor** — Intel Pentium-class, Celeron, or compatible processor; 166MHZ processor or higher.
- **Free disk space (agent)** — 10MB.
- **Free disk space (products)** — Sufficient disk space on client computers for each McAfee product that you plan to deploy. For more information, see the corresponding product documentation.
- **Memory** — 8MB RAM.
- **Network environment** — Microsoft or Novell NetWare networks. NetWare networks require TCP/IP.
- **NIC** — Network interface card; 10MB or higher.

### Software requirements

Software requirements for the agent are:

- **Citrix** — These Citrix products are supported on operating systems that ePolicy Orchestrator supports:
  - Citrix Metaframe 1.8 for Windows.
  - Citrix Metaframe XP for Windows.
- **Cluster** — If using cluster services, Microsoft Cluster Server (MSCS) is supported.

- **Operating system** — Any of the following Microsoft Windows operating systems:
  - Windows 2000 Advanced Server with Service Pack 1, 2, 3, or 4.
  - Windows 2000 Datacenter Server with Service Pack 1, 2, 3, or 4.
  - Windows 2000 Professional with Service Pack 1, 2, 3, or 4.
  - Windows 2000 Server with Service Pack 1, 2, 3, or 4.
  - Windows 95.
  - Windows 98.
  - Windows 98 Second Edition (SE).
  - Windows Millennium Edition (Me).
  - Windows NT 4.0 Enterprise Server, with Service Pack 4, 5, 6, or 6a.
  - Windows NT Server 4.0 with Service Pack 4, 5, 6, or 6a.
  - Windows NT Workstation 4.0 with Service Pack 4, 5, 6, or 6a.
  - Windows Server 2003 Enterprise.
  - Windows Server 2003 Standard.
  - Windows Server 2003 Web.
  - Windows XP Home with Service Pack 1.
  - Windows XP Professional with Service Pack 1.

### Windows 95 and Windows 98

Client computers using Windows 95A, Windows 95B, and Windows 95C must install:

- VCREDIST.EXE, free from Microsoft. At press time, this program and instructions for installation were available on the Microsoft web site.
- DCOM95 1.3, free from Microsoft. At press time, this program and instructions for installation were available on the Microsoft web site

Client computers using Windows 98 must install:

- VCREDIST.EXE, free from Microsoft. At press time, this program and instructions for installation were available on the Microsoft web site.



Client systems using Windows 98 SE do *not* need this program installed.

## SuperAgent requirements

You can enable the ePolicy Orchestrator agent for Windows as a SuperAgent, which communicates with other agents and can store a distributed repository.

- **Operating system** — Any of the following Microsoft Windows operating systems:
  - Windows 2000 Datacenter Server with Service Pack 1, 2, 3, or 4.
  - Windows 2000 Professional with Service Pack 1, 2, 3, or 4.

Windows 2000 Server with Service Pack 1, 2, 3, or 4.

Windows NT 4.0 Enterprise Server, with Service Pack 4, 5, 6, or 6a.

Windows NT Server 4.0 with Service Pack 4, 5, 6, or 6a.

Windows NT Workstation 4.0 with Service Pack 4, 5, 6, or 6a.

Windows XP Home with Service Pack 1.

Windows XP Professional with Service Pack 1.

#### Distributed repository

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

## Non-Windows agent requirements

The ePolicy Orchestrator agent for NetWare installs and runs on any system that meets the requirements below.

- **Operating system** — Any of the following Novell operating systems:

NetWare 4.11 with Support Pack 9.

NetWare 4.2 with Support Pack 9.

NetWare 5.0 with Support Pack 6a.

NetWare 5.1 with Support Pack 5.

NetWare 6.0.



Client systems using NetWare 4.11 or 4.2 must install NW4WSOCK.EXE, free from Novell. At press time, this program and instructions for installation were available on the Novell web site.

- **Product** — McAfee NetShield 4.6 for NetWare.
- **Network environment** — TCP/IP.

#### WebShield appliances requirements

The ePolicy Orchestrator agent for WebShield appliances installs and runs on:

- WebShield e250 appliance.
- WebShield e500 appliance.
- WebShield e1000 appliance.

## Operating systems language support

This version of the ePolicy Orchestrator software runs on the following language versions of supported operating systems:

- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Spanish
- Swedish

## Supported products

ePolicy Orchestrator 3.6 supports managing the following products to the following extents:

**Table 1-1 Supported products**

Product and Version	Deployment	Updating	Configuration Management	Presence Reporting	Event Reporting
Alert Manager 4.7	Yes	Yes	Yes	No	Yes
Alert Manager 4.7.1	Yes	Yes	Yes	No	Yes
AntiSpyware 7.1	Yes	Yes	Yes	Yes	Yes
AntiSpyware 8.0	Yes	Yes	Yes	Yes	Yes
Desktop Firewall 8.0	Yes	Yes	Yes	Yes	Yes
Desktop Firewall 8.5	Yes	Yes	Yes	Yes	Yes
Entercept 5.x	Yes	Yes	No	Yes	Yes
GroupShield Domino 5.3	No	Yes	Yes	Yes	Yes
GroupShield Domino 7.0	Yes	Yes	Yes	Yes	Yes
GroupShield for Exchange 6.0.2 (Service Pack 2)	Yes	Yes	Yes	Yes	Yes
LinuxShield 1.2	No	No	Yes	Yes	Yes
NetShield for NetWare 4.6.2	No	No	Yes	Yes	Yes
NetShield for NetWare 4.6.3	No	No	Yes	Yes	Yes
Oubreak Manager 4.6	No	Yes	Yes	No	No
PortalShield 1.0	Yes	Yes	Yes	Yes	Yes
PortalShield 1.0.1	Yes	Yes	Yes	Yes	Yes
Secure Content Management 4.0	No	Yes	Yes	Yes	Yes
SecurityShield 1.0	Yes	Yes	Yes	Yes	Yes
Stinger 1.2	Yes	Yes	Yes	Yes	Yes
Symantec AntiVirus 8.1	No	Yes	Yes	Yes	Yes
Symantec AntiVirus 9.0	No	Yes	Yes	Yes	Yes
System Compliance Profiler 1.1	No	Yes	Yes	Yes	Yes
Virex 7.6	No	No	Yes	Yes	Yes

**Table 1-1 Supported products**

<b>Product and Version</b>	<b>Deployment</b>	<b>Updating</b>	<b>Configuration Management</b>	<b>Presence Reporting</b>	<b>Event Reporting</b>
Virex 7.7	No	No	Yes	Yes	Yes
VirusScan 4.5.1	No	Yes	Yes	Yes	Yes
VirusScan Enterprise 7.1	Yes	Yes	Yes	Yes	Yes
VirusScan Enterprise 8.0i	Yes	Yes	Yes	Yes	Yes
VirusScan for NetApp 7.1	Yes	Yes	Yes	Yes	Yes
WebShield 2.7	No	No	No	Yes	Yes
WebShield 3.0	No	No	No	Yes	Yes

# 2 Pre-Installation

Which procedures you need to complete before installing the new version of the software depends on whether you are installing the software for the first time or upgrading from version 3.0.1 or higher. The following topics are covered here:

- [Pre-installation guidelines and requirements on page 13.](#)
- [Installing or upgrading the database software on page 13.](#)
- [Proxy settings on page 17.](#)

---

## Pre-installation guidelines and requirements

Complete the tasks and read the following information before you install the software:

- **Microsoft updates and patches** — Update both the ePolicy Orchestrator server and the database server with the latest Microsoft security updates. (Specifically, be sure to install Service Pack 3 on all MSDE 2000 and SQL Server 2000 database servers.)
- **Security software**
  - Install and/or update the anti-virus software on the ePolicy Orchestrator server and scan for viruses.
  - Install and/or update firewall software on the ePolicy Orchestrator server.
- **Ports**
  - Avoid using port 80 for any HTTP communication via ePolicy Orchestrator, because it can be disabled during virus outbreaks.



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

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

---

## Installing or upgrading the database software

Depending on which database you are using and whether you are upgrading it to the most recent version, you need to complete different tasks.

If your system already meets the database requirements outlined in [Requirements and Recommendations](#), go to the appropriate topic:

- [First-Time Installation on page 18.](#)
- [Upgrading to ePolicy Orchestrator 3.6 on page 25.](#)

To install or upgrade the required database, go to the appropriate topic:

- [Installing MSDE 2000 \(with Service Pack 3\) for the first time on page 14.](#)
- [Upgrading MSDE to MSDE 2000 \(with Service Pack 3\) on page 15.](#)
- [Installing SQL Server 2000 \(with Service Pack 3\) on page 15.](#)
- [Upgrading to SQL Server 2000 \(with Service Pack 3\) on page 16.](#)

## Installing MSDE 2000 (with Service Pack 3) for the first time

Typically, install MSDE or MSDE 2000 on the same system as the ePolicy Orchestrator server. You can install Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) Service Pack 3 as the ePolicy Orchestrator database as part of the ePolicy Orchestrator software installation. If you choose to install MSDE 2000 as part of the Setup program, go to [First-Time Installation on page 18](#).

You can also install MSDE 2000 manually, prior to installing ePolicy Orchestrator 3.6. To install the database software on a computer other than the ePolicy Orchestrator server, you must install MSDE 2000 manually. Continue to [Step 1](#).

To install MSDE 2000 manually:

- 1 Insert the product CD into the CD-ROM drive of the computer.
- 2 On the taskbar, select **Start | Run**. The **Run** dialog box appears.
- 3 In **Open**, type one of the commands (depending on whether you are using SQL or Windows NT authentication).

- If using NT authentication:

```
SETUP.EXE TARGETDIR="C:\PROGRAM FILES\MCAFEE\EPO\"
COLLATION=SQL_LATIN1_GENERAL_CP1_CI_AS REBOOT=R
DISABLENETWORKPROTOCOLS=0 /! *v C:\MSDEINSTALL.Log
```

- If using SQL authentication:

```
"E:\SETUP\MSDE\SETUP.EXE" TARGETDIR="C:\PROGRAM FILES\NETWORK
ASSOCIATES\EPO\" COLLATION=SQL_LATIN1_GENERAL_CP1_CI_AS
SAPWD=<PASSWORD> REBOOT=R DISABLENETWORKPROTOCOLS=0 /! *v
C:\MSDEINSTALL.LOG
```

Where `TARGETDIR` is the installation path of the ePolicy Orchestrator software, and where `<password>` is the password for the System Administrator (sa) user account.

- 4 Click **OK** to begin installing MSDE.
- 5 Go to [First-Time Installation on page 18](#).

### MSDE or MSDE 2000 installed on a remote server

If you are using a remote database server, you must manually install the database before you install the ePolicy Orchestrator software.

## Upgrading MSDE to MSDE 2000 (with Service Pack 3)

If you are currently using Microsoft Data Engine (MSDE) as the ePolicy Orchestrator database and want to upgrade the database to MSDE 2000 Service Pack 3, you must manually upgrade the database. You must upgrade it before you upgrade the ePolicy Orchestrator software.

If you are using an existing database server, you must manually install or upgrade the database before you install the ePolicy Orchestrator software.



Be sure to back up the existing database before you upgrade the database software. For instructions, see *Backing up ePolicy Orchestrator MSDE databases* in the *ePolicy Orchestrator 3.6 Product Guide*.

To perform this upgrade, consider the following:

- You must be logged in as a local administrator.
- You can upgrade a database that uses SQL authentication as long as you are logged in as a local administrator.
- The command in this procedure creates a log file (MSDEUPGRADE.LOG) at the specified path.
- The MSDE 2000 SP3 Setup program can be found in the root of the download, or the root of the CD under the Setup\MSDE folder.

To upgrade MSDE to MSDE 2000 Service Pack 3:

- 1 Insert the product CD into the CD-ROM drive of the computer.
- 2 On the taskbar, click the **Start** button, then point to **Run**. The **Run** dialog box appears.
- 3 In the **Open** text box, type one of the following commands (depending on whether you are using SQL or Windows NT authentication):
  - If using NT authentication:

```
SETUP UPGRADE=1 DISABLENETWORKPROTOCOLS=0 /1*v C:\MSDEUpgrade.Log
```
  - When using SQL Authentication "Mixed Mode" (where AnAdminLogin is a member of the sysadmin fixed server role)

```
SETUP UPGRADE=1 SECURITYMODE=SQL UPGRADEUSER=AnAdminLogin  
UPGRADEPWD=AdminPassword DISABLENETWORKPROTOCOLS=0 /1*v  
C:\MSDEUpgrade.Log
```
- 4 Click **OK** to begin the installation.
- 5 Restart the ePolicy Orchestrator services.
- 6 Go to [Upgrading to ePolicy Orchestrator 3.6 on page 25](#).

## Installing SQL Server 2000 (with Service Pack 3)

If you are installing SQL Server 2000 for the first time, you must install it manually before you install the ePolicy Orchestrator software. Be sure to then install Service Pack 3 for SQL Server 2000. For instructions, see the SQL Server product documentation. If you installed SQL Server remotely, verify that it is visible on the network before you install the ePolicy Orchestrator software.

Once you have completed installing SQL Server 2000 and Service Pack 3, go to [First-Time Installation on page 18](#).

## Upgrading to SQL Server 2000 (with Service Pack 3)

To upgrade existing ePolicy Orchestrator databases to SQL Server 2000 with Service Pack 3, you must upgrade them before you upgrade the ePolicy Orchestrator software. Be sure to back up existing databases first. For instructions, see the Microsoft SQL Server product documentation. If you installed SQL Server remotely, verify that it is visible on the network before you install the ePolicy Orchestrator software.



If you are currently using SQL Server as the ePolicy Orchestrator database and it is installed on a separate computer from the ePolicy Orchestrator server, you need to upgrade these remote database servers to Microsoft Data Access Components (MDAC) 2.8. For instructions, see [Upgrading to MDAC 2.8 on page 16](#).

If you are upgrading from SQL Server 7, first upgrade to SQL Server 2000, then apply Service Pack 3.

If your database server is installed locally (on the same computer as the ePolicy Orchestrator server), go to [Proxy settings on page 17](#) to continue.



If you have installed the database server locally, but you installed the Chinese (Simplified), Chinese (Traditional), or Korean language version of the database software, go to [Upgrading to MDAC 2.8](#) to continue.

If your database server is installed remotely (on a different computer than the ePolicy Orchestrator server), go to [Upgrading to MDAC 2.8](#) to continue.

## Upgrading to MDAC 2.8

Now that you have installed the database server, you must ensure that all remote ePolicy Orchestrator consoles have Microsoft Data Access Components (MDAC) version 2.8 currently installed. All remote database servers use the same version to avoid performance and functionality issues.

MDAC 2.8 is installed automatically on local database servers, but must be installed manually on all remote ePolicy Orchestrator database servers running these language versions of the database software:

- English
- French
- German
- Japanese
- Spanish

MDAC 2.8 must be installed manually on ePolicy Orchestrator database servers running these language versions of the database software regardless of whether it is installed locally or remotely:

- Chinese (Simplified)
- Chinese (Traditional)
- Korean

To determine the version number of the current installation of MDAC and upgrade to MDAC 2.8, if necessary:

- 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**.

- If the MDAC version number is not 2.8, close the dialog boxes and proceed to [Step 4](#).
- If the MDAC version number is 2.8, close the dialog boxes and proceed to [Proxy settings](#).

- 4 Run the MDAC 2.8 Setup program.

For English, French, German, Japanese, and Spanish language versions, the setup program is available on the product CD:

SETUP\MDAC\MADC\_TYPE\_<LANGUAGE>.EXE

At press time, instructions for installation were available on the Microsoft web site.

The MDAC 2.8 Setup program and instructions for Chinese (Simplified), Chinese (Traditional), and Korean language versions of the database software are available on the Microsoft web site.

---

## Proxy settings

Before you install and use the software, be sure to specify to bypass the proxy server for local addresses:

- 1 In Microsoft Internet Explorer, select **Internet Options** from the **Tools** menu. The **Internet Options** dialog box appears.
- 2 Click the **Connections** tab.
- 3 Click **LAN Settings** to open the **Local Area Network (LAN) Settings** dialog box.
- 4 Select **Bypass proxy server** for local addresses.
- 5 Click **OK** on the **Local Area Network (LAN) Settings** dialog box.
- 6 Click **OK** on the **Internet Options** dialog box.

# 3

## First-Time Installation

This chapter provides instructions to install ePolicy Orchestrator 3.6 software for the first time.



If you are upgrading from a prior version of ePolicy Orchestrator, Protection Pilot 1.0, or are migrating from beta or evaluation versions, please go to Chapter 4, [Upgrading to ePolicy Orchestrator 3.6 on page 25](#).

This section includes the following topics:

- [Before you begin](#).
- [Installing the server and console](#).
- [Installing remote consoles on page 24](#).

---

### Before you begin

Before installing ePolicy Orchestrator 3.6, ensure that:

- The systems you intend to use meet the requirements listed in [Requirements and Recommendations on page 5](#).
- You have completed all tasks in [Pre-Installation on page 13](#).

---

### Installing the server and console

To install the ePolicy Orchestrator 3.6 server and console:

- 1 Log on to the desired system using a user account with local administrator permissions.



You must monitor the installation process because it may require you to restart the system.

- 2 If you are using Microsoft SQL Server 2000 as the ePolicy Orchestrator database, verify that the SQL Server 2000 service (**MSSQLSERVER**) is running. For instructions, see the Microsoft product documentation.



Verify TCP/IP is enabled in SQL Server. Launch **Server Network Utility** in SQL and verify TCP/IP is listed under **Enabled Protocols**.

- 3 *If installing the software from the product CD:*

- a Insert the CD into the CD-ROM drive of the computer.
- b In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 3.6**.

*If you downloaded the software from the McAfee web site, go to the location where you extracted the files and double-click SETUP.EXE.*

- 4 When the ePolicy Orchestrator 3.6 Setup wizard appears, click **Next**.

- 5 In the **End User License Agreement** dialog box, select the appropriate license type and the location 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.



If the information in this dialog box does not display correctly, read the appropriate license agreement in the LICENSEAGREEMENT.PDF file supplied with the software.

- 6 Accept the agreement and click **OK** to continue, or click **Cancel** if you do not agree to the terms and end the installation process. The **Installation Options** dialog box appears.
- 7 In the **Installation Options** dialog box, select **Install Server and Console** and either accept the default installation path in **Install to Folder**, or click **Browse** to select a different location, then click **Next**.

**Figure 3-1 Installation Options dialog box**



- 8 In the Set Administrator Password dialog box, enter and verify the password you will use when logging onto this ePolicy Orchestrator server for the first time. For security purposes, ePolicy Orchestrator does not allow accounts with blank passwords.



The Set Administrator Password dialog box appears during a server and console installation, not during a console-only installation.

**Figure 3-2 Set Administrator Password dialog box**



- 9 In the Select Database Server dialog box, specify the desired server, then click Next.

**Figure 3-3 Select Database Server dialog box**



- Install a database server on this computer and use it — Installs Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) as the ePolicy Orchestrator database.

- Use the existing database server on this computer — Uses the existing MSDE 2000, or SQL 2000 Server database server on this computer. If you use a non-default instance, select **Use an existing server on the network**, then select the desired server/instance from the drop-down list.
  - Use an existing server on the network — Uses the remote database server that you select from the **Server name** list. If the desired database server doesn't appear, type its name.
- 10 In the **Database Server Account** dialog box, specify the type of account to log on to the database server, then click **Next**.

**Figure 3-4 Database Server Account dialog box**



- a Select a Windows NT user account or a SQL Server user account.
- b Specify the NetBIOS name of the **Domain** associated with the desired domain administrator user account. available only when you select **This is an NT account**.
- c Specify the **User Name** and **Password** of the desired user account.

If you selected to use a SQL Server user account, type `sa` for the **User Name** and specify a password. For security purposes, ePolicy Orchestrator does not allow accounts with blank passwords.

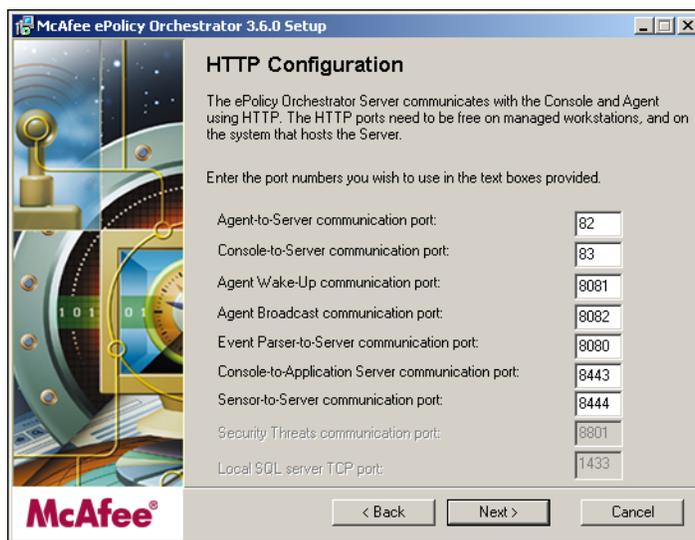


The **Verify Password** field is only available when you install MSDE 2000 as a part of the ePolicy Orchestrator 3.6 installation, and **This is a SQL Server account** is selected. (The **User Name** field is disabled also in this scenario.)

- d Retype the password, then click **Next**.

- 11 Specify the port numbers used for communication to and from the server, as indicated below, then click **Next**.

**Figure 3-5 HTTP Configuration dialog box**



- **Agent-to-Server communication port** — The port that the agent uses to communicate with the server.



McAfee recommends using a port other than 80.

- **Console-to-Server communication port** — The port the console uses to communicate with the server.
- **Agent Wake-Up communication port** — The port used to send agent wakeup calls.
- **Agent Broadcast communication port** — The port used to send SuperAgent wakeup calls.
- **Event Parser-to-Server communication port** — The port used by the Event Parser to send event file information to the server.
- **Console-to-Application Server communication port** — The port used by the console to access user interfaces through an SSL-encrypted connection.
- **Sensor-to-Server communication port** — The port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL.
- **Security Threats communication port** — The port used by McAfee AVERT to provide information on security threats and the required DAT and engine versions to protect against them. This port cannot be changed.
- **Local SQL server TCP port** — The port used by the database for TCP communication.

- 12 In the Set E-Mail Address dialog box, enter the e-mail address for the recipient of messages from ePolicy Orchestrator Notifications. For more information, see the ePolicy Orchestrator Notifications chapter in the ePolicy Orchestrator 3.6 Product Guide.



Change this address at this time is not required. If you choose not to, leave the default address in the field.

Figure 3-6 Set E-Mail Address



- 13 In the Ready To Install dialog box, click Install to begin the installation. This dialog box includes the estimated time for the installation.

The Executing Setup dialog box appears, providing the installation status.

Figure 3-7 Executing Setup dialog box



- 14 In the **Installation Complete** dialog box, view the Readme file or the steps to start the software, then click **Finish** to complete the installation. The installation procedure also installs CMA on the computer.

---

## Installing remote consoles

To install the ePolicy Orchestrator 3.6 remote console:

- 1 Log on to the desired computer using a user account with local administrator permissions.



You must monitor the installation process because it may require you to restart the computer.

- 2 *If installing the software from the product CD:*
  - a Insert the CD into the CD-ROM drive of the computer.
  - b In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 3.6**.

*If you downloaded the software from the McAfee web site, go to the location to which you extracted all the files and double-click the SETUP.EXE file.*

- 3 In the **ePolicy Orchestrator 3.6 Setup** wizard, click **Next** to begin the installation.
- 4 In the **End User License Agreement** dialog box, select the appropriate license type and the location 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.



If the information in this dialog box does not display correctly, read the appropriate license agreement in the LICENSEAGREEMENT.PDF file supplied with the software.

- 5 Accept the agreement and click **OK** to continue, or click **Cancel** if you do not agree to the terms and end the installation process.
- 6 In the **Installation Options** dialog box, select **Install Console** and either accept the default installation location, or click **Browse** to select a different location, then click **Next**.
- 7 In the **Ready To Install** dialog box, click **Install** to begin the installation. The **Executing Setup** dialog box appears, providing the installation status.
- 8 In the **Installation Complete** dialog box, view the Readme file or the steps to start the software, then click **Finish** to complete the installation.

# 4

## Upgrading to ePolicy Orchestrator 3.6

You can upgrade or migrate to ePolicy Orchestrator 3.6 if you are currently using:

- ePolicy Orchestrator 3.0.2 or higher.
- Protection Pilot 1.0 or higher.
- Evaluation versions of ePolicy Orchestrator version 3.6.

This chapter is divided into the following sections:

- [Backing up ePolicy Orchestrator databases on page 26.](#)
- [Upgrading the server and console on page 27.](#)
- [Upgrading remote consoles on page 30.](#)
- [Migrating to a licensed version on page 31.](#)



The following instructions assume that your systems meet the minimum requirements.

### Product removal

The list of products ePolicy Orchestrator 3.6 manages is different than prior versions. The following products that were supported with prior versions of ePolicy Orchestrator are no longer supported in version 3.6 and are removed from the repository when you upgrade:

- Alert Manager 4.5 and 4.6
- Desktop Firewall 7.5 and 7.5.1
- GroupShield Dominon 5.0, 5.2.0, and 5.2.1
- GroupShield Exchange 5.0 and 5.2 for Exchange 5.5
- GroupShield Exchange 5.2 and 6.0 for Exchange 2000
- Klez/Elkern 1.x
- Lightweight Installer 1.0 and 1.0.1
- NetShield 4.6.0 and 4.6.1 for NetWare
- NetShield 4.0.3 and 4.5.0 for Windows NT
- NimdaScan 1.x
- NimdaScan 2.x
- System Compliance Profiler 1.0 and 1.0.1

- ThreatScan 2.0, 2.1, and 2.5
- VirusScan 4.0.3 for Windows
- VirusScan 4.0.3 for Windows NT
- VirusScan 4.5.0 for Windows
- VirusScan Thin Client 6.0 and 6.1
- GroupShield Domino 5.0.0

---

## Before you begin

Before you begin upgrading the ePolicy Orchestrator software, ensure that:

- The systems you intend to use meet the requirements listed in [Requirements and Recommendations on page 5](#).
- You have completed all tasks in [Pre-Installation on page 13](#).

---

## Backing up ePolicy Orchestrator databases

Before you upgrade to version 3.6, back up all ePolicy Orchestrator databases:

- [Microsoft SQL Server on page 26](#).
- [MSDE on page 26](#).

Once your ePolicy Orchestrator databases are backed up, go to [Upgrading the server and console on page 27](#).

### Microsoft SQL Server

If you are using Microsoft SQL Server as the ePolicy Orchestrator database, see the Microsoft product documentation.

Once your ePolicy Orchestrator databases are backed up, go to [Upgrading the server and console on page 27](#).

### MSDE

If you are using MSDE as the ePolicy Orchestrator databases, you can back up ePolicy Orchestrator MSDE databases using the McAfee Database Backup Utility (DBBAK.EXE). You can back up and restore MSDE databases to the same path on the same database servers using this utility.



This tool cannot change the database location.

- 1 Stop the McAfee ePolicy Orchestrator 3.6.0 Server service and ensure that the SQL Server (MSSQLSERVER) service is running.
- 2 Close all ePolicy Orchestrator consoles and remote consoles.

- 3** Double-click DBBAK.EXE. If you are upgrading from version 3.0.x, the default location is:  
  
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.0.X  
  
If you are upgrading from Protection Pilot 1.0 or higher, the default location is:  
  
C:\PROGRAM FILES\NETWORK ASSOCIATES\PROTECTION PILOT\1.X
- 4** Type the **Database Server Name**.
- 5** Select **NT Authentication** or **SQL Account**.  
  
If you select **SQL Account**, type a user **Name** and **Password** for this database.
- 6** Type the **Backup File path**, then click **Backup**.
- 7** Click **OK** when the backup process is done.
- 8** Start the **McAfee ePolicy Orchestrator 3.0 Server** service and ensure that the **MSSQLSERVER** service is running.
- 9** Once the ePolicy Orchestrator databases are backed up, go to [Upgrading the server and console on page 27](#).

---

## Upgrading the server and console

You must upgrade ePolicy Orchestrator to version 3.6 on every ePolicy Orchestrator server and console.

This procedure upgrades the ePolicy Orchestrator server and console from ePolicy Orchestrator version 3.0.2 or higher, and Protection Pilot version 1.0 or higher. This upgrade also installs the ePolicy Orchestrator agent on the server system. The default location of the agent on ePolicy Orchestrator 3.0.2 or higher and ProtectionPilot 1.0.0 or higher is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO



You must monitor the installation process because it may require you to restart the system.

To upgrade the server and console:

- 1** Log on to the desired computer using a user account with local administrator permissions.
- 2** If you are using Microsoft SQL Server 2000 as the ePolicy Orchestrator database, verify that the SQL Server 2000 service (**MSSQLSERVER**) is running.
- 3** Close all ePolicy Orchestrator consoles.
- 4** *If installing the software from the product CD:*
  - a** Insert the CD into the CD-ROM drive of the computer.
  - b** In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 3.6**.

If you downloaded the software from the McAfee web site, go to the location where you extracted all the files and double-click SETUP.EXE.

- 5 In the ePolicy Orchestrator 3.6 Setup wizard, click **Next** to begin the installation.
- 6 In the **End User License Agreement** dialog box, select the appropriate license type and the location in which you purchased the software. The license type you select must match the license you purchased. If you are unsure which license you purchased, contact your account manager.



If the information in this dialog box does not display correctly, read the appropriate license agreement in the LICENSEAGREEMENT.PDF file supplied with the software.

- 7 Accept the agreement and click **OK** to continue.

A warning message notifies you which products are no longer supported with this version of the software. These products are removed from the **Repository** when you click **Next**.

- 8 Click **Next** to proceed with the upgrade process.
- 9 In the **Database Server Account** dialog box, specify the type of account to log on to the database server, then click **Next**.

**Figure 4-1 Database Server Account dialog box**



- a Select whether to specify a Windows NT user account or a SQL Server user account.
- b Specify the NetBIOS name of the **Domain** associated with the desired domain administrator user account available only when you select **This is an NT account**.
- c Specify the **User Name** and **Password** of the desired user account.

- 10 Specify the port numbers used for communication to and from the server, as indicated, then click **Next**. Depending on which version you are upgrading from, some of these boxes are grayed out. If you want to reassign ports that were used in a prior version of ePolicy Orchestrator, we recommend that you uninstall the prior version, then perform a fresh installation of ePolicy Orchestrator 3.6.

**Figure 4-2 HTTP Configuration dialog box**



- **Agent-to-Server communication port** — The port that the agent uses to communicate with the server.



We recommend using a port other than 80.

- **Console-to-Server communication port** — The port the console uses to communicate with the server.
- **Agent Wake-Up communication port** — The port used to send agent wakeup calls.
- **Agent Broadcast communication port** — The port used to send SuperAgent wakeup calls.
- **Event Parser-to-Server communication port** — The port used by the Event Parser to send event file information to the server.
- **Console-to-Application Server communication port** — The port used by the console to access user interfaces through an SSL-encrypted connection.
- **Sensor-to-Server communication port** — The port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL.
- **Security Threats communication port** — The port used by McAfee AVERT to provide information on security threats and the required DAT and engine versions to protect against them. This port cannot be changed.
- **Local SQL server TCP port** — The port used by the database for TCP communication.

- 11 In the **Set E-Mail Address** dialog box, provide an e-mail address to receive messages from ePolicy Orchestrator Notifications. For more information, see the *ePolicy Orchestrator 3.6 Product Guide*.



You can choose to provide other addresses once the software is installed. If you choose to do this, please leave the default address in the text box.

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

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

- 13 In the **Installation Complete** dialog box, view the Readme file or the steps to start the software, then click **Finish** to complete the installation.

---

## Upgrading remote consoles

Be sure to upgrade ePolicy Orchestrator to version 3.6 on every ePolicy Orchestrator remote console. This procedure upgrades the ePolicy Orchestrator remote console from version 3.0.2 or higher:



You must monitor the installation process because it may require you to restart the system.

All of the ePolicy Orchestrator utility programs (for example, Database Merge) must reside in the installation directory to be updated by the Setup program. The default location is:

```
C:\PROGRAM FILES\MCAFFEE\EPO\3.X.X
```

To upgrade a remote console:

- 1 Log on to the desired system using a user account with local administrator permissions.
- 2 Close all ePolicy Orchestrator consoles.
- 3 *If installing the software from the product CD:*
  - a Insert the CD into the CD-ROM drive of the computer.
  - b In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 3.6**.

*If you downloaded the software from the McAfee web site, go to the location where you extracted all the files and double-click SETUP.EXE.*
- 4 In the **ePolicy Orchestrator 3.6 Setup** wizard, click **Next** to begin the installation.
- 5 In the **End User License Agreement** dialog box, select the appropriate license type and the location in which you purchased the software.

The license type must match the license you purchased. If you are unsure which license you purchased, contact your account manager.



If the information in this dialog box does not display correctly, read the appropriate license agreement in the LICENSEAGREEMENT.PDF file supplied with the software.

- 6** Accept the agreement and click **OK** to continue.
- 7** In the **Ready To Install** dialog box, click **Install** to begin the installation.  
  
The **Executing Setup** dialog box appears, providing the status of the installation.
- 8** In the **Installation Complete** dialog box, view the Readme or the steps to start the software, then click **Finish** to complete the installation.

---

## Migrating to a licensed version

Use this procedure to migrate an evaluation version of the software to a licensed version.



To migrate any pre-release software to a licensed version, you must first uninstall the existing version of the software. For instructions, see [Uninstalling the software on page 34](#).

- 1** Log on to the desired computer using a user account with local administrator permissions.
- 2** Close all ePolicy Orchestrator consoles.
- 3** *If you downloaded the software from the McAfee web site*, go to the location where you extracted all the files and double-click SETUP.EXE.



Be sure that you selected the Setup program for the licensed version of the software.

*If installing the software from the product CD:*

- a** Insert the CD into the CD-ROM drive of the computer.
- b** In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 3.6**.
- 4** In the **ePolicy Orchestrator 3.6 Setup** wizard, click **Next** to begin the migration.
- 5** A message appears indicating that the migration was completed successfully.

# 5

## Post-Installation Procedures

After completing the Setup wizard, you still have several configurations to perform before you can use the software. The procedures to complete the installation, depend on whether you are installing the product first time, or upgrading from a previous version. Refer to the appropriate section:

- [Completing a first-time installation on page 32.](#)
- [Completing an upgrade on page 32.](#)
- [Checking in files manually on page 33.](#)
- [Configuring the software for a server that has multiple NICs on page 33.](#)
- [Uninstalling the software on page 34.](#)

---

### Completing a first-time installation

To complete the first-time installation:

- 1 Plan your ePolicy Orchestrator Directory and updating scheme.
- 2 Create the ePolicy Orchestrator Directory.
- 3 Distribute agents to the systems you wish to manage with ePolicy Orchestrator.
- 4 Create the updating repositories.
- 5 Check in the products ePolicy Orchestrator is to manage, and configure their policy settings. For a list of the type of files you must check in manually, see [Checking in files manually on page 33.](#)
- 6 Deploy products to the managed computers.
- 7 Configure the advanced features of ePolicy Orchestrator.

For instructions and information, see the *ePolicy Orchestrator 3.6 Product Guide*.

---

### Completing an upgrade

The version and product you are upgrading determines which procedures you must perform to complete your installation of ePolicy Orchestrator 3.6:

- 1 Plan and implement any ePolicy Orchestrator Directory and repository changes.
- 2 Upgrade the agents on your network to version 3.5, if desired. If you do not upgrade legacy agents, full functionality is not present.
- 3 Check in and deploy new products you want to manage.

For instructions and information, see the the *ePolicy Orchestrator 3.6 Product Guide*.

---

## Checking in files manually

These are the file that you must check into the master repository or the Repository after you install the software for the first time. For more information, see the *ePolicy Orchestrator 3.6 Product Guide*.

- **Contents of the McAfee AutoUpdate Architect 1.0 master repository** — Packages that were checked into the McAfee AutoUpdate Architect master repository are not migrated to the ePolicy Orchestrator 3.6 master repository.
- **Custom packages** — Only custom packages created with McAfee Installation Designer 7.0 can be checked into the master repository.
- **Policy pages** — If the policy page for a product was not added to the Repository during the installation, you must manually add it to the Repository.
- **Product plug-in files** — Any product plug-in (.DLL) files that were not checked in as part of the installation must be checked into the master repository manually.
- **Products** — If you are installing the software for the first time, you must check in all products that you want to deploy via ePolicy Orchestrator. If you are upgrading the software, any supported products that were not already present must be checked into the master repository manually.



VirusScan ThinClient 6.0 and 6.1 are exceptions. You need to check these products into the master repository even if they were already in the Repository.

- **Product updates** — You must check in all product updates that you want to deploy via ePolicy Orchestrator. One exception is product plug-in (.DLL) files that were converted as part of the installation.

---

## Configuring the software for a server that has multiple NICs

When you install ePolicy Orchestrator on a server that has multiple network interface cards (NICs), you should ensure that ePolicy Orchestrator is bound to the desired NIC.

To configure the software for a server that has multiple NICs:

- 1 Open the SERVER.INI file. The default location is:

```
c:\Program Files\McAfee\ePO\3.6.0\DB
```

- 2 Add the following line at the end of the file:

```
ServerIPAddress=XXX.XXX.XXX.XXX
```

Where `xxx.xxx.xxx.xxx` is the IP address of the NIC to which you want ePolicy Orchestrator bound.

- 3 Save and close the `SERVER.INI` file.
- 4 Restart all of the ePolicy Orchestrator services.

---

## Uninstalling the software

If and when you must uninstall this software, use this procedure to remove the software. If you used the ePolicy Orchestrator Setup program to install MSDE, you can remove it during uninstallation.

- 1 Close all ePolicy Orchestrator consoles.
- 2 Close all database management software; for example, SQL Enterprise Manager.
- 3 Use **Add/Remove Programs** in the **Control Panel** to remove the software. For instructions, see the Windows Help file. To open this file, click the **Start** button, then select **Help**.

To remove the existing MSDE database, select **Remove MSDE**.

- 4 Click **Remove**.

# 6

## Troubleshooting

The most common messages that appear during an installation and their solutions are listed in [Table 6-1 on page 35](#) in alphabetical order.

If you are unable to resolve an issue using the information in this table, be sure to gather the following information before you contact McAfee Technical Support:

- Verify that you have met the minimum installation requirements. For a complete list, see [System requirements on page 5](#).
- Review the *ePolicy Orchestrator 3.6 Release Notes* (README.TXT) for any known installation issues.
- Verify that the user account you used to log on to the computer on which you are installing the software has full administrator permissions to that computer.
- Collect the exact text of all messages, and be sure to take note of any message codes that appear.
- Gather the installation log files. The default location of these files are:
  - CONSOLE.LOG — c:\program files\mcafee\epo\3.6.0
  - SERVER.LOG — c:\program files\mcafee\epo\3.6.0\db\logs
  - TRACE.LOG and DBINIT.LOG — %Temp%\nailogs

**Table 6-1 Common installation messages and their solutions**

If this message appears...	Then...
You are attempting to upgrade from a product version that is not supported. Please see the ePolicy Orchestrator Installation Guide for upgrade requirements.	The ePolicy Orchestrator 3.0.2 or higher software (or Protection Pilot 1.0 or higher software) has not been installed on this computer. You can only upgrade from these versions of ePolicy Orchestrator or Protection Pilot.
ePolicy Orchestrator requires Internet Explorer 6.0 or later.	The computer on which you are attempting to install the software is using a non-supported version of the browser.  Install Internet Explorer 6.0 before you install the software.
ePolicy Orchestrator Setup is already running.	The ePolicy Orchestrator 3.6 Setup program is already running.  You cannot have more than one instance of Setup running.
For security reasons we do not allow blank passwords. Please enter a value in the "Password" field provided.	The <b>Password</b> box is blank.  Specify the password of the user account that you want to use.

**Table 6-1 Common installation messages and their solutions** (Continued)

If this message appears...	Then...
For security reasons we do not allow blank passwords. Please enter a value in the "Verify Password" field provided.	The <b>Verify Password</b> box is blank. Specify the password of the user account that you want to use.
It is required that the video display be set to 1024x768 or higher.	The computer on which you are attempting to install the software does not meet the minimum monitor resolution requirement.  Change the monitor resolution to 1024x768 or higher, then continue the installation. Otherwise, you might not be able to view the entire application window after you start the software. For instructions on changing the monitor resolution, see the Windows Help File. To open this file, click the <b>Start</b> button, then select <b>Help</b> .
It is required that this computer have at least 512 MB of RAM.	The computer on which you are attempting to install the software does not meet the minimum memory requirement.  For a list of requirements, see <a href="#">Server and console requirements on page 5</a> or <a href="#">Remote console requirements on page 6</a> , respectively.
Microsoft Windows 2000 Service Pack 3 is not installed. ePolicy Orchestrator requires Windows 2000 Service Pack 3 or later be installed.	The computer on which you are attempting to install the software is using a non-supported version of the operating system.  The supported operating systems differ depending on whether you are installing the server and console or remote console only. For a list of requirements, see <a href="#">Server and console requirements on page 5</a> or <a href="#">Remote console requirements on page 6</a> , respectively.
Please enter a value in the "Agent Broadcast communication" field.	The <b>Agent Broadcast communication port</b> box is blank. Specify the port number (default is 8082) that the ePolicy Orchestrator server will use to send agent wakeup calls to SuperAgents.
Please enter a value in the "Agent-to-Server communication" field.	The <b>Agent-to-Server communication port</b> box is blank. Specify the port number that the agent will use to communicate with the server.
Please enter a value in the "Agent Wake-Up communication" field.	The <b>Agent Wake-Up communication port</b> box is blank. Specify the port number (default is 8081) that the ePolicy Orchestrator server will use to send agent wakeup calls.
Please enter a value in the "Console-to-Application Server communication" field.	The <b>Console-to-Application Server communication port</b> box is blank. Specify the port number that the console will use to communicate with the server.
Please enter a value in the "Install to Folder" field.	The <b>Install to Folder</b> box is blank. Type the installation path in <b>Install to Folder</b> , or click <b>Browse</b> to select a location. The default location is: C:\PROGRAM FILES\MCA\FEE\NEPO
Please enter a value in the "User Name" field.	The <b>User name</b> box is blank. Specify the user name of the user account that you want to use.
Please make sure that you have granted SQL Server Administrator-level access to this NT account.	Be sure that you grant SQL Server administrator permissions to the Windows NT user account you specified.

**Table 6-1 Common installation messages and their solutions** (Continued)

<b>If this message appears...</b>	<b>Then...</b>
The License file is corrupt. Please contact support for assistance.	Setup is unable to read the license information required to install the software. Contact McAfee Customer Service.
The License file is missing. Please contact support for assistance.	Setup is unable to read the license information required to install the software. Contact McAfee Customer Service.
The operating system you are using is not currently supported. For a complete list of system requirements, see the "ePolicy Orchestrator Installation Guide."	The computer on which you are attempting to install the software is using a non-supported version of the operating system.  The supported operating systems differ depending on whether you are installing the server and console or remote console only. For a list of requirements, see <a href="#">Server and console requirements on page 5</a> or <a href="#">Remote console requirements on page 6</a> , respectively.
The passwords you entered do not match. Please try again.	The values you typed in <b>Password</b> and <b>Verify Password</b> do not match.  Specify the password of the user account that you want to use.
This BETA version of ePolicy Orchestrator has expired.	Your license to use the software has expired.  Go to the beta feedback page on the McAfee web site, where you can supply your comments about the beta software.
This EVALUATION version of ePolicy Orchestrator has expired.	Your license to use the software has expired.  Go to the McAfee web site, where you can purchase a full version of the software.
This system is not currently configured with a static IP address, which is recommended for ePolicy Orchestrator Server.	The computer on which you are attempting to install the software does not use a static IP address.  We recommend using static IP addresses for ePolicy Orchestrator servers to improve performance and reduce bandwidth usage.
Unable to determine the edition of your license. Please contact support for assistance.	Setup is unable to read the license information required to install the software. Contact McAfee Customer Service.
Unable to determine the state of your license. Please contact support for assistance.	Setup is unable to read the license information required to install the software. Contact McAfee Customer Service.
Unable to make a connection to the database server.  Verify that you have entered the user name, password, and database server name correctly, then try again.  If this message still appears, see the ePolicy Orchestrator Installation Guide for more information about resolving this issue.	A connection could not be made to the corresponding ePolicy Orchestrator database server.  <ol style="list-style-type: none"> <li>1 Verify that the <b>Domain</b>, <b>User Name</b>, and <b>Password</b> you provided are typed correctly.</li> <li>2 Verify that the database server is running.</li> <li>3 Verify that the user account you provided is valid for the database server.</li> </ol>

**Table 6-1 Common installation messages and their solutions** (Continued)

<b>If this message appears...</b>	<b>Then...</b>
We are unable to connect using the information you provided. Please check to make sure you have entered them correctly and try again.	The user account that you specified could not be accessed.  1 Verify that the <b>Domain, User Name, and Password</b> you provided are typed correctly.  2 Verify that the user account you used to log on to this computer has access to this domain.
You must reboot before installing ePolicy Orchestrator again.	The ePolicy Orchestrator software has been previously removed.  You must restart this computer before you can reinstall the software.

# A

## High Availability Ensuring failover support

The ePolicy Orchestrator software now provides high availability for server clusters with Microsoft Cluster Server (MSCS) software.

This section covers the following topics:

- [Requirements.](#)
- [Setting up and testing the ePolicy Orchestrator cluster on page 39.](#)

---

### Requirements

Before running ePolicy Orchestrator as a clustered application, ensure the following is true:

- MSCS is set up and running for a cluster of two or more servers.
- ePolicy Orchestrator 3.6 is installed on all nodes of the cluster.
- Remote Microsoft SQL Server 2000 with Service Pack 3 is installed for the ePolicy Orchestrator database.

---

### Setting up and testing the ePolicy Orchestrator cluster

Once the requirements are met, use these procedures to set up the nodes of the cluster. To set up the ePolicy Orchestrator cluster, you must complete these tasks:

- 1 [Stopping the ePolicy Orchestrator services on all nodes on page 39.](#)
- 2 [Running the ePolicy Orchestrator Clustering Setup wizard on page 40.](#)
- 3 [Directing secondary nodes to a common database on page 42.](#)
- 4 [Creating and configuring the cluster group on page 43.](#)
- 5 [Testing the ePolicy Orchestrator cluster on page 47.](#)

### Stopping the ePolicy Orchestrator services on all nodes

For each node you must stop the following three ePolicy Orchestrator services:

- McAfee ePolicy Orchestrator 3.6.0 Server

- McAfee ePolicy Orchestrator 3.6.0 Application Server
- McAfee ePolicy Orchestrator 3.6.0 Event Parser

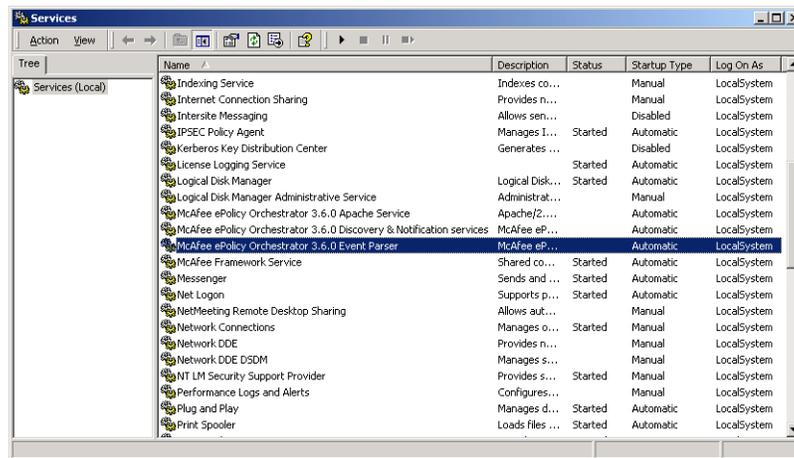


This procedure may be slightly different depending on the operating system you are using. This procedure was created using Microsoft Windows 2000 Server with Service Pack 3.

To stop the ePolicy Orchestrator services on a node:

- 1 From the Start menu, select **Settings | Control Panel | Administrative Tools | Services**. The Services dialog box appears.

**Figure A-1 Services dialog box**



- 2 Individually, right-click each of the services and select **Stop**.
- 3 Individually, right-click each of the services and select **Properties**. The Properties dialog box appears for each service.
- 4 On the General tab, change the Startup type to **Manual**.
- 5 Exit the Services dialog box when finished.

## Running the ePolicy Orchestrator Clustering Setup wizard

Run the ePolicy Orchestrator Clustering Setup wizard on each node of the cluster.

Have the following information before running the wizard:

- Location of the DB folder.
- Virtual address information for the Cluster Group.

To launch the ePolicy Orchestrator Clustering Setup wizard:

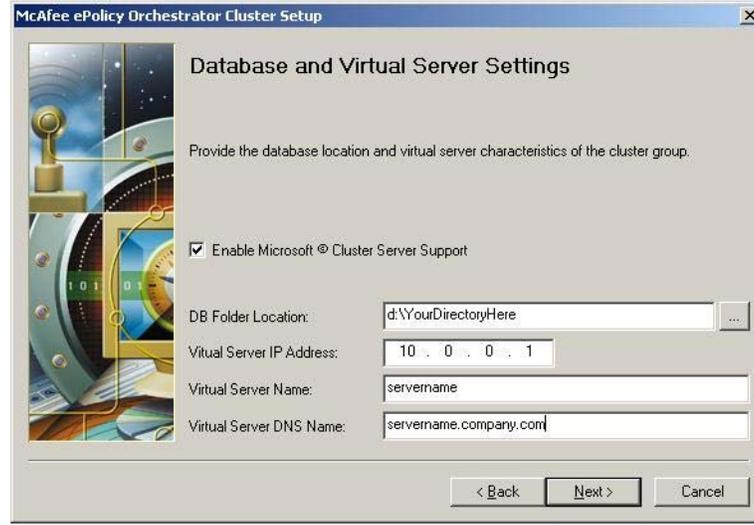
- 1 Go to the installation folder, and double-click CLUSTEREPO.EXE. By default, this is:

```
<Drive>:\Program Files\McAfee\ePO\3.6.0
```

- 2 Click **Next** on the Welcome panel of the wizard.

- 3 Select Enable Microsoft Cluster Server Support.

**Figure A-2 McAfee ePolicy Orchestrator Clustering Setup wizard**



The screenshot shows the 'McAfee ePolicy Orchestrator Cluster Setup' wizard window. The title bar reads 'McAfee ePolicy Orchestrator Cluster Setup'. The main window is titled 'Database and Virtual Server Settings'. Below the title, there is a decorative graphic on the left and a text area on the right that says 'Provide the database location and virtual server characteristics of the cluster group.' Below this, there is a checkbox labeled 'Enable Microsoft © Cluster Server Support' which is checked. There are four input fields: 'DB Folder Location:' with a text box containing 'd:\YourDirectoryHere' and a browse button (...); 'Virtual Server IP Address:' with a text box containing '10 . 0 . 0 . 1'; 'Virtual Server Name:' with a text box containing 'servername'; and 'Virtual Server DNS Name:' with a text box containing 'servername.company.com'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 4 Type, browse to, or create a location for the DB folder on the Quorum using the ... button.
- 5 Provide the following identifying information of the ePO group:
  - Virtual server IP address.
  - Virtual server name.
  - Virtual Server DNS name.



Although you haven't created the ePO group yet, this procedure assumes that you will know what these characteristics will be when you create it.

- 6 Click Next.

- 7 Review the settings provided. If accurate, click **Next**, then **Finish**.

**Figure A-3 McAfee ePolicy Orchestrator Clustering Setup wizard**



## Directing secondary nodes to a common database

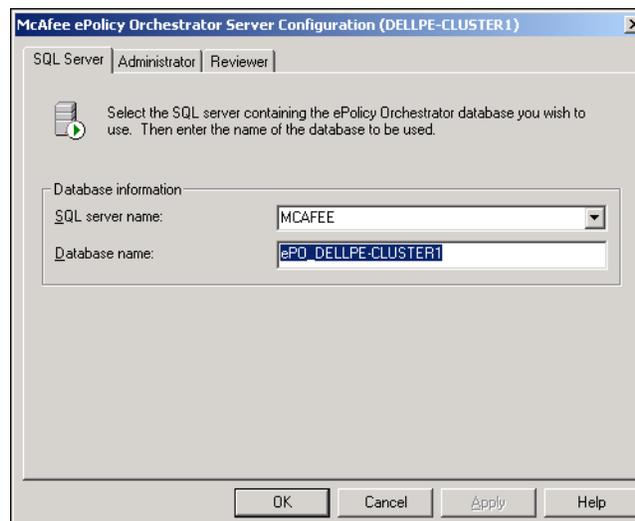
On all secondary nodes, you must use the CFGNAIMS.EXE utility to direct the secondary ePolicy Orchestrator servers to the primary node's database:

- 1 Go to the installation folder, and double-click CFGNAIMS.EXE. By default, this is:

```
<Drive>:\Program Files\McAfee\ePO\3.6.0
```

The McAfee ePolicy Orchestrator Server Configuration dialog box appears.

**Figure A-4 SQL Server tab**



- 2 On the SQL Server tab, change the database name to that of the primary node.
- 3 On the Administrator and Reviewer tabs, change the user credentials as needed.

## Creating and configuring the cluster group

When setting up the cluster group, you must perform the following:

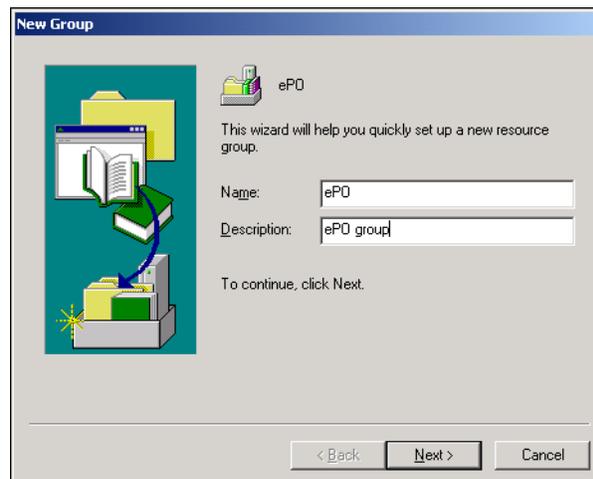
- *Creating the ePolicy Orchestrator group*
- *Creating the IP Address resource.*
- *Creating the Network Name resource.*
- *Moving the Quorum drive to the ePO group.*
- *Creating the Generic Service resources.*

### Creating the ePolicy Orchestrator group

From the primary node of the cluster:

- 1 From the Start menu, select Program Files | Administrative Tools | Cluster Administrator. The Cluster Administrator appears.
- 2 Right-click **Groups** in the console tree, then select **New | Group**. The **New Group** dialog box appears.

**Figure A-5 New Group dialog box**



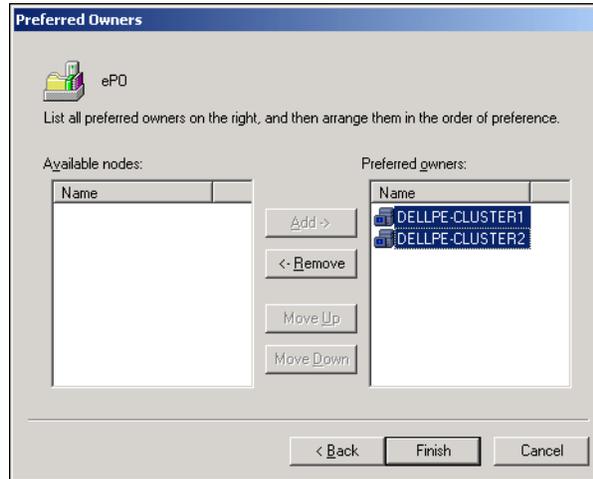
- 3 Type the **Name** and **Description** of the group, then click **Next**.



For the purposes of showing this procedure, the new group is called ePO, although you can choose any name.

- 4 In the Preferred Owners dialog box, identify the desired owners of the group. Select the desired node under **Available Nodes**, then click **Add**. Repeat until all preferred owners are added, then click **Next**.

**Figure A-6 Preferred Owners dialog box**



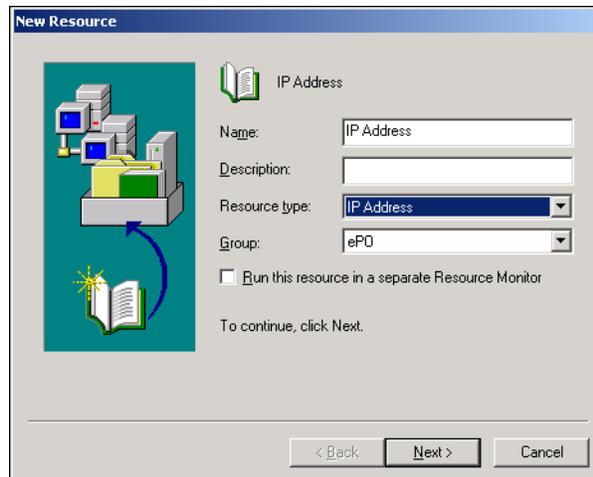
- 5 Click **Finish**.

### Creating the IP Address resource

You must also create the IP Address resource manually for the ePO group:

- 1 Right-click the ePO group, select **New | Resource**. The **New Resource** dialog box appears.
- 2 Type the **Name** and **Description** of the resource. For example, **IP Address**.
- 3 Select **IP Address** from the **Resource Type** drop-down list.

**Figure A-7 IP Address resource**



- 4 Ensure ePO is the selected group, then click **Next**.

- 5 In the **Possible Owners** dialog box, identify the possible owners of the resource. Select the desired node, then click **Add**. Repeat until all possible owners are added, then click **Next**.
- 6 In the **Dependencies** dialog box, click **Next**.
- 7 Provide the virtual IP address and subnet mask for the ePO group, then click **Finish**.

## Creating the Network Name resource

You must also manually create the Network Name resource for the ePO group:

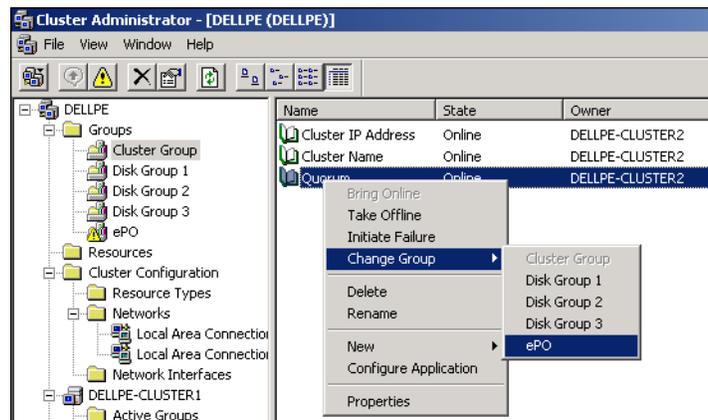
- 1 Right-click the ePO group, select **New | Resource**. The **New Resource** dialog box appears.
- 2 Type the **Name** and **Description** of the resource. For example, ePO Server Name.
- 3 Select **Network Name** from the **Resource Type** drop-down list.
- 4 Ensure **ePO** is selected, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the possible owners of the resource. Select the desired node, then click **Add**. Repeat until all possible owners have been added, then click **Next**.
- 6 In the **Dependencies** dialog box, select **IP Address**, then click **Next**.
- 7 Provide the virtual server name for the ePO group, then click **Finish**.

## Moving the Quorum drive to the ePO group

Once the group has been created, you must move the Quorum drive to the ePO group:

- 1 Select the **Cluster Group**, right-click **Quorum**, then select **Change Group | ePO**.

**Figure A-8 Change Group action**



- 2 Verify this action when prompted.

## Creating the Generic Service resources

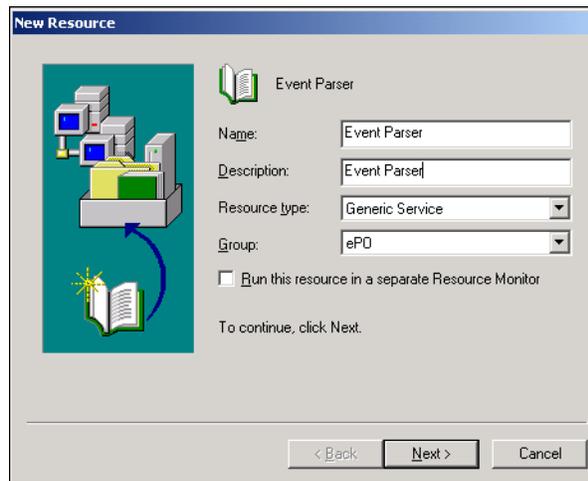
You must create a Generic Service resource for the ePO group to add the ePolicy Orchestrator services for the group. For each node you must perform the procedure twice, once for the McAfee ePolicy Orchestrator 3.6.0 Event Parser service, and once for the other two services:



The McAfee ePolicy Orchestrator 3.6.0 Event Parser service must be added first due to its dependence on the McAfee ePolicy Orchestrator 3.6.0 Server service.

- 1 Right-click the ePO group, then select **New | Resource**. The **New Resource** dialog box appears.
- 2 Type the **Name** and **Description** of the resource. For example, `Event Parser`.

**Figure A-9 New Resource dialog box**



- 3 Select **Generic Service** from the **Resource type** drop-down list.
- 4 Ensure **ePO** is the selected group, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the possible owners of the resource. Select the desired node, then click **Add**. Repeat until all possible owners are added, then click **Next**.
- 6 In the **Dependencies** dialog box:
 

When adding the McAfee ePolicy Orchestrator 3.6.0 Event Parser service and the McAfee ePolicy Orchestrator 3.6.0 Application Server service, add the Quorum drive as a dependency, then click **Next**.

When adding the McAfee ePolicy Orchestrator 3.6.0 Server service, add the McAfee ePolicy Orchestrator 3.6.0 Event Parser service and the Quorum drive as dependencies, then click **Next**.
- 7 Type the **Service Name** and leave the **Start Parameters** field blank, then click **Finish**.



The service name for the Event Parser service is `EVENTPARSER360`.  
 The service name for the Server service is `APACHE2FOREPO`.  
 The service name for the Application Server service is `RSDSERVER360`.

## Testing the ePolicy Orchestrator cluster

The ePolicy Orchestrator cluster should now be set up and running. To test the functionality:

- 1 Select the ePO group, and select **Bring online**.
- 2 Right-click any of the resources for the ePO group, then select **Initiate Failover**. The resources should fail and come back online.

You can also test the functionality by moving the ePO group:

- 1 Right-click the ePO group.
- 2 Select **Move Group**. All the ePO group resources should fail over successfully.

# Index

## A

- agent for NetWare
  - system requirements, 10
- agent for WebShield appliances
  - system requirements, 10
- agent for Windows
  - system requirements, 8

## C

- Chinese reports, requirements, 8
- client computer requirements on Windows 95, 8
- console requirements, 5

## D

- database
  - backing up, 26
  - calculating number of SQL licenses, 7
  - system requirements, 7
- database software
  - determining when to install, 13, 18, 26
  - upgrading to MDAC, 16
- distributed repository requirements, 8

## E

- error messages
  - list of, 35

## F

- first-time installation
  - calculating number of SQL licenses, 7
  - pre-installation checklist, 13, 18, 26
  - remote consoles, 24
  - server and console, 18

## I

- installing the software
  - calculating number of SQL licenses, 7
  - pre-installation checklist, 13, 18, 26

## K

- Korean reports, requirements, 8

## L

- language support of operating systems, 11
- licenses for SQL, calculating, 7

## M

- MDAC
  - upgrading, 16
- messages
  - list of, 35

## O

- operating systems language support, 11

## P

- pre-installation checklist, 13, 18, 26

## R

- remote console requirements, 6
- reporting requirements, 8
- requirements, 5
  - agent for NetWare, 10
  - agent for WebShield appliances, 10
  - agent for Windows, 8
  - console, 5
  - database, 7
  - distributed repositories, 8
  - operating systems language support, 11
  - remote console, 6
  - reporting, 8
  - server, 5
  - SuperAgent, 9

## S

- server and console
  - upgrade, 27
- server requirements, 5
- SQL licenses, calculating number of, 7
- starting the software, 17
- SuperAgent
  - system requirements, 9
  - system requirements, 5
  - agent for NetWare, 10
  - agent for WebShield appliances, 10
  - agent for Windows, 8
  - console, 5
  - database, 7
  - distributed repositories, 8
  - operating systems language support, 11
  - remote console, 6
  - reporting, 8
  - server, 5
  - SuperAgent, 9

- system requirements, 9
- system requirements, 5
- agent for NetWare, 10
- agent for WebShield appliances, 10
- agent for Windows, 8
- console, 5
- database, 7
- distributed repositories, 8
- operating systems language support, 11
- remote console, 6
- reporting, 8
- server, 5
- SuperAgent, 9

## T

- troubleshooting
  - list of messages, 35

## U

- update repository requirements, 8
- upgrade installation
  - backing up databases, 26
  - calculating number of SQL licenses, 7
  - pre-installation checklist, 13, 18, 26
  - remote consoles, 30
  - server and console, 27

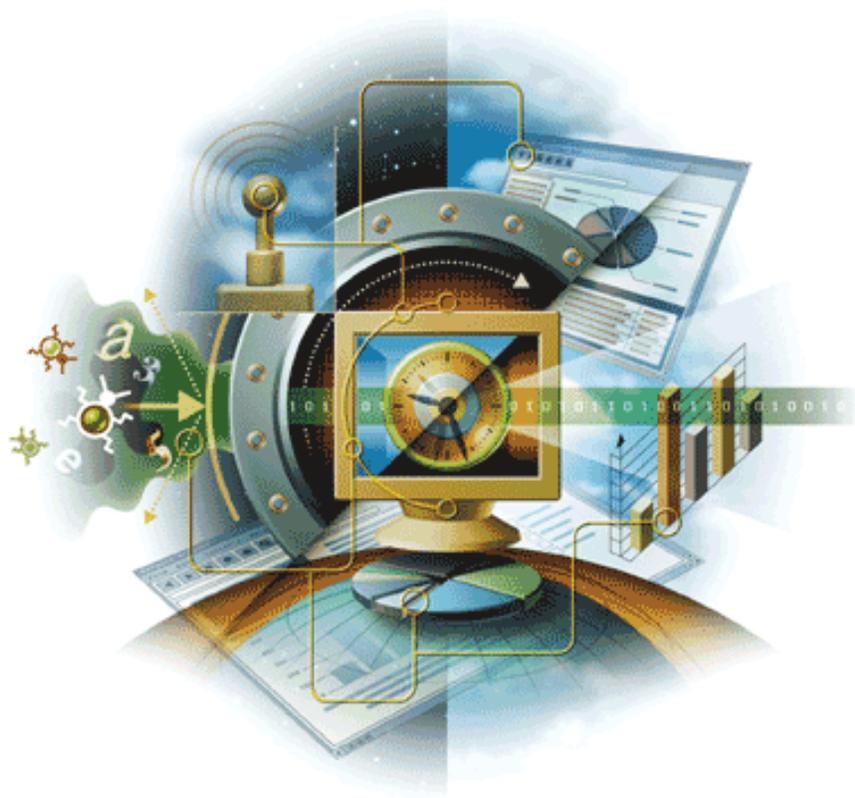
## W

- Windows 95 computers requirements, 8

# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6



## McAfee® System Protection

Industry-leading intrusion prevention solutions

**McAfee®**



# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6

**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

---

**McAfee®**

## COPYRIGHT

Copyright © 2005 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 WEB SITE 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 pro+34vide 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](http://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/Æ Optimizer/Æ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In/Æ Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In/Æ 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](http://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](mailto: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](mailto: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](mailto: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](mailto: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.

## PATENT INFORMATION

Protected by US Patents 6,470,384; 6,493,756; 6,496,875; 6,553,377; 6,553,378.

# Contents

<b>1</b>	<b>Introducing ePolicy Orchestrator</b>	<b>10</b>
	About ePolicy Orchestrator . . . . .	10
	What's new in this release? . . . . .	11
	Named policies . . . . .	12
	High availability . . . . .	12
	More detailed server task log . . . . .	13
	Server-side replication . . . . .	13
	Selective repository replication . . . . .	13
	Selective package replication . . . . .	14
	Enhanced administrator permissions . . . . .	14
	MyAVERT Security Threats integration . . . . .	14
	Enhanced audit logging . . . . .	15
	Using this guide . . . . .	15
	Setting up ePolicy Orchestrator for the first time? . . . . .	16
	Audience . . . . .	17
	Conventions . . . . .	18
	Resources . . . . .	19
	Getting product information . . . . .	19
	Contact information . . . . .	19
<b>2</b>	<b>Configuring ePolicy Orchestrator Servers</b>	<b>21</b>
	Logging onto ePolicy Orchestrator servers . . . . .	22
	Logging off from servers without removing them . . . . .	22
	Logging onto additional servers . . . . .	22
	Installing the security certificate . . . . .	23
	About ePolicy Orchestrator accounts . . . . .	24
	Global administrator . . . . .	25
	Site administrators . . . . .	25
	Global reviewers . . . . .	26
	Site reviewers . . . . .	26
	Viewing current user accounts . . . . .	26
	Adding user accounts . . . . .	27
	Server settings, tasks, and events . . . . .	27
	ePolicy Orchestrator server settings . . . . .	27
	Changing server settings . . . . .	29
	Server tasks and the server task log . . . . .	30
	Viewing server events from the console . . . . .	31
	Viewing the server version number . . . . .	33
<b>3</b>	<b>Creating a Directory of Managed Systems</b>	<b>34</b>
	About the Directory . . . . .	35
	Sites and groups . . . . .	35
	Lost&Found groups . . . . .	36
	Inheritance . . . . .	36
	Considerations when planning your Directory . . . . .	37
	Administrator access . . . . .	37
	Environmental borders . . . . .	37
	Subnets and IP ranges . . . . .	38
	Operating systems and software . . . . .	39

Creating the Directory . . . . .	39
Importing Active Directory containers . . . . .	40
Importing NT domains . . . . .	41
Importing systems and groups from a text file . . . . .	43
Creating sites and groups manually . . . . .	45
IP address filters and sorting . . . . .	47
Adding WebShield appliances . . . . .	49
Maintaining the Directory . . . . .	50
Using Active Directory Discovery . . . . .	50
Synchronizing Directory segments with NT domains . . . . .	53
Maintaining IP filters for sites and groups . . . . .	55
Using Directory searches to find systems . . . . .	59
Moving systems manually within the Directory . . . . .	60
<b>4   Distributing Agents</b> . . . . .	<b>61</b>
About agents and SuperAgents . . . . .	62
Agent installation folder . . . . .	62
Agent language packages . . . . .	62
The agent installation package . . . . .	63
Agent-server communication . . . . .	65
Agent installation command-line options . . . . .	66
SuperAgents and broadcast wakeup calls . . . . .	67
Agent activity logs . . . . .	69
Agent policy settings . . . . .	69
Immediate event forwarding . . . . .	69
Full and minimal properties . . . . .	70
Agent policy and distributed repositories . . . . .	71
Proxy settings . . . . .	71
Configuring agent policy settings . . . . .	71
Distributing agents . . . . .	76
Deploying the agent from ePolicy Orchestrator . . . . .	77
Installing the agent with login scripts . . . . .	80
Installing the agent manually . . . . .	82
Enabling the agent on unmanaged McAfee products . . . . .	84
Including the agent on an image . . . . .	85
Distributing the agent using other deployment products . . . . .	85
Distributing the agent to WebShield appliances and Novell NetWare servers . . . . .	85
Upgrading existing agents . . . . .	86
Upgrading agent version 3.x using login scripts or manual installation . . . . .	86
Upgrading the agent using ePolicy Orchestrator . . . . .	86
Uninstalling the agent . . . . .	88
Running FRMINST.EXE from a command line . . . . .	88
Uninstalling the agent by removing systems from the Directory . . . . .	88
Uninstalling the agent from systems after a Directory search . . . . .	89
Maintaining the agent . . . . .	89
Sending manual agent and SuperAgent wakeup calls . . . . .	89
Sending scheduled agent wakeup calls . . . . .	90
Viewing properties of the agent and products from the console . . . . .	92
Viewing the agent activity logs . . . . .	92
Agent tasks on the managed system . . . . .	94
Locating inactive agents . . . . .	96
<b>5   Creating Repositories</b> . . . . .	<b>99</b>
About repositories . . . . .	100
The repository list . . . . .	100
Master repository . . . . .	100
Source repository . . . . .	101
Fallback repository . . . . .	101
Master, source, and fallback repositories working together . . . . .	102
Distributed repositories . . . . .	102

About repository branches . . . . .	105
Creating and configuring your repositories . . . . .	106
Configuring proxy settings . . . . .	106
Configuring source and fallback repositories . . . . .	108
Creating SuperAgent repositories . . . . .	110
Creating FTP, HTTP, and UNC file server repositories . . . . .	111
<b>6 Configuring Product Policies and Tasks</b>	<b>115</b>
About policy management . . . . .	116
Policy NAP files . . . . .	116
Policy enforcement . . . . .	116
Policy enforcement interval . . . . .	116
Policy categories and named policies . . . . .	117
Policy assignment and inheritance . . . . .	118
Policy ownership . . . . .	119
Assignment locking . . . . .	119
Product filtering . . . . .	119
Supported products . . . . .	120
About client tasks . . . . .	120
Policy conversion when upgrading . . . . .	121
Adding policy NAP files . . . . .	121
Viewing policy information . . . . .	122
Viewing information about named policies . . . . .	122
Viewing policy information for Directory nodes . . . . .	124
Managing the Policy Catalog . . . . .	125
Creating a named policy . . . . .	125
Duplicating a named policy . . . . .	126
Modifying the settings of a named policy . . . . .	127
Renaming a named policy . . . . .	128
Deleting a named policy from the Policy Catalog . . . . .	128
Changing the owner of a policy . . . . .	129
Exporting and importing named policies . . . . .	129
Managing policies from the Assign Policies pages . . . . .	131
Assigning a named policy to a specific node . . . . .	131
Creating or duplicating a named policy at a Directory node . . . . .	131
Enforcing policy for a product or category . . . . .	132
Locking assignment . . . . .	133
Copying and pasting assignments . . . . .	133
Creating and scheduling client tasks . . . . .	134
Scheduling options . . . . .	135
Frequently asked questions . . . . .	135
<b>7 Deploying Software and Updates</b>	<b>137</b>
About product and update packages . . . . .	138
Package signing and security . . . . .	139
Legacy product support . . . . .	140
Package ordering and dependencies . . . . .	140
About deploying and updating products . . . . .	140
Product deployment and updating process . . . . .	141
Deployment task . . . . .	141
Update tasks . . . . .	141
Global updating . . . . .	142
Pull tasks . . . . .	143
Replication tasks . . . . .	144
Server task log . . . . .	144
Repository selection . . . . .	145
Repository selection by agents . . . . .	146
Checking in product deployment packages manually . . . . .	146
Configuring the deployment task to install products on client systems . . . . .	148
Configuring updating . . . . .	149
Enabling global updating . . . . .	150

Using pull tasks to update the master repository . . . . .	151
Scheduling a regular pull task . . . . .	151
Running a Pull now task . . . . .	152
Replicating the master repository contents to distributed repositories . . . . .	152
Scheduling a repository replication server task . . . . .	152
Replicating to distributed repositories immediately . . . . .	153
Configuring agent policies to use appropriate distributed repository . . . . .	155
Using local distributed repositories that are not managed . . . . .	156
Exporting the repository list to a file . . . . .	157
Importing a repository list file . . . . .	157
Checking in engine, DAT and EXTRA.DAT updates manually . . . . .	157
Distributing DAT and engine files with client update tasks . . . . .	158
Creating and scheduling a daily update task . . . . .	158
Confirming that clients have updated to the latest DATs . . . . .	161
Evaluating new DATs and engines before distribution . . . . .	161
Create a scheduled pull task to use the Evaluation branch . . . . .	161
Designate systems to update from the Evaluation branch . . . . .	161
Schedule a client update task for your evaluation group to update from the Evaluation branch . . . . .	162
Monitor the systems during the evaluation period . . . . .	162
Move the new DATs to the Current branch . . . . .	162
<b>8 Determining Compliance . . . . .</b>	<b>164</b>
System Compliance Profiler . . . . .	164
Compliance Check server task . . . . .	165
MyAVERT Security Threats . . . . .	167
Viewing and managing notifications on new threats . . . . .	168
Proxy settings . . . . .	169
<b>9 Rogue System Detection . . . . .</b>	<b>171</b>
About Rogue System Detection . . . . .	172
The Rogue System sensor . . . . .	172
Machine status and rogue type . . . . .	175
Subnet status . . . . .	176
Distributing Rogue System sensors . . . . .	177
Configuring sensor policy settings . . . . .	177
Deploying Rogue System sensors . . . . .	180
Installing the sensor manually . . . . .	182
Uninstalling the sensor . . . . .	183
Configuring Rogue System Detection . . . . .	185
Changing sensor-to-server port number in SERVER.XML . . . . .	188
Viewing information about detected systems and deployed sensors . . . . .	189
Customizing table data in Rogue System Detection . . . . .	189
Monitoring systems and subnets . . . . .	190
Viewing coverage summary information . . . . .	191
Viewing the list of systems detected on your network . . . . .	192
Viewing details about specific detected systems . . . . .	192
Viewing your subnets . . . . .	193
Viewing status of actions taken and event history . . . . .	194
Taking actions on detected rogue systems manually . . . . .	196
Deploying agents to rogue systems . . . . .	197
Adding systems to the Directory . . . . .	198
Marking specific systems for later action . . . . .	198
Marking systems as exceptions . . . . .	199
Configuring automatic responses for specific events . . . . .	200
Configuring automatic e-mail alerts . . . . .	201
Using command-line executables in automatic responses . . . . .	205
Configuring Rogue System Detection for Notifications . . . . .	207
Configuring an automatic response to send ePO server events . . . . .	207
Creating a notification rule based on Rogue System Detection events . . . . .	208
Rogue System sensor command-line options . . . . .	208

Frequently asked questions .....	209
<b>10 ePolicy Orchestrator Notifications</b>	<b>210</b>
About Notifications .....	211
Throttling and aggregation .....	212
Notification rules and Directory scenarios .....	212
Default rules .....	214
Determining when events are forwarded .....	215
Determining which events are forwarded .....	216
Planning .....	216
Configuring Notifications .....	216
Basic configurations of Notifications .....	217
E-mail contacts list .....	218
SNMP servers .....	219
Configuring external commands .....	219
Creating and editing rules .....	220
Viewing the history of Notifications .....	226
Notification summary .....	226
Notification list .....	226
Product and component list .....	228
Frequently asked questions .....	229
<b>Glossary</b>	<b>231</b>
<b>Index</b>	<b>241</b>

# 1

## Introducing ePolicy Orchestrator An overview of version 3.6

ePolicy Orchestrator® software version 3.6 provides a scalable tool for centralized policy management and enforcement of your anti-virus and security products. It also provides comprehensive graphical reporting and product deployment capabilities, all through a single point of control.

---

### About ePolicy Orchestrator

The ePolicy Orchestrator software is comprised of the following components:

- ePolicy Orchestrator server — The center of your managed environment. The server delivers security policy, controls updates, processes events, and serves tasks for all managed systems.
- Master repository — The central location for all McAfee updates and signatures, residing on the ePolicy Orchestrator. Update repositories provide user-specified updates and signatures to the managed systems from the master repository.
- Distributed repositories — Placed strategically throughout your environment to provide access for managed systems to receive DAT files, product updates, and product installations. Depending on how your network is set up, you may want to set up HTTP, FTP, or UNC share distributed repositories, or create update repositories by converting agents into a SuperAgent repositories.
- ePolicy Orchestrator consoles — Used to access the ePolicy Orchestrator server and reports from another system. From the consoles, you can configure policies, create or edit tasks, and run reports.
- ePolicy Orchestrator agent — A vehicle of information and enforcement between the ePolicy Orchestrator server and each managed system. The agent retrieves updates, ensures task implementation, enforces policies and forwards events for each of the managed systems.
- Rogue System sensor — Resides on at least one system per subnet and notifies the server when a rogue system enters the environment. The server can then initiate an automatic response to perform on that system, such as deploying an agent, based on the events from the sensor.

#### The ePolicy Orchestrator server

The ePolicy Orchestrator server acts as a repository for all data collected from agents and includes the following features:

- A robust database that accrues information about product operation on the client systems in your network.

- A reporting engine that lets you monitor the virus protection status in your company.
- A software repository that stores the products and product updates (for example, DAT files) that you deploy to your network.

The ePolicy Orchestrator server can segment the user population into discrete groups for customized policy management. Each server can manage up to 250,000 systems.

### The ePolicy Orchestrator agent

The ePolicy Orchestrator agent is installed on the systems you intend to manage with ePolicy Orchestrator.

While running silently in the background, the agent performs the following:

- Gathers information and events from the managed systems and sends these to the ePolicy Orchestrator server.
- Installs products and updates on the managed systems.
- Enforces policies and tasks on the managed systems and sends events back to the ePolicy Orchestrator server.

You can deploy the agent from the console or copy the agent installation package onto removable media or into a network share for manual or login script installation on your systems.

### The ePolicy Orchestrator console

Housed within the Microsoft Management console (MMC), the ePolicy Orchestrator console provides a single point of control for using all functionality of ePolicy Orchestrator, including:

- Managing your entire company's anti-virus and security software policies.
- Viewing client system properties.
- Generating reports on specific activity.
- Updating or installing managed products on specific systems, or groups of systems.
- Viewing the compliance of managed systems.
- Detecting and acting on rogue systems in your environment.

---

## What's new in this release?

This release of the ePolicy Orchestrator software introduces the following new features:

- [Named policies](#).
- [High availability on page 12](#).
- [More detailed server task log on page 13](#).
- [Server-side replication on page 13](#).
- [Selective repository replication on page 13](#).
- [Selective package replication on page 14](#).
- [Enhanced administrator permissions on page 14](#).

- [MyAVERT Security Threats integration on page 14.](#)
- [Enhanced audit logging on page 15.](#)

## Named policies

<b>Current release</b>	<p>ePolicy Orchestrator software's policy management is more robust with this release. You can now create and manage policies independent of the Directory structure.</p> <p>You can also quickly drill-down into a named policy and view where the policy is assigned, and where inheritance is broken.</p>
<b>Benefits</b>	<p>The new policy management feature saves time by requiring you to create a policy only once and applying it to multiple, independent locations in the Directory.</p> <p>This feature can also save valuable time by allowing you to view where the policy is assigned and where inheritance of the policy is broken.</p>
<b>Where to find</b>	<p>In the console tree, select any Directory node, then click the <b>Policy</b> tab in the details pane to view and change policy assignments for the selected node.</p> <p>In the console tree, select <b>Policy Catalog</b> to view and manage the global list of all named policies.</p>
<b>For more information</b>	<p>See <a href="#">Configuring Product Policies and Tasks on page 115.</a></p>

## High availability

<b>Current release</b>	<p>ePolicy Orchestrator software now supports Microsoft Clustering Services. You can ensure your ePolicy Orchestrator server software is always available, even if the primary ePolicy Orchestrator server shuts down for any reason.</p>
<b>Benefits</b>	<p>This feature saves you valuable time and ensures continuity.</p>
<b>Where to find</b>	<p>The McAfee ePolicy Orchestrator Clustering Setup wizard (ClusterEPO.exe) is located in the ePolicy Orchestrator 3.6 installation directory.</p>
<b>For more information</b>	<p>See the <i>ePolicy Orchestrator 3.6 Installation Guide</i>.</p>

## More detailed server task log

<b>Current release</b>	The server task log now provides additional information for replication and pull tasks, including: <ul style="list-style-type: none"><li>■ Start and end times.</li><li>■ Any errors or warnings and their codes.</li><li>■ Status of each package that is checked into the master repository (by pull tasks only).</li><li>■ Information regarding any new packages that are being checked into the master repository via a pull task.</li></ul>
<b>Benefits</b>	Saves you valuable time in the event that replication and pull tasks fail. You can attain and view this information easily.
<b>Where to find</b>	The <b>Task Logs</b> tab when the ePolicy Orchestrator server is selected in the console tree.
<b>For more information</b>	See <a href="#">Server task log on page 144</a> .

## Server-side replication

<b>Previous release</b>	Replication tasks were performed on the console.
<b>Current release</b>	Replication tasks are now performed on the server.
<b>Benefits</b>	Performance of replication tasks is improved up to 300%.

## Selective repository replication

<b>Previous release</b>	When replicating master repository contents through your environment, ePolicy Orchestrator replicated all packages to all available distributed repositories.
<b>Current release</b>	This release of ePolicy Orchestrator allows you to select to which distributed repositories master repository contents replicate, on a per replication task basis.
<b>Benefits</b>	Saves valuable bandwidth resources during the execution of a replication task.
<b>Where to find</b>	Select desired repositories when creating or editing a replication task.
<b>For more information</b>	See <a href="#">Scheduling a repository replication server task on page 152</a> .

## Selective package replication

<b>Current release</b>	This release of ePolicy Orchestrator allows you to select specific product packages to replicate to distributed repositories, on a per repository basis.
<b>Benefits</b>	This feature allows you to balance available bandwidth more effectively by ensuring that only necessary content is replicated to the desired distributed repositories at the desired times.
<b>Where to find</b>	Select specific packages for a distributed repository when you create or edit a distributed repository.
<b>For more information</b>	See <a href="#">Creating and configuring your repositories on page 106</a> .

## Enhanced administrator permissions

<b>Current release</b>	<p>This release of ePolicy Orchestrator allows you to specify multiple sites and specific products to which a site administrator has permissions.</p> <p>Also, when creating either a global administrator or site administrator account, you can now choose whether the administrator can use Windows NT authentication or ePolicy Orchestrator authentication.</p>
<b>Benefits</b>	<p>These enhancements provide:</p> <ul style="list-style-type: none"><li>■ More control over the access of site administrators in your environment.</li><li>■ Site administrators the ability to view information for multiple sites together.</li><li>■ All administrators the opportunity to use their NT authentication information throughout ePolicy Orchestrator.</li><li>■ Easier enforcement of policies for password changes.</li></ul>
<b>Where to find</b>	In the console tree, select the ePolicy Orchestrator server, then select the <b>Users</b> tab.
<b>For more information</b>	See <a href="#">Adding user accounts on page 27</a> .

## MyAVERT Security Threats integration

<b>Current release</b>	This release of ePolicy Orchestrator provides a recurring task that delivers security threat information from McAfee AVERT, including current threats and the DAT and engine files in the Current branch.
<b>Benefits</b>	This feature provides easy access to information in the product interface regarding the top ten medium-to-high risk threats for corporate users, as well as which versions of DAT and engine files are in the Current branch of the repository.
<b>Where to find</b>	A link is provided on the <b>General</b> tab when the ePolicy Orchestrator server is selected in the console tree.
<b>For more information</b>	See <a href="#">MyAVERT Security Threats on page 167</a> .

## Enhanced audit logging

<b>Previous release</b>	The previous release of ePolicy Orchestrator contained an audit log based on a SQL trace.
<b>Current release</b>	<p>This release of ePolicy Orchestrator provides an audit log that runs daily as a server task. This log captures more information, including all administrative actions and the administrator who executed the action.</p> <p>The audit log contains 30 days of data.</p>
<b>Benefits</b>	This feature provides easy access to comprehensive audit data of administrative actions.
<b>Where to find</b>	<p>The audit log (ePOAuditLog.csv) file is automatically created in the folder:</p> <pre>C:/Program Files/ePO/3.6.0/DB</pre>
<b>For more information</b>	See the Audit log topic in Help.

---

## Using this guide

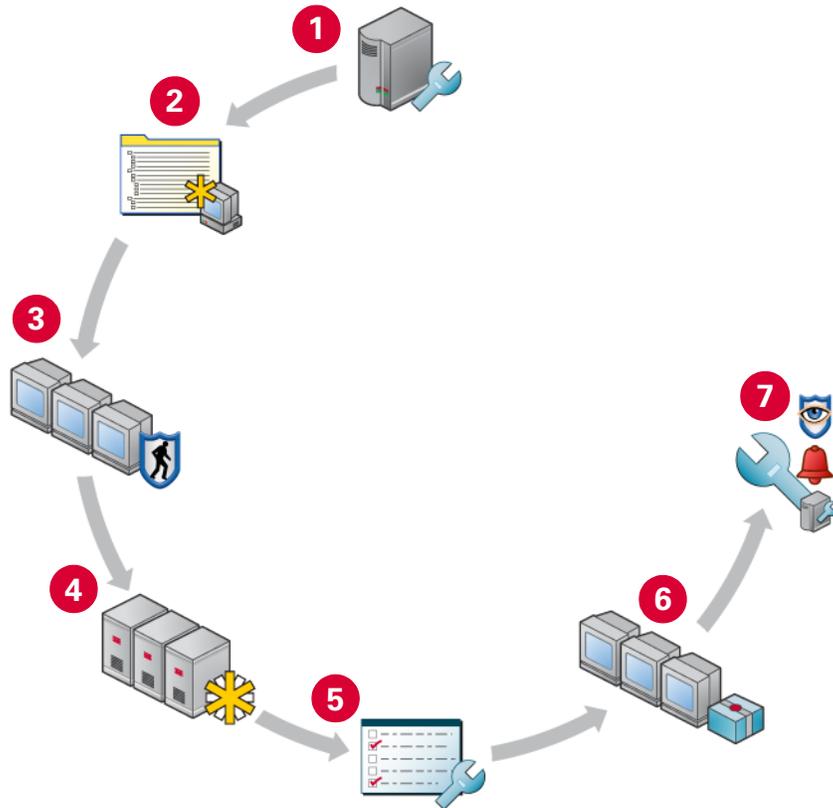
This guide provides information on configuring and using your product. For system requirements and installation instructions, refer to the *Installation Guide*.

This material of this guide is organized in the order which McAfee recommends to set up ePolicy Orchestrator in a production environment for the first time, while at the same time, the information is accessible to anyone seeking to reference specific topics.

## Setting up ePolicy Orchestrator for the first time?

This guide was created as both a tool to help administrators set up their ePolicy Orchestrator environment for the first time, and as a reference tool for more experienced users. Depending on your environment, you may perform some of these tasks in a slightly different order.

McAfee recommends setting up ePolicy Orchestrator for the first time in the following order:



- 1 **Configuring ePolicy Orchestrator servers** — Learn how to log on and off the server, set up user accounts, and get familiar with the user interface.
- 2 **Creating a Directory of managed systems** — The Directory allows you to organize and act on all the systems you manage with ePolicy Orchestrator. Before configuring other features, you must create your Directory of managed systems.
- 3 **Distributing agents** — Each system you want to manage must have an ePolicy Orchestrator agent installed. This chapter provides detailed information on distributing and maintaining agents in your environment.
- 4 **Creating repositories** — Before deploying any products or updates to your managed systems with ePolicy Orchestrator, you must configure and create update repositories.
- 5 **Managing product policies and tasks** — Before deploying any products, components, or updates to your managed systems with ePolicy Orchestrator, McAfee recommends configuring the policy settings for these products and components. Although it is not required to configure policy settings before deployment, by doing so, you can ensure that the products and components have the desired settings as soon as possible.
- 6 **Deploying software and updates** — Once your update repositories and policy settings have been created and configured, deploy the products, components, and updates to the desired systems with ePolicy Orchestrator.
- 7 **Configuring advanced features** — Once your managed environment is up and running, you can configure and implement ePolicy Orchestrator's advanced features, including: Rogue System Detection, Notifications, and System Compliance Profiler

## Audience

This information is intended primarily for network administrators who are responsible for their company's anti-virus and security program.

This guide assumes the customer has already read the *ePolicy Orchestrator 3.6 Walkthrough Guide* and has installed and used ePolicy Orchestrator in a lab environment.

## Conventions

This guide uses the following conventions:

<b>Bold</b>	All words from the user interface, including options, menus, buttons, and dialog box names.
<b>Condensed</b>	<p><b>Example:</b></p> Type the <b>User</b> name and <b>Password</b> of the desired account.
<i>Courier</i>	<p>The path of a folder or program; a web address (URL); text that represents something the user types exactly (for example, a command at the system prompt).</p> <p><b>Examples:</b></p> The default location for the program is: <code>C:\Program Files\McAfee\EPO\3.6.0</code> Visit the McAfee web site at: <code>http://www.mcafee.com</code> Run this command on the client system: <code>C:\SETUP.EXE</code>
<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><b>Example:</b></p> Refer to the <i>VirusScan Enterprise Product Guide</i> for more information.
<TERM>	<p>Angle brackets enclose a generic term.</p> <p><b>Example:</b></p> In the console tree under ePolicy Orchestrator, right-click <SERVER>.
	<p><b>Note:</b> Supplemental information; for example, an alternate method of executing the same command.</p>
	<p><b>Tip:</b> Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.</p>
	<p><b>Caution:</b> Important advice to protect your system, enterprise, software installation, or data.</p>
	<p><b>Warning:</b> Important advice to protect a user from bodily harm when interacting with a hardware product.</p>

## Resources

Refer to these sections for additional resources:

- Getting product information
- Contact information

## Getting product information

Unless otherwise noted, the product documentation is provided as Adobe Acrobat PDF files available on the product CD or from the McAfee download site.

The ePolicy Orchestrator documentation is designed to provide you with the information you need during each phase of the product implementation from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledge Base available on ServicePortal.

<b>Evaluation Phase</b>	<b>Installation Phase</b>	<b>Setup Phase</b>	<b>Maintenance Phase</b>
 <p>How can my company benefit from this product?</p>	 <p>Before, during, and after the installation.</p>	 <p>Getting up-and-running with the product.</p>	 <p>Maintaining the software over time.</p>
<p><b>Walkthrough Guide</b></p> <ul style="list-style-type: none"> <li>■ Procedures on preparing for, installing and deploying software in a test environment.</li> <li>■ Detailed instructions for common tasks.</li> </ul>	<p><b>README</b></p> <ul style="list-style-type: none"> <li>■ Known issues in the current release.</li> <li>■ Issues resolved since the last release.</li> <li>■ Last-minute changes to the product or its documentation.</li> </ul> <p><b>Installation Guide</b></p> <ul style="list-style-type: none"> <li>■ Procedures on preparing for, installing and deploying software in a production environment.</li> </ul>	<p><b>Product Guide</b></p> <ul style="list-style-type: none"> <li>■ Procedures on setting up and customizing the software for your environment.</li> <li>■ Detailed information about options in the product.</li> </ul> <p><b>Configuration Guide</b> (managed products)</p> <ul style="list-style-type: none"> <li>■ Procedures for managing and deploying products through ePolicy Orchestrator.</li> </ul>	<p><b>Help file</b></p> <ul style="list-style-type: none"> <li>■ Procedures on maintaining the software.</li> <li>■ Reference information.</li> <li>■ All information found in the product guide.</li> </ul> <p><b>Quick Reference Card</b></p> <ul style="list-style-type: none"> <li>■ Detailed instructions for both common and infrequent, but important tasks.</li> </ul> <p><b>Knowledge Base</b></p> <ul style="list-style-type: none"> <li>■ Supplemental product information.</li> <li>■ Workarounds to known issues.</li> </ul> <p><a href="https://mysupport.nai.com">https://mysupport.nai.com</a></p>

## Contact information

### Technical Support

Home Page	<a href="http://www.mcafeesecurity.com/us/support/">http://www.mcafeesecurity.com/us/support/</a>
KnowledgeBase Search	<a href="https://knowledgemap.mcafeesecurity.com/phpclient/homepage.aspx">https://knowledgemap.mcafeesecurity.com/phpclient/homepage.aspx</a>
PrimeSupport Service Portal *	<a href="https://mysupport.mcafeesecurity.com">https://mysupport.mcafeesecurity.com</a>

## McAfee Beta Program

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

## Security Headquarters — AVERT: Anti-virus & Vulnerability Emergency Response Team

Home Page	<a href="http://www.mcafeesecurity.com/us/security/home.asp">http://www.mcafeesecurity.com/us/security/home.asp</a>
Virus Information Library	<a href="http://vil.mcafeesecurity.com">http://vil.mcafeesecurity.com</a>
AVERT WebImmune, *	<a href="https://www.webimmune.net/default.asp">https://www.webimmune.net/default.asp</a>
Submitting a Sample	
AVERT DAT Notification Service	<a href="http://vil.mcafeesecurity.com/vil/join-DAT-list.asp">http://vil.mcafeesecurity.com/vil/join-DAT-list.asp</a>

## Download Site

Home Page	<a href="http://www.mcafeesecurity.com/us/downloads/">http://www.mcafeesecurity.com/us/downloads/</a>
DAT File and Engine Updates	<a href="http://www.mcafeesecurity.com/us/downloads/updates/default.asp">http://www.mcafeesecurity.com/us/downloads/updates/default.asp</a> <a href="ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x/">ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x/</a>
Product Upgrades *	<a href="https://secure.nai.com/us/forms/downloads/upgrades/login.asp">https://secure.nai.com/us/forms/downloads/upgrades/login.asp</a>

## Training

On-Site Training	<a href="http://www.mcafeesecurity.com/us/services/security/home.htm">http://www.mcafeesecurity.com/us/services/security/home.htm</a>
McAfee University	<a href="http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm">http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm</a>

## Customer Service

Web	<a href="http://www.mcafeesecurity.com/us/index.asp">http://www.mcafeesecurity.com/us/index.asp</a> <a href="http://www.mcafeesecurity.com/us/support/default.asp">http://www.mcafeesecurity.com/us/support/default.asp</a>
US, Canada, and Latin America toll-free:	<b>+1-888-VIRUS NO</b> or <b>+1-888-847-8766</b> Monday – Friday, 8 a.m. – 8 p.m., Central Time

For additional information on contacting McAfee — including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

\* Logon credentials required.

# 2

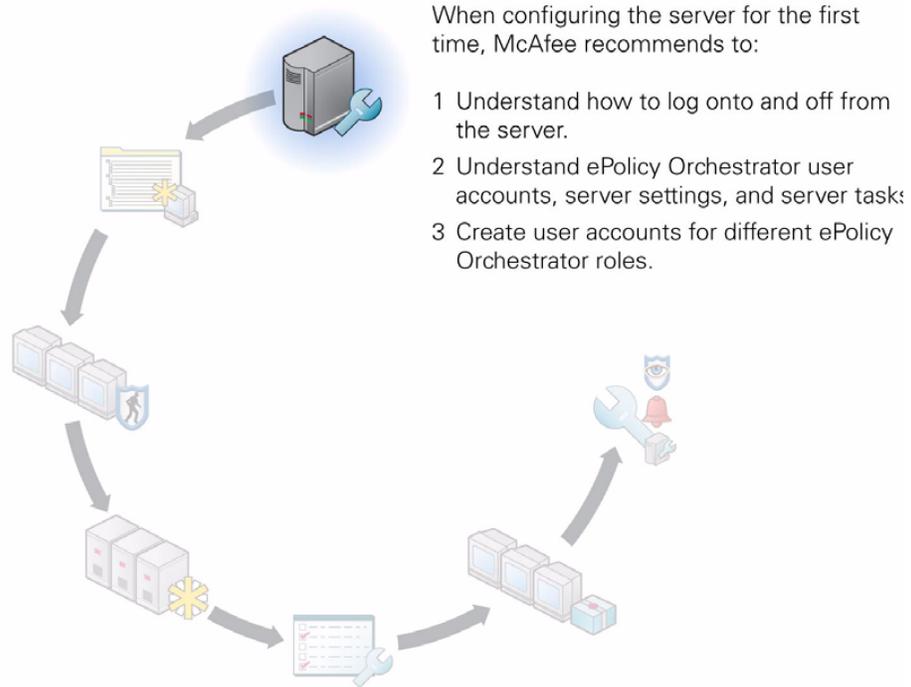
## Configuring ePolicy Orchestrator Servers

### An introduction to the server, console, and user accounts

The ePolicy Orchestrator server is the center of your managed environment, providing a single location from which to administer system security throughout your network.

Before you begin using ePolicy Orchestrator, there are a few concepts and tasks you should understand about the ePolicy Orchestrator server and console.

#### Configuring the server for the first time?



---

## Logging onto ePolicy Orchestrator servers

When you open an ePolicy Orchestrator console, you must log onto an ePolicy Orchestrator server. This allows you access to the server's resources and functionality.

You can use the ePolicy Orchestrator console to log onto any ePolicy Orchestrator server. The console does not need to be on the same system as the server.



You do not need to be logged onto the server in the ePolicy Orchestrator console for the server service to run. Similarly, the server service does not stop when you log off or remove a server from the console.

To log onto an ePolicy Orchestrator server:

- 1 Choose **Start | Programs | McAfee | ePolicy Orchestrator** to launch the console.
- 2 In the console tree, select **ePolicy Orchestrator**, then click **Log on to server** in the details pane. The **ePolicy Orchestrator Login** dialog box appears.
- 3 If you are at the ePolicy Orchestrator server, accept the default **Server name** that appears. If you are using a console on another system, ensure the correct computer name is in the **Server name** field.
- 4 Type the **User name** and **Password** of the account to use to log onto the server. This account must be a valid account that already exists on the server.



User names and passwords are case-sensitive.

- 5 Type the **HTTPS Port** number used by the server for console-to-server communication. If you are logging onto a server running on the local system, the **HTTP Port** field is automatically populated with the correct port number. If you are at a remote console, type the port number. This is the port number you specified in the installation wizard (8443 by default).
- 6 Click **OK** to log onto the server.

## Logging off from servers without removing them

You can log off from a server without removing it. To do this, right-click the server in the console tree under **ePolicy Orchestrator**, then select **Log off**.

## Logging onto additional servers

You can log onto multiple servers and manage policies in each during the same console session. To do this, you must be able to provide a user name and password for a valid user account on each server.

### Best practices information

If your organization is very large, or divided into multiple large sites, consider installing a separate server at each site. This can reduce network traffic when managing agents, sending updates, and replicating to distributed repositories all within a local LAN. Network traffic has a larger impact on your resources when this communication takes place across WAN, VPN, or other slower network connections typically found between remote sites.

---

## Installing the security certificate

ePolicy Orchestrator 3.6 uses Secure Socket Layer (SSL) to improve security for communication between the console and the server components.

When you log onto the console, you are prompted to accept a security certificate to view the interface in the console. To avoid having to accept this certificate every time you access these features in the console, install the certificate the first time you log onto the console.

To install the security certificates a single time:

- 1 Log onto your server.

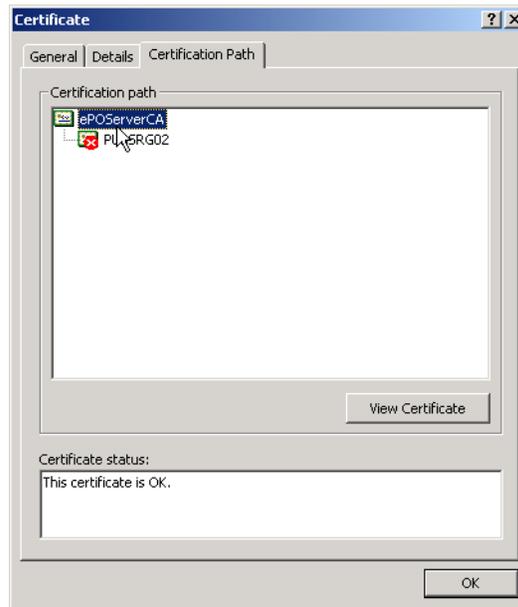
**Figure 2-1 Security Alert dialog box**



- 2 Click **View Certificate** when the **Security Alert** dialog box appears.
- 3 In the **Certificate** dialog box, select the **Certification Path** tab.

- 4 Select **ePOServerCA** to enable certificate import.

**Figure 2-2 Certificate dialog box**



- 5 Click **View Certificate** to open the second **Certificate** dialog box.
- 6 Click **Install Certificate** to open the **Certificate Import Wizard**.
- 7 Click **Next**, then **Next** again, then **Finish** to accept all wizard defaults and import the certificate.
- 8 Click **Yes** in the **Root Certificate Store** dialog box.
- 9 Click **OK** twice to close the two **Certificate** dialog boxes.
- 10 Click **Yes** on the final **Security Alert** dialog box.

You will no longer be prompted to accept the certificate whenever you start the console.

---

## About ePolicy Orchestrator accounts

If you plan to have multiple people administer ePolicy Orchestrator in your environment, you can create multiple user accounts in the console. Fellow administrators can use these accounts to log onto the server.

The different types of user accounts include:

- [Global administrator](#).
- [Site administrators on page 25](#).
- [Global reviewers on page 26](#).
- [Site reviewers on page 26](#).

## Global administrator

Global administrators have read and write permissions and rights to all operations. When you install the server and console, a global administrator account with the user name `admin` is created.

You can create additional global administrator accounts for other people who need global administrative rights to all aspects of the console.

Global administrators can use the console to deploy agents and security products, change agent or product policies, create and run client tasks for updating DAT files or performing on-demand scans for any node in any site in the Directory. In addition, only global administrators can perform certain server-based functions.

Only global administrators can perform the following repository management functions:

- Define, edit, or remove source and fallback repositories.
- Create, change, or delete global distributed repositories.
- Export or import the repository list from the server.
- Schedule or perform pull tasks to update the Master Repository
- Schedule or perform replication tasks to update distributed repositories
- Check packages into the master repository, move packages between branches, or delete packages from the master repository.

Only global administrators can perform the following server management functions:

- Change server settings and work with server events.
- Schedule Synchronize Domains server tasks.
- Verify the integrity of IP management settings, or change site-level IP subnet masks.
- Run enterprise-wide reports.
- Add and delete user accounts.
- View and change all options on all tabs in the **Events** dialog box, if using authentication.
- Import events into ePolicy Orchestrator databases and limit events that are stored there.
- Create, rename, or delete sites.

## Site administrators

Site administrators have read, write, and delete permissions and rights to all operations (except those restricted to global administrator user accounts) for:

- One or more products.
- One or more Directory sites.
- The global Lost&Found group.

Site administrators can use the console to deploy agents and security products, change agent or product policies, create and run client tasks for all groups or systems within their sites in the Directory (for products to which they have permissions). Site administrators can also run reports, but the reports show only data on systems located within their sites. The site administrator is able to see, but not change, other sites in the Directory.

### Best practices information

Create site administrator accounts if you have a very decentralized network with no single global administrator account or where different local administrators have local control over their parts of the network. For example, your organization may have sites located in different cities or countries, and these sites may have local IT or network administrators with rights to install and manage software on systems in that part of the network.

## Global reviewers

Global reviewers can view, but not edit, all settings in the console (except for Rogue System Detection), including property settings, policy, and task settings for all nodes in the Directory.

## Site reviewers

Site reviewers can only view settings for specified products within specified sites of the Directory.

## Viewing current user accounts

To view the user accounts currently created for a particular server:

- 1 In the console tree, select the server.
- 2 In the details pane, click the **Users** tab.

Figure 2-3 Users tab



The screenshot shows the 'Users' tab in the console. At the top, there are navigation tabs: General, Scheduled Tasks, Task Logs, Settings, and Users. Below the tabs, the title is 'Server Users' and it indicates 'Currently logged on as: admin'. There are four action buttons: 'Create user', 'Modify user', 'Delete users', and 'Help'. Below the buttons is a table with three columns: User Name, Role, and Site.

User Name	Role	Site
admin	Administrator	All Sites
Site Admin 1	Site Administrator	edg
Site Admin 2	Site Administrator	edg

The **Server Users** table shows the user accounts that have been created for the selected server. From here, you can add new accounts, or edit or delete existing ones.

## Adding user accounts

You must be a global administrator to add, edit, or delete user accounts in the console.

To add a user account to the server:

- 1 In the console tree, select the server.
- 2 In the details pane, click the **Users** tab, then select **Create user**.
- 3 In the **Add New User** dialog box, type a descriptive name for the user in the **Name** field. This name is case-sensitive.
- 4 Select whether the new account uses **NT Authentication** or **ePolicy Orchestrator Authentication**.



The ability to use NT authentication for ePolicy Orchestrator accounts is a new feature in ePolicy Orchestrator 3.6.

- 5 Select the type of user account from the **Role** drop-down list.
- 6 If you selected **Site administrator** or **Site reviewer** in [Step 5](#), select **All current and future sites**, or select one or more sites from the **Site** list, which shows the sites currently created in the **Directory** tree.



When creating site administrators or site reviewers, the site for which they are assigned must already be created.

- 7 If you selected **Site administrator** or **Site reviewer** in [Step 5](#), select **All current and future products**, or select one or more products from the **Product** list, which shows the products that currently have NAP files installed.



The abilities to select multiple sites and specific products to which an administrator has rights is a new feature in ePolicy Orchestrator 3.6.

- 8 Type a **Password** (a minimum of one character), then **Confirm password**. Passwords are case-sensitive.
- 9 Click **Save** to save the current entries and return to the **Users** tab.

---

## Server settings, tasks, and events

You can change various settings that control how the ePolicy Orchestrator server behaves. You can change most settings at anytime. However, you must reinstall the software to change the name of the server or the port number the server uses for HTTP communication.

### ePolicy Orchestrator server settings

The **Server Settings** tab displays the current configuration for server functionality such as agent-to-server communication settings. A global administrator can change the server settings on a selected server. Make sure you understand a specific setting before modifying it. The following sections detail these settings.

### Client-to-server connection settings

You can configure many settings to define how agents, SuperAgents, and Rogue System sensors communicate with the server.

The client-to-server connection settings are defined in [Table 2-1](#).

**Table 2-1 Client-to-server connection settings**

Server setting	Description
Event log size	The maximum size of the event log file. The default is 2,048kb and the maximum is 10,000,000kb.
Agent & Console-to-Server communication port	The HTTP port the agent and console use to communicate to the server. This port is set during the installation wizard (80 by default). <b>Note:</b> If you change this port number, wakeup calls are disabled until the next agent-to-server communication.
Agent Wakeup communication port	The HTTP port the server uses to send agent wakeup calls (8081 by default). <b>Note:</b> If you change this port number, wakeup calls are disabled until the next agent-to-server communication.
Agent Broadcast communication port	The HTTP port the server uses to send SuperAgent wakeup calls (8082 by default).
Event Parser-to-Server communication port	The HTTP port used to receive events from the Event Parser on the ePolicy Orchestrator server (8080 by default).
Console-to-Server communication port	The HTTPs port used for communication to the server. Inbound communication relative to the ePolicy Orchestrator server. Used to display the HTML for the user interface (8443 by default).
Sensor-to-Server communication port	The HTTPs port used for Rogue System sensor-to-server communication. XML messages only, no events. Fully authenticated SSL. Inbound communication relative to the ePolicy Orchestrator server (8444 by default).

### Global updating server settings

Global updating allows your server to update the systems in your environment, automatically when new updates are checked into the master repository. You can select the specific types of updates that initiate a global update. For more information, see [Global updating on page 142](#).

The global updating settings are defined in [Table 2-2](#).

**Table 2-2 Global updating settings**

Server setting	Description
Enable global updating	Enables or disables global updating. When this is selected, checking in updates and signatures of the selected components initiates a global update, which includes a repository replication, SuperAgent wakeup call and client update.

**Table 2-2 Global updating settings**

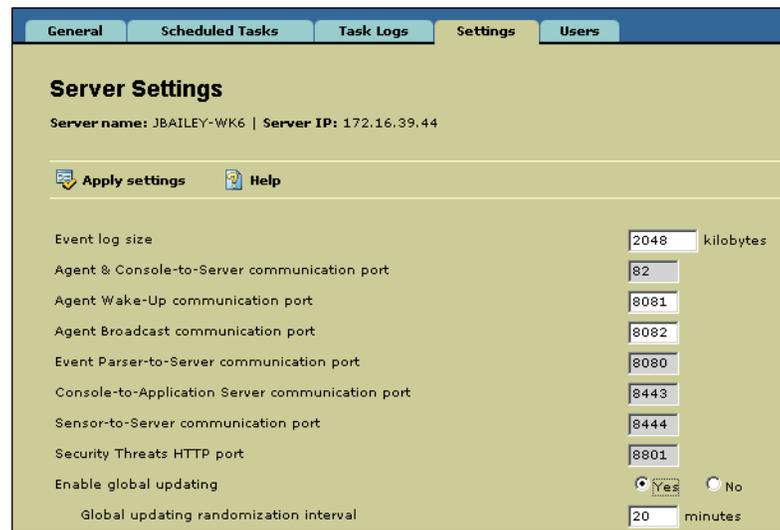
Server setting	Description
Global updating randomization interval	Sets the global updating randomization interval, in minutes. Each client update occurs at some randomly selected time within the randomization window, which helps distribute network load.  For example, if you update 1000 clients using the default randomization interval of 20 minutes, roughly 50 clients update each minute, lowering the load on your network and on your server at any point in time. Without the randomization, all 1000 clients would try to update simultaneously.
Only the following component check-ins trigger a global update	Select exactly which updates initiate a global update. When packages of the specified types are checked into the master repository, a global update is initiated. When other package types are checked in, no global update is initiated.  If network traffic is a significant concern, select <b>DAT</b> and possibly <b>Engine</b> only to initiate a global update.

## Changing server settings

To change server settings:

- 1 In the console tree, select the server.
- 2 In the details pane, select the **Settings** tab. A list of the server settings that the global administrator can define appears.

**Figure 2-4 Settings tab**



- 3 Make the desired changes to the server settings, then click **Apply settings**. For information about these settings, see [Server settings, tasks, and events on page 27](#).



You should not change the HTTP port on which the server listens for communications from deployed agents. If you do this, deployed agents cannot communicate with the server. There is not an easy way to re-configure the agents to find the new port. If you need to change this port, back up all ePolicy Orchestrator databases and uninstall the server. Re-install the server and assign the new port number.

## Server tasks and the server task log

The default set of server tasks is described here. For details on each of these, see the appropriate section of this guide that covers that server task.

- Inactive Agent Maintenance — Moves systems with inactive agents to a specified group or deletes them from the Directory. This task does not uninstall the agent. For instructions, see [Locating inactive agents on page 96](#).
- Synchronize Domains — Synchronizes select Windows NT domains that you have imported into the Directory. This task can also be performed manually. For instructions, see [Synchronizing Directory segments with NT domains on page 53](#).
- Repository Replication — Updates distributed repositories from the master repository. For instructions, see [Replication tasks on page 144](#).
- Repository Pull — Retrieves packages from the source repository, then places them in the master repository. For instructions, see [Pull tasks on page 143](#).
- Active Directory Computer Discovery — Imports any new systems in Active Directory to the appropriate Lost&Found site in the Directory. For instructions, see [Using Active Directory Discovery on page 50](#).
- Compliance Check — Runs one or more compliance rules that check your managed systems for compliance with specified DAT, engine, agent or VirusScan versions. For instructions, see [Compliance Check server task on page 165](#).
- Event Purge — Deletes events from the database based on user-configured criteria. For instructions, see Help.

## Reviewing the server task log

To review the status of server tasks that are in-progress:

- 1 In the console tree, select the server.
- 2 In the details pane, click the **Task Logs** tab.

Figure 2-5 Task Logs tab

Start Time	Duration	Task Name	Task Type	Status
12/22/2004 5:20:54 PM	0 Secs	Replicate DAT, Engine and Pr...	Repository Re...	Waiting
NaiFTP				
Not yet started				
Job paused, waiting for pull task to complete				
3/21/2005 9:56:45 AM	0 Secs	__MirrorNow	Repository Mir...	In Progress (50%)
NAIFtp				
50%				
Package VSCANDAT1000\4450\DAT\0000 checked in				
Checking in package VSCANDAT1000\4450\DAT\0000				
12/23/2004 5:15:18 PM	0 Secs	Replicate only DAT and Engin...	Repository Re...	Failed
BeavertonFTP				
25%				
Replicate only DAT and Engine to all locations in India				
DallasFTP				
35%				
Failed to check in package NaiFTP				

- 3 Click **Refresh** to refresh the log. The date and time that the server task log was last updated appears in **Current as of**.

The status of each server task appears in the **Status** column:

**Completed** — Task completed successfully.

**Failed** — Task was started but did not complete successfully.

**In progress** — Task was started.

**Waiting** — This message appears when the task is waiting for another task to finish.

- 4 Expand the desired entry for more details.

### Filtering the server task log

As the server task log grows, you can filter the server task log to show only the most recent activity. You can filter the log to show only entries from the last one day, last seven days, last 30 days, or to show all entries.

To filter the server task log:

- 1 In the console tree, select the ePolicy Orchestrator server.
- 2 In the details pane, select the **Task Logs** tab.
- 3 Select the desired filter from the **Filter** drop-down list.
- 4 Click **Refresh** if necessary.

### Purging the server task log

As the server task log grows, you can purge items older than a user-configurable number of days from the log.

To purge items from the server task log:

- 1 In the console tree, select the ePolicy Orchestrator server.
- 2 In the details pane, select the **Task Logs** tab.
- 3 Below the log table, type the number of days old of log entries you want to purge. All items of this age and older will be deleted.
- 4 Click **Purge Now**.

---

## Viewing server events from the console

In the console, you can view, save, and print all events for each ePolicy Orchestrator server. Checking the **Server Event Viewer** dialog box is useful to confirm the success or failure of actions initiated from the server, such as an agent deployment.

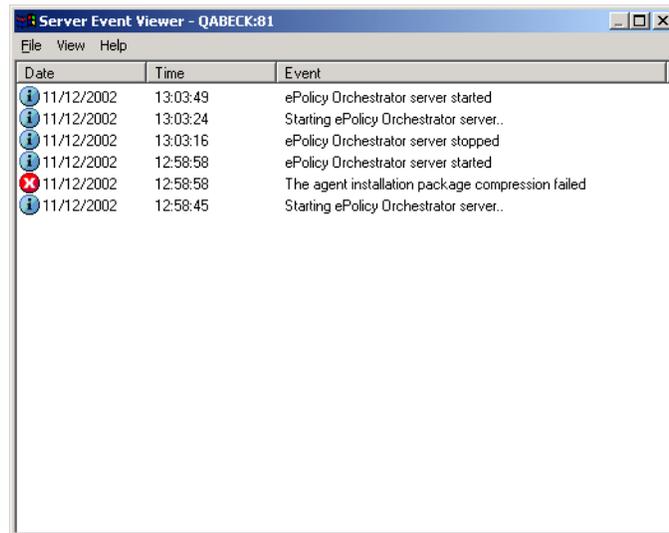
You can also manage which events are saved in the database. For more information, see Help.

To view, save, or print server events from the console:

- 1 In the console tree, select the server,
- 2 In the details pane, select the **General** tab.

- 3 Click **Server Events** to open the **Server Event Viewer** dialog box.

**Figure 2-6 Server Event Viewer dialog box**



- 4 Select **View | Refresh** to ensure the event list is current.

#### Viewing details of a particular event

To view a detailed description of a server event, double-click the desired event. The **Server Event Detail** dialog box appears.

#### Saving events to a log file

To save all server events to a Server Log (.LOG) file, select **File | Save As**. To save only selected server events to a Server Log file, select the desired events, then select **File | Save As**. In the **Save As** dialog box, select **Selected Items only**.

#### Printing server events

To print all server events to the default printer, click **Print** on the **File** menu.

To print only selected server events to the default printer, select the desired events, then select **File | Print**.

---

## Viewing the server version number

You can view the version number, edition, and license information of the ePolicy Orchestrator server or console, and the version number of policy (.NAP) pages.

To view the version number, edition, and license information, log onto the desired ePolicy Orchestrator server. This information appears below the title in the details pane.

**Figure 2-7** Version number of the software



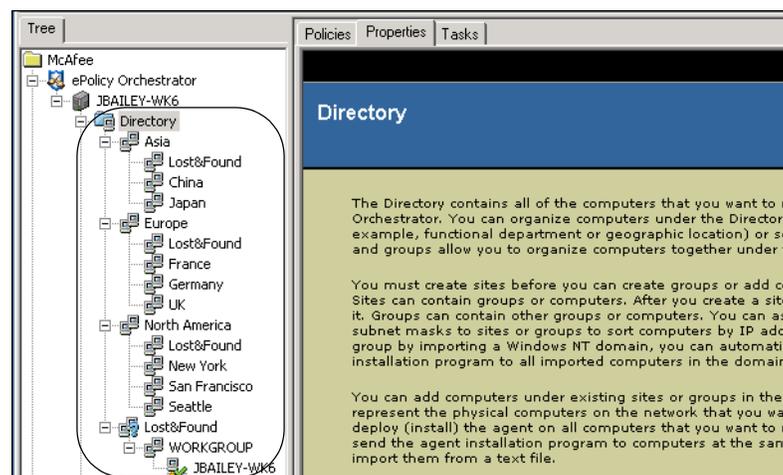
# 3

## Creating a Directory of Managed Systems

### Organize your systems for management

The Directory contains all of the systems managed by ePolicy Orchestrator; it is the link to the primary interfaces for managing these systems. You can organize systems under the Directory into logical groupings (for example, functional department or geographic location) or sort them by IP address. You can manage policies (product configuration settings) and schedule tasks (for example, updating virus definition files) for systems at any level of the Directory.

Figure 3-1 The Directory

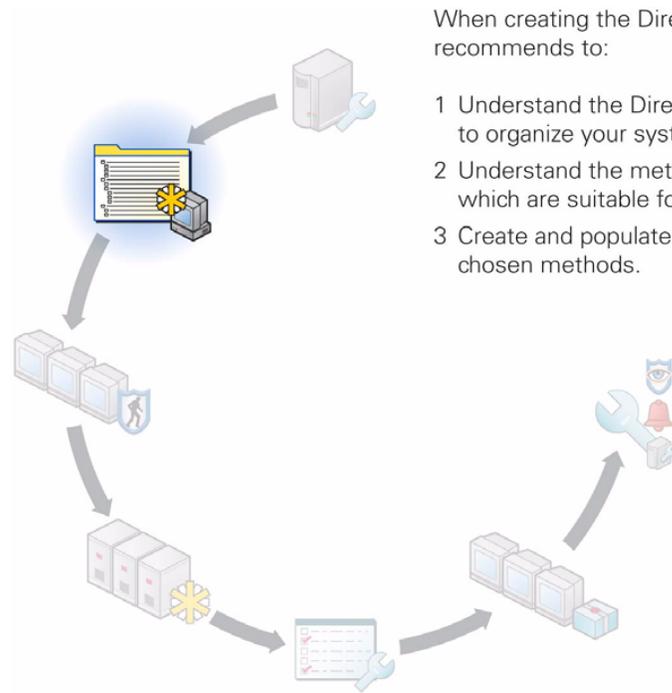


Before configuring the software to deploy or manage the anti-virus and security software in your environment, you must conduct some preliminary planning. This planning includes deciding how to best organize systems for management and selecting which methods to use to bring systems into the Directory.



Many factors can influence how you should create and organize your Directory. McAfee recommends that you take some time to review this entire guide before you begin creating your Directory.

### Creating the Directory for the first time?



When creating the Directory, McAfee recommends to:

- 1 Understand the Directory and how to use it to organize your systems.
- 2 Understand the methods of creation and which are suitable for your environment.
- 3 Create and populate the Directory with the chosen methods.

---

## About the Directory

The Directory organizes managed systems in units for monitoring, assigning policies, and scheduling tasks. Before creating your Directory, it is important to understand:

- [Sites and groups](#).
- [Lost&Found groups on page 36](#).
- [Inheritance on page 36](#).

### Sites and groups

The Directory is a hierarchical tree structure that allows you to group your systems within units called *sites* and *groups*. Grouping systems with similar properties or requirements into these units allows you to manage policies for collections of systems in one place, rather than having to set policies for each system separately.

As part of the planning process, consider the best way to divide systems into sites and groups prior to building the Directory.

#### Sites

A site is a primary-level unit immediately under the Directory root in the console tree. Traits of sites include:

- Sites can only be created by global administrators.
- A site can include both groups and systems.

- Sites (and their groups and systems) are administered by a global administrator or by a site administrator who has ownership of the specific site. (Site administrators have administrative rights only over the sites to which ownership has been assigned.)
- Each site contains a Lost&Found group; a temporary container for systems for which ePolicy Orchestrator wasn't able to automatically place in the correct location within the site.

### Groups

A group is a secondary-level (or subsequent level) unit of the Directory. Traits of groups include:

- Groups can be created by global administrators, or the site administrator of the site to which the group belongs.
- A group can include both groups and systems.
- Groups are administered by a global administrator or by the site administrator of the site to which the group belongs.
- Groups do not contain a Lost&Found group.

## Lost&Found groups

The Directory root and each site includes a Lost&Found group. Depending on the methods you use to create and maintain Directory segments, the server uses different characteristics to determine where to place systems within the Directory. Lost&Found groups store systems whose locations could not be determined by the server.

### Best Practices information

If you delete systems from the Directory, you also need to uninstall the agent from these systems. Otherwise, these systems continue to appear in the Lost&Found group because the agent continues to communicate to the server.

## Inheritance

Inheritance is an important property that makes policy administration simpler. Because of inheritance, child nodes in the Directory hierarchy inherit policies that have been set at their parent nodes. For example:

- Policies set at the Directory level are inherited by sites.
- Site policies are inherited by groups and individual systems within that site.
- Group policies are inherited by sub-groups or individual systems within that group.

Inheritance is enabled by default for all sites, groups and individual systems that you add to your Directory. This allows you to set policies and schedule scan tasks in fewer places.

However, inheritance can be turned off at any location of the Directory to allow for customization.

---

## Considerations when planning your Directory

An efficient and well-organized Directory can make maintenance much easier. Many administrative, network, and political realities of each unique environment can affect how your Directory is structured. It is important that you think ahead about these before you build your Directory. Especially for a large network, you want to build the Directory only once.

Because every network is different and requires different policies throughout — and possibly even different management — McAfee recommends that you plan your Directory before beginning to implement the software.

Regardless of the methods you choose to create and populate the Directory, consider your environment while planning the Directory.

### Administrator access

When planning your Directory organization, consider administrators and other individuals who manage these systems and require access to the information about them.

For example, you may have very decentralized network administration in your organization, where different administrators have responsibilities over different parts of the network. For security reasons, you may not have one global administrator account that can access every part of your network. In this scenario, you may not be able to set policies and deploy agents using a single global administrator account. Instead, you may need to organize the Directory into sites and create site administrator accounts to allow other administrators to set policies for these systems.

Questions to consider include:

- Who will be responsible for managing which systems?
- Who will require access to view information about the systems?
- Who should not have access to the systems and the information about them?

When considering these, remember that ePolicy Orchestrator provides two types of administrator roles, two types of reviewer roles, and two types of authentication for individuals who have access to ePolicy Orchestrator.

### Environmental borders

How you implement ePolicy Orchestrator and organize the systems for management depends significantly on the borders that exist in your network. Borders influence the organization of the Directory differently than the organization of your network topology.

McAfee recommends evaluating the following borders in your network and organization, and whether they must be taken into consideration when defining the organization of your Directory.

#### Topological

Your network is already defined by domains or Active Directory containers. The better organized your network environment, the easier it is to create and use the Directory.

## Geographical

If your organization includes facilities in multiple geographic locations, even on multiple continents, this must be taken into consideration when building your Directory. Available bandwidth and administrative roles must be considered when your organization has multiple locations.

Managing security is a constant balance between protection and performance. Organize your Directory to make the best use of limited network bandwidth. Consider how the server connects to all the parts of your network, especially remote locations that are often connected by slower WAN or VPN connections, instead of faster LAN connections. You may want to set updating and agent-to-server communication policies differently for these remote sites to minimize network traffic over slower WAN or VPN connections.

Grouping systems first by geography provides several advantages for setting policies:

- You can set update policies for the site or group so that all systems update from one or more distributed software repositories located nearby.
- If sites are located in other countries, you can deploy language-specific versions of the agent or security software to these systems at once.
- You can configure the update and product deployment policies for these systems once.
- You can schedule tasks to run at off-peak hours.

## Political

Many large networks are divided because different individuals or groups are responsible for managing various portions of the network. Sometimes these borders do not coincide with the topological or geographical borders. Who you want to access and manage the various segments of the Directory can affect how you structure it.

## Functional

Some networks are divided by the roles of the groups and individuals using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you may need to organize the Directory by functionality if different groups of users require different policies.

Different business groups may run different kinds of software that require special anti-virus or security policies. For example, you may want to arrange your e-mail exchange servers or SQL database servers into a group and set specific exclusions for VirusScan Enterprise on-access scanning.

## Subnets and IP ranges

In many cases, organizational units of a network use specific subnets or IP ranges, so you can create a site for a geographic location and set IP filters for it. Also, if your network isn't spread out geographically, you can use network location, such as IP address, as the primary grouping criterion.

If possible, consider using IP filters to automate Directory creation and maintenance. Set IP subnet masks or IP address ranges for sites and also for any groups within each site in the Directory. These filters automatically populate locations with the appropriate systems.

## Operating systems and software

Consider organizing systems with similar operating systems together in groups to manage operating system-specific products and policies more easily. For example, you may have some older systems running Windows 95 or Windows 98. You can group these legacy systems together to deploy and manage security products on these systems separately. Or, you may organize Novell NetWare file servers into a group to define NetShield for NetWare policies.

---

## Creating the Directory

There is no single way to organize a Directory, and because every network is different, your Directory organization can be as unique as your network layout. Although you won't use each method offered, you can use more than one.

For example, if you use Active Directory in your network, consider importing your Active Directory containers rather than your NT domains. If your Active Directory or NT domain organization does not make sense for policy management, you may prefer to create your Directory organization in a text file and import it into your Directory. If you have a smaller network, you can create your Directory by hand and import each system manually.

### Best practices information

While you won't use all of the Directory creation methods, you also probably won't use just one. In many cases, the combination of methods you choose is to balance ease of creation, and the need for additional structure to make policy management more efficient.

For example, you might create the Directory in two phases. First, you can create 90% of the Directory structure by importing whole NT domains or Active Directory containers into sites. Then, you can manually create groups within each site to classify systems together that may have similar anti-virus or security policy requirements. If one NT domain is very large or spans several geographic areas, you can create groups under the site and point the systems in each to a separate distributed repository for efficient updating. Or, you can create smaller functional groupings, such as for different operating system types or business functions, to manage unique policies for these types of groupings.

If you choose, you can create a very detailed Directory with many sites, groups, and sub-groups. McAfee recommends, however, that you create only as much structure as is useful for the functionality of ePolicy Orchestrator you intend to use. In large networks, it would not be uncommon to have hundreds or even thousands of systems together in the same container. Being able to assign policies in fewer places may be easier than having to maintain an elaborate Directory structure.

Although you can add all systems into one site in the Directory, such a flat list makes setting different policies for different systems very difficult, especially for large networks.

## Importing Active Directory containers

The Active Directory integration feature allows you to import systems from your network's Active Directory containers directly into your ePolicy Orchestrator Directory. You can map Active Directory source containers to import systems to the root or sites of the Directory.

If part or all of your network runs Active Directory, you can create and populate all or segments of the Directory with the **Active Directory Import** wizard. Once created, you can use the Active Directory System Discovery task to regularly ensure your Directory is up-to-date with any new systems in your Active Directory.

You must be logged into the console as a global administrator to be able to import Active Directory into your Directory.

### Best practices recommendations

Implementation of this feature depends on whether you are creating the Directory for the first time or if you have an existing Directory structure and are upgrading from a previous version where you were not using Active Directory integration.

For new installations, McAfee recommends you perform two tasks to use this feature optimally. McAfee suggests that you first run the **Active Directory Import** wizard to populate your Directory. Then use the Active Directory System Discovery task to maintain these Directory segments.

If you have been using a previous version of ePolicy Orchestrator and already have a fully-populated Directory, you can still take advantages of Active Directory integration. Use the Active Directory System Discovery task to map your existing Directory structure to your Active Directory containers. You can use this feature to create mapping points between Active Directory containers and Directory sites, allowing you to import any new systems found in Active Directory to the appropriate location of the Directory.

To import systems from Active Directory:

- 1 In the console tree, right-click **Directory**, then select **All Tasks | Import Active Directory Computers**.
- 2 Click **Next** when the **Active Directory Import** wizard appears.
- 3 On the **ePolicy Orchestrator Destination Group** dialog box, select the Directory root or site to which you want to import new systems from Active Directory, then click **Next**.

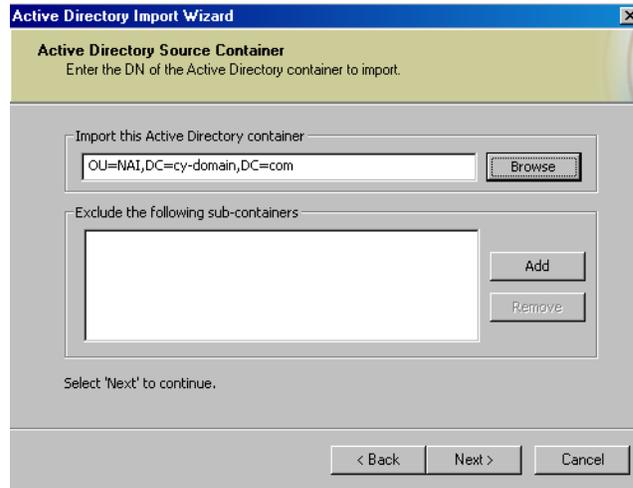


You can import only to the Directory root or sites.

- 4 Provide the Active Directory user credentials, then click **Next**.

- 5 In the **Active Directory Source Container** dialog box, click **Browse** to select the desired source container in the **Active Directory Browser** dialog box, then click **OK**.

**Figure 3-2 Active Directory Import wizard**



- 6 To exclude a specific sub-container of the selected Active Directory container, click **Add** under **Exclude the following sub-containers**, select the desired sub-container to exclude, then click **OK**.
- 7 Click **Next**, and view the activity log for any new systems that have been imported. Verify in the Directory that these systems were imported.
- 8 Click **Finish**.

Once the systems are imported, distribute agents to these systems. Also, consider setting up a recurring Active Directory System Discovery task to keep these parts of your Directory up-to-date with any new systems in your Active Directory containers.

## Importing NT domains

You can create and populate sites or groups automatically with systems from your network by importing entire NT domains. This method is an easy way to add all the systems in your network to the Directory tree in one click.

If your domain is very large, you may want to also create sub-groups to assist with policy management or Directory organization. To do this, first create a site by importing the domain into your Directory, then manually create logical groups under the site, and drag the appropriate systems into them.

When using this method, consider setting up IP filters (if address information corresponds to your domain structure) and running the Domain Synchronization task regularly to ensure easy maintenance.

You can use the NT domain importing feature to create and populate sites and groups or to add systems of an NT domain to an existing site or group.

## Importing NT domains to create sites and groups

Use this procedure to create sites or groups by importing NT domains.

To create Directory segments of the same name and listing all the systems of a Windows NT domain:

- 1 In the console tree, right-click **Directory** or the desired site, then select **New | Site** or **New | Group**.
- 2 In the **Add Sites** dialog box, click **Browse** to open the **Directory Browser** dialog box.
- 3 Select the desired domain from the list of domains that can be accessed, then click **OK**. The domain name is added to the **Sites to be added** list.
- 4 To add one or more IP filters, select the site from the **Sites to be added** list and click **Edit**.



Although not recommended for large networks due to potential bandwidth impact, you can deploy the agent to all systems in the sites that appear in **Sites to be added** as you create the site.

- 5 Click **OK**.

## Importing NT domains to existing sites or groups

In addition to creating a site or group from an NT domain import, you can also import all systems belonging to the selected Windows NT domain to an existing site or group.

This is useful if you have several smaller domains on your network that would all use the same policies and tasks. To define them all in one place, you can import these systems into the same site or group and manage their policies from that group level.

Use this procedure to import systems from your network to sites or groups you have created manually.



Import each NT domain into a separate site or group if possible. This helps you keep track of which systems belong to which domain. Also, having sites and groups named after NT domains helps place systems in the correct site or group automatically using IP and domain filters.

To manage the same policies across several domains, manually create a site, then import each domain as a group within the site.

To import all the systems in an NT domain into an existing site or group:

- 1 In the console tree, right-click the desired site or group and select **New | Computer**.
- 2 In the **Add Computers** dialog box, click **Browse** to open the **Computer Browser** dialog box and select the desired systems.
- 3 Click **OK** to save the selected systems and return to the **Add Computers** dialog box.



Although not recommended for large networks due to potential bandwidth impact, you can deploy the agent to all systems in the sites that appear in **Sites to be added** as you create the site.

- 4 Click **OK**.

The systems are added to the selected site or group.

## Deploying the agent when adding systems to the Directory

You can use ePolicy Orchestrator to deploy the agent to new systems that you import into the Directory using the NT domain import feature.

Before you deploy agents to your network at all, be sure to first review the information in this guide regarding agent deployment and management. For more information, see [Chapter 4, Distributing Agents](#).



McAfee recommends that you do not deploy the agent during an NT domain import if the domain is large. Deploying the 1.45 MB agent package to many systems at once may cause network traffic issues. Instead, import the domain, then deploy the agent to groups of systems at a time, rather than all at once.

You can deploy agents to all systems in a site listed in the **Sites to be added** dialog box during the NT domain import.

To deploy the agent while importing systems:

- 1 In the **Sites to be added** dialog box, select **Send agent package**.
- 2 To hide the installation of the agent from the user, select **Suppress agent installation GUI**.
- 3 Accept the default **Installation path** or type a different one. This is the location on the system where the agent is installed. (Click  to insert variables into the **Installation path**.)
- 4 Specify a user name and password for a user account with administrator rights to the desired systems.
- 5 Check the **Server Events** page (right-click the ePolicy Orchestrator server in the console tree, then select **Server Events**) to verify the agent installation was successful. If the page shows a failed agent installation, the deployment failed. If nothing is shown regarding agent installation, the installation did not fail. (The **Server Events** page does not indicate whether the agent installation was successful.)

## Importing systems and groups from a text file

You can define the groups and systems that belong in a particular site by typing the group and system names in a text file, then importing that information into ePolicy Orchestrator. You may have network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate complete text files containing complete lists of the systems on your network. Then you can edit the text file to manually create groups of systems, and import the entire structure into the Directory.

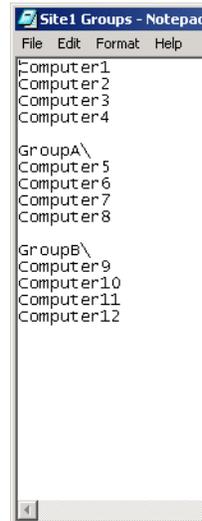
To import systems into an existing site or group in the Directory:

- 1 [Create a text file of groups and systems](#).
- 2 [Import the systems from the text file into the Directory](#).

## Create a text file of groups and systems

Create a text file containing the NetBIOS names for the systems in your network that you want to import into a site. You can import a flat list of systems, or organize the systems into groups, then add the specified systems to them. You can create the text file by hand. More likely, especially in large networks, you can use other network administration tools to generate a text file list of systems on your network.

**Figure 3-3 Import groups and systems from a text file into a site or group**



Regardless of how you generate the text file, you must format it using the correct syntax before you can import it into the Directory. List each system separately on its own line. To organize systems into groups, type the group name followed by a backslash (\), then list the systems belonging to that group beneath it, each on a separate line.

```
GroupA\  
system1  
system2  
system3  
system4
```

Be sure to verify the names of groups and systems and text file syntax before importing systems. When you are done, save the text file to a temporary folder on your server.

## Import the systems from the text file into the Directory

Once you have created and saved the text file of systems to import, you can import the file into the Directory.

To import systems or groups of systems into the Directory from the text file:

- 1 In the console tree, right-click the desired site or group into which you want to import the systems, then select **All Tasks | Import computer**.
- 2 In the **Importing computers from a Text File** dialog box, click **Continue**.
- 3 Use the **Import From File** dialog box to browse and select the text file.

- 4 When you locate the text file, select it and click **OK**. The systems are imported to your selected site or group in the Directory. If your text file organized the systems into sub-groups, it creates the groups and imports appropriate systems into them.

## Creating sites and groups manually

If you don't want to create sites or groups by other available methods, you can create them manually. You can then populate these sites and groups with systems, either by typing NetBIOS names for individual systems or by importing selected systems directly from your Network Neighborhood.

In addition, you may want to manually create sub-groups for logical collections of certain systems after importing an entire NT domain or Active Directory container into the Directory. For example, you may want to create a Servers or Exchange sub-group to set policies for special server applications.

### Best practices information

You can deploy the agent to systems when creating the Directory. However, sometimes people are unable to deploy the agent from ePolicy Orchestrator and, instead, distribute the agent through another means, choosing to use ePolicy Orchestrator for its other features.

When using another method to deploy the agent, ePolicy Orchestrator adds the system to the Directory the first time that the agent on that system calls into the server. If you have created no sites or groups in the Directory, ePolicy Orchestrator adds all the systems to the global Lost&Found site. In a large deployment, hundreds or thousands of systems can be listed together in any Lost&Found group, which makes policy management difficult.

If your organization's IP address information coincides with your needs for organizing the ePolicy Orchestrator Directory, consider applying IP filters to these sites and groups you create manually, before the agent distribution, to ensure that when agents check into the server for the first time, the systems are automatically placed in the correct location.

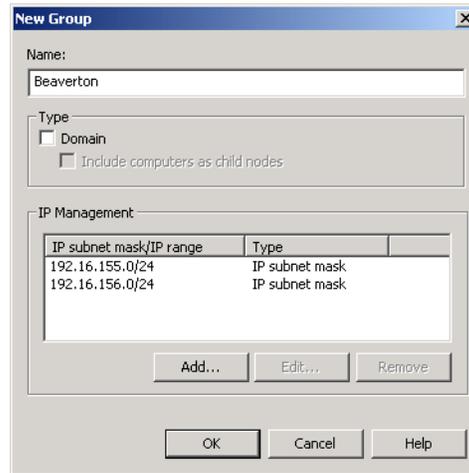
Use this procedure to create a site or group manually.

To create sites or groups manually:

- 1 In the console tree, right-click **Directory**, then select **New | Site** or **New | Group**. The **Add Sites** dialog box appears.

- Click **Add** to open the **New Site** or **New Group** dialog box and define the site that you want to add to the Directory.

**Figure 3-4 New Group dialog box**



- Type a **Name** for the new site.
- To add one or more IP filters, select the site from the **Sites to be added** list and click **Edit**. For more information, see [Adding WebShield appliances on page 49](#).
- You can deploy the agent to all systems in the sites that appear in **Sites to be added** as you create the site. For more information, see [Adding WebShield appliances on page 49](#).
- Click **OK**.

Once these sites and groups are created, populate them with systems by typing computer names for individual systems or by importing selected systems directly from your Network Neighborhood.

### Adding specific systems manually to an existing site or group

Use this procedure to import systems from your Network Neighborhood to sites or groups you have created manually. You can also import systems into a site or group you have created by importing a network domain.

To manually add a system to a site or group:

- In the console tree, right-click the desired site or group, then select **New | Computers**.
- Click **Add** in the **Add Computers** dialog box.
- In the **New Computers** dialog box, type the NetBIOS name for the system in the **Name** field. Alternatively, you can click **Browse** to find the system on your network and select it.
- Click **OK** to add the system and return to the **Add Computers** dialog box.

- 5 Deploy the agent to the systems as you add them to the Directory. To do this, check **Send agent package**.
- 6 Click **OK**.

## IP address filters and sorting

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. If these organizational units reflect your needs to organize systems for policy management, consider using them to create your Directory structure by setting IP address filters for sites and groups. ePolicy Orchestrator provides tools, such as an IP sorting task that can automatically place systems in the correct site or group according to IP address. This can be a very powerful tool for automatically populating your Directory and making sure systems stay in the intended locations.

If you use IP filters, you must set the IP filtering properties at each level of the Directory properly. Know that:

- To set an IP filter for a group, you must also set IP filters in parent groups or sites.
- The IP ranges specified in lower-level groups must be a subset of the IP range of the parent.
- IP filters cannot overlap between different groups. Each IP range or subnet mask in a given site or group must cover a unique set of IP addresses that cannot be contained in other filter settings in other sites or groups.

After creating groups and setting your IP filters, run an IP integrity check task to make sure your IP filter hierarchy is valid. This task alerts you if there are any conflicts or overlaps between IP filters for different sites or groups. For more information, see [Checking integrity of IP filters on page 56](#).

You can assign IP ranges or IP subnet mask values to sites and groups as you create them, or add or edit them at any time later.

### IP filtering for the first time

When the agent calls into the server for the first time, the system is placed in the Directory location to which it has been assigned. The server searches for the appropriate site whose IP mask or range matches the agent's IP address.

Automatically populating the Directory with this method is the result of an algorithm that uses both IP filters you create and domain information for the NT domain to which the new system belongs.



Be careful if you have sites or groups in your Directory with the same name as NT domains. The domain name search rule takes precedence over the IP group rule.

If you want the system to populate the appropriate location, create the IP group under the site or group associated with the domain, or do not create the domain group under the site.

The server uses the following search algorithm to place systems in the Directory based on the criteria in this order:

- 1 Site IP filter** — If a site with a matching IP filter is found, the system is placed in that site based on the criteria in this order:
  - a** In a group named the same as the NT domain to which the system belongs.
  - b** In a group with a matching IP filter.



If no group match for IP address or domain name is found, the system is placed in the Lost&Found group of the site.

- 2 Site Domain name** — If no site is found with a matching IP filter, the server searches for a site with the same name as the NT domain to which the system belongs. If such a site is found, the server searches for a group with a matching IP filter and places the system within. If no group is found, the system is placed in the Lost&Found group of the site.
- 3 No site IP filter or domain name match is found** — If the server cannot find an IP or domain name match in any site, the server adds the system to the global Lost&Found.

### Best practices information

This feature is useful when not using ePolicy Orchestrator to deploy agents to systems on your network. If you use another distribution method, the agent is installed on the system before the system is added to the Directory. After the agent installs and calls into the server for the first time, ePolicy Orchestrator adds it to the Directory. If you set IP filters for the sites and groups, the system is added to the appropriate location. Otherwise, it is added to the Lost&Found group and you must move it manually to the appropriate group. Especially in a large network, using IP filters to get the system in the right location can save time.



Automatic IP address sorting does not apply to systems that you add to the Directory using Active Directory integration.

## Adding IP filters when creating sites and groups

You can specify IP filters for a site or group as you create them. Or, you can create them later at any time.

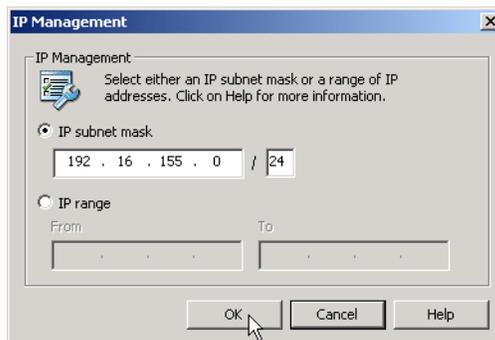
When creating a new site or group, specify the IP filter information in the **New Site** or **New Group** dialog box. The procedure for creating IP filters is the same for both sites and groups. The example in this procedure shows creating an IP filter for a new site.

To assign an IP filter to a new site or group:

- 1** In the **Add Site** or **Add Group** dialog box, select the site from **Sites to be added**, then click **Add** to open the **New Site** or **New Group** dialog box.

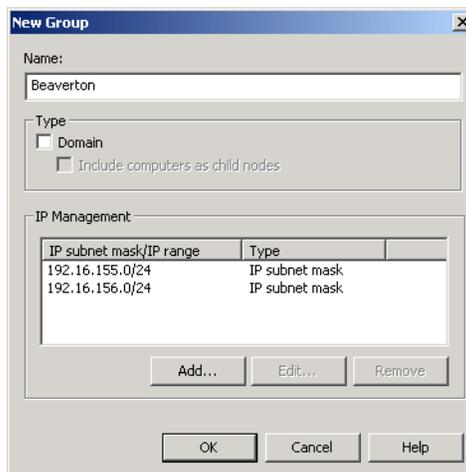
- In the **IP Management** section, click **Add**. The **IP Management** dialog box appears.

**Figure 3-5 IP Management dialog box**



- Select **IP subnet mask** or **IP range** and type the appropriate IP values.
- Click **OK** to save the IP information. In the **New Site** or **New Group** dialog box, you can see the IP range displayed in the **IP Management** list.

**Figure 3-6 New Group dialog box**



- You can add additional IP filters for the site by clicking **Add** again and entering another IP range or subnet mask. As you create and save more IP filters, each is listed in the **IP Management** list.
- When you have created all the IP filters required for your site, click **OK**.

## Adding WebShield appliances

If you have McAfee WebShield gateway appliances installed on your network and want to manage them with ePolicy Orchestrator, you can add them to an existing site or group in the Directory once the WebShield appliance is installed on your network.

To add an existing WebShield appliance to a site or group:

- 1 In the console tree, right-click the desired site or group, then select **New | WebShield Appliance**.
- 2 In the **New WebShield Appliance Configuration** dialog box, type a **Name**. You must use a different name than that of the site or group, and a different name than the host name of the appliance.
- 3 In **URL**, type the same URL that you use to access the WebShield user interface from a web browser, such as `https://MyWebShieldAppliance`.
- 4 Click **OK**.

---

## Maintaining the Directory

Performing regular maintenance ensures the Directory is up-to-date. An up-to-date Directory makes other on-going tasks easy and effective. If the Directory does not accurately reflect all network systems, you cannot attain a true picture of your security coverage.

Over time, you may need to make adjustments to the Directory as your network changes:

- Systems no longer on the network need to be removed from the Directory.
- New systems on the network require proper placement in the Directory to ensure proper policies and tasks are assigned.
- New systems with agents installed may appear in Lost&Found groups and need proper placement in the Directory to ensure proper policies and tasks are assigned.
- Specific systems may need troubleshooting.

## Using Active Directory Discovery

The Active Directory Discovery task allows you to schedule a polling interval to import new systems in Active Directory into the ePolicy Orchestrator Directory. By allowing you to only import systems that do not already exist in the Directory, this feature makes identifying new systems and ensuring that they are protected easier.

Use this procedure if you created and populated Directory segments by importing Active Directory containers. You can also use this procedure to add new systems from Active Directory to existing Directory segments created with another method.

To schedule and configure the Active Directory Discovery task:

- 1 In the console tree, select the server.
- 2 In the details pane, select the **Scheduled Tasks** tab.
- 3 If you did not create an Active Directory Discovery task while in the **Active Directory Import** wizard, click **Create task**. The **Configure New Task** page appears.

If you created an Active Directory Computer Discovery task while in the **Active Directory Import** wizard, select the task, then click **Modify task**. The **Modify Task** page appears.

- 4 Under **Task settings**, type the desired name of the task.

**Figure 3-7 Task settings page**

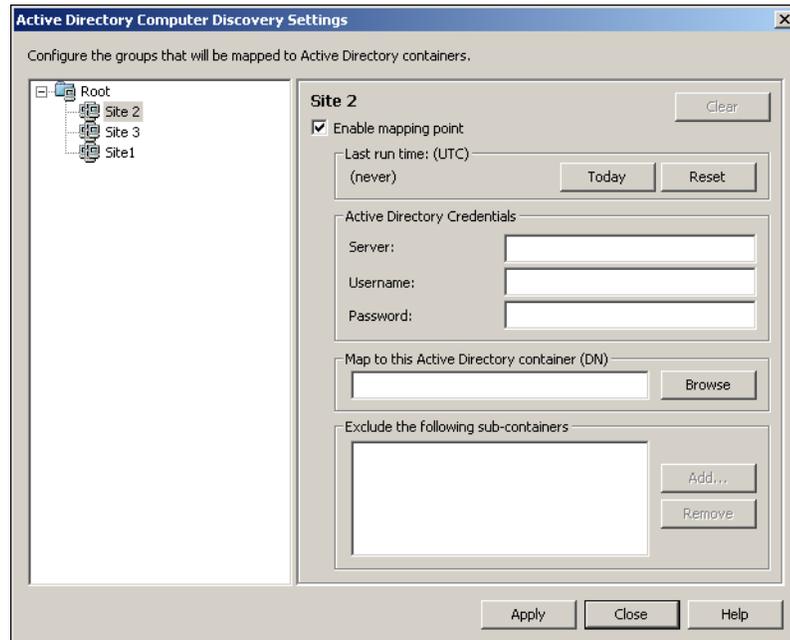
The screenshot shows a 'Task settings' dialog box with the following fields and options:

- Task settings:**
  - Name:
  - Task type:
  - Enable task:  Yes  No
  - Schedule type:
- Hourly:**
  - Every  hours
  - Start time:
  - Start date:
  - Stop time:
  - Stop date:
- Additional settings:**
  - Run missed task
  - Delay missed task by  minutes

- 5 In the **Task type** drop-down list, select **Active Directory Discovery**.
- 6 Choose whether to enable or disable the task.
- 7 In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 8 The section under the **Task settings** section is named for the **Schedule type** you selected and allows you to configure its details. (For example, if you selected **Weekly** from the **Schedule type** drop-down list, you can choose the days of the week on which you want to run the task.) Define the settings as appropriate.
- 9 Under **Additional settings**, choose whether to run missed tasks, or stop the task if its execution time exceeds a defined limit (if you choose to stop the task if its execution time exceeds the limit, you must define the limit), then click **Next** at the top of the page.
- 10 Click **Configure Active Directory Computer Discovery** on the page that appears.

The **Active Directory Computer Discovery** dialog box appears.

**Figure 3-8 Active Directory Computer Discovery dialog box**



- 11** In the left pane of the dialog box, select **Root** or the desired site to which you want to map an Active Directory container.
- 12** Select **Enable mapping** in the right pane of the dialog box, then enter the Active Directory credentials, which must have read rights to the desired Active Directory container.
- 13** Under **Map to this Active Directory container**, click **Browse** and select the desired Active Directory container.
- 14** To exclude a specific sub-container, click **Add** under **Exclude the following sub-containers**, select the desired sub-container to exclude from the task, then click **OK**.
- 15** To map another Directory node to an Active Directory container, select the desired Directory node in the console tree, and repeat [Step 12](#) through [Step 15](#).
- 16** Click **Apply**, then **Close**.



If you click **Close** before clicking **Apply**, task configurations are not applied.

The task appears in the list of server tasks. The **Next Run Time** field indicates the next time the task runs, based on your schedule settings.

In addition to the task running at the scheduled time, you can also run this task immediately by selecting the desired task in the list and clicking **Run Now**.

## Synchronizing Directory segments with NT domains

The Synchronize Domains server task allows you to update (on a scheduled or immediate basis) the Directory segments you created by importing Windows NT domains. The Update Domain task allows you to perform this task immediately. This task ensures that the Directory segments are up-to-date with the contents of the specified domains, allowing you to:

- Add new systems that have recently appeared on the network to the specified Directory segment.
- Delete systems that are no longer logged into the domain.

### Creating a regular Synchronize Domains server task

If an existing site or group has the same name as the domain you select, the systems in the domain are added to that site or group. If the domains you select do not already exist in the Directory, they are added as sites automatically.

Use this procedure if you have created sites or groups by importing NT domains when you created your Directory.

The task does the following when adding new systems from the domain:

- Adds the systems to the corresponding Directory segment.
- Deploys the agent using the provided user account. Deploying the agent is part of this task. When the task runs and imports new systems to the Directory, the agent is automatically deployed to the new systems.



The agent cannot be deployed to all operating systems in this manner. You might need to distribute the agent manually to some systems. For information and instructions, see [Distributing Agents](#).

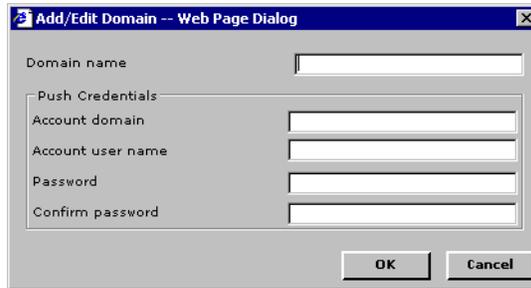
- Applies policies and tasks of the site or group to the new systems.
- Removes systems from the Directory that are no longer in the domain.

#### To create a Synchronize Domains task:

- 1 In the console tree, select the server.
- 2 In the details pane, select the **Scheduled Tasks** tab.
- 3 Click **Create Task**.
- 4 Under **Task settings**, type the desired name of the task.
- 5 In the **Task type** drop-down list, select **Synchronize domains**.
- 6 Choose whether to enable or disable the task.
- 7 In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 8 The section under **Task settings** is named for the **Schedule type** you selected and allows you to configure its details. (For example, if you selected **Weekly** as the **Schedule type**, you can choose the days of the week on which you want to run the task.) Configure the settings as appropriate.

- 9 Under **Additional settings**, choose whether to randomize the execution time, to run missed tasks, and whether to stop the task if its execution time exceeds a defined limit (if you choose to stop the task if its execution time exceeds the limit, you must define the limit), then click **Next**. The **Synchronize domains** page appears.
- 10 To add another domain, click **Add**. The **Add/Edit Domain** dialog box appears.  
To provide a different set of credentials for a domain, select the domain, then click **Modify**. The **Add/Edit Domain** dialog box appears.

**Figure 3-9 Add/Edit Domain dialog box**



- 11 Type the domain administrator credentials, then click **OK**.
- 12 To remove a domain from the task, select the desired domain, then click **Delete**.
- 13 Click **Finish** when complete. The task appears in the **Scheduled Tasks** tab.

In addition to the task running at the scheduled time, you can run this task immediately by selecting the desired task in the list and clicking **Run Now**.

## Running the Update Domain task

In addition to scheduling a server task, you can synchronize Directory segments with NT domains immediately with the Update Domain task. As you update from the domain, you can:

- Add systems currently in the domain.
- Remove systems from your Directory that are no longer in the domain.
- Uninstall agents from all systems that no longer belong to the specified domain.

### To update your Directory with an Update Domain task:

- 1 In the console tree, right-click the desired site or group, then select **All Tasks | Update Domain**. The **Update Domain** dialog box appears.
- 2 Click **Add All** or **Add** to import all or selected systems from the network domain to the selected site or group.  
Click **Remove All** or **Remove** to delete all or selected systems from the selected site or group.
- 3 If you are removing systems, select **Uninstall agent from computers when they are removed from the group** to uninstall the agent from the selected systems.
- 4 Click **OK** when finished.

## Maintaining IP filters for sites and groups

Perform regular maintenance of your IP filters to keep sites and groups organized. This section contains the following topics:

- [Adding, modifying, or deleting IP filters for existing sites or groups on page 55.](#)
- [Checking integrity of IP filters on page 56.](#)
- [Sorting systems by IP address on page 57.](#)

### Adding, modifying, or deleting IP filters for existing sites or groups

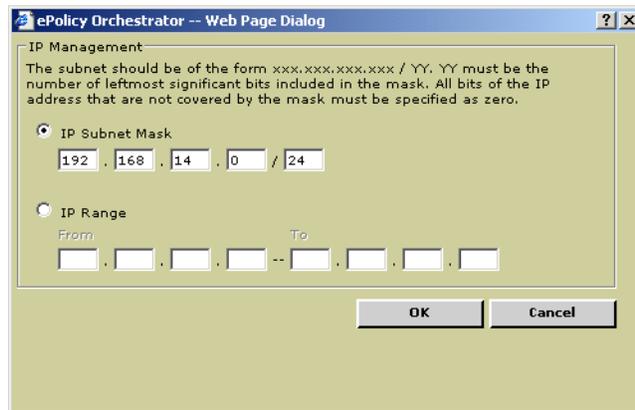
If you use IP filters in sites and groups, you can assign new IP filters or change existing ones.

#### Adding IP filters

To add an IP address filter to an existing site or group:

- 1 In the console tree, select the desired site or group.
- 2 Click the **Properties** tab in the details pane to display the **IP Management** page, which lists any IP filters that have already been configured for the selected site or group.
- 3 Click **Add** to open the **IP Management** dialog box.

Figure 3-10 IP Management dialog box



- 4 Select **IP Subnet Mask** or **IP Range** and type the appropriate values.
- 5 Click **OK**.
- 6 Click **Apply** to save the changes.



Your IP filter changes, additions, or deletions are not saved unless you click **Apply** on the **IP Management** page. If you leave the page without clicking **Apply**, your changes are lost.

### Modifying IP filters

To change the IP management settings:

- 1 In the console tree, select the desired site or group.
- 2 Click the **Properties** tab in the details pane to display the **IP Management** page.
- 3 Select the desired IP filter from the list, then click **Edit**.
- 4 Modify the **IP Subnet Mask** or **IP Range** as needed, then click **OK**.
- 5 Click **Apply** to save the current entries.

### Deleting IP filters from existing sites or groups

To delete IP management settings:

- 1 In the console tree, select the desired site or group.
- 2 Click the **Properties** tab in the details pane. The **IP Management** page appears.
- 3 Select the desired IP filter from the list.
- 4 Click **Delete**.
- 5 Click **Apply** to save the changes.

### Checking integrity of IP filters

Running a Sort Computers by IP task automatically moves new systems to the correct location based on IP address. However, for IP sorting to function correctly, all IP filters must be valid and not conflict with each other. To verify the integrity of IP filters, use the IP Integrity Check task.

To run an IP Integrity Check task:

- 1 In the console tree, right-click **Directory**, then select **All Tasks | IP Integrity Check**.
- 2 In the **Check IP Integrity** dialog box, click **Start**.

If the search returns any conflicting IP addresses and IP subnet masks, the type of conflict found and the site, group, or system causing the conflict appears under **List of conflicts**.

**Table 3-1 IP address conflicts**

<b>If the Type column displays...</b>	<b>Then the First node column displays...</b>	<b>And the Second node column displays...</b>
<b>Site</b>	The site without an IP address range or IP subnet mask.	The group under this site with an IP address range or IP subnet mask.
<b>Subset</b>	The site with an IP address range or IP subnet mask.	The group under this site whose IP address range or IP subnet mask falls outside the range defined by the site.
<b>Overlap</b>	The group whose IP address range or IP subnet mask overlaps with the group in the <b>Second node</b> column.	The group whose IP address range or IP subnet mask overlaps with the group in the <b>First node</b> column.

- 3 Select the conflict to review in **List of conflicts**. A description of the conflict displays under **Details**.
- 4 Click the **First node** or **Second node** button, respectively to go to the site or group listed. The **IP Management** page appears in the details pane.
- 5 Resolve conflicts, add, change, or delete IP address ranges or IP subnet masks as needed.
- 6 Repeat [Step 2](#) through [Step 5](#) until no conflicts are found.

## Sorting systems by IP address

If you have added IP address filters to your sites and groups, you can run the Sort Computers by IP task to sort the systems accordingly. The task moves systems to the appropriate site or group automatically for that IP address. Systems that do not match the IP filter of a site or group are moved to a Lost&Found group.

Run the Sort Computers by IP task periodically, such as once a week, to ensure systems are still located in the appropriate site or group for their IP address. The task moves systems to sites or groups based on the specified criteria for non-explicit or explicit sorting.

New systems that call into the server for the first time are added automatically to the correct site or group for their IP address. However, if you define any IP filters after the initial agent-to-server communication, you must run the IP sort to re-sort the systems and move them to the appropriate site or group.

IP sorting does not work if there are conflicts between the IP filters of different sites or groups. Run an IP Integrity Check task on your Directory before running the Sort computers by IP task.

The Sort Computers by IP task uses two sorting methods, non-explicit and explicit:

The *non-explicit sorting method* is the default and sorts as follows:

- Uses the rules set by the explicit sorting method, unless one of the rules set in the non-explicit sorting methods takes precedence.
- If the system is in a group that does not have an IP range, but that group is part of a Directory segment that matches the system's IP range, the system is left where it was found.
- If a system resides under a group that is less appropriate than a location that has the correct IP range, the system is moved to the more correct location.

The *explicit sorting method* is an alternate method you can enable by inserting a new key in the CONSOLE.INI file. The explicit sorting method sorts as follows:

- System IP address must match the IP range of its parent site. If no suitable site is found, the system is moved to the site specified by the user (default is the Lost&Found site).
- If the system belongs to a site, and no other groups are valid under that site, a new group must be created under the Lost&Found group before the system can be moved. The new group must be named after the domain to which the system belongs. This functionality is optional and can be enabled in the CONSOLE.INI file.

The **Use Explicit Lost Found** option determines systems which need to be moved to the Lost&Found or a site. If this option is enabled, systems are moved directly to the global Lost&Found or appropriate site. If the **Use Explicit Lost Found** option is not enabled (default), and a system needs to be moved to a site, the system is moved to the site-level Lost&Found.

In addition, if a system must be moved to any Lost&Found (including the explicit move from site level), ePolicy Orchestrator creates the group under the Lost&Found with the name of the domain to which the system belongs, and moves the system under the new Lost&Found/domain group.

This section includes the following topics:

- [Configuring explicit and non-explicit IP sorting on page 58.](#)
- [Running the Sort computers by IP task on page 58.](#)

### Configuring explicit and non-explicit IP sorting

To specify the sorting method and rules to move systems used by the **IP Sorting** wizard:

- 1 In a text editor, open the `CONSOLE.INI` file located in the installation directory. The default location is:

```
c:\program files\mcafee\epo\3.6.0
```

- 2 To enable the explicit sorting method or rules for moving systems, make this change:

```
[Sorting]  
UseExplicitLostFound=1  
UseExplicit=1
```

- 3 Save the file.

### Running the Sort computers by IP task

To run the Sort computers by IP task:

- 1 Run an IP Integrity Check task on your Directory to confirm all IP filters are valid and don't conflict. For instructions, see [Checking integrity of IP filters on page 56](#).
- 2 In the console tree, right-click **Directory**, then select **All Tasks | Sort Computers by IP**.
- 3 In the **IP Sorting** wizard, click **Next**.
- 4 Under **Options** on the **IP Sorting Options** dialog box, configure actions to remediate systems found to be in the wrong container for their IP address.
- 5 To exclude systems without IP management settings from being sorted, select **Ignore machines with no IP address**.
- 6 Click **Next** to sort the systems in the Directory using their IP management settings.
- 7 Click **Next**, then **Finish**.

## Using Directory searches to find systems

Use this procedure to quickly find systems using predefined search queries. Once systems are found, take selected actions on any, such as deleting them from the Directory or deploying an agent to them.

### Available Directory searches

The following table lists and describes the available Directory searches:

**Table 3-2 Directory searches**

Directory Search	Description
Computers in domain	Find a system by NetBIOS name that also belongs to a specific network domain. Use this search instead of the generic Specific computers search if you have systems with the same name in different domains.
Computers in a specific group or site	Find a system by NetBIOS name within a specific site or group in your Directory. Use this search instead of the generic Specific computers search if you have systems with the same name in different domains.
Computers with a specific DAT version	Search for all systems currently running a specific DAT version.
Computers with a specific engine version	Search for all systems running a specific anti-virus engine version.
Duplicate computer names	Find multiple entries of the same system so you can remove the duplicates.
Inactive agents	This is a manual search similar to the scheduled Inactive Agent search.
Operating system	Find systems running a particular version of Windows.
Specific computers	Find specific systems by NetBIOS name.
Specific ePO agent version	Search for all systems running a specific agent version.
Specific plugin version	Find systems with a specific plugin version.

### Running a Directory search

To find systems in the Directory:

- 1 In the console tree, right-click **Directory** or a site or group, then select **Search**. The **Directory Search** dialog box appears.
- 2 Select the desired query in **Search for**.
- 3 For each **Field Name**, specify the **Operator** and **Value** to apply to the selected query.
- 4 Click **Search Now**. Systems that match the search criteria display under **Search Results**.
- 5 Select the desired systems in **Search Results**, right-click, and select:
  - **Send Agent Install** to deploy the agent. For instructions, see [Distributing agents on page 76](#).
  - **Agent Wakeup Call** to send an agent wakeup call. For instructions, see [Sending scheduled agent wakeup calls on page 90](#).
  - **Move To** to move systems to another site or group.

- **Delete** to remove systems from the **Directory**. (You can also remove the agent from these systems, by selecting **Uninstall agent from all connected computers**.)
- **Save As** or **Print** to save or print the search results.

## Using wildcard characters with Directory searches

The **Directory Search** dialog box allows you to use the following wildcard characters with the **Operator like** option to find systems in the Directory.

**Table 3-3 Wildcard characters**

Use this character...	To find...	For example...
%	Any string of zero or more characters.	<b>like</b> <code>computer%</code> finds <code>computer1</code> , <code>computerNT</code> , and <code>computers</code> . <b>like</b> <code>%computer%</code> finds <code>computer1</code> , <code>computerNT</code> , <code>computers</code> , and <code>my computer</code> .
_	Any single character.	<b>like</b> <code>computer_</code> finds <code>computer1</code> and <code>computers</code> . <b>like</b> <code>computer__</code> finds <code>computerNT</code> .
[ ]	Any single character within a specified range, such as [a-f]; or set, such as [abcd].	<b>like</b> <code>PDX[abc]</code> finds <code>PDXA</code> , <code>PDXB</code> , and <code>PDXC</code> . <b>like</b> <code>IT[a-b]-Test</code> finds <code>ITA-Test</code> , and <code>ITB-Test</code> .
[^]	Any single character that is not within a specified range, such as [^a-f]; or set, such as [^abcd].	<b>like</b> <code>PDX[^abc]</code> finds <code>PDXD</code> , <code>PDXF</code> , and <code>PDXG</code> . <b>like</b> <code>IT[^a-b]-Test</code> finds <code>ITD-Test</code> and <code>ITF-Test</code> .

## Moving systems manually within the Directory

Even if you have a perfectly organized Directory that mirrors your actual network hierarchy, and you use automated tasks and tools to regularly synchronize your Directory, you may need to move systems manually between sites or groups. For example, you may need to periodically move systems from the Lost&Found.

If you are using IP filters in your Directory, make sure that the IP address information for the system (or group) you are moving fits within any IP filters you have created in the parent site or group. IP information must be consistent between parent and child nodes.

When you need to move systems and groups manually from one Directory location to another, you can use standard Windows drag-and-drop or cut-and-paste functionality.

# 4

## Distributing Agents

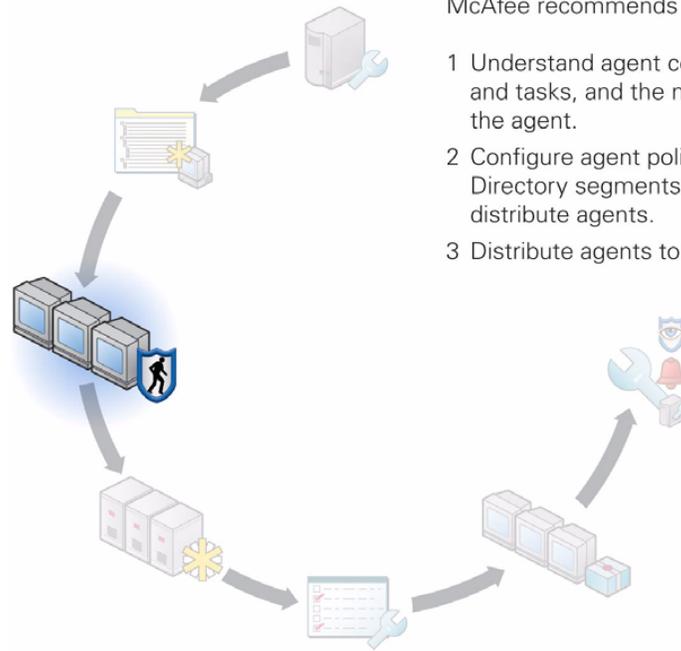
### Prepare your network systems for management

Managing your network systems effectively is dependent on each system running an active, up-to-date agent.

There are several methods to distribute the agent. You may use more than one distribution method, depending on:

- The realities of your environment.
- Whether you are upgrading agents or distributing them for the first time.

#### Distributing agents for the first time?



When distributing agents for the first time, McAfee recommends to:

- 1 Understand agent concepts, its policies and tasks, and the methods to distribute the agent.
- 2 Configure agent policy settings for the Directory segments to which you want to distribute agents.
- 3 Distribute agents to the desired locations.

## About agents and SuperAgents

The agent is the distributed component of ePolicy Orchestrator that must be installed on each system in your network that you want to manage. SuperAgents are agents that have been enabled to distribute broadcast wakeup calls. SuperAgents can also be used as repositories from which to distribute products and product updates.

The agent collects and sends information among the server, update repositories, managed systems, and products. Systems cannot be managed without an installed agent.

Consider the following topics when planning to distribute agents:

- [Agent installation folder on page 62.](#)
- [Agent language packages on page 62.](#)
- [The agent installation package on page 63.](#)
- [Agent-server communication on page 65.](#)
- [Agent installation command-line options on page 66.](#)
- [SuperAgents and broadcast wakeup calls on page 67.](#)

## Agent installation folder

The location of the agent installation folder depends on whether the agent is located on managed systems or the server.

- On the server, the agent is installed in this location:

```
<system_drive>\program files\mcafee\common framework
```

- On the client system, if the agent was installed as part of another product installation or pushed from the console to the system, it is installed by default in this location:

```
<system_drive>\program files\mcafee\common framework
```

- On the client system, if you are upgrading the agent from version 2.5.1, the new agent is also installed after the existing agent is uninstalled, by default in this location:

```
<system_drive>\program files\network associates\common framework
```



Once the agent has been installed, you cannot change its installation directory without first uninstalling it.

## Agent language packages

Agent installation packages, both default and custom, install in English. To use other language versions of the agent on the systems you want to manage, you must check the desired agent language packages into the master repository.

Each agent language package includes only those files needed to display the user interface for that language. Agent language packages can be replicated to distributed repositories.

After the initial ASCII, the agent retrieves the new package that corresponds to the in-use locale and applies it. In this way, the agent retrieves only language packages for the locales being used on each managed system.



The agent software continues to appear in the current language until the new language package has been applied.

Multiple language packages can be stored on managed systems at the same time to allow users to switch between available languages by changing the locale. If a locale is selected for which a language package is not available locally, the agent software appears in English.

Agent language packages are available for these languages:

- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English
- French (Standard)
- German (Standard)
- Italian
- Japanese
- Korean
- Polish
- Spanish (Traditional Sort)
- Swedish

For more information on checking packages into the master repository, see [Checking in product deployment packages manually on page 146](#).

## The agent installation package

The FRAMEPKG.EXE file is created when you install the server. It is a customized installation package for agents that report to your server. The agent installation package contains the server name, its IP address, ASCII port number, and other information that allows the agent to communicate with the server.

By default, the agent installation package is installed in this location:

```
C:\PROGRAM FILES\MCAFEE\EPO\3.6.0\DB\SOFTWARE\CURRENT\  
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

This is the installation package that the ePolicy Orchestrator server uses to deploy agents.

The default agent installation package contains no embedded user credentials. When executed on the system, the installation uses the account of the currently logged-on user.

## Custom agent installation packages

If you use a distribution method other than ePolicy Orchestrator software's own deployment capabilities (such as login scripts or third-party deployment software), you must create a custom agent installation package (FRAMEPKG.EXE) with embedded administrator credentials if users do not have local administrator permissions. The user account credentials you embed are used to install the agent.



Microsoft Windows XP Service Pack 2 and later operating systems do not allow embedded administrator credentials until the package file name has been added to the exception list of the Windows firewall.

To create a custom agent installation package:

- 1 In the console tree, select the server.
- 2 In the details pane, select the **General** tab, then click **Agent Installation Package Creation Wizard**.
- 3 Click **Next**. The **User Credentials** dialog box appears.

**Figure 4-1 Agent Installation Package Creation wizard – User Credentials**

- 4 Type the **User Name** (<DOMAIN>\<USER>) and **Password** you want to embed in the package, then click **Next**.
- 5 On the **Install Directory** dialog box, click **Browse** and select the location to which you want to save the custom agent installation package.
- 6 Click **Next**. The **Create Package** dialog box appears, showing the progress of the creation.
- 7 Click **Next**, then **Finish**.

You can distribute the custom installation package file as needed.

If you plan to deploy the custom installation package with ePolicy Orchestrator, check the package into your master repository.

## Agent-server communication

During agent-server communication, the agent and server exchange information using SPIPE, a proprietary network protocol used by ePolicy Orchestrator for secure network transmissions. At each communication, the agent collects its current system properties and sends them to the server. The server sends any new or changed policies, tasks, and repository list to the agent. The agent then enforces the new policies locally on the managed system.

Agent and server communication can be initiated in three ways:

- [Agent-to-server-communication interval](#).
- [ASCI after agent startup on page 65](#).
- [Wakeup calls on page 66](#).

### Agent-to-server-communication interval

The agent-to-server-communication interval (ASCI) is set on the **General** tab of the **ePO Agent 3.5.0** policy pages. This setting determines how often the agent calls into the server for data exchange and updated instructions. By default, the ASCI is set to 60 minutes. With this setting, the agent checks into the server once every hour. This is a configurable setting on the agent policy pages.

#### Best practices information

When considering whether to leave this policy setting at the default, or to modify it, you must consider your organization's threat response requirements, available bandwidth, and the hardware hosting the server. Be aware that ASCI communication can generate significant network traffic, especially in a large network. In such a case, you probably have agents in remote sites connecting to the server over slower network connections. For these agents, you may want to set a less frequent ASCI. The following table lists general ASCI recommendations for several common network connection speeds.

**Table 4-1 General recommended ASCI settings**

Network Size	Recommended ASCI
Gigabit LAN	60 minutes
100MB LAN	60 minutes
WAN	360 minutes
* Dial-up or RAS	360 minutes
10MB LAN	180 minutes
Wireless LAN	150 minutes
* When you connect to a corporate intranet via dial-up or RAS, the agent communicates to the ePolicy Orchestrator server when the connection is detected.	



For complete information on balancing bandwidth, server hardware, and ASCI, see the *ePolicy Orchestrator 3.6 Hardware Sizing and Bandwidth Usage* white paper.

### ASCI after agent startup

After the installation, or if the agent service is stopped and restarted, the agent calls into the server at a randomized interval within ten minutes. The second and subsequent ASCI after startup occurs with the ASCI set in the agent policy (60 minutes by default).

You can force the agent to communicate to the server immediately after the installation by running the CMDAGENT.EXE with the `/P` command-line option.

For instructions, see [Configuring agent policy settings on page 71](#).

## Wakeup calls

When you send a wakeup call from the server to agents in your environment, the agents are prompted to call into the server. Wakeup calls can be sent manually or scheduled as a task and are useful when you have made policy changes or checked in updates to the master repository that you want to be applied to the managed systems sooner than when the ASCII may occur.

## Agent installation command-line options

Depending on whether the agent is already installed, you can use command-line options when you run the agent installation package (FRAMEPKG.EXE) or the agent framework installation (FRMINST.EXE) program.

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

The following table describes all of the agent installation command-line options. These options are *not* case-sensitive, but their values are.

**Table 4-2 FRAMEPKG.EXE command-line options**

Command	Description
/DATADIR	<p>Specifies the folder on the system to store agent data files. The default location is:</p> <pre>&lt;Documents and Settings&gt;\All Users\Application Data\McAfee\Common Framework</pre> <p>If the operating system not have a Documents and Settings folder, the default location is the Data folder within the agent installation folder</p> <p><b>Sample</b> FRAMEPKG /INSTALL=AGENT /DATADIR=&lt;AGENT DATA PATH&gt;</p>
/DOMAIN /USERNAME /PASSWORD	<p>Specifies an NT domain, and account credentials used to install the agent. The account must have rights to create and start services on the desired system. If left unspecified, the credentials of the currently logged-on account are used.</p> <p>If you want to use an account that is local to the desired system, use the system's name as the domain.</p> <p><b>Sample</b> FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=jdoe /PASSWORD=password</p>
/INSTALL=AGENT	<p>Installs and enables the agent.</p> <p><b>Sample</b> FRAMEPKG /INSTALL=AGENT</p>
/INSTALL=UPDATER	<p>Enables the AutoUpdate 7.0 component if it has already been installed, and does NOT change whether the agent is enabled.</p> <p>This command-line option upgrades the agent.</p> <p><b>Sample</b> FRAMEPKG/INSTALL=UPDATER</p>

**Table 4-2 FRAMEPKG.EXE command-line options**

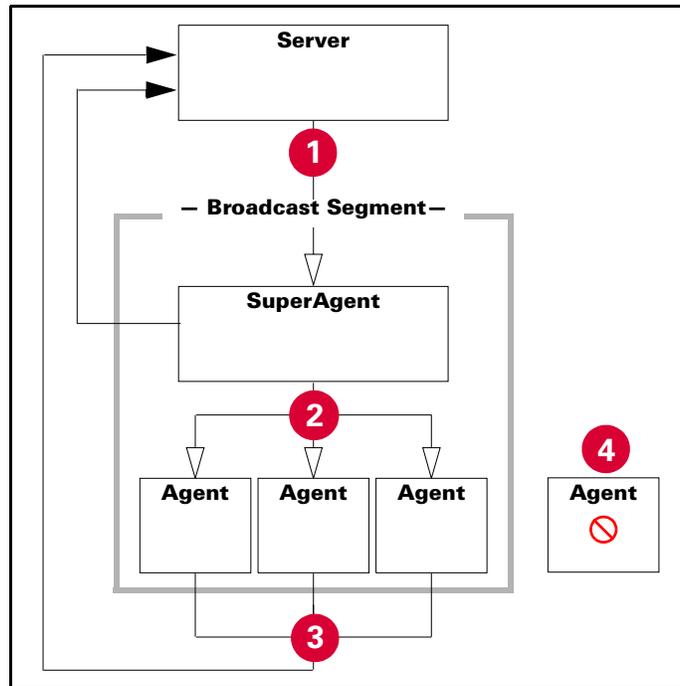
Command	Description
/INSTDIR	Specifies the installation folder on the desired system. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default location is:  <DRIVE>:\program files\mcafee\common framework  <b>Sample</b> FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent
/REMOVE=AGENT	Disables the agent, and removes it if not in use.  <b>Sample</b> FRMINST /REMOVE=AGENT
/SILENT or /S	Installs the agent in silent mode, hiding the installation interface from the end-user.  <b>Sample</b> FRAMEPKG /INSTALL=AGENT /SILENT
/SITEINFO	Specifies the folder path to a specific repository list(SITELIST.XML) file. For more information about the repository list, see <a href="#">Exporting the repository list to a file on page 157</a> .  <b>Sample</b> FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\MYSITELIST.XML
/USELANGUAGE	Specifies the language version of the agent that you want to install.  If you select a locale other than the 12 languages with locale IDs, the software appears in English.  If you install multiple language versions, the locale selected in operating system determines the language version that displays.  <b>Sample</b> FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404  For more information see <a href="#">Locale IDs on page 391</a> .

## SuperAgents and broadcast wakeup calls

If you plan to use agent wakeup calls in your network to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent. SuperAgents distribute the agent wakeup call's bandwidth impact, minimizing network traffic. Depending on your network environment, you may find SuperAgent wakeup calls to be a more resource-efficient method of prompting agents to call in, than relying on the server to send wakeup calls to all agents.

Instead of sending agent wakeup calls from the server to every agent, the server sends the SuperAgent wakeup call to SuperAgents in the selected Directory segment. When SuperAgents receive this wakeup call they send broadcast wakeup calls to all the agents in their network broadcast segments. This reduces network traffic. This is beneficial in large networks where ePolicy Orchestrator may manage agents in remote sites over lower-speed WAN or VPN connections.

**Figure 4-2 Broadcast wakeup calls**



- 1 Server sends a wakeup call to all SuperAgents.
- 2 SuperAgents send a broadcast wakeup call to all agents in the same broadcast segment.
- 3 All agents (regular agents and SuperAgents) exchange data with the server.
- 4 Any agents without an operating SuperAgent on its subnet are not be prompted to communicate with the server.

#### Best practices information

To deploy the right number of SuperAgents to the right locations, first analyze the divisions of broadcast segments in your environment and select a system (preferably a server) to host the SuperAgent. Any agents that do not have a SuperAgent in the local broadcast segment do not receive the broadcast wakeup call.

Similar to the regular agent wakeup call, the SuperAgent wakeup call utilizes the SPIPE protocol. Ensure that the agent wakeup port (8081 by default) is not blocked by your firewall.

## Agent activity logs

The agent log files are useful when determining agent status or troubleshooting problems. There are two log files that record agent activity, both are located in the agent installation folders on the managed system:

- Agent activity log

The agent activity log is an XML file named AGENT\_<SYSTEM>.XML where <SYSTEM> is the NetBIOS name of the system on which the agent is installed. This log file records agent activity related to such things as policy enforcement, agent-to-server communication, and event forwarding. You can define a size limit of this log file.

You can configure the level of logging of agent activity on the **Logging** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

- Detailed agent activity log

The detailed agent activity log (AGENT\_<SYSTEM>.LOG) file where <SYSTEM> is the NetBIOS name of the system on which the agent is installed. In addition to the information stored in the agent activity log, the detailed activity log contains troubleshooting messages. This file has a 1MB size limit. When this log file reaches 1MB, a backup copy is made (AGENT\_<COMPUTER>\_BACKUP.LOG).

---

## Agent policy settings

Agent policy settings determine agent performance in your environment, including:

- How often the agent calls into the server.
- How often the agent enforces policy on the managed systems.
- How often the agent delivers event files to the server.

Before you deploy and install agents on your systems, McAfee recommends that you first configure the agent policy settings for the different Directory segments to which you intend to distribute the agent.

## Immediate event forwarding

The agent and security software on the managed system generate software events continuously during normal operation. These can range from information events about regular operation, such as when the agent enforces policies locally, to critical events, such as when a virus is detected and not cleaned. These events are logged by the agent and sent to the server at each ASCI and stored in the database. A typical deployment of ePolicy Orchestrator in a large network can generate thousands of these events an hour. Most likely, you won't want to see each of these.

However, you may want to know about higher severity events immediately. You can configure the agent to forward events that are equal to or greater than a specified severity, to the server immediately. If you plan to utilize the Notifications or global updating features of ePolicy Orchestrator, enabling immediate uploading of higher severity events is necessary for those features to function as intended.

You can enable immediate uploading of events on the **Events** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

## Full and minimal properties

The agent sends information from the managed system to the server at each agent-server communication, allowing you to view the properties of individual systems from the ePolicy Orchestrator console. You can use the ePolicy Orchestrator console to view current properties for a specific system.

The agent sends the complete set of properties during the initial communication. After the initial communication, the agent sends only those properties that have changed since the last communication. However, the agent sends the complete set again if:

- Policy is set to send full properties.
- Properties versions on the agent and those on the ePolicy Orchestrator server differ by more than two.

The properties listed depend on whether you selected to send full or minimal properties on the **General** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

### Full properties

If you specify to collect the full set of properties, the agent collects:

- System properties — including:
  - System hardware information.
  - Installed software information.
  - Processor speed
  - Operating system
  - Time zone
  - Most recent date and time that properties were updated.
- Product properties — including:
  - Installation path.
  - Virus definition (DAT) file version number.
  - Product version number.
  - Specific policy settings configured for each product.

### Minimal properties

If you specify to collect only minimal properties, the agent collects only these product properties:

- Installation path.
- Virus definition (DAT) file version number.
- Product version number.
- Specific policy settings configured for each product.

## Agent policy and distributed repositories

By default, the agent can attempt to update from any repository in its repository list (SITE.LIST.XML) file. The agent can use a network ICMP ping command or the repository's subnet address to determine the distributed repository with the fastest response time. Usually, this is the distributed repository that is closest to the system on the network. For example, a managed system in a remote site far from the ePolicy Orchestrator server probably selects a local distributed repository. By contrast, an agent in the same LAN as the server probably updates directly from the master repository.

If you require tighter control over which distributed repositories the agents use for updating, you can enable or disable specific distributed repositories on the **Repositories** tab of the **ePO Agent 3.5.0 | Configuration** policy pages. However, McAfee does not recommend doing this. Allowing agents to update from any distributed repository ensures they get the update from some location. Using a network ICMP ping, the agent should update from the closest distributed repository.

The agent performs repository selection each time the agent (**McAfee Framework Service**) service starts or when the repository list changes.

## Proxy settings

In order to access the default fallback repository, the agent must be able to access the Internet. Use the agent policy settings to configure proxy server settings for the managed systems.

The **Proxy** tab of the **ePO Agent 3.5.0 | Configuration** policy pages includes settings to:

- Use Internet Explorer proxy settings.
- Configure custom proxy settings.
- Disable any proxy use.

This default setting is **Use Internet Explorer Proxy Settings**, allowing the agent to use the current proxy server location and credential information currently configured in the Internet Explorer browser installed on that system.

However, you may need to use ePolicy Orchestrator to configure custom proxy server settings for systems in your network. For example, maybe they use a different browser and don't have Internet Explorer installed.

## Configuring agent policy settings

Before distributing a large number of agents to Directory segments, consider carefully how you want the agent to behave in the segments of your environment. Although you can configure, and re-configure, agent policy after the agent has been distributed, McAfee recommends that you set agent policy prior to the distribution to prevent unnecessary resource impact.

This section provides details concerning all of the policy settings you can configure for the agent. It describes the options you can select on the agent policy pages and their affect on agent behavior.

For information and instructions regarding assigning and managing policies with ePolicy Orchestrator, see [Configuring Product Policies and Tasks on page 115](#).

The agent policy settings are organized across six tabs:

- [General tab](#).
- [Events tab on page 73](#).
- [Logging tab on page 74](#).
- [Repositories tab on page 74](#).
- [Updates tab on page 75](#).
- [Proxy tab on page 75](#).

## General tab

The **General** tab allows you to configure the following types of agent policy:

- [General options](#)
- [Software installation on page 72](#).
- [Agent communication intervals on page 73](#).

## General options

Settings you can configure under **General options**, include:

- **Show Agent tray icon**

Allows you to choose whether the agent icon displays in the system tray of the managed system.
- **Enable Agent wakeup call support**

Allows you to send agent wakeup calls (manual or scheduled) to prompt the agent to call into the server, instead of waiting for the next ASCII.
- **Enable Agent Upgrade from version 2.x to the current version**

Forces agents version 2.x to upgrade to the current agent version at the next ASCII.
- **Enable SuperAgent functionality**

Converts the existing agent into a SuperAgent. This setting is only available when configuring agent policy on individual systems.
- **Enable SuperAgent repository**

Allows you to utilize SuperAgents and the systems that host them, as update repositories for the systems in a SuperAgent's broadcast segment.

For instructions to use SuperAgent repositories, see [Creating SuperAgent repositories on page 110](#).
- **Policy enforcement interval**

Allows you to define, in minutes, how often the agent enforces all agent and product policies on the managed system. Because policy enforcement occurs on the managed system, network traffic is not impacted by the frequency of the policy enforcement interval.

## Software installation

Policy settings you can configure under **Software installation** include:

- **Prompt user when software installation requires reboot**

Allows you to choose whether the end user of a managed system is prompted to reboot the system after a software installation completes that requires a reboot of the system. When using ePolicy Orchestrator to deploy and install products on systems, the installation occurs silently without the end-user's knowledge. Selecting this ensures the end-user is prompted to reboot after such an installation.

- **Automatic reboot with timeout**

Forces the managed system to reboot after the timeout period (in seconds).

## Agent communication intervals

Policy settings you can configure under **Agent communication intervals** include:

- **Enable agent to server communication**

Enables agent-to-server communication using the secure SPIPE protocol. This allows the agent to communicate to the server during the agent-to-server communication interval. Do not disable this without a specific, necessary reason.

- **Agent-to-server communication interval**

Allows you to define, in minutes, how often the agent calls into the server. The agent calls into the server once during each interval, sending properties and events to the server and collecting any policy changes. This interval is randomized to reduce bandwidth and resource impact.

For more information, see [Agent-server communication on page 65](#).

- **Policy age to trigger 10-minute communication interval**

Allows you to define, in days, a threshold for out-dated policies. Any agents with policies older than this threshold call into the server every 10 minutes until policies are up-to-date.

- **Full properties or Minimal properties**

Allows you to set whether the agent sends full properties or minimal properties to the server at each ASCI.

For more information, see [Full and minimal properties on page 70](#).

## Events tab

Policy settings you can configure on the **Events** include:

- **Enable immediate uploading of events**

Allows you to set whether the agent forwards events of the severity you specify to the ePolicy Orchestrator server when they occur.

- **Report any events with severity value equal or greater than**

Allows you to set the severity threshold for which events are forwarded immediately to the ePolicy Orchestrator server. Set this to send only the most important events to reduce network traffic.

- **Interval between immediate uploads**

Allows you to set an amount of time between immediate uploads. This allows you to ensure network traffic is reduced during a virus outbreak or other situations that may generate many event files.

- **Maximum events per immediate upload**

Specifies the maximum number of individual events allowed in each immediate upload.

## Logging tab

Policy settings you can configure on the **Logging** tab include:

- **Enable agent log**

Allows you to choose whether to enable the agent log (enabled by default). McAfee recommends that you enable this log file.

- **Message limit**

Allows you to specify a limit on the number of messages recorded in the agent activity log. On average, 200 messages result in a file about 16KB in size.

- **Enable detailed logging**

Allows you to enable the detailed agent activity log. This log file can grow very large. McAfee recommends enabling this log file only when you are troubleshooting communication issues.

- **Enable remote access to log**

Allows you to view the log file from an ePolicy Orchestrator console or from Microsoft Internet Explorer.

## Repositories tab

Policy settings you can configure on the **Repositories** tab include:

- **Use ePO-configured repositories or Use client-configured repositories**

Allows you to select whether to use repositories you configured with ePolicy Orchestrator or repositories you have created outside of ePolicy Orchestrator's management.

- **Repository selection**

Selects how agents determine to which repositories they go to for updates. You can choose:

- **Ping time** — Sends an ICMP ping to all repositories and sorts them by response time.

- **Subnet value** — Compares the IP addresses of all repositories and sorts repositories based on how closely the bits match. The more closely the repository and agent IP addresses resemble each other, the higher in the list the repository is placed.

- **User defined list** — Selects repositories based on their order in the list.

- **Repository list**

The list of available repositories includes the master, source, fallback, and any distributed repositories you have configured.

This list is only available for edit if you selected **User defined list** in **Repository selection**. To edit the list:

- Select a repository in the list, click **Move up** or **Move down** to specify the repository in the desired location of the list.
- Select or deselect the checkbox next to a repository list to enable or disable access to the repository by the specified agent.



Any changes you make in this list are reflected in the SITELIST.XML file.

## Updates tab

Policy settings you can configure on the **Updates** tab include:

- **Log file**  
Specifies the path (desired location) for the update log file. This file logs update activity.
- **Run options**  
Specifies the path to any executable you want to run on the managed systems after updates are performed.
- **Allow downgrade of DAT files**  
Selects whether the agent can update with DAT files from the repository when the DAT files are older than the DAT files already installed on the system. In the unlikely event that you find a new DAT file causes issues in your environment, this allows you to install a previous DAT file version.  
  
If you need to do install a previous DAT file version at some point in the future, select this option and apply the policy change, distribute the previous version of the DAT file, then deselect this option again to not accidentally install old DATs in the future.
- **Repository Branch Update Selection**  
Selects from which update branch the agent uses. If you are using the **Previous** or **Evaluation** repository branches to test new DAT file and engine updates, configure the repository branch from which the agent should update. By default updating occurs from the **Current** branch.

## Proxy tab

Policy settings on the **Proxy** tab include:

- **Use Internet Explorer proxy settings**  
Selects the proxy settings in Internet Explorer. This is the default and recommended setting. However, a user must be logged onto the server system for server tasks requiring proxy settings to run.  
  
If a user is not logged onto the system, the system is not able to access the Internet.

- **Don't use proxy**

Selects not to use any proxy settings. Choose this if the systems don't use a proxy and access the Internet directly.

- **Manually configure the proxy settings**

Selects to use custom proxy settings. If you select this option, enter the appropriate location and login credential information for HTTP and FTP proxies.

If using Windows 2000 or above, you must manually configure the proxy settings.

---

## Distributing agents

Due to the variety of scenarios and requirements of different environments, there are several methods you can use to distribute the agent to the systems you want to manage. Before using any of these methods, you should consider each.

The following table details the advantages and disadvantages of the different methods to distribute the agent.

**Table 4-3 Advantages and disadvantages of agent distribution methods**

Method	Advantages	Disadvantages
Deploying agents while creating Directory	By deploying the agent automatically while creating the sites and groups of the Directory, you don't have to complete any additional steps.	If you are creating sites by importing large NT domains or Active Directory containers, too much network traffic may be generated for your network resources.
Deploying agents from ePolicy Orchestrator	This is an efficient method for distributing the agent.	You must embed user credentials with administrator rights to the desired systems. Also, you must ensure that systems running Microsoft XP Service Pack 2, have the FRAMEPKG.EXE file added to the firewall exceptions list.
Using login scripts	This is an efficient method for an environment where systems log onto the network frequently. You do the work once, and the agent is deployed automatically.	Systems that don't log onto the network frequently, may not be running the most up-to-date agent.
Installing manually	This is an efficient method if you are not using ePolicy Orchestrator to deploy the agent, or if you have many Windows 95 and Windows 98 systems and do not want to enable file and print sharing on them.	This is not a time-efficient method if you have many systems.

**Table 4-3 Advantages and disadvantages of agent distribution methods**

Method	Advantages	Disadvantages
Including the agent on an image	Installing the agent as part of an image prevents the bandwidth impact that other forms of distribution can incur. This method also reduces the overhead by integrating the task into another one that must occur.	If you do not use images consistently, this method would not be efficient to ensure coverage.
Enabling the agent on unmanaged McAfee products	Enabling an agent that is already on the client system rather than deploying the 1.5MB package, can save significant bandwidth and time.	The disabled agent may be out-of-date and require you run the deployment task to upgrade the agent to the current release.  You cannot change the agent installation folder without uninstalling and reinstalling the agent — agents that you enable may be located in a different folder than agents that you deploy in your network by some other method.

## Deploying the agent from ePolicy Orchestrator

You can use ePolicy Orchestrator to deploy agents to your systems. This method uses Windows NT push technology.

### When to use this method

This is a desirable method to install agents if you already have large sections of your Directory populated. This is an efficient method if you were able to build Directory segments by importing domains or Active Directory containers.

### Requirements

If you want to use this method, several requirements must be met, including:

- Systems to which you want to deploy the agent must already be added to the Directory.

For information and instruction, see [Chapter 3, Creating a Directory of Managed Systems](#).



If you have not yet created the Directory, you can send the agent installation package to systems at the same time that you are adding sites, groups, and systems to the Directory.

However, McAfee does not recommend this procedure if you are creating your Directory by importing large NT domains or Active Directory containers. This can generate too much network traffic.

- Specify domain administrator credentials.  
Domain administrator rights are required to access the default `Admin$` shared folder on the desired systems. The ePolicy Orchestrator server service requires access to this shared folder in order to install agents and other software.
- Verify the ePolicy Orchestrator server can communicate with the desired systems.

Before beginning a large agent deployment, use ping commands to verify that the server can communicate with a few systems in each segment of your network to which you want to deploy agents.

If the targeted systems respond to the ping, then ePolicy Orchestrator can communicate with them.



The ability to successfully utilize ping commands from the ePolicy Orchestrator to the managed systems is not required for the agent to communicate with the server after the agent is installed. This is only a useful test for determining if you can deploy agents from the server to them.

- Verify that the `Admin$` share folders on the desired systems are accessible from the server.

This test also confirms your administrator credentials, as you cannot access remote `Admin$` shares without administrator rights.

To access `Admin$` shares on desired systems from the ePolicy Orchestrator server:

- Select **Start | Run**.
- Type the path to the client `Admin$` share by specifying either the system name or IP address.

If the systems are properly connected over the network, your credentials have sufficient rights, and the `Admin$` shared folder is present, you should see a **Windows Explorer** dialog box.

- Ensure file and print sharing is enabled. (This is disabled by default on Windows 95, Windows 98, and Windows ME systems.)

In addition, if you have systems in your network running these operating systems, you must make sure they are able to be managed by ePolicy Orchestrator. By default, these systems do not allow ePolicy Orchestrator administration. To enable these systems for ePolicy Orchestrator administration, download `VCREDIST.EXE` and `DCOM 1.3` updates from the Microsoft web site and install them on each client as required.

- Ensure network access is enabled on Windows XP Home systems.

If you want to deploy the agent from the ePolicy Orchestrator console or install a custom agent installation package on systems running Windows XP Home, you must enable network access.

To enable network access on systems running Windows XP Home:

- Select **Start | Control Panel**.
- Click **Performance and Maintenance**.
- Click **Administrative Tools**.
- Select **Local Security Policy**. The **Local Security Settings** application window appears.
- In the console tree under **Security Settings | Local Policies**, select **Security Options**. The available policies appear in the details pane.

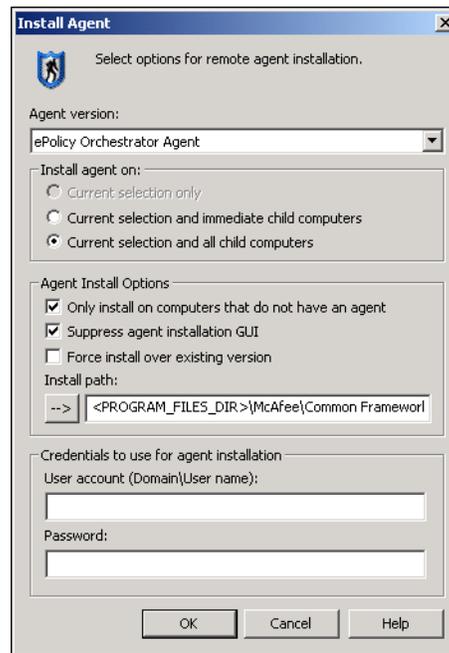
- f Select **Network access: Sharing and security model for local accounts** to open the **Network access** dialog box.
- g Select **Classic - local user authenticate as themselves**, then click **OK**. Local users are able to authenticate and access resources on the system from the network.

### Deploying the agent

To deploy the agent installation package (FRAMEPKG.EXE) from ePolicy Orchestrator to desired systems in the Directory:

- 1 In the console tree, right-click the desired node of the Directory, then select **Send Agent Install**. The **Install Agent** dialog box appears.

**Figure 4-3 Install agent dialog box**



- 2 Choose whether to install the agent on the **Current selection only**, **Current selection and immediate child computers**, or **Current selection and all child computers**.
- 3 Choose whether to **Only install on computers that do not have an agent**.
- 4 Choose whether to **Suppress agent installation GUI** on the systems.
- 5 Select **Force install over existing version** if you need to downgrade the agent version.



This might be necessary if you experience issues with a new agent and need to re-install the earlier version. Selecting this option forces installation of the agent package that is checked into the software repository, even if a newer version of the agent is already installed on the managed system.

- 6 Accept the default **Installation path** or type a different path to install the agent on selected systems. You can also click the arrow button next to the text box to insert variables into the **Installation path**. For a list, see [Variables on page 393](#).

- 7 Specify credentials that have rights to the desired systems.
- 8 Click **OK** to send the agent installation package to the selected systems.

## Installing the agent with login scripts

Using network login scripts is a very reliable and popular way to make sure that every system logging onto your network is running an agent. You can create a login script to call a batch file that checks if the agent is installed on systems attempting to log onto the network. If no agent is present, the batch file can install the agent before allowing the system to log on. Within ten minutes of being installed, the agent calls into the server for updated policies, and the system is added to the Directory.

### When to use this method

This is a desirable method to use when:

- You assigned IP sorting filters or NT domain names when creating the segments of your Directory.
- You already have a managed environment and you want to ensure that new systems logging onto the network become managed as a result.
- You already have a managed environment and you want to ensure systems are running a current version of the agent.

### Best practices information

McAfee recommends that you first create segments of your Directory that use either network domain names or IP address filters that add the expected systems to the desired sites and groups when the agents call into the server for the first time automatically. If you don't, all systems are added to the Lost&Found group and you must move them later manually.

Especially when distributing agents to systems in a very large network, creating a Directory that uses some automated sorting method *before* installing agents with login script can save valuable time.

The details of the login script used to install the agent can vary, depending on your needs. Consult your operating system documentation for more details on how to write login scripts. This section illustrates a basic example.

### Using login scripts to install the agent

To set up network login scripts to install the agent on systems logging onto the network, perform the following steps:

- 1 [Copy the agent installation package to a central folder to which all users have permissions on page 81.](#)
- 2 [Create a custom agent installation package if necessary on page 81.](#)
- 3 [Create a batch file that checks new systems for an existing agent on page 81.](#)
- 4 [Save the batch file to your primary domain controller on page 82.](#)
- 5 [Update your network login scripts to call the batch file on page 82.](#)

## Copy the agent installation package to a central folder to which all users have permissions

Copy the FRAMEPKG.EXE agent installation package on your server to a shared folder on a network server to which all systems have permissions. Systems logging onto the network are directed to this folder to run the agent installation package and install the agent when they log in.

By default, the agent installation package is in the following location:

```
C:\PROGRAM FILES\MCAFFEE\EPO\3.6.0\DB\SOFTWARE\CURRENT\
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

For more information about the agent installation package, see [The agent installation package on page 63](#).

## Create a custom agent installation package if necessary

When installing the agent via a login script, you may need to create a custom agent installation package with embedded administrator user credentials. These administrator credentials are required for the script to install the agent on the system.

For more information and instructions, see [The agent installation package on page 63](#).

## Create a batch file that checks new systems for an existing agent

Create a batch file, such as EPO.BAT, that contains the lines you want to execute on systems when they log onto the network. The contents of this batch file may differ depending on your needs, but its purpose is to:

- Check whether the agent has been installed in the expected location.
- Run FRAMEPKG.EXE if it is not present.

Below is a sample batch file that checks whether the agent is installed and, if it is not, runs the FRAMEPKG.EXE to install the agent. This example checks:

- The default installation location of the older agent version 2.5.1 and, if present, upgrades it to the agent version 3.5.
- The default installation folder for the agent version 3.5 and, if not present, installs the new agent.

### Example

```
IF EXIST "C:\Windows\System32\ePOAgent\NAIMAS32.EXE"

\\<COMPUTER>\<FOLDER>\UPDATE$\FRAMEPKG.EXE /FORCEINSTALL /INSTALL=AGENT

IF EXIST "C:\ePOAgent\FRAMEWORKSERVICE.EXE" GOTO END_BATCH

\\MyServer\Agent\UPDATE$\FRAMEPKG.EXE /FORCEINSTALL /INSTALL=AGENT

:END_BATCH
```



The installation folders for your distribution may be different than in this example, depending on where you have configured ePolicy Orchestrator to install the agent.

## Save the batch file to your primary domain controller

Save the EPO.BAT batch file to the `NETLOGON$` folder of your primary domain controller (PDC) server. The batch file runs from the PDC every time a system logs onto the network.

## Update your network login scripts to call the batch file

Add a line to your login scripts that calls the batch file on your PDC server. This line would look similar to this example:

```
CALL \\PDC\NETLOGON\EPO.BAT
```

Each system runs the script and installs the agent when it logs onto the network.

## Installing the agent manually

A simple way to install the agent is to run the installer directly from the desired system.

### When to use this method

This is a desirable method to install agents for the following circumstances:

- Your organization requires that software is installed on systems manually.
- You intend to use ePolicy Orchestrator for policy management only.
- You have systems running Windows 95, Windows 98, or Windows ME and do not want to enable file and print sharing on them.
- You assigned IP sorting filters or NT domain names when creating the segments of your Directory.

You can install the agent on the system, or distribute the `FRAMEPKG.EXE` installer to users in your organization and have them run the installation program themselves.

After the agent is installed, it calls into the server and adds the new system to the Directory.

Having assigned IP sorting filters or NT domain names to the desired Directory segments saves valuable time.

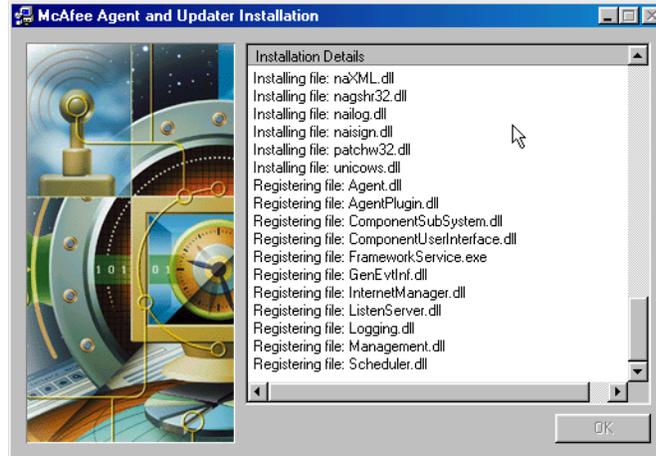
To install the agent manually:

- 1 Distribute the agent installation package.

If you want users on your network to install the agent on their own systems, distribute the agent installation package file to them. You can attach it to an e-mail message, copy it to media, or save it to a shared network folder accessible by the desired users on your network.

- 2 Double-click FRAMEPKG.EXE. Wait a few moments while the agent installs.

**Figure 4-4 McAfee Agent and Updater Installation dialog box**



Within ten minutes, the agent calls into the ePolicy Orchestrator server for the first time.

### Forcing the agent to call into the server

You can bypass the ten-minute interval and force the new agent to call into the server immediately. You can do this from any system on which an agent has just been installed, not only systems where you have installed the agent manually.

To force the agent to call into the server:

- 1 From the system where you just installed the agent, open a DOS command window by selecting **Start | Run**, type `command`, and press **Enter**.
- 2 In the command window, navigate to the agent installation folder containing the `CMDAGENT.EXE` file.
- 3 Type the following command:  

```
CMDAGENT /p
```
- 4 Press **Enter**. The agent calls into the ePolicy Orchestrator server immediately.
- 5 From the console on your server, refresh the Directory by pressing **F5**. The new system on which you have just installed the agent should now appear in your Directory.

### The first time the agent calls into the server

When the agent calls into the server for the first time, the system is added to the Directory as a managed system. If you configured IP address filtering for the Directory segments, the system is added to the appropriate location for its IP address. Otherwise, the system is added to the **Lost&Found** group. Once the system is added to the Directory, you can manage its policies through ePolicy Orchestrator.

## Enabling the agent on unmanaged McAfee products

Before purchasing ePolicy Orchestrator, you may have already been using McAfee products in your network. Some of the more recent McAfee products that use the AutoUpdate updater, such as VirusScan Enterprise, install with the agent in a disabled state. When you want to start managing these products with ePolicy Orchestrator, you do not need to install the agent on these systems. Instead, you can simply enable the agent that is already on the system.

Enabling the agent in this way, rather than re-deploying the 1.5MB agent installation package to each system, can save significant network bandwidth when you have many systems with disabled agents on the network.



You cannot change the agent installation folder without uninstalling and reinstalling the agent. Agents that you enable may be in a different folder location than agents that you deploy in your network using another method.

Having assigned IP sorting filters or NT domain names to the desired Directory segments saves valuable time.

You must copy the SITELIST.XML repository list file from the ePolicy Orchestrator server to the desired systems. The repository list contains network address information the agent requires to call into the server after installing.

To enable the agent on unmanaged systems running a McAfee product with a disabled agent:

- 1 Export the repository list (SITELIST.XML) from the ePolicy Orchestrator server and copy it to a temporary folder on the system, such as `c:\TEMP`

For instructions, see [Exporting the repository list to a file on page 157](#).

- 2 Run the following command line on the desired system:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

`/SITEINFO` is the location of the SITELIST.XML file that you exported.

Reference the SITELIST.XML file in the temporary folder. By default, the FRMINST.EXE file is installed in the following location:

```
c:\program files\mcafee\common framework
```



Such products were most likely installed with an older version of the agent. These agents are *not* automatically upgraded to the latest agent version that is on the ePolicy Orchestrator server. To upgrade the agent, you should also enable and run the deployment task to install the new agent on the managed system.

For instructions, see [Upgrading agents version 3.x with ePolicy Orchestrator on page 87](#).

## Including the agent on an image

You can install the ePolicy Orchestrator agent on systems used to create common images for your environment. The first time the user logs into a system built using a common image that includes the agent, the system is assigned a unique ID called a *global unique identifier* (GUID).



Before creating an image for this purpose, remove the agent GUID registry value from the agent registry key. A GUID is regenerated on the first ASCII with the ePolicy Orchestrator server.

### When to use this method

This is a desirable method to use when:

- Your organization uses standard installation images for new systems.
- You may not have access to systems in some portions of your environment except when they are brought in for repair.

For instructions, see the documentation for your preferred image-creation product.

## Distributing the agent using other deployment products

You may already use other network deployment products in your organization to deploy software. You can use many of these tools, such as Microsoft Systems Management Server (SMS), IBM Tivoli, or Novell ZENworks, to deploy agents. Configure your deployment tool of choice to distribute the FRAMEPKG.EXE agent installation package located on your ePolicy Orchestrator server.

For instructions, see the documentation of the desired deployment tool.

For information about the agent installation package, see [The agent installation package on page 63](#).

## Distributing the agent to WebShield appliances and Novell NetWare servers

You cannot use ePolicy Orchestrator to deploy agents to WebShield appliances or Novell NetWare servers. Instead, use a method such as a login script or manual installation.



These systems require different agents, which can be downloaded from the McAfee web site. These agent installation packages are not installed on the ePolicy Orchestrator server by default.

See your product documentation for specific details.

---

## Upgrading existing agents

If you have been using an older version of ePolicy Orchestrator and have previous agent versions in your environment, you can upgrade those agents once you've installed your ePolicy Orchestrator 3.6 server. The procedure for upgrading the agent depends on which previous agent version is running on your managed systems.



Previous agent versions are not fully functional in ePolicy Orchestrator 3.6. For full agent functionality, you must upgrade to the latest agent version.

## Upgrading agent version 3.x using login scripts or manual installation

If you don't use ePolicy Orchestrator to deploy agents or products to managed systems, you can use your preferred agent distribution method to upgrade existing agents version 3.x to version 3.5. Upgrading agents without using ePolicy Orchestrator, such as upgrading manually or using network login scripts, is the same as installing agents for the first time. You must distribute the FRAMEPKG.EXE installation file and launch it on the system using your preferred method.

For instructions, see [Installing the agent with login scripts on page 80](#) or [Installing the agent manually on page 82](#).

## Upgrading the agent using ePolicy Orchestrator

If you use ePolicy Orchestrator to deploy agents in your network, the procedure differs slightly depending from which previous version of the agent you are upgrading.

### Best practices information

If you are upgrading your agent from a previous version, and your network is very large, consider the size of the agent installation package file and your available bandwidth before deciding how many agents to upgrade at once. Consider using a phased approach. For example, upgrade one site or group in your Directory at a time. In addition to balancing your network traffic, this approach makes tracking progress and troubleshooting issues easier.

If you upgrade agents version 2.5.1, change the upgrade policy setting for one site or group at a time, allow the upgrade to complete, then change the policy for another site or group. Repeat this until all agents are upgraded. If you're upgrading 3.0 agents using a client update task, consider scheduling the task to run at different times for different sites or groups in the Directory.

### Upgrading agents version 2.5.1 with ePolicy Orchestrator

To upgrade agents version 2.5.1 with ePolicy Orchestrator, you must adjust the agent policy settings:

- 1 In the console tree, select a site, group, or individual system whose agent(s) you want to upgrade to 3.5.
- 2 In the details pane, select the **Policies** tab, then expand the policy list to **ePO Agent 3.5.0 | Configuration**.
- 3 Click **Edit**, then click the icon next to the policy's name. The policy pages appear.

- 4 On the **General** tab, deselect **Inherit** to enable configuration options.
- 5 Select **Enable agent upgrade from 2.x to the current version**.
- 6 Click **Apply All** to save the change.

The next time agents of the specified Directory segment call into the server, the agent installation package is retrieved and upgrades the agent to the desired version.

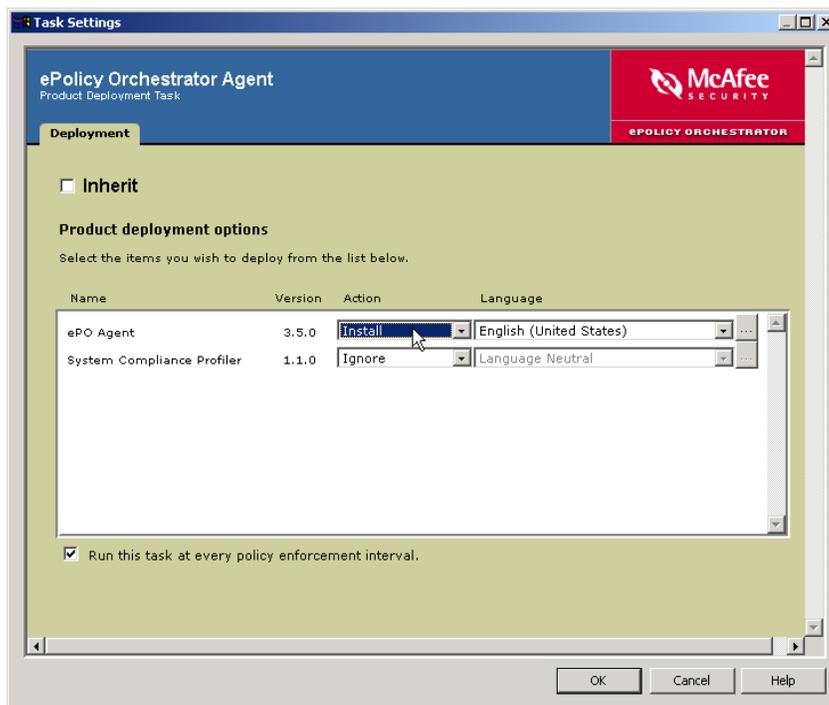
## Upgrading agents version 3.x with ePolicy Orchestrator

To provide more control over agent upgrades, you can run the deployment task. This is the same deployment task that can be used to deploy products such as VirusScan Enterprise or Desktop Firewall to systems that are already running agents.

To upgrade the agent version 3.x or later to version 3.5, configure and run the deployment task from the ePolicy Orchestrator console:

- 1 Make sure that the desired agent installation package is checked into the master software repository. The procedure is the same as checking in product packages.
- 2 Select the desired location of the Directory for which you want to upgrade the agent.
- 3 In the details pane, click the **Tasks** tab.
- 4 Double-click **Deployment** in the list.
- 5 On the **Task** tab, deselect **Inherit** and select **Enable (scheduled task runs at specified time)**.
- 6 Click **Settings**.
- 7 On the **Task Settings** dialog box, deselect **Inherit**.

Figure 4-5 Task Settings dialog box



- 8 Click **OK**.
- 9 Click the **Schedule** tab and schedule the task appropriately.
- 10 When finished, click **OK** to close the **ePolicy Orchestrator Scheduler** dialog box.

The deployment task's **Enabled** status is **True**. Agents on managed systems pick up the task information the next time the agents call into the server and run the task at the scheduled time.

#### Best practices information

You can use the deployment task to upgrade agents released in the future. McAfee releases newer versions of the agent periodically. You can deploy and manage these newer versions of the agent with ePolicy Orchestrator. When available, you can download the agent installation package from the McAfee update site and check it into the master repository. Then utilize the deployment task to upgrade the agents.



Upgrading the agent using the deployment task is not the same as updating an existing agent using the ePolicy Orchestrator Agent Update task. Upgrading the agent using the deployment task is for installing a new version of the agent over an older one, such as installing the agent version 3.5 over the version 3.0x. The update task is used to update an existing version of the agent with additional updates, such as DAT files and patches, or updating the agent version 3.0.1 to version 3.02.

---

## Uninstalling the agent

You can uninstall the ePolicy Orchestrator agent from a system using one of three methods:

- [Running FRMINST.EXE from a command line on page 88.](#)
- [Uninstalling the agent by removing systems from the Directory on page 88.](#)
- [Uninstalling the agent from systems after a Directory search on page 89.](#)



You cannot remove the agent using the deployment task, which you use to remove other products, such as VirusScan Enterprise.

## Running FRMINST.EXE from a command line

Uninstall the agent from a command line by running the agent framework installation (FRMINST.EXE) program with the `/REMOVE` command-line option.

## Uninstalling the agent by removing systems from the Directory

To remove the agent from one or more systems using the ePolicy Orchestrator console, delete the system from the Directory and select the option to uninstall the agent. You can delete sites, groups, or individual systems with this method.



Know that when you delete a group or site, all child groups and systems are also deleted. If you select the **Uninstall agent from all connected computers** option when deleting systems, ePolicy Orchestrator uninstalls agents from all child systems.

To remove the agent from systems in the Directory:

- 1 In the console tree, right-click the desired site, group, or system, then select **Delete**.
- 2 Select **Uninstall agent from all connected computers**.
- 3 Click **Yes**.

## Uninstalling the agent from systems after a Directory search

You can remove the agent from desired systems after finding them using one of the Directory search queries. These search queries are available in the ePolicy Orchestrator console.

To remove an agent from a system that is returned in a Directory search:

- 1 Right-click the desired system name in the list of **Search Results** at the bottom of the **Directory Search** dialog box, then select **Delete**.
- 2 In the confirmation dialog box, select **Uninstall agent from all connected computers**.
- 3 Click **Yes**.

The agent is uninstalled after the next agent-server communication.

---

## Maintaining the agent

Although you have already distributed the agent to the desired systems, there are some tasks you may need to perform to ensure all of your agents are up-to-date and functioning as you expect.

The tasks described in this section are those you may need to perform on a regular basis to ensure systems are running active, up-to-date agents.

## Sending manual agent and SuperAgent wakeup calls

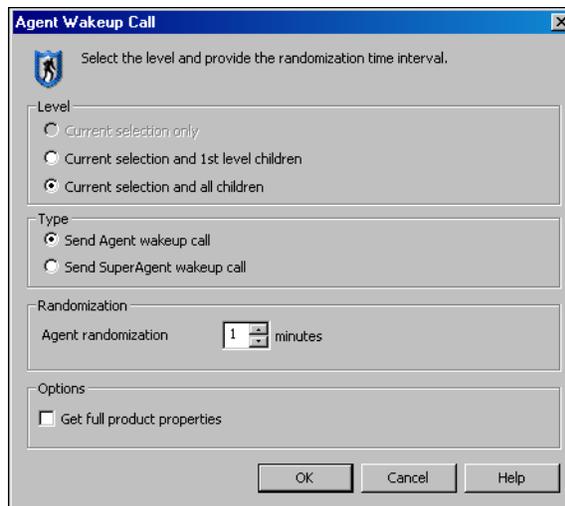
You can send a manual agent or SuperAgent wakeup call to any site, group, or individual system in the Directory. This is useful when you have made policy changes or checked in updates to the master repository and you want agents to call in for an update.

Before sending the agent wakeup call to a Directory segment, make sure that wakeup support for that node is enabled and applied on the **General** tab of the **ePO Agent 3.5.0 | Configuration** policy pages (enabled by default).

To send an agent or SuperAgent wakeup call:

- 1 In the console tree, right-click the desired site, group, or system, then select **Agent Wakeup Call**. The **Agent Wakeup Call** dialog box appears.

**Figure 4-6 Agent Wakeup Call**



- 2 Select the **Level** at which you want to send the agent wakeup call. Typically, send to the default, which is the selected node and all children.
- 3 Under **Type**, select **Send Agent wakeup call** or **Send SuperAgent wakeup call**, depending on your needs.
- 4 Accept the default or type a different **Agent randomization interval** (0 - 60 minutes). If you type 0, agents on all selected systems respond immediately.
- 5 Typically, the agent sends only properties that have changed since the last agent-to-server communication. To send the complete properties, select **Get full product properties**.
- 6 Click **OK** to send the agent or SuperAgent wakeup call.

## Sending scheduled agent wakeup calls

To create a scheduled agent wakeup call:

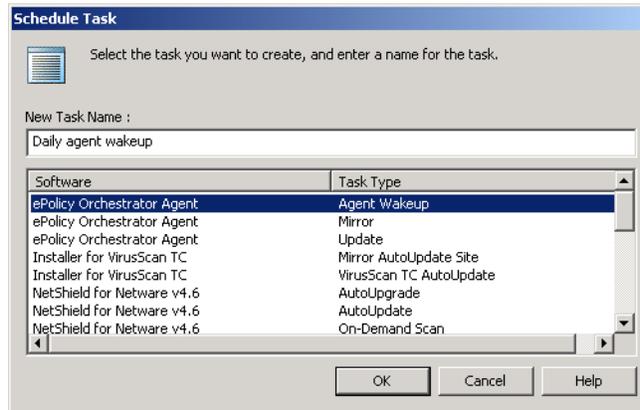


SuperAgent wakeup calls cannot be scheduled.

- 1 In the console tree, right-click the desired site, group, or system, then select **Schedule Task**.

- In the **Schedule Task** dialog box, type a descriptive name for the task, such as `Daily agent wakeup`, in the **New Task Name** field.

**Figure 4-7 Schedule Task dialog box**



- Select **ePolicy Orchestrator Agent | Agent Wakeup** from the list of available tasks, then click **OK**.
- Refresh the console and make the new task appear in the list on the **Task** tab.
 

Note that it is scheduled to run daily at the current day and time. Also note that the **Enabled** flag is set to **False**. You now need to set this to **True** and schedule it to run daily.
- Right-click the new task in the task list and select **Edit Task** to edit the task in the **ePolicy Orchestrator Scheduler** dialog box.
 

By default, the agent returns only incremental properties that have changed since the last agent-to-server communication. To have the agent send full properties when it receives the wakeup call, click **Settings** on the **Task** tab in the **ePolicy Orchestrator Scheduler** dialog box, deselect **Inherit** in the **Task Settings** dialog box, and select **Collect full properties**. Click **OK** when done.
- Under **Schedule Settings** on the **Task** tab of the **ePolicy Orchestrator Scheduler** dialog box, deselect **Inherit**.
- Select **Enable** to define the scheduling options. If you do not select this, the task does not start.
- Click the **Schedule** tab of the **ePolicy Orchestrator Scheduler** dialog box to specify when the task runs.
- Deselect **Inherit**.
- Set the **Schedule Task** option to run **Daily**. To run the task multiple times a day, click the **Advanced** button, select **Repeat Task** and set the task to repeat every X hours, such as every 12 hours for twice a day or every 8 hours for three times a day.
- Click **OK** when you have finished configuring and scheduling the task.

When complete, the scheduled task appears in the list of available tasks on the **Task** tab of the selected Directory node. The **Enabled** flag is now set to **True**. The task runs at the next scheduled time.

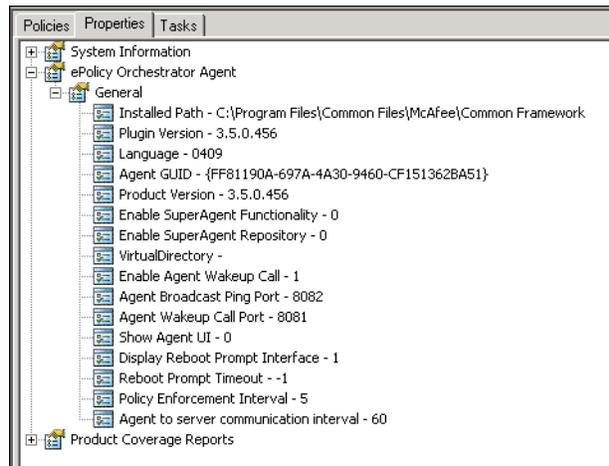
## Viewing properties of the agent and products from the console

When troubleshooting problems a great first step is to verify that the properties match the policy changes you have made. The properties available depend on whether you configured the agent to send full or minimal properties on the **ePO Agent 3.5.0 | Configuration** policy pages.

To view properties for a selected system:

- 1 In the console tree, select the desired system.
- 2 In the upper-details pane, select the **Properties** tab to display properties for the selected system.

**Figure 4-8 Properties for selected computers**



- 3 Expand the desired property types to view details of specific properties. Properties for the agent are listed under the **ePolicy Orchestrator Agent**.

## Viewing the agent activity logs

Agent activity logs record an agent's activity. The amount of detail depends on the policy settings you selected on the **Logging** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

These log files can be viewed from the managed system or remotely.

### Viewing agent activity log files from the managed system

To view the agent activity log from the system on which the agent is installed:

- 1 Right-click the agent icon in the system tray.



The agent icon is available in the system tray only if the **Show agent tray icon** option is selected on the **General** tab of the **ePO Agent 3.5.0 | Configuration** policy pages. If it is not visible, select this option and apply it. When you finish viewing the log file content, you can hide the icon again by deselecting the option and applying the change.

- 2 Select **Status Monitor** from the menu. When the status monitor appears, the agent activity log is displayed.

- 3 Close the status monitor when finished.

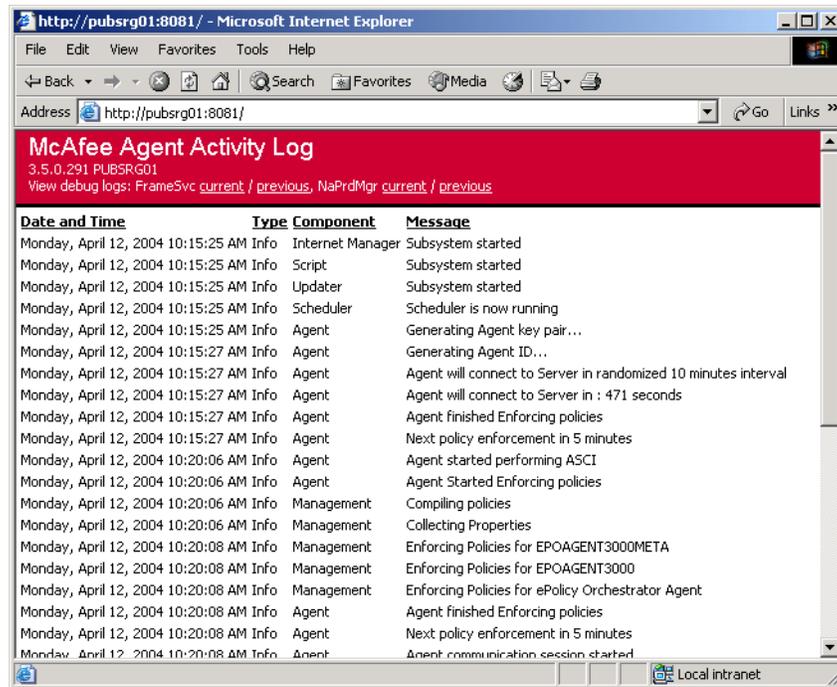
## Viewing agent activity log files remotely

You can view agent activity log files of another system remotely through a web browser. This is useful when you are at the server and want to view the current status of a managed system.

To view activity log files in a web browser:

- 1 Open a web browser and type the computer name and port number used for agent wakeup call (8081 by default) in the format: `http://MyComputer:8081/`

Figure 4-9 Agent activity log



You can determine the agent wakeup call port for a selected system on the **ePolicy Orchestrator Agent | General** properties for the selected system.

- 2 To view the detailed agent activity log file, click **current** to view either the FRAMESVC.EXE or NAPRDMGR.EXE detailed logs.
- 3 To view the backup copy of the FRAMESVC.EXE or NAPRDMGR.EXE detailed log, click **previous**.



Although remote viewing of log files is enabled by default, you can disable remote viewing of the log files. If you can't view the log remotely, verify that the **Enable remote access to log** option is selected on the **Logging** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

## Agent tasks on the managed system

Although you can control each aspect of the agent functionality from the ePolicy Orchestrator console on the ePolicy Orchestrator server, you can also perform selected tasks from the system where the agent is installed.

If you can access the client system where the agent is installed, you can view and manage some aspects of the agent functionality through the agent interface.



The agent user interface is available on the managed system only if you selected **Show agent tray icon** on the **General** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

### Running an update task

To run an update task from the managed system:

- 1 Right-click the agent tray icon.
- 2 Select **Update Now**. The agent performs an update from the nearest repository. Product updates include:
  - Patch releases
  - Legacy product plug-in (.DLL) files.
  - Service pack releases.
  - SuperDAT (SDAT\*.EXE) packages.
  - Supplemental virus definition (EXTRA.DAT) files.
  - Virus definition (DAT) files.

### Sending full properties to the server

To send full properties to the server from the managed system:

- 1 Right-click the agent icon in the system tray of the desired system, and select **Status Monitor**. The **ePolicy Orchestrator Agent Monitor** appears.
- 2 Click **Collect and Send Props**.

### Sending events to the server immediately

To send events to the server immediately from the managed system:

- 1 Right-click the agent icon in the system tray of the desired system, and select **Status Monitor**. The **ePolicy Orchestrator Agent Monitor** appears.
- 2 Click **Send Events**.

## Updating policies

To prompt the agent from the managed system to call into the server for updated policy settings:

- 1 Right-click the agent icon in the system tray of the desired system, and select **Status Monitor**. The **ePolicy Orchestrator Agent Status Monitor** appears.
- 2 Click **Check New Policies**.

## Enforcing policies

To prompt the agent from the managed system to enforce all configured policies on the managed system:

- 1 Right-click the agent icon in the system tray of the desired system, and select **Status Monitor**. The **ePolicy Orchestrator Agent Status Monitor** appears.
- 2 Click **Enforce Policies**.

## Viewing agent settings

To view the agent settings from the managed system, right-click the agent icon in the system tray of the desired system, and select **Settings**.

Agent settings include:

- Agent ID.
- System name.
- User name of the logged-in user.
- Policy enforcement interval.
- ASCII.

**Table 4-4 Agent Status Monitor options**

Task Option	Description
<b>Collect and Send Props</b>	Send full properties to the server. This updates the properties displayed in the console. See <a href="#">Viewing properties of the agent and products from the console on page 92</a> .
<b>Send Events</b>	Immediately sends events to the server.
<b>Check New Policies</b>	Agent calls into the server to see if any policies have changed. If so, it downloads the new policy settings.
<b>Enforce Policies</b>	Enforces policies set on the server locally on the client system.
<b>Agent Settings</b>	View selected agent settings.
<b>Save contents</b>	Saves the current contents of the agent activity log file.

## Viewing agent and product version numbers

Looking up the agent and version product numbers from the managed system is useful to troubleshoot problems when installing new agent versions or confirming that the version of the agent installed is the same as the version displayed in the agent properties on the server.

To view the product version numbers of the agent and installed security products, right-click the agent system tray icon, then select **About**.

## Command Agent command-line options

You can use the Command Agent (CMDAGENT.EXE) tool to perform selected agent tasks remotely. CMDAGENT.EXE is installed on the managed system at the time of agent installation. You can perform these same tasks locally on client systems using this program or the agent system tray icon.

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

```
c:\program files\mcafee\common framework
```

**Table 4-5 CMDAGENT.EXE command-line options**

Option	Description
/C	Checks for new policies. This command has the agent contact the ePolicy Orchestrator server for new or updated policies, then enforce them immediately upon receipt.
/E	Prompt the agent to enforce policies locally.
/P	Send properties and events to the ePolicy Orchestrator server.
/S	Displays the agent monitor.

## Locating inactive agents

An inactive agent is an agent that has not communicated with the ePolicy Orchestrator server within a user-specified time period. Some agents may become disabled or be uninstalled by end users. In other cases, the system hosting the agent may have been removed from the network. McAfee recommends performing regular weekly searches for systems with these inactive agents.

When you find inactive agents, determine whether the system is still on the network. If the system is still on the network but the agent is inactive, re-install the agent. If the system has been removed from the network, you can delete the system from your Directory.

The most reliable method to determine inactive agents is to schedule a regular Inactive Agent Maintenance task. In addition to locating inactive agents, you can configure the task to move any systems with inactive agents to a special group for this purpose. You can check this group periodically and take remediating action on any system moved into this group, such as deleting the system from the Directory or re-installing the agent on the system.

To schedule a regular task to locate inactive agents.

- 1 In the console tree, select the ePolicy Orchestrator server.
- 2 In the details pane, select the **Scheduled Tasks** tab, then click **Create Task**.

- 3 On the **Configure New Task** page, under **Task settings**, type a descriptive name for the task in the **Name** field, such as `Daily inactive agent maintenance task`.

Figure 4-10 Task settings

- 4 Select **Inactive Agent Maintenance** from the **Task Type** drop-down list.
- 5 Select **Yes** next to **Enable task**.
- 6 Select **Daily** from the **Schedule type** drop-down list. You can also select other schedule types.
- 7 Click **Next** at the top of the page.
- 8 On the **Inactive Agent Maintenance Task** page, type the number of days that should define an inactive agent in **Period of inactivity**. Use the default of 10 days unless you have specific reasons for changing it.

Figure 4-11 Inactive Agent Maintenance Task page

- 9 To move systems with inactive agents to another group, select **Move** under **Action to perform**.

**10** Type the name of a group to which any systems with inactive agents should be moved in the **Move computers with inactive agents to this group** field. If this group doesn't already exist, it is created when the task runs.

**11** Click **Finish**.

The new task appears in the **Scheduled Tasks tab** list, and the next time the task is scheduled to run is under **Next Run Time**. You can run the task manually at any time by selecting the task in the list and clicking **Run Now**.

# 5

## Creating Repositories

### Ensure systems receive products and updates

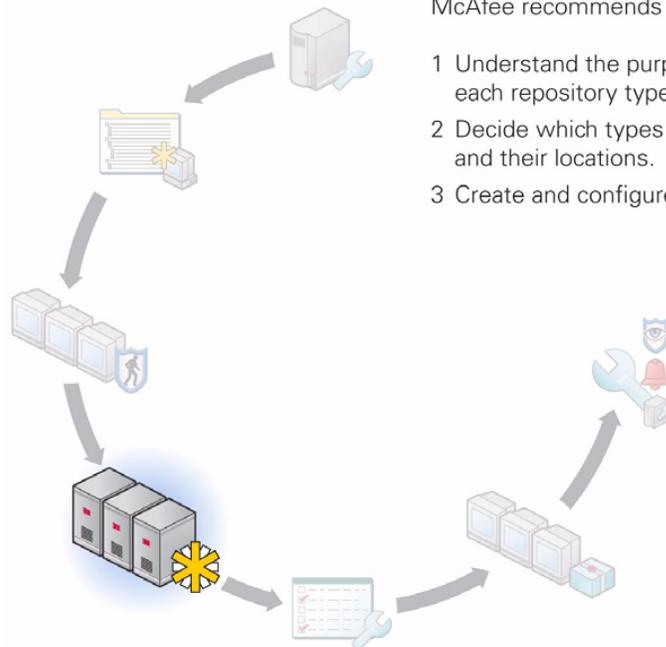
Security software is only as effective as the latest installed updates. For example, if your DAT files are out-of-date, even the best anti-virus software cannot detect new threats. It is critical that you develop a robust updating strategy to keep your security software as up-to-date as possible.

ePolicy Orchestrator software's repository architecture offers flexibility to ensure deploying and updating software is as easy and automated as your environment allows. Once your repository infrastructure is in place, create update tasks that determine how, where, and when your software is updated.

#### Creating repositories for the first time?

When creating repositories for the first time, McAfee recommends to:

- 1 Understand the purpose and function of each repository type and repository branch.
- 2 Decide which types of repositories to use and their locations.
- 3 Create and configure the repositories.



---

## About repositories

To deliver products and updates throughout your network, McAfee offers several types of repositories to create a robust update infrastructure. These provide the flexibility to develop an updating strategy to ensure your systems stay up-to-date.

### The repository list

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

If needed, you can export the repository list to an external (SITEMGR.XML) file, then distribute and apply it to managed systems using command-line options. An exported repository list file can be used to:

- Back up your repository list if you need to reinstall the ePolicy Orchestrator server.
- Import to a product at installation; for example, VirusScan Enterprise.
- Import to an agent at installation.
- Import an existing repository list from a previous installation of ePolicy Orchestrator or from another McAfee product.

### Master repository

The master software repository maintains the latest versions of security software and updates for your environment. This repository is the source of software and updates for the rest of your environment. There is only one master repository for each ePolicy Orchestrator server.

The master repository is configured when installed. However, you must ensure that proxy server settings are configured correctly. By default, ePolicy Orchestrator uses Microsoft Internet Explorer proxy settings.

#### Proxy settings

If a source repository must be accessed via the Internet, such as the McAfee update sites, the master repository uses proxy settings to retrieve packages. If your organization uses proxy servers for connecting to the Internet, you must use the proxy server.

You must also configure agent policy settings for managed systems to use proxy servers to access the fallback site.

By default, ePolicy Orchestrator is configured to use the proxy settings for the Internet Explorer browser that is installed on your ePolicy Orchestrator server. Therefore, you must make sure that the Internet Explorer proxy settings are configured correctly, and then confirm that ePolicy Orchestrator is configured to use those proxy settings.



If you choose to use Internet Explorer proxy settings, a user must be logged onto the ePolicy Orchestrator server for the scheduled tasks to run. If you do not want to leave an account logged onto the server (even if locked), you must manually enter proxy authentication information.

To confirm that Internet Explorer's proxy settings are configured correctly, open an instance of Internet Explorer on the ePolicy Orchestrator server and browse to a publicly accessible web site, such as your organization's home page or to [www.mcafee.com](http://www.mcafee.com). If you can access these sites, your proxy settings are correct.

## Source repository

The source repository provides all updates for your master repository. The default source repository is the McAfee HTTP update site (HttpSite), but you can change the source repository or even configure multiple source repositories if you require. McAfee recommends using the McAfee HTTP (HttpSite) or FTP (FTPSite) update sites as your source repository.



Source repositories are not required. You can download updates manually and check them into your master repository. However, using a source repository automates this process.

McAfee posts software updates to these sites regularly. For example, DAT files are posted daily. Update your master repository with updates as they are available.

Use pull tasks to copy source repository contents to the master repository.

The McAfee update sites provide virus definition (DAT) and scanning engine file updates only. All other packages and updates must be checked into the master repository manually.

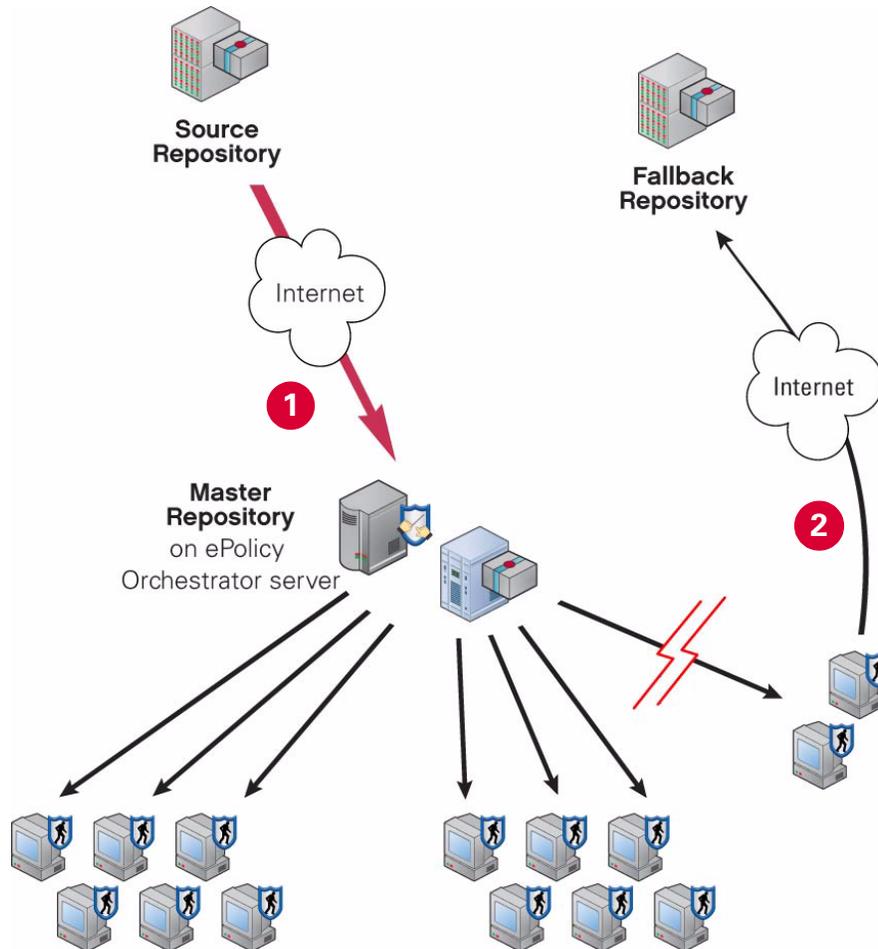
## Fallback repository

The fallback repository is a repository from which managed systems can retrieve updates when their usual repositories are not accessible. For example, when network outages or virus outbreaks occur, accessing your established update infrastructure may be difficult. Therefore, managed systems can remain up-to-date in such situations. The default fallback repository is the McAfee FTP download site (FTPSite). You can only define one fallback repository.

## Master, source, and fallback repositories working together

The master, source, and fallback repositories are designed to work together in your network environment.

**Figure 5-1 Master, source, and fallback repositories**



- 1** The master repository regular pulls DAT and engine update files from the source repository.
- 2** If client systems are unable to access the master repository, they can receive updates from the fallback repository.

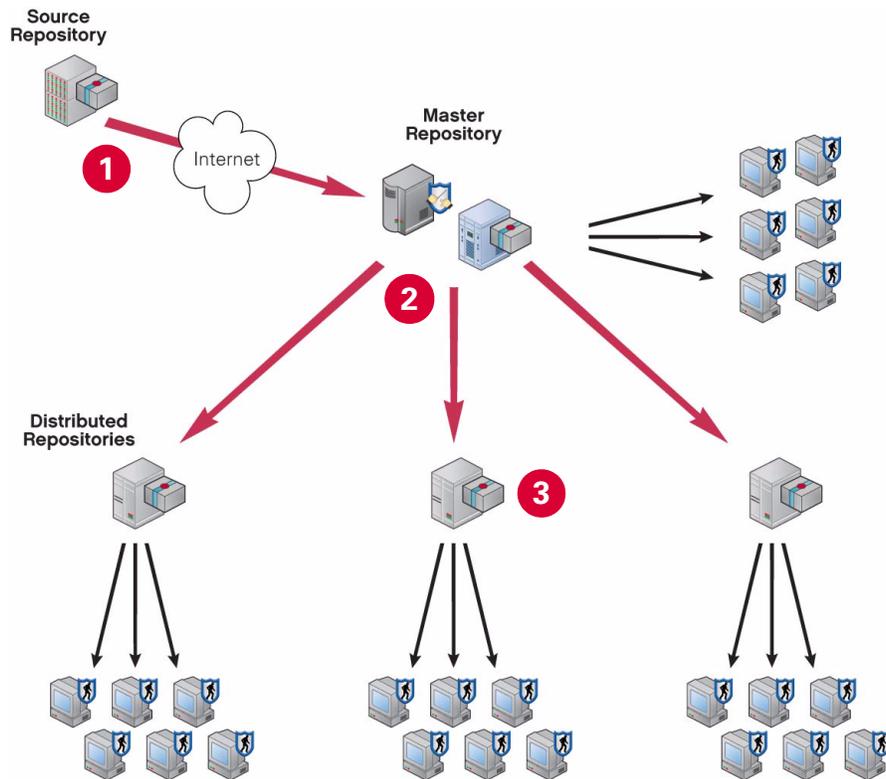
## Distributed repositories

Distributed repositories host copies of your master repository contents. Consider using distributed repositories and placing them throughout your network strategically to ensure managed systems are updated while network traffic is minimized, especially across slow connections.

As you update your master repository, ePolicy Orchestrator replicates the contents to the distributed repositories, instead of to each system.

A large organization can have multiple locations with limited bandwidth connections between them. Distributed repositories limit updating traffic across low-bandwidth connections. If you create a distributed repository in the remote location and configure the systems within the remote location to update from this distributed repository, the updates are copied across the slow connection only once — to the distributed repository — instead of once to each system in the remote location.

**Figure 5-2 Distributed repositories in your environment**



- 1 The source repository provides update files for the master repository.
- 2 The master repository distributes the updates to client systems in the local LAN, and to distributed repositories in the greater network.
- 3 The client systems in the greater network retrieve updates from the closest distributed repository.

### Systems to use for distributed repositories

Use an existing server to host the distributed repository. Although you do not need to use a dedicated server, the server should be large enough for the desired systems to connect for updates. Servers are better than workstations because they are more likely to be running all the time.

## Types of distributed repositories

ePolicy Orchestrator supports four different types of distributed repositories. Consider your environment and needs when determining which type of distributed repository to use. You are not limited to using one type, and may have the need to use several, depending on the nature of your network.

### SuperAgent repositories

Use systems hosting SuperAgents as distributed repositories. If global updating is enabled, SuperAgent repositories update managed systems automatically as soon as selected updates and packages are checked into the master repository. You do not need to spend additional time creating and configuring repositories or the update tasks.



McAfee recommends using SuperAgent repositories and global updating together to ensure your managed environment is up-to-date.

SuperAgent repositories have several advantages over other types of distributed repositories:

- Folder locations are created automatically on the host system before adding the repository to the repository list.
- File sharing is enabled automatically on the SuperAgent repository folder.
- SuperAgent repositories don't require replication or updating credentials.



Although SuperAgent broadcast wakeup call functionality requires a SuperAgent in each broadcast segment, this is not a requirement for SuperAgent repository functionality. Managed systems only need to "see" the system hosting the repository.

SuperAgent's and global updating utilize a proprietary protocol, SPIPE.

### FTP repositories

If you are unable to utilize SuperAgent repositories, you can use an existing FTP server to host a distributed repository. Use your existing FTP server software such as Microsoft Internet Information Services (IIS) to create a new folder and site location for the distributed repository. See your web server documentation for details to create a site.

### HTTP repositories

If you are unable to utilize SuperAgent repositories, you can use an existing HTTP server to host a distributed repository. Use your existing HTTP server software such as Microsoft Internet Information Services (IIS) to create a new folder and site location for the distributed repository. See your web server documentation for details to create a site.

### UNC share repositories

If you are unable to utilize SuperAgent repositories, create a UNC shared folder to host a distributed repository on an existing server. Be sure to enable sharing across the network for the folder so that the ePolicy Orchestrator server can copy files to it.

## Unmanaged repositories

If you are unable to use managed distributed repositories, ePolicy Orchestrator administrators can create and maintain distributed repositories that are not managed by ePolicy Orchestrator.

If a distributed repository is not managed, a local administrator must keep the repository up-to-date manually.

Once the distributed repository is created, you can use ePolicy Orchestrator to configure managed systems of a specific Directory site or group to update from it.



McAfee recommends that you manage all distributed repositories through ePolicy Orchestrator. Managing distributed repositories with ePolicy Orchestrator and using global updating, or scheduled replication tasks frequently ensures your managed environment is up-to-date. Only use non-managed distributed repositories if your network or organizational and policy do not allow them.

## About repository branches

ePolicy Orchestrator provides three repository branches, allowing you to maintain three versions of update files in your master or distributed repositories. The repository branches are Current, Previous, or Evaluation. By default, ePolicy Orchestrator only uses the Current branch. You can specify branches when adding packages to your master repository. You can also specify branches when running or scheduling update and deployment tasks to distribute different versions to different parts of your network.

Update tasks can retrieve updates from any branch of the repository, but deployment tasks use the Current branch only.

### Current branch

The current branch is the main repository branch for the latest packages and updates. Product deployment packages can be added only to the Current branch.

### Evaluation branch

You may want to test new DAT and engine updates with a small number of network segments or systems before deploying them to your entire organization. Specify the Evaluation branch when checking in new DATs and engines to the master repository, then deploy them to a small number of test systems. After monitoring the test systems for several hours, you can add the new DATs to your Current branch and deploy them to your entire organization. See [Evaluating new DATs and engines before distribution on page 161](#) for complete details on how to use the Evaluation branch feature.

### Previous branch

Use the Previous branch to save and store the prior week's DAT and engine files before adding the new ones to the Current branch. In the event that you experience an issue with new DAT or engine files in your environment, you have a copy of previous versions that you can re-deploy to your systems if necessary. ePolicy Orchestrator saves only the most immediate previous version of each file type.

You can enable the Previous branch feature by selecting **Move existing packages to the 'previous' branch** when you add new files to your master repository. The option is available both when you pull updates from a source repository and when you manually check in packages to your master repository.

For more information, see [Checking in engine, DAT and EXTRA.DAT updates manually on page 157](#).

---

## Creating and configuring your repositories

Once you have planned your implementation of the update repositories, you can begin creating and configuring them.

### Configuring proxy settings

For both master repository and managed systems, you must ensure the Internet can be accessed when using the HttpSite and the FTPSite sites as source and fallback repositories. McAfee recommends using the Internet Explorer proxy server settings.

You can also configure proxy servers from within the ePolicy Orchestrator console. You may need to do this if you cannot have ePolicy Orchestrator use the proxy settings in your Internet Explorer browser or if you do not use a proxy server.

### Using Internet Explorer proxy settings for the master repository

To use the Internet Explorer proxy settings

- 1 [Configure Internet Explorer proxy settings](#).
- 2 [Configure ePolicy Orchestrator to use Internet Explorer proxy settings](#).



If you choose to use Internet Explorer proxy settings, a user must be logged onto the ePolicy Orchestrator server for the scheduled tasks to run. If you do not want to leave an account logged onto the server (even if locked), you should manually enter proxy authentication information.

### Configure Internet Explorer proxy settings

If you cannot access the Internet from the ePolicy Orchestrator server with your browser, configure your Internet Explorer LAN connection and proxy configuration:

- 1 Launch Internet Explorer.
- 2 Select **Tools | Internet Options** from the menu bar.
- 3 Select the **Connections** tab, then select **LAN Settings** at the bottom of the dialog box.
- 4 In the **LAN Settings** dialog box, select **Use a proxy server for your LAN**.
- 5 Click **Advanced**. The **Proxy Settings** dialog box appears.
- 6 Type proxy information into the appropriate fields. If you plan to use the default source and fallback repositories, be sure to enter the information for HTTP and FTP.
- 7 Select **Use the same proxy for all protocols** so both FTP and HTTP correctly use the proxy.

- 8 Click **OK** to close the **Proxy Settings** dialog box.
- 9 Select **Bypass proxy for local addresses** options. This allows you to correctly view HTML-based sections of the ePolicy Orchestrator console.
- 10 Click **OK** to close the **LAN Settings** dialog box.
- 11 Click **OK** to close the **Internet Options** dialog box.

### Configure ePolicy Orchestrator to use Internet Explorer proxy settings

ePolicy Orchestrator is, by default, configured to use the Internet Explorer proxy settings. To verify:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Configure proxy settings**. The **Edit** proxy dialog appears.
- 3 Ensure the **Use Internet Explorer proxy settings** option is selected.
- 4 Click **OK**.

### Configuring proxy settings for the master repository

To manually configure ePolicy Orchestrator proxy settings:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Configure proxy settings**. The **Edit Proxy** dialog box appears, select **Manually configure the proxy settings**.

If your ePolicy Orchestrator server does not need a proxy to access the Internet, select **Don't use proxy**.

- 3 Click the **Servers** tab. The **Servers** tab doesn't appear until you select **Manually configure the proxy settings**.
- 4 Type the address and port number of the proxy server you want to use to gain access to distributed repositories using HTTP or FTP protocols. In **Address**, type the IP address or fully-qualified domain name of the proxy server. In **Port**, type the port number of the proxy server.



If you are using the default source and fallback repositories, or if you configure another HTTP source repository and FTP fallback repository (or vice versa), configure both HTTP and FTP proxy authentication information here.

- 5 To specify distributed repositories to which the server can connect directly, select **Bypass Local Addresses**, then type the IP addresses or fully-qualified domain name of those systems separated by a semi-colon (;).
- 6 Click the **Authentication** tab.
- 7 Configure the proxy authentication settings as appropriate, depending on whether you pull updates from HTTP repositories, FTP repositories, or both.
- 8 Click **OK** to save your proxy settings.

## Configuring source and fallback repositories

You must be a global administrator to define, change, or delete source or fallback repositories. You can change settings, delete existing source and fallback repositories, or switch between them.

McAfee recommends using the default source and fallback repositories. If your needs require different repositories for this purpose, you can create new ones.

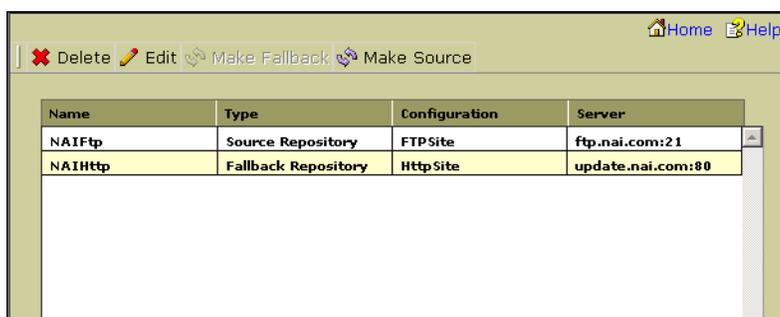
### Switching source and fallback repositories

Depending on your network configuration, you may find that HTTP or FTP updating works better. Therefore, you may want to switch the source and fallback repositories. You must be a global administrator to define source or fallback repositories.

To switch the source and fallback repositories:

- 1 In the console tree, select **Repository**.
  - a In the details pane, select **Source Repository** to access the **Source and Fallback Repositories** page, which lists the configured source and fallback repositories.

**Figure 5-3 Source and Fallback Repositories page**



Name	Type	Configuration	Server
NAIFtp	Source Repository	FTP Site	ftp.nai.com:21
NAIHttp	Fallback Repository	Http Site	update.nai.com:80

- 2 Select the source repository from the list, then click **Make Fallback**.

### Adding source repositories

You must be a global administrator to add source repositories.

To add a source repository:

- 1 In the console tree, select **Repository**.
- 2 In the details pane under **AutoUpdate Tasks**, click **Add source repository**. The **Add repository** wizard appears.

- 3 Click **Next** to open the repository configuration panel.

**Figure 5-4 Add repository wizard – repository configuration dialog box**

ePolicy Orchestrator™ -- Web Page Dialog

### Wizard: Add repository

Enter a repository name and select the repository type to add.

Name

Type

Choose the repository configuration.

FTP  
 HTTP  
 UNC

**FTP**  
 Choose this option if your repository resides on an FTP server

To continue, click **Next**.

McAfee SECURITY

Back Next Finish Cancel Help

- 4 Type a descriptive name for this repository in the **Name** field. Repository names must be unique.
- 5 Select **Source Repository** from the **Type** drop-down list.
- 6 Specify the type of server or path (**FTP**, **HTTP**, or **UNC**) of the repository, then click **Next**.
- 7 In the protocol configuration panel, provide the address and port information of the repository, then click **Next**.

**Figure 5-5 Add repository wizard – FTP protocol configuration dialog box**

ePolicy Orchestrator™ -- Web Page Dialog

### Wizard: Add repository

Enter the replication credentials.

Username

Password  Verify

Re-Enter Password

**Replication credentials**  
 The replication credentials are used to check in software updates on the master repository. Supply credentials with both read and write access to the FTP server that hosts the repository.

To continue, click **Next**.

McAfee SECURITY

Back Next Finish Cancel Help

- If you selected **FTP** in [Step 6](#), type the web address in **URL** and the FTP port number in **Port**.

- If you selected **HTTP** in [Step 6](#), type the web address in **URL** and the HTTP port number in **Port**.
  - If you selected **UNC** in [Step 6](#), type the network directory where the repository resides in **Path**. Use this format: \\<COMPUTER>\<FOLDER>. You can use variables to define this location. For a list, see [Variables on page 393](#).
- 8** Provide the download credentials used by managed systems to connect to this repository, then click **Next**. Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository.
- If you selected **FTP** in [Step 6](#), select **Use anonymous login** or type the user account information in **User name**, **Password**, and **Re-Enter Password**.
  - If you selected **HTTP** in [Step 6](#) and the HTTP server requires authentication, select **Use Authentication**, then type the user account information in **User name**, **Password**, and **Re-Enter Password**.
  - If you selected **UNC** in [Step 6](#), select **Use Logged On Account** or type the user account information in **Domain**, **User name**, **Password**, and **Confirm password**.
- To authenticate the user account you specified, click **Verify**.
- 9** Click **Finish** to add the repository to the repository list.
- 10** After the repository is added, click **Close**.

## Creating SuperAgent repositories

To create SuperAgent repositories, agents must be distributed to the systems you want to host SuperAgent repositories. You cannot create these until after agents have been distributed to the desired systems.

To create a SuperAgent repository:

- 1** In the console tree, select the desired system on which to create a SuperAgent repository.
- 2** In the details pane, select **ePO Agent 3.5.0 | Configuration**.
- 3** Click **Edit**, then click the policy name. The policy pages appear.
- 4** Select the **General** tab, then deselect **Inherit**.
- 5** If the system is not already hosting a SuperAgent, select **Enable SuperAgent functionality** to convert the agent into a SuperAgent.
- 6** Select **Enable SuperAgent repository**.
- 7** Type a folder path location for the repository. This is the location to which the master repository copies updates during replication. You can use standard Windows variables, such as <PROGRAM\_FILES\_DIR>.



Managed systems updating from this SuperAgent repository are able to access this folder. You do not need to manually enable file sharing.

- 8** Click **Apply All** at the top of the dialog box.

The next time the agent calls into the server, the new configuration is retrieved. When the distributed repository is created, the folder you specified is created on the system if it did not already exist. If ePolicy Orchestrator cannot create the folder you specify, it creates one of two folders:

- <DOCUMENTS AND SETTINGS>\ ALL USERS\APPLICATION  
DATA\MCAFFEE\FRAMEWORK\DB\SOFTWARE
- <AGENT INSTALLATION PATH>\DATA\DB\SOFTWARE

In addition, the location is added to the repository list (SITELIST.XML) file. This makes the site available for updating by systems in your Directory.

### Choosing packages that are replicated to SuperAgent repositories

ePolicy Orchestrator 3.6 provides the ability to choose to which repository specific packages are replicated.

To specify which packages get replicated to a SuperAgent repository:

- 1 In the console tree, select **Repository | Software Repositories**.
- 2 Select the desired distributed repository from the list, then click **Edit**. The dialog box appears.
- 3 Select the **Packages** tab.
- 4 Choose **Select the following packages**, then deselect all package types that you do not want replicated to this repository.



The ability to select only specific package-types for replication to individual repositories is new to ePolicy Orchestrator 3.6.



Ensure that all packages required by any managed system that uses this repository is not deselected. Managed systems go to one repository for all packages — the task fails for any system that are expecting to find a package type that is not present in the repository. This feature was designed to ensure packages that are used by a few systems only and do not require replication throughout your entire environment.

- 5 Click **OK**.

## Creating FTP, HTTP, and UNC file server repositories

You can use existing FTP, HTTP, or UNC file servers to host distributed repositories, allowing you to use standard protocols and existing servers.

To create any of these distributed repositories, follow these steps:

- 1 [Create a folder location on an existing FTP, HTTP, or UNC server.](#)
- 2 [Enable folder sharing for UNC and HTTP sites on page 112.](#)
- 3 [Create the distributed repository in ePolicy Orchestrator on page 112.](#)

You must be a global administrator to create repositories.

## Create a folder location on an existing FTP, HTTP, or UNC server

The first step in creating an HTTP, FTP, or UNC distributed repository is to create the folder location on the desired system for the distributed repository.

For UNC repositories, create the folder on the system and enable sharing.

For FTP or HTTP repositories, you can use your existing FTP or HTTP server software, such as Microsoft Internet Information Services (IIS), to create a new folder and site location for the distributed repository. See your web server documentation for details to create a site.

When complete, go to [Enable folder sharing for UNC and HTTP sites](#).

## Enable folder sharing for UNC and HTTP sites

For HTTP and UNC repositories, ePolicy Orchestrator requires that you enable folder sharing for the repository folder to replicate to it. You must set the folder to enable sharing across the network so that your ePolicy Orchestrator server can copy files to it. This is for replication purposes only. Managed systems configured to use the distributed repository update using the appropriate protocol (HTTP, FTP, or UNC) do not require folder sharing.

To create a shared folder for an HTTP or UNC distributed repository folder:

- 1 On the desired system, locate the folder you created using Windows Explorer.
- 2 Right-click the folder, then select **Sharing**.
- 3 On the **Sharing** tab, select **Share this folder**.
- 4 Configure share permissions as needed. Systems updating from the repository require only read access, but administrator accounts, including the account used by the ePolicy Orchestrator server service, require write access. See your Microsoft Windows documentation to configure appropriate security settings for shared folders.
- 5 Click **OK**.
- 6 Go to [Create the distributed repository in ePolicy Orchestrator](#).

## Create the distributed repository in ePolicy Orchestrator

Add a distributed repository to the ePolicy Orchestrator repository list and configure it to use the folder you created.

To add the distributed repository:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Add distributed repository**.
- 3 Click **Next** on the first panel of the wizard.

- 4 Type a name into the **Name** field. This is the name that appears in the repository list. The name does not need to be the name of the system hosting the repository.

**Figure 5-6 Create a FTP, HTTP, or UNC distributed repository**



- 5 Select **Distributed Repository** from the **Type** drop-down list.
- 6 Under **Choose the repository configuration**, select the protocol of the repository.
- 7 Click **Next**.
- 8 On the next wizard panel, enter the address location information for the FTP, HTTP, or UNC site, depending on your selection in [Step 6](#).
  - For FTP or HTTP sites, type the URL address information in the **URL** field, such as `HTTP://MyRepository`, then type the port number in the **Port** field.
  - For UNC folders, type the valid UNC path, such as `\\FileServerName\ePOShare` where `FileServerName` is the DNS system name and `ePOShare` is the name of the UNC shared folder you created.
- 9 Click **Next**.
- 10 On the download credentials panel, enter authentication credential information as needed for systems that update from the repository. Read-only permissions are sufficient.

The options available on the download credentials page vary depending on which type of repository you are creating.

**Table 5-1 Client download credential information**

Type	Credential use
FTP	Select <b>Use anonymous login</b> or type the user account information in <b>User name</b> , <b>Password</b> , and <b>Re-Enter Password</b> .
HTTP	Select <b>Use Logged On Account</b> or type the user account information in <b>Domain</b> , <b>User name</b> , <b>Password</b> , and <b>Confirm password</b> .
UNC	If the HTTP server requires authentication, select <b>Use Authentication</b> , then type the user account information in <b>User name</b> , <b>Password</b> , and <b>Re-Enter Password</b> .

- 11 Click **Verify** to test the download credentials. After a few seconds, you should see a confirmation dialog box confirming that the site is accessible to systems using the authentication information.

If your site is not verified, check that you typed the URL or path correctly on the previous panel of the wizard and that you correctly configured the HTTP, FTP or UNC site on the host.

**12** Click **Next**.

**13** Enter replication credential information by typing a domain, user name and password in the appropriate text boxes.

The ePolicy Orchestrator server uses these credentials when it replicates DAT files, engine files, or other product updates from the master repository to the distributed repository. These credentials must have both read and write permissions in the domain of the distributed repository.

**Table 5-2 Replication credential information**

Type	Credential use
FTP	If you selected <b>FTP</b> , type the user account information in <b>User name</b> , <b>Password</b> , and <b>Re-Enter Password</b> .
UNC	Type the UNC share name of the physical folder hosting the repository in <b>Replication UNC</b> . Use this format: \\<COMPUTER>\<FOLDER>. You can use system variables to define this location.  <b>Note:</b> This is not the HTTP address of the web site, but rather the physical folder location on the server.  Next, type the user account information for the network directory in <b>Domain</b> , <b>User name</b> , <b>Password</b> , and <b>Re-Enter Password</b> .
HTTP	Type the user account information in <b>Domain</b> , <b>User name</b> , and <b>Password fields</b> .

**14** Click **Verify** to test that your ePolicy Orchestrator server can write to the shared folder on the remote system. After a few seconds, you should see a confirmation dialog box, then click **Next**.

**15** Choose whether to include all packages or select specific packages to include, during a replication to this distributed repository, then click **Next**.



The ability to select only specific package-types for replication to individual repositories is new to ePolicy Orchestrator 3.6.



Ensure that all packages required by any managed system that uses this repository is not deselected. Managed systems go to one repository for all packages — if a package type for which it is expecting is not present in the repository, the task fails. This feature was designed to ensure packages that are only used by a few systems did not require replication throughout your entire environment.

**16** Click **Finish** to add the repository. Wait a few moments while ePolicy Orchestrator adds the new distributed repository to its database.

**17** Click **Close**.

# 6

## Configuring Product Policies and Tasks

### Manage the security products in your network

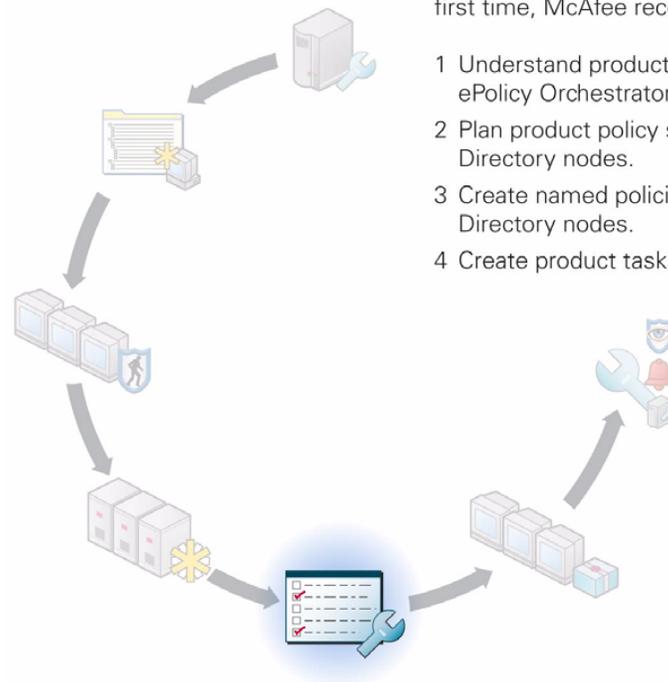
Managing products installed on systems in your network from a single location is a central feature of ePolicy Orchestrator. Policies contain the configuration settings for managed products and components. For example, you can specify which types of files VirusScan Enterprise scans or ignores.



The ability to assign policies independently of your Directory structure, and the ability to quickly view assignments and broken inheritance is new in ePolicy Orchestrator 3.6.

Tasks allow you to schedule on-going product actions and maintenance.

#### Configuring product policies and tasks for the first time?



When configuring policies and tasks for the first time, McAfee recommends to:

- 1 Understand product management in ePolicy Orchestrator.
- 2 Plan product policy settings and tasks for Directory nodes.
- 3 Create named policies and assign them to Directory nodes.
- 4 Create product tasks for Directory nodes.

---

## About policy management

A policy is a collection of software settings that you create, configure, then enforce on managed systems. Policies ensure that the security software products on managed systems are configured as you want them. For example, if end users disable anti-virus scans, you can set a policy that re-enables the scan at the policy enforcement interval (five minutes by default).

You can create customized, named policies which you can assign to any node of the Directory to which you have permissions. You can configure and assign named policies before or after a product is deployed.

For some products, policy settings are the same as the settings you configure in the interface of the product. For other products and components, the policy pages are the primary interface for configuring the product or component. The ePolicy Orchestrator console allows you to configure policy settings for all your systems from a central location.

## Policy NAP files

A product's policy NAP file contains the policy pages and tasks used for managing a specific version of a product. Some products' NAP files are installed with ePolicy Orchestrator by default. To manage other products, you must check their NAP files into the repository manually.

## Policy enforcement

For each product or component that you manage, you can choose to whether to enforce all or none of the policy selections on any node of the Directory.

In the **Assign Policies** page, you can choose whether to enforce policies for products or components at that node.

In the **Policy Catalog** page, you can view assignments, per named policy, where the policy is applied but not enforced.

## Policy enforcement interval

When you reconfigure policy settings, the changes are delivered to and enforced on the managed systems at the next agent-server communication. The frequency of this communication is determined by the **Agent-to-server-communication interval** setting on the **General** tab of the **ePO Agent 3.5.0 | Configuration** policy pages, or the Agent Wakeup task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Once the policy settings are in effect on the managed system, the agent continues to enforce the policy settings locally at a regular interval. This enforcement interval is determined by the **Policy enforcement interval** setting on the **General** tab of the **ePO Agent 3.5.0 | Configuration** policy pages. This interval is set to occur every five minutes by default.

Policy settings for McAfee products are enforced immediately at the policy enforcement interval and at agent-server communication.



There is a delay of up to three minutes after the interval before policies for Norton AntiVirus products are enforced. The agent first updates the GRC.DAT file with policy information, then the Norton AntiVirus product reads the policy information from the GRC.DAT file, which occurs approximately every three minutes.

## Policy categories and named policies

Two terms referred to most often when discussing ePolicy Orchestrator policy management are *named policies* and *policy categories*. Named policies are the specific configurations of policy categories.

### Policy categories

Policy settings for most products are grouped by category. Each policy category refers to a specific subset of policy settings. In the **Policy Catalog** and **Assign Policies** pages, each product's policy categories are displayed when you expand the product name.

Figure 6-1 Policy categories

Category	Policy Name	Inherited From	Inherited By	Lock	Edit Row
Enforce Policies	Yes	Global Default	all inherit	<input type="checkbox"/>	Edit
Alert Manager Alerts Policies	McAfee Default	Global Default	all inherit	<input type="checkbox"/>	Edit
Access Protection Policies	McAfee Default	Global Default	all inherit	<input type="checkbox"/>	Edit
Buffer Overflow Protection Policies	McAfee Default	Global Default	all inherit	<input type="checkbox"/>	Edit
On-Access Default Processes Policies	McAfee Default	Global Default	all inherit	<input type="checkbox"/>	Edit
On Delivery E-Mail Scan Policies	McAfee Default	Global Default	all inherit	<input type="checkbox"/>	Edit

### Named policies

A named policy is a customized subset of product policy settings corresponding to a policy category. You can create, modify, or delete as many named policies as needed for each policy category.

In the **Policy Catalog** page, named policies for a specific category are displayed when you expand the category name.

In the **Assign Policies** page, named policies for a specific category are displayed from the drop-down list next to the category name.



A McAfee Default named policy exists for each category. You cannot delete, edit, or rename these policies.

**Figure 6-2 Named policies in the Policy Catalog**

Policy Name	Owner	Assignments	Rename	Duplicate	Delete	Export
Agent 1	All ePO Administrators	none				
Agent 2	All ePO Administrators	2 assignments				
McAfee Default	All ePO Administrators	1 assignment				
Mine2	All ePO Administrators	1 assignment				

Define new policy...

## Policy assignment and inheritance

Named policies are applied to any node either by:

- *Inheritance*
- *Assignment*

### Inheritance

Inheritance determines whether the policy settings and client tasks for any node of the Directory are taken from its parent. By default, inheritance is enabled throughout the Directory.

When you break this inheritance by assigning a new named policy anywhere in the Directory, all child systems inherit the new policy.

Inheritance can come from the assignment of a named policy (all tabs), or from the Inherit option on any single tab of the policy pages.

### Assignment

ePolicy Orchestrator 3.6 introduces the ability to create named policies and assign them to any node of the Directory for which you have permissions. Named policies allow you to define policy settings once for a specific need, then apply the named policy to multiple locations.

In previous versions, you had to break inheritance and create a new policy at each location of the Directory you wanted to apply the policy.

However, it is important to note that inheritance still applies. When you assign a new policy to a particular node of the Directory, then all systems under that node with inheritance intact, inherit the new policy.

## Policy ownership

All named policies for products and features to which you have permissions are available for use from the **Policy Catalog** page. To prevent any user from modifying other users' named policies, each policy is assigned an owner: the global or site administrator who created it.

Ownership provides that no one can modify or delete a named policy except the policy's creator or a global administrator. Any administrator can use any named policy in the **Policy Catalog** page, but only the owner or global administrator can modify it.

### Best practices information

If you assign a named policy that you do not own to segments of the Directory, be aware that if the owner of the named policy modifies it, all systems to which this policy is assigned receive these modifications.

Therefore, if you wish to use a policy owned by a different administrator, McAfee recommends that you first duplicate the desired policy, then assign the duplicate to the desired locations. This provides you ownership of the duplicate.

## Assignment locking

An administrator can lock the assignment of a named policy at any location within the Directory. Policy assignment locking prevents other users from replacing a named policy.

Assignment locking is inherited with the policy settings.

### Best practices information

Assignment locking is useful if the global administrator configures and assigns a certain policy at the top of the Directory to ensure no other administrators replace it anywhere in the Directory.

Assignment locking only locks the assignment of the policy, but does not prevent the policy owner from making changes to the named policy's settings. Therefore, if you intend to lock a policy assignment, then ensure that you are the owner of the policy.

## Product filtering

Product filtering allows you to view policies only for those products that are currently in use on the selected system or Directory segment.

If the **Show all products** checkbox is not selected on the **Assign Policies** page, the only policies that are displayed are those for products that have a NAP file checked in, and either:

- Have a corresponding current product deployment package (PKG.CATALOG.Z) checked into the master repository.
- Pre-installed on, or below the selected node.

To configure policy settings for products you have not yet deployed, but have checked in the NAP file, be sure to select the **Show all products** checkbox.

## Supported products

Use ePolicy Orchestrator policy pages to manage configuration settings for security products installed and running on client systems in your network.

ePolicy Orchestrator installs with the following NAP files already checked into the repository:

- Alert Manager 4.7.0
- Alert Manager 4.7.1
- ePO Agent for WebShield Appliance 2.0
- ePO Agent for NetWare 2.1.0
- ePO Agent 3.5.0
- ePO Agent for Linux 3.0.0
- ePO Agent for WebShield 3.0.0
- Installer for VirusScan TC 1.0.1
- NetShield 4.5 for Windows
- Norton Antivirus Corporate Edition 7.5x/7.6/8.0/9.0
- NetShield for NetWare 4.6.0
- System Compliance Profiler 1.1.0
- Rogue System Sensor 1.0.0
- VirusScan TC 6.1.0 for Windows
- VirusScan Enterprise 8.0

To manage other supported products released after ePolicy Orchestrator 3.6, their NAP files must be checked into the repository manually if you wish to manage them.

See the configuration guide of the specific product for complete details on all policy options. Configuration guides are available on your product CD and from the McAfee web site.

---

## About client tasks

In addition to customizing policies for products deployed in your network using the policy pages, the ePolicy Orchestrator console allows you to configure client tasks that run on the managed systems. These are the same tasks you might configure to run through the managed product's interface. You can create, schedule, and configure client tasks from the console.

You can define tasks for the entire Directory, a specific site or group, or an individual system. Like policy settings, client tasks are inherited from parent nodes in the Directory.

Which NAP files are installed on your ePolicy Orchestrator server determines which client tasks are available.

Most client tasks are for either:

- Product functionality. (For example, the VirusScan Enterprise 8.0i on-demand scan task.)
- Upgrades and updates.

See the configuration guides for your managed products for information and instructions for these products' tasks.

## Policy conversion when upgrading

When you upgrade to ePolicy Orchestrator 3.6 from a previous version, your existing policy settings are converted to the new format. Although you do not lose the settings you had previously configured, they appear differently.

After an upgrade, the policies are converted to the new format of named policies. Please know that:

- At each location in the Directory where inheritance had been broken, a new named policy was created for the category that had uninherited settings.
- The names that are given to named policies follow the path from the site to the NodeID in the Directory.
- Ownership of all named policies defaults to the global administrator.

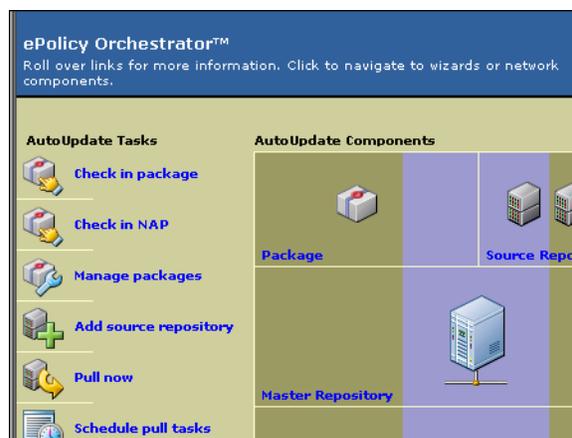
## Adding policy NAP files

Before you can configure policy settings for a product, that product's NAP file must be checked into the repository.

To check a NAP file into the repository:

- 1 Save the NAP file to a temporary folder accessible from the ePolicy Orchestrator server. NAP files are usually located on the product CD or in the downloaded product installation ZIP file. See the configuration guide of the specific product's documentation set for the exact location.
- 2 In the console tree, select **Repository**.
- 3 In the details pane, select **Check in NAP**.

**Figure 6-3 Check in NAP**



- 4 In the **Software Repository Configuration** wizard, select **Add new software to be managed** and click **Next**.
- 5 In the **Select a Software Package** dialog box, browse to and select the NAP file you saved to a temporary folder, then click **OK**.

Wait a few moments while ePolicy Orchestrator loads the product NAP file. Once completed, it appears in the policy list, provided that one of the following is true:

- The **Show all products** checkbox is selected.
- The product's PKGCATALOG.Z file is checked into the master repository.
- The product is already installed on a system in your environment.

---

## Viewing policy information

Unlike previous versions, ePolicy Orchestrator 3.6 has two locations on the console tree to view policy-related information, the **Assign Policies** and **Policy Catalog** pages. Each of which are used to manage policies.

### Assign Policies pages

As with previous versions of ePolicy Orchestrator, clicking on any of the Directory nodes and selecting the **Policies** tab allows you to view, modify, or create the policy configurations and assignment information relating to the selected node.

### Policy Catalog page

The **Policy Catalog** node of the console tree allows you to view all of the defined policy objects, their assignments, and where inheritance is broken.

## Viewing information about named policies

From the **Policy Catalog** page, you can view all the policies, policy assignment, and policy enforcement information in your environment.

### Viewing all policies

To view all policies that have been created:

- 1 In the console tree, select **Policy Catalog**. All created named policies, grouped under products by policy category, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the policy category to expose the named policies associated with that category.

### Viewing nodes to which a policy is assigned

ePolicy Orchestrator allows you to view the nodes of the Directory to which a policy is assigned. This list shows the assignment points only, not each node that inherits the policy.

To view nodes to which a policy is assigned:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products by category, are available in the details pane.
- 2 Click the triangle icon next to a product name to expose its policy categories.

- 3 Click the triangle icon next to a policy category to expose the named policies associated with that category.
- 4 Under **Assignments** on the row of the desired named policy, click the blue text that indicates the number of nodes to which the policy is assigned (for example, **6 assignments**).

On the **View assignments** page, each node to which the policy is assigned appears with its **Node Name** and **Node Type**.

**Figure 6-4 View assignments page**



Node Name	Node Type
Directory\Asia	site

- 5 Click the node name to see the **Assign Policies** page for that node.

## Viewing the settings of a named policy

To view the specific settings of a named policy:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products by category, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the policy category to expose the named policies associated with that category.
- 4 Click the name of the policy. The policy pages, and their settings, for the named policy appear.

## Viewing policy ownership

To view the owner of a named policy:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products by category, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the policy category to expose the named policies associated with that type.
- 4 The owner of the named policy is displayed under **Owner**.



Only global administrators can change the owner of a named policy.

## Viewing assignments where policy enforcement is disabled

From the **Policy Catalog** page, you can easily view where policy assignments, per policy category, are unenforced.

To view assignments where policy enforcement is disabled:

- 1 In the console tree, select **Policy Catalog**.
- 2 In the details pane, select the desired policy category.
- 3 Above the category name, click the blue text next to **Enforcement**, which indicates the number of assignments where enforcement is disabled. The **View assignments where policy enforcement is disabled page** appears.
- 4 Click any nodes in the list to go to the **Assign Policies** page for that node.

## Viewing policy information for Directory nodes

When accessing policy information from nodes of the Directory, you can view policy information as it pertains to specific Directory nodes.

### Viewing named policies assigned to a node

To view the named policies assigned to a specific node:

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products, are available in the details pane.
- 3 Click the triangle icon next to the product names to expose the named policies assigned for each category.
- 4 Click the triangle icon next to the policy category to expose the specific named policy assigned to

### Viewing the policy inheritance of a node

To view the policy inheritance of a specific node:

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products, are available in the details pane.
- 3 Click the triangle icon next to the product names to expose the specific named policies assigned to the node.
- 4 On the desired policy row, under **Inherited By**, is the name of the node from which the policy is inherited.

### Viewing and resetting broken inheritance

To view where policy is broken below a specific node:

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products, are available in the details pane.
- 3 Click the triangle icon next to the product names to expose the specific named policies assigned to the node.

- On the desired policy row, under **Inherited By**, is the number of nodes to which this policy's inheritance is broken.



This is the number of nodes where the policy is broken, not the number of systems which do not inherit the policy. For example, if only one particular group node does not inherit the policy, this is represented by **1 doesn't inherit**, regardless of the number of systems within the group.

- Click the blue text indicating the number of child nodes that do not inherit. The **View broken inheritance** page appears with a list of the names of these nodes.

**Figure 6-5 View broken inheritance page**



- To reset the inheritance of any of these nodes, select the checkbox next the node name, then click **Reset Inheritance**.

## Managing the Policy Catalog

From the **Policy Catalog** page, you can perform many of your policy management tasks:

- [Creating a named policy.](#)
- [Duplicating a named policy on page 126.](#)
- [Modifying the settings of a named policy on page 127.](#)
- [Renaming a named policy on page 128.](#)
- [Deleting a named policy from the Policy Catalog on page 128.](#)
- [Exporting and importing named policies on page 129.](#)

### Creating a named policy

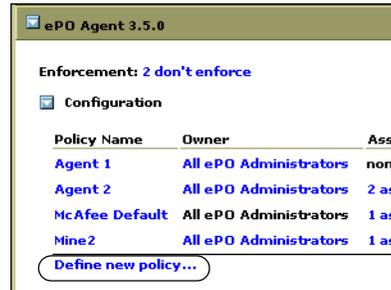
From the **Policy Catalog** page, you can create new named policies, which by default are not assigned to any particular nodes. When you create a policy here, you are adding a custom named policy to the **Policy Catalog** page.

To create a new named policy in the **Policy Catalog** page:

- In the console tree, select **Policy Catalog**. All created policies, grouped under products, are available in the details pane.
- Click the triangle icon next to the product names to expose the policy categories.
- Click the triangle icon next to the desired policy category to expose the named policies associated with that category.

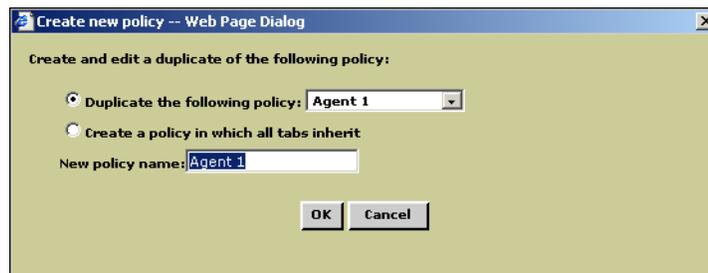
- Click **Define new policy** under the last listed named policy for this type. The **Create new policy** dialog box appears.

**Figure 6-6 Define new policy option**



- If you want to base your new policy on an existing policy, select the named policy you wish to duplicate from the **Duplicate the following policy** drop-down list.

**Figure 6-7 Create new policy dialog box**



If you want to create a policy in which all tabs inherit by default from the parent node, select **Create a policy in which all tabs inherit**.

- Type a name for the new policy in the **New policy name** field, then click **OK**. The **Policy Settings** dialog box appears with the policy pages.
- Click the name of the new named policy in the list. The **Policy Settings** dialog box appears with the policy pages in edit mode.
- Deselect **Inherit** on the desired tab, edit the selections as needed, and click **Apply All**.
- Repeat on each tab as desired.
- Click **Close** at the bottom of the dialog box.

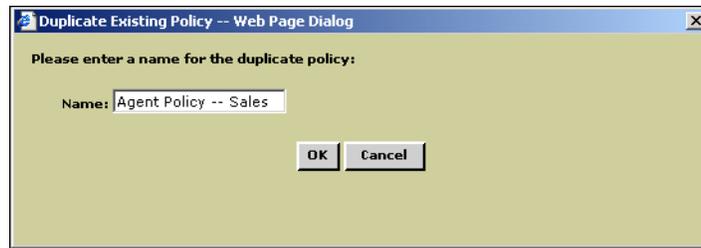
## Duplicating a named policy

From the **Policy Catalog** page, you can create a new named policy based on an existing named policy. For example, if you already have an existing policy in the catalog that is similar to one you want to create, you can duplicate the existing one, then make the desired changes.

To duplicate a named policy:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the desired policy category to expose the named policies associated with that category.
- 4 Locate the policy to duplicate, and click the icon under **Duplicate** in the desired policy's row. The **Duplicate Existing Policy** dialog box appears.

**Figure 6-8 Duplicate Existing Policy dialog box**



- 5 Type the name of the new named policy in the field and click **OK**. (For example, `Sales Europe`.) The **Policy Settings** dialog box appears with the policy pages.
- 6 Deselect **Inherit** on the desired tab, edit the selections as needed, and click **Apply**.
- 7 Repeat on each tab as desired.
- 8 Click **Close** at the bottom of the dialog box. The new named policy appears in the list of named policies.

## Modifying the settings of a named policy

From the **Policy Catalog** page, you can edit the settings of any policy, provided you have the rights to do so.

To modify the settings of a named policy:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the desired policy category to expose the named policies associated with that category.
- 4 Locate the desired policy, then click the name of the policy. The **Policy Settings** dialog box appears with the policy pages.
- 5 Deselect **Inherit** on the desired tab, edit the selections for your needs, and click **Apply All**.
- 6 Repeat on each tab as desired.

- 7 Click **Close** at the bottom of the dialog box. The modifications are saved and enforced on each system to which it is applied at the next agent-server-communication interval.

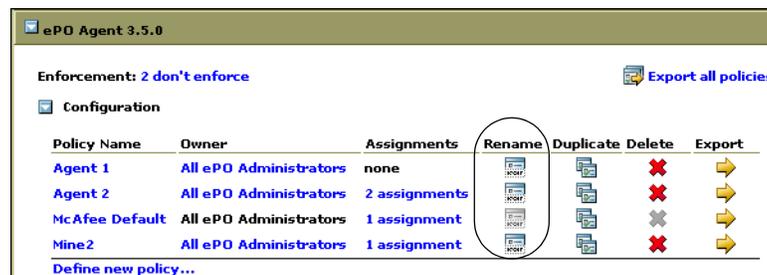
## Renaming a named policy

From the **Policy Catalog** page, you can rename any named policy providing you have the rights to do so.

To rename a named policy:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the desired policy category to expose the named policies associated with that category.
- 4 Locate the desired policy and click the icon under **Rename** in the desired policy's row. The **Rename Policy** dialog box appears.

**Figure 6-9** Rename option



- 5 Type the new name for the existing policy in the field, then click **OK**.

## Deleting a named policy from the Policy Catalog

From the **Policy Catalog** page, you can delete any named policy, except for the McAfee Default policy, provided you are the owner.



When you delete a named policy, all nodes to which it is currently applied inherit the named policy of this category from their parent nodes. Before deleting a policy, you should look at all of the nodes to which it is assigned, and assign a different named policy if you don't want the policy to inherit from the parent node.

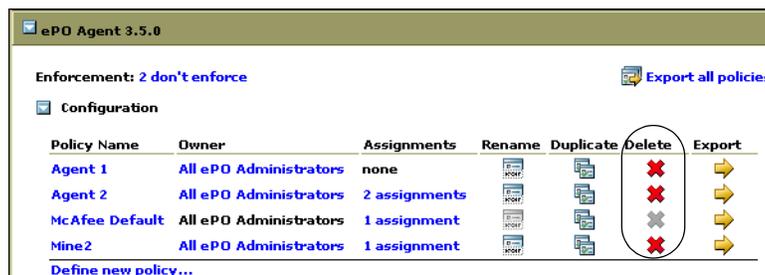
If you delete a policy that is applied at the Directory, the McAfee Default policy of this category is applied.

To delete a named policy from the **Policy Catalog** page:

- 1 In the console tree, select **Policy Catalog**. All created policies, grouped under products, are available in the details pane.
- 2 Click the triangle icon next to the product names to expose the policy categories.
- 3 Click the triangle icon next to the desired policy category to expose the named policies associated with that category.

- 4 Locate the desired policy, and click the icon under **Delete** in the desired policy's row.

**Figure 6-10 Delete option**



- 5 Click **OK** when prompted.

## Changing the owner of a policy

To change the owner of a policy:

- 1 In the console tree, select **Policy Catalog**.
- 2 In the details pane, select the desired named policy.
- 3 Click the **Owner** of the named policy. The **Assign policy owner** dialog box appears.
- 4 Select the desired new owner of the policy from the list, then click **OK**.

## Exporting and importing named policies

If you have multiple servers, you can export and import named policies between them. In such an environment, you need only create a named policy once.

You can export and import individual named policies, or all named policies for a given product.

This feature can also be used to back up named policies, in case you must re-install the server at a future time.

To share named policies between servers, you must export the named policy to a policy XML file from the **Policy Catalog** page of the source server, then import it to the **Policy Catalog** page on the target server:

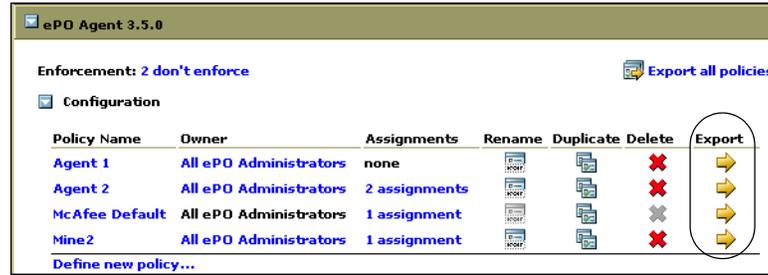
### Exporting a named policy

To export a named policy to a policy XML file:

- 1 In the console tree, select **Policy Catalog**.
- 2 Select the desired named policy.

- 3 Click **Export** at the end of the row.

**Figure 6-11 Export option**



- 4 Name and save the policy XML file to the desired location. Ensure that this location is accessible to the target ePolicy Orchestrator server.

### Exporting all named policies for a product

To export all named policies for a product to a policy XML file:

- 1 In the console tree, select **Policy Catalog**.
- 2 In the details pane, click the triangle icon next to the desired product.
- 3 Click **Export all policies**.
- 4 Browse to the desired location to which to save the policy XML file.
- 5 Type the desired name of the file in **File Name**.
- 6 Click **Save**.

### Importing named policies

Regardless of whether you exported a single policy, or all named policies, the import procedure is the same.

To import a policy XML file:

- 1 In the console tree, select **Policy Catalog**.
- 2 In the details pane, click **Import**.

**Figure 6-12 Import Policy option**



- 3 Browse to and select the desired policy XML file, then click **OK**.

The imported named policy appears in the appropriate location of the **Policy Catalog** page.

## Managing policies from the Assign Policies pages

From the Directory nodes, you can:

- [Assigning a named policy to a specific node.](#)
- [Creating or duplicating a named policy at a Directory node on page 131.](#)
- [Enforcing policy for a product or category on page 132](#)
- [Locking assignment on page 133.](#)
- [Copying and pasting assignments on page 133.](#)

### Assigning a named policy to a specific node

From the console tree, you can assign available named policies.

To assign a named policy to a specific node of the Directory:

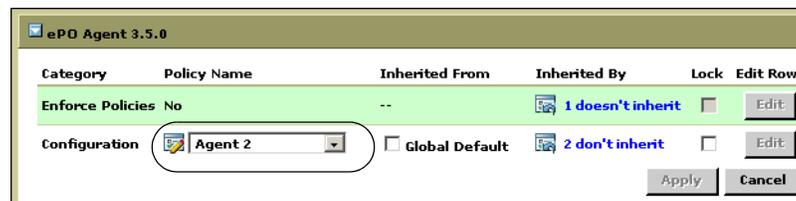
- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products by category, are available in the details pane.
- 3 Click the triangle icon next to the product names to expose the specific named policies assigned to the node.
- 4 Locate the desired named policy, then click **Edit**.
- 5 Deselect the checkbox under **Inherited From**.



This is necessary only when the policy is currently inherited from the parent node.

- 6 Select the desired named policy from the drop-down list under **Policy Name**.

**Figure 6-13 Policy Name drop-down list**



- 7 Click **Apply**.

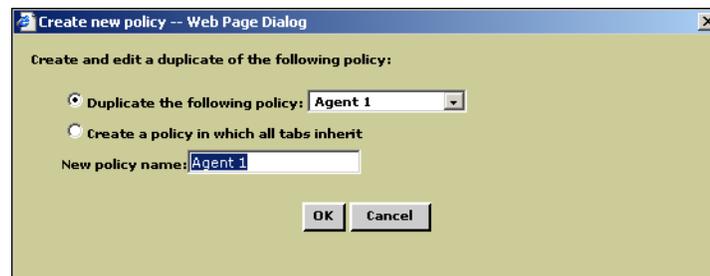
### Creating or duplicating a named policy at a Directory node

In addition to creating a new named policy in the **Policy Catalog** page, you can also create a new named policy at any of the nodes in the Directory, provided you have the rights to do so.

To create a new named policy at a Directory node:

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products by category, are available in the details pane.
- 3 Click the triangle icon next to the product names to expose the specific named policies assigned to the node.
- 4 Locate the desired policy category for which you want to create a new named policy, then click **Edit**.
- 5 Select **New Policy** from the drop-down list under **Policy Name**. The **Create new policy** dialog box appears.
- 6 If you want to base your new policy on an existing policy, select the named policy you want to duplicate from the **Duplicate the following policy** drop-down list.

**Figure 6-14 Create new policy dialog box**



If you want to create a policy in which all tabs inherit by default from the parent node, select **Create a policy in which all tabs inherit**.

- 7 Type a name for the new policy in the **New policy name** field, then click **OK**. The **Policy Settings** dialog box appears with the policy pages.
- 8 Deselect **Inherit** on the desired tab, edit the selections as needed, then click **Apply**.
- 9 Repeat on each tab as desired.
- 10 Click **Close** at the bottom of the dialog box. The modifications are saved and enforced on each system to which it is applied on the next agent-server-communication.

## Enforcing policy for a product or category

Once policies are assigned, you can choose whether to enforce all or none of the assigned policies for a given product on the **Assign Policies** page for any node. Policy enforcement is enabled by default.



Policy enforcement is inherited by child nodes.

To disable or re-enable policy enforcement:

- 1 In the console tree, select the desired Directory node.
- 2 In the details pane, select the **Policies** tab.

- 3 Click the triangle icon next to the product or component name. The top row, above all categories, is **Enforce Policies**.
- 4 Click **Edit** to the right of this row.
- 5 Under **Policy Name**, select **Yes** or **No** from the drop-down list. Selecting **Yes** enables policy enforcement while selecting **No** disables policy enforcement.
- 6 Click **Apply**.

## Locking assignment

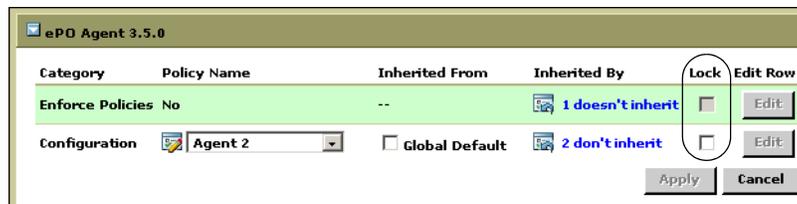
To lock the assignment of a named policy:



Only administrators can lock a named policy.

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products by category, are available in the details pane.
- 3 Click the triangle icon next to the product names to expose the specific named policies assigned to the node.
- 4 Locate the desired policy category that you want to lock, then click **Edit**.
- 5 Select the **Lock** checkbox to lock the assignment.

Figure 6-15 Lock option



- 6 Click **Apply**.

## Copying and pasting assignments

ePolicy Orchestrator 3.6 allows you to copy and paste policy assignments from one node to another node.

To copy and paste policy assignments of a node:

- 1 In the console tree, select the desired Directory node from which you want to copy policy assignments.
- 2 In the details pane, click **Copy policy assignments**.
- 3 Select the desired products or features for which you want to copy policy assignments from the selected node, then click **OK**.
- 4 In the console tree, select the desired Directory node to which to paste the copied policy assignments.

- 5 In the details pane, select **Paste policy assignments**.
- 6 Confirm the replacement of assignments as prompted.

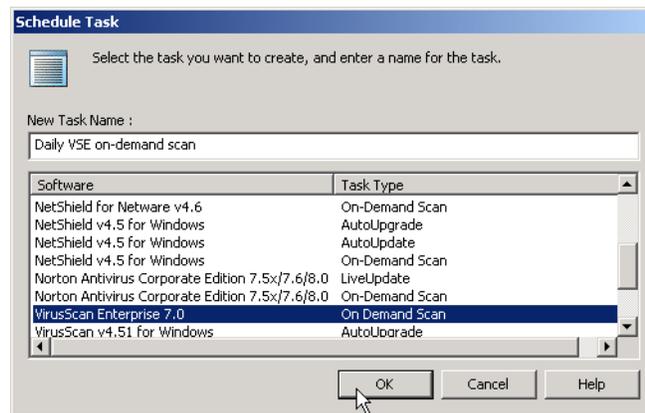
## Creating and scheduling client tasks

The process for creating and scheduling client tasks is similar for all client tasks. This section uses an on-demand scan task for VirusScan Enterprise as an example.

To create a client task:

- 1 In the console tree, select the desired Directory node, then select **Schedule Task**. The **Schedule Task** dialog box appears.
- 2 Type a descriptive name for the task you are creating, then select the desired task from the list. For example, **VirusScan Enterprise | On Demand Scan**.

**Figure 6-16** Schedule Task dialog box



- 3 Click **OK**.
- 4 Click the refresh button on the toolbar. The new task may not appear in the list of available tasks on the **Tasks** tab until you refresh the console.
- 5 Right-click the new task, then select **Edit Task**.
- 6 On the **Task** tab of the **ePolicy Orchestrator Scheduler** dialog box, deselect **Inherit** to enable the options.
- 7 Select **Enable**. Tasks do not run unless enabled.
- 8 Click **Settings**. The **Task Settings** dialog box appears.
 

This step is unique for each task type. The **Task Settings** dialog box includes product- and task-specific settings. For example, a VirusScan Enterprise on-demand scan task includes settings for anti-virus scanning configuration options. For details on a specific task's options, see that product's configuration guide.
- 9 Click **OK** when complete.
- 10 On the **ePolicy Orchestrator Scheduler** dialog box, click the **Schedule** tab and deselect **Inherit** to enable the scheduling options.

**11** Schedule as needed.

There are many scheduling options. For more information, see [Scheduling options on page 135](#).

**12** Click **OK** when complete.

**13** Verify the task is enabled in the list of tasks on the **Tasks** tab in the details pane.

## Scheduling options

Client tasks include many scheduling options. [Table 6-1](#) provides details on each:

**Table 6-1 Client task scheduling options**

Scheduling option	Description
<b>Stop the task if it runs for</b>	On the <b>Schedule Settings</b> section of the <b>Task</b> tab. Limits the length of time the task can run before it is cancelled.
<b>Schedule Task</b>	Set the frequency of schedule. Such as daily, weekly, or when the managed system is powered on.
<b>Start Time</b>	The time of day when the task should begin running.
<b>GMT or Local</b>	Select <b>Local</b> to run the task based on the managed system's clock. This is useful for scheduling processor-intensive tasks for non-business hours.  Select <b>GMT</b> to run the task based on Greenwich Mean Time, regardless of a system's location. This option causes the task to run at the same time for all managed systems, regardless of the local system time on the system.
<b>Enable Randomization</b>	The task does not run at exactly the specified start time. Instead, it starts over a randomized period.
<b>Run missed task</b>	Ensures the task starts if the managed system is shutdown or otherwise not available during the scheduled start time. Selecting this option runs the task the next time the managed system becomes available.
<b>Delay missed task by</b>	On the <b>Advanced Schedule Options</b> dialog box. Selecting this option sets a delay after the managed system becomes available before the missed task runs.
<b>Start Date / End Date</b>	On the <b>Advanced Schedule Options</b> dialog box. Enter start and end dates if you want the task to run temporarily.
<b>Repeat Task</b>	On the <b>Advanced Schedule Options</b> dialog box. Select this option and set the interval to run a task multiple times in the same day.

---

## Frequently asked questions

### What is a named policy?

A named policy is a customized subset of product policy settings corresponding to a policy category. You can create, modify, or delete as many named policies as needed for each policy category.

**What is the McAfee Default named policy?**

Upon installation, each policy category contains at least one named policy. This is named McAfee Default. This is the only named policy present for first-time installations.

The McAfee Default named policies cannot be edited, renamed, or deleted.

**What happens to the nodes of the Directory under a node where I assigned a new named policy?**

All nodes, provided they have inheritance enabled for the specific policy category, inherit the policy applied to a parent node.

**How are the nodes to which a named policy is applied affected when the named policy is modified in the Policy Catalog?**

All nodes to which a named policy is applied receive any modification made to the named policy at the next agent-server communication. The named policy is then enforced at each policy enforcement interval.

**I assigned a new named policy, but it's not being enforced on the managed systems?**

New policy assignments are not enforced until the next agent-server communication after the assignment has been made.

# 7

## Deploying Software and Updates

### Install security products and updates on systems

In addition to managing security products, ePolicy Orchestrator can deploy products to your network systems. Use ePolicy Orchestrator to deploy products and their updates.

If you plan to deploy security products and updates with a tool other than ePolicy Orchestrator, skip this section.

#### Deploying software or updates for the first time?

When deploying software or updates for the first time, McAfee recommends to:

- 1 Understand product deployment, and the package types that ePolicy Orchestrator can deploy.
- 2 Configure pull and replication tasks.
- 3 Configure deployment and update tasks.
- 4 Check in product or update packages to the master repository.



## About product and update packages

The ePolicy Orchestrator deployment infrastructure supports deploying products and ePolicy Orchestrator components, as well as updating both.

Each McAfee product that ePolicy Orchestrator can deploy provides a product deployment package (PKG.CATALOG.Z) file. ePolicy Orchestrator can deploy these packages to any of your managed systems, once they are checked into the master repository. The package catalog file contains the product installation files, which are compressed in a secure format.

PKG.CATALOG.Z files are used for both virus definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. McAfee recommends configuring policy settings before deploying the product to network systems, this can save time and ensure that your systems are protected as desired as soon as possible.

Global administrators can check these package types into the master repository with pull tasks, or manually:

**Table 7-1 Supported packaged types**

Package type	Description	Origination
Virus definition (DAT) files. File type: PKG.CATALOG.Z	The regular, daily DAT files released by McAfee.	FTP Site and Http Site update sites, and the McAfee web site.  Use a pull task to download DAT files directly into the master repository, or download and check them into the master repository manually.
Scanning engine. File type: PKG.CATALOG.Z	The updated scanning engine for McAfee anti-virus products, such as VirusScan Enterprise. Engines are usually updated once or twice a year.	FTP Site and Http Site update sites, and the McAfee web site.  Use a pull task to download engine files directly into the master repository, or download and check them into the master repository manually.
SuperDAT (SDAT.EXE) files. File type: SDAT.EXE	The SuperDAT files contain both DAT and engine files in one update package.  If bandwidth is a concern, McAfee recommends updating DAT and engine files separately.	McAfee web site.  Download and check SuperDAT files into the master repository manually.

**Table 7-1 Supported packaged types**

Package type	Description	Origination
Supplemental virus definition (EXTRA.DAT) files. File type: EXTRA.DAT	The EXTRA.DAT files address one or a few specific viruses that have appeared since the last DAT file was posted. If the threat has a high severity, distribute the EXTRA.DAT immediately, rather than wait until that signature is added to the next DAT file.  EXTRA.DAT files are from the McAfee web site. You can distribute them through ePolicy Orchestrator.  Pull tasks do not retrieve EXTRA.DAT files.	McAfee web site.  Download and check supplemental virus definition files into the master repository manually.
Product deployment packages File type: PKGCATALOG.Z	A product deployment package contains the installation software of a McAfee product.	Product CD or downloaded product ZIP file.  Check product deployment packages into the master repository manually. For a specific location, see the <i>Configuration Guide</i> for the product.  Only the ePolicy Orchestrator agent and System Compliance Profiler deployment packages are checked into the master repository as part of the ePolicy Orchestrator server installation.
Agent installation package File type: PKGCATALOG.Z	An agent installation package contains the installation software for the ePolicy Orchestrator agent.	Master repository — checked in at installation.  For future versions of the agent, you must check agent installation packages into the master repository manually.
Agent language packages File type: PKGCATALOG.Z	An agent language package contains files necessary to display agent information in a local language.	Master repository — checked in at installation.  For future versions of the agent, you must check agent language packages into the master repository manually.

## Package signing and security

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

You are notified when you check in packages that are not signed by McAfee. If you are confident of the content and validity of the package, continue with the check-in. These packages are secured in the same manner described above, but are signed by ePolicy Orchestrator when they are checked in.

Using digital signatures guarantees that packages originated from McAfee or were checked in by you, and that they have not been tampered with or corrupted. The agent only trusts package catalog files signed by ePolicy Orchestrator or McAfee. This protects your network from receiving packages from unsigned or untrusted sources.

## Legacy product support

Older products use a flat directory structure in conjunction with the AutoUpdate and AutoUpgrade client tasks to install product updates. New products that take advantage of AutoUpdate 7.0 use a hierarchical directory structure and the update task to install product updates.

If the update location you specify in the AutoUpdate or AutoUpgrade task settings is a distributed repository managed by ePolicy Orchestrator, you must enable legacy product support when you check the corresponding package into the master repository. Doing so copies the packages into both directory structures, enabling you to support legacy products.

## Package ordering and dependencies

If one product update is dependent on another, you must check their packages into the master repository in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them back in, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.

---

## About deploying and updating products

The ePolicy Orchestrator repository infrastructure allows you to deploy products and update packages to your managed systems from a central location. Although the same repositories are used, there are differences.

**Table 7-2 Comparison of product deployment and update packages**

Product deployment packages	Update packages
Must be manually checked into the master repository.	DAT and engine update packages can be copied from the source repository automatically with a pull task. All other update packages must be checked into the master repository manually.
Can be replicated to the distributed repositories and installed on managed systems with global updating.	Can be replicated to the distributed repositories and installed on managed systems <i>automatically</i> with global updating.
If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.	If not implementing global updating for product updating, an <i>Update task</i> must be configured and scheduled for managed systems to retrieve the package.

## Product deployment and updating process

The high-level process for distributing DAT and engine update packages follows:

- 1 Check the update package into the master repository with a pull task or manually.
- 2 If using global updating, nothing else is necessary provided global updating has been configured and enabled.

If not using global updating, use a replication task to copy the contents of the master repository to the distributed repositories.

- 3 If not using global updating, create and schedule an update or deployment task for agents to retrieve and install the update on managed systems.

## Deployment task

Once you have checked in the product deployment package, you can use the deployment task to install the product on managed systems. The deployment task is a unique client task created automatically when ePolicy Orchestrator installs. It installs any product that is deployable through ePolicy Orchestrator and has been checked into the master repository.

### Best practices information

You can run the product deployment task at any site, group, or individual system. When deciding how to stage your product deployment, McAfee recommends considering the size of the package and the available bandwidth between the master or distributed repositories and the managed systems. In addition to potentially overwhelming the ePolicy Orchestrator server or your network, deploying products to many systems can make troubleshooting problems complicated.

Consider a phased roll-out to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred clients at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

If you chose to deploy server-based McAfee products, deploy them to specific systems, rather than groups or sites.

## Update tasks

Once an update package has been checked into the master repository and replicated to the distributed repositories, the agents on the managed systems still need to know when to go to the distributed repositories for updates. This is unnecessary if you are using global updating.

You can create and configure client update tasks to control when and how managed systems receive update packages. If you are not using global updating, creating these client update tasks are the only way you can control client updating with ePolicy Orchestrator.

If you are using global updating, a client update task is unnecessary, although you can create a daily client update task for redundancy.

## Considerations when creating client update tasks

Consider the following when scheduling client update tasks:

- Create a task to update DAT and engine files daily at the highest level of the Directory that is inherited by all systems. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact of all systems updating at the same time. Also, for large networks with offices in different time zones, running the task at the local system time on the managed system, rather than at the same time for all systems, helps balance network load.
- Schedule the update task at least an hour after the scheduled replication task, if you are using scheduled replication tasks.
- Run update tasks for DAT and engine files at least once a day. Managed systems can be logged off from the network and miss the scheduled task; running the task frequently ensures these systems receive the update.
- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one update task to update only DAT files, then create another to update both DAT and engine files weekly or monthly — engine packages are released less frequently.
- Create and schedule additional update tasks for products that do not use the agent for Windows.
- Create two update tasks for your main workstation applications, such as VirusScan Enterprise, to ensure they all receive the update files. Schedule one to run daily or several times a day. Schedule a second to **Run Immediately**. This second task runs once for each system in your Directory the first time the agent calls into the server. This can be useful if systems are logged off from the network at the scheduled update time; the second update task ensures they update immediately when they log onto the network.

## Global updating

McAfee recommends using global updating with your updating strategy. Global updating automates replication to your distributed repositories and updating managed systems. Replication and update tasks are not required. Checking contents into your master repository initiates a global update. The entire process should complete within an hour in most environments.

Additionally, you can specify which packages and updates initiate a global update. However, when you only specify that certain content initiates a global update, ensure that you create a replication task to distribute content that was not selected to initiate a global update.



When using global updating, McAfee recommends scheduling a regular pull task (to update the master repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, network traffic over the updating time period is increased.

## Global updating process

Global updating updates your environment within an hour in most environments using the following steps:

- 1 Contents are checked into the master repository.
- 2 Contents of the master repository are replicated automatically to the distributed repositories.
- 3 A SuperAgent wakeup call with the SITESTAT.XML file is broadcast to all agent. This file lists the contents of the master repository. If a package the managed systems requires is in the list, the agent goes to a distributed repository to get the package.
- 4 All agents go to their local distributed repositories for new updates.

## Requirements

The following requirements must be met to implement global updating:

- A SuperAgent is installed on each broadcast segment. Managed systems cannot receive a SuperAgent wakeup call if there is no SuperAgent on the same broadcast segment. Global updating utilizes the SuperAgent wakeup call to alert agents that new updates are available.
- Distributed repositories are set up and configured throughout your environment. McAfee recommends SuperAgent repositories, but they are not required — global updating functions with all types of distributed repositories.
- If using SuperAgent repositories, managed systems must be able to “see” the repository from which it updates. Although, a SuperAgent is required on each broadcast segment for systems to receive the wakeup call, SuperAgent repositories are not required on each broadcast segment, but the managed systems must “see” the SuperAgent repository from which to update.

## Pull tasks

Use pull tasks to update your master repository with DAT and engine update packages from the source repository. DAT and engine files must be updated often. McAfee releases new DAT files daily and engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.



EXTRA.DAT files must be checked into the master repository manually. They are available from the McAfee web site.

A scheduled pull task runs automatically and regularly at times and days you specify. For example, you can schedule a weekly repository pull task at 5:00 am every Thursday.

You can also use the Pull now task to check updates into the master repository immediately. For example, when McAfee alerts you to a fast-spreading virus and releases a new DAT file to protect against it.

If a pull task fails you must check the packages into the master repository manually.

Once you have updated your master repository, you can distribute these updates to your systems automatically with global updating or with replication tasks.

## Considerations when scheduling a pull task

Consider the following when scheduling pull tasks:

- Bandwidth and network usage. If you are using global updating, as recommended, schedule a pull task to run when bandwidth usage by other resources is low. With global updating, the update files are distributed automatically after the pull task completes.
- Frequency of the task. DAT files are released daily, but you may not want to use your resources daily for updating.
- Replication and update tasks. Schedule replication tasks and client update tasks to ensure the update files are distributed throughout your environment.

## Replication tasks

Use replication tasks to copy the contents of the master repository to distributed repositories. Unless you have replicated master repository updates to all your distributed repositories, some systems do not receive them. Ensure all your distributed repositories are up-to-date.



If you are using global updating, replication occurs automatically — replication tasks are not necessary.

Scheduling regular replication tasks is the best way to ensure that your FTP, HTTP, and UNC distributed repositories are up-to-date. Scheduling daily replication tasks ensures that managed systems stay up-to-date.

Creating scheduled replication tasks automates replication to your distributed repositories. Occasionally, you may add files to your master repository that you want to replicate to distributed repositories immediately, rather than wait for the next scheduled replication. Run a Replicate now task to update your distributed repositories manually.

## Full vs. incremental replication

When creating a replication task, select incremental or full replication. Incremental replication uses less bandwidth and copies only the new updates in the master repository that are not yet in the distributed repository. Full replication copies the entire contents of the master repository.



McAfee recommends scheduling a daily incremental replication task and a weekly full replication task. This maximizes network bandwidth efficiency by updating only essential, incremental changes during the week and guarantees completeness.

## Server task log

The server task log allows you to view information about your pull and replication tasks, in addition to all server tasks. This information allows you to understand more easily the status of the task and any errors that may have occurred.



Providing additional troubleshooting information in the server task log is a new feature to ePolicy Orchestrator 3.6.

To view the server task log:

- 1 In the console tree, select the ePolicy Orchestrator server.
- 2 In the details pane, select the **Task Logs** tab.
- 3 Select the desired filter from the **Filters** drop-down list to limit the log contents by a time period.
- 4 Click the triangle icon next to the desired log entry to view the details of the log entry.

For complete information on using the server task log, see [Reviewing the server task log on page 30](#).

## Replication task information

The following information is available for replication tasks on the **Server Task Log** page:

- Start and end times.
- Status of task at each site (when expanded).
- Any errors or warnings, their codes, and the site to which they apply.

## Pull task information

The following information is available for pull tasks on the **Server Task Log** page:

- Start and end times.
- Any errors or warnings and their codes.
- Status of each package that is checked into the master repository.
- Information regarding any new packages that are being checked into the master repository.

## Repository selection

New distributed repositories are added to the repository list (SITELIST.XML) file containing all available distributed repositories. The agent of a managed system updates its repository list each time it communicates with the ePolicy Orchestrator server. The agent performs repository selection each time the agent (**McAfee Framework Service**) service starts and when the repository list changes.

Selective replication provides more control over the updating of individual repositories. When scheduling replication tasks, you can choose:

- Specific distributed repositories to which the task applies. Replicating to different distributed repositories at different times lessens the impact on bandwidth resources. These repositories can be specified when you create, or edit, the replication task.

- Specific files and signatures that are replicated to the distributed repositories. Selecting only those types of files that are necessary to each system that checks into the distributed repository lessens the impact on bandwidth resources. When you define or edit your distributed repositories, you can choose which packages you want to replicate to the distributed repository.



This functionality is intended for updating products that are installed only on several systems in your environment, like GroupShield and Webshield. The functionality allows you to distribute such updates only to the distributed repositories these systems check into.

## Repository selection by agents

By default, agents can attempt to update from any repository in the repository list (SITE.LIST.XML) file. The agent can use a network ICMP ping or subnet address compare algorithm to find the distributed repository with the quickest response time. Usually, this is the closest distributed repository to the system on the network.

You can also tightly control which distributed repositories agents use for updating by enabling or disabling distributed repositories in the agent policy settings. McAfee does not recommend disabling repositories in the policy settings. Allowing agents to update from any distributed repository ensures they receive the updates.

---

## Checking in product deployment packages manually

Check in the PKGCATALOG.Z product deployment package files to the master repository to be able to deploy them using ePolicy Orchestrator.

You must be a global administrator to check in product deployment packages.



You cannot check in packages to your master repository while pull or replication tasks are executing.

To check in a product deployment package:

- 1 Locate the PKGCATALOG.Z file you want to check in. See the product's configuration guide for details on the location.
- 2 Copy the entire contents of the folder containing the package, then save it to a temporary folder on your ePolicy Orchestrator server.

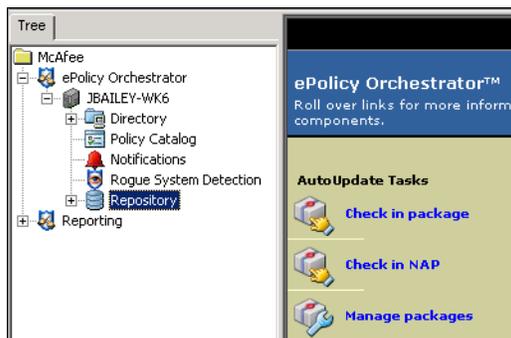


You must copy *all* the files in the PKGCATALOG.Z folder, or the package check-in fails.

- 3 In the console tree, select **Repository**.

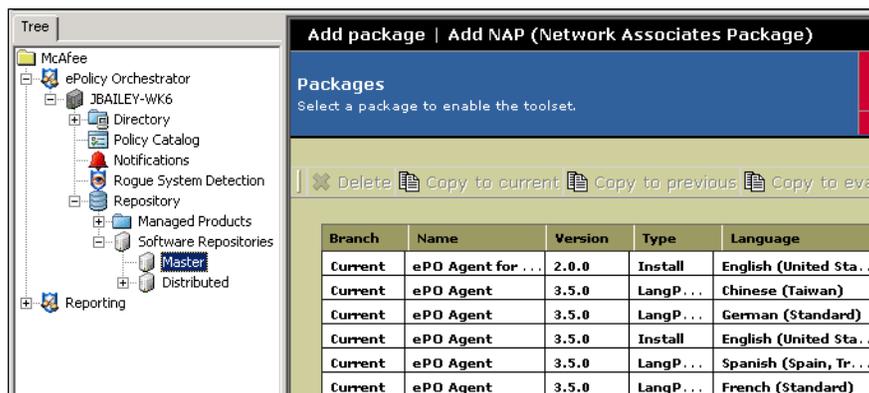
- In the details pane, under **AutoUpdate Tasks**, click **Check in package**. The **Check-in package** wizard appears.

**Figure 7-1 Check-in package wizard**



- Click **Next** to open the **Package Type** dialog box.
- Select **Products or updates** as the package type, then click **Next**.
- Browse to the PKGCATALOG.Z file that you saved in a temporary folder in [Step 1](#).
- Click **Next** to view the package check-in summary information.
- Click **Finish** to begin checking in the package. Wait a few minutes while the package checks into the repository.
- Click **Close** when complete.
- In the console tree, select **Repository | Software Repositories | Master**.

**Figure 7-2 Packages list**



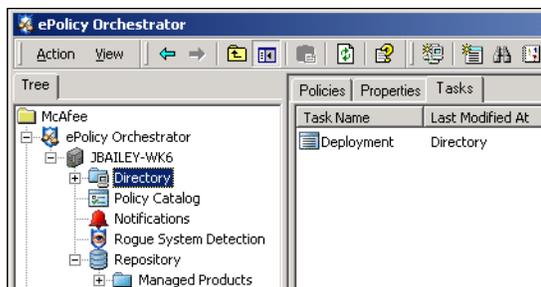
- In the details pane, scroll through the list and locate the product and version of the deployment package to verify the action was successful.
- If you are using distributed repositories in your environment, be sure to replicate the package to them.

## Configuring the deployment task to install products on client systems

To deploy products using the product deployment task:

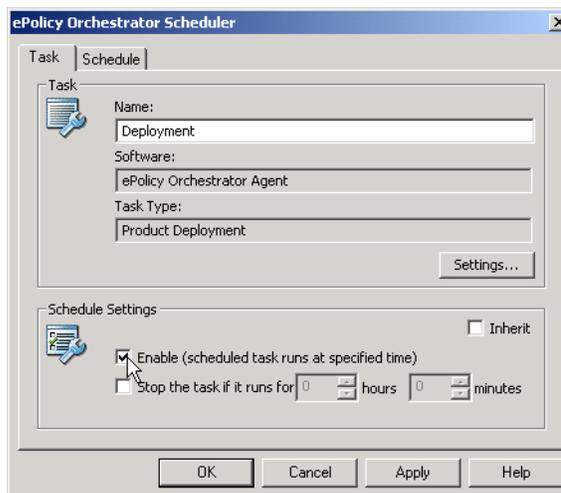
- 1 In the console tree, select the site, group, or individual system to which to deploy the product.
- 2 In the details pane, select the **Task** tab, then double-click **Deployment** in the task list. the **ePolicy Orchestrator Scheduler** dialog box appears.

**Figure 7-3 Deployment task for the selected node in the Directory**



- 3 Select the **Task** tab and deselect **Inherit** under **Schedule Settings**.

**Figure 7-4 ePolicy Orchestrator Scheduler dialog box**

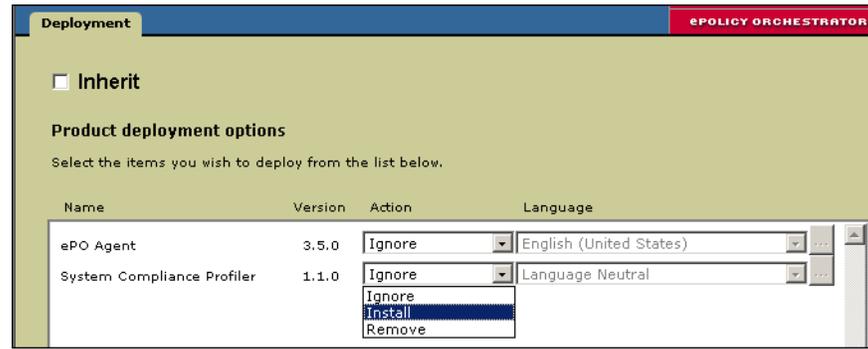


- 4 Under **Schedule Settings**, select **Enable (scheduled task runs at specified time)**. The task does not run unless you enable it here.
- 5 Click **Settings**.
- 6 On the **Deployment** tab, deselect **Inherit** to enable product deployment options.

The **Product deployment options** list shows which products are available to deploy through ePolicy Orchestrator. The products listed are those for which you have already checked in a PKGCATALOG.Z file to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product's PKGCATALOG.Z file.

- 7 Set the **Action** to **Install** for the product you want to deploy.

**Figure 7-5 Task Settings dialog box**



- 8 To specify command-line install options, click  and type the desired command-line options in the **Command line** text field. See your product documentation for information on command-line options.
- 9 Click **OK** to save the product deployment options and return to the **ePolicy Orchestrator Scheduler** dialog box.
- 10 On the **ePolicy Orchestrator Scheduler** dialog box, select the **Schedule** tab.
- 11 Deselect **Inherit** to enable scheduling options.
- 12 Schedule as desired.
- 13 Click **OK** to save your changes.

In the task list on the **Tasks** tab of the details pane, the **Enabled** status for the deployment task is set to **True**.

Once configured, the agents receive the deployment instruction when they call into the ePolicy Orchestrator server.

## Configuring updating

Once your repositories have been created, you must perform several tasks, depending on the updating strategy you are implementing.

If you are implementing a global updating strategy:

- 1 Enable global updating.
- 2 Run a Pull now task.
- 3 Schedule a recurring pull task.

If you are implementing an update strategy with FTP, HTTP, or UNC file server repositories:

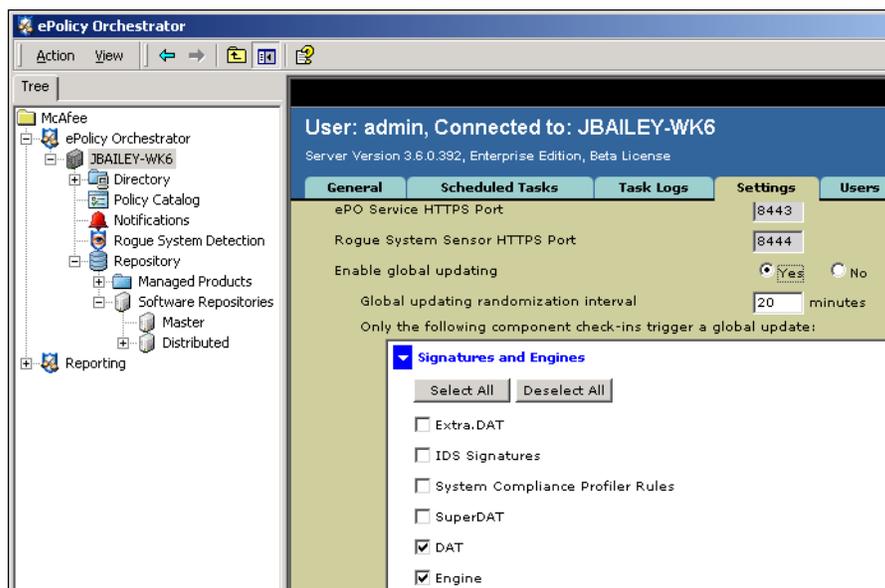
- 1 Run a Pull now task.
- 2 Run a Replicate now task.
- 3 Schedule a recurring pull task.
- 4 Schedule a recurring replication task.

## Enabling global updating

To enable global updating on the server:

- 1 In the console tree, select the server.
- 2 In the details pane, select the **Settings** tab.
- 3 On the **Server Settings** page, select **Yes** next to **Enable global updating**.

Figure 7-6 Settings tab



- 4 Configure a randomization interval, if desired.
- 5 Under **Only the following component check-ins trigger a global update**, select which components you want to initiate an update.

Global updating initiates an update only if new packages for the components specified here are checked into the master repository. Select these components carefully.

- 6 Click **Apply Settings** at the top of the **Server Settings** page to save the changes.

Once enabled, global updating initiates an update the next time you check in updates for the specified components.

## Using pull tasks to update the master repository

These procedures assume that proxy server settings have been configured to allow the master repository to pull updates from the source repository.

You can schedule pull tasks or run them immediately.

## Scheduling a regular pull task

Use this procedure to schedule a recurring pull task that updates the master repository from the source repository. You must be a global administrator to schedule pull tasks.

To schedule a repository pull task:

- 1** In the console tree, select **Repository**.
- 2** In the details pane, select **Schedule pull tasks** to open the **Configure Server Tasks** page.
- 3** Click **Create task** to open the **Configure New Task** wizard.
- 4** Under **Task Settings**, type a descriptive name in the **Name** field, such as `Daily Repository Pull task`.
- 5** Select **Repository Pull** from the **Task type** drop-down list.
- 6** Choose whether to enable or disable the task.
- 7** In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 8** The section under the **Task settings** section is named for the **Schedule type** you selected and allows you to configure its details. (For example, if you selected **Weekly** from the **Schedule type** drop-down list, you can choose the days of the week on which you want to run the task.) Define the settings as appropriate.
- 9** Under **Additional settings**, choose whether to run missed tasks, and how long (in minutes) to delay running a missed task, then click **Next** at the top of the page.
- 10** Select the source repository from the **Source repository** drop-down list, which shows all source repositories you have created. If you have not created any custom source repositories, the list shows the McAfee Http default source repository and also the McAfee Ftp default fallback repository.
- 11** Select the repository branch.  
  
If you use the Evaluation branch feature for testing DATs and engines before deploying to your entire organization, select **Evaluation**.  
  
If you do not use the Evaluation branch, select **Current**.
- 12** If you have older versions of McAfee products, such as VirusScan 4.5.1 deployed in your network, select **Support Legacy product update**.
- 13** Select **Move existing packages to the 'previous' branch** to save the current DAT and engine versions.
- 14** Click **Finish**.

The scheduled pull task is added to the task list on the **Scheduled Tasks** tab. It shows the date and time the task runs next.

## Running a Pull now task

To initiate a repository pull to update the master repository immediately:

- 1 In the console tree, select **Repository**. The **Repository** page appears in the details pane.
- 2 In the details pane under **AutoUpdate Tasks**, click **Pull now** to launch the **Pull Now Wizard**.
- 3 Click **Next**.
- 4 Select the source repository from the list of available repositories and click **Next**.
- 5 Select the repository branch.

If you use the Evaluation branch feature for testing DAT and engine files before deploying to your entire organization, select **Evaluation**.

If you do not use the Evaluation branch, select **Current**.



Don't pull new DAT or engine files into the **Previous** branch.

- 6 If you have older versions of McAfee products such as VirusScan 4.5.1 deployed in your network, select **Support Legacy product update**.
- 7 Select **Move existing packages to the 'previous' branch** to save the current DAT and engine versions saved in the current branch to the previous branch.
- 8 Click **Finish** to begin the task.
- 9 Select whether to jump to the task log after exiting the wizard, then click **Close**.

You can confirm that the DAT files are updated by viewing the contents of the master repository and confirming that the DAT version number is the most current.

---

## Replicating the master repository contents to distributed repositories

Replicate contents of the master repository to distributed repositories with a scheduled replication task that occurs regularly, or by running a Replicate now task for immediate replication.

## Scheduling a repository replication server task

To create a scheduled replication task:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Schedule pull tasks** to open the **Configure Server Tasks** page.
- 3 Select **Create task** to open the **Configure New Task** page.
- 4 Type a name into the **Name** field, such as `Daily Distributed Repository Replication task`.
- 5 Select **Repository Replication** from the **Task type** drop-down list.

- 6 Select **Yes** next to **Enable Task**.
- 7 In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 8 The section under the **Task settings** section is named for the **Schedule type** you selected and allows you to configure its details. (For example, if you selected **Weekly** from the **Schedule type** drop-down list, you can choose the days of the week on which you want to run the task.) Define the settings as appropriate.
- 9 Under **Additional settings**, choose whether to run missed tasks, and how long (in minutes) to delay running a missed task, then click **Next** at the top of the page



If you are using a source repository to update your master repository, schedule your replication task for at least one hour after your scheduled pull task begins. Depending on your network and Internet connections, your pull task may require more or less time — set your replication task start time accordingly.

- 10 Click **Next** at the top of the page.
- 11 Select **Incremental replication** or **Full replication**.
- 12 Select **Replicate to all the repositories** or **Replicate to the selected repositories**.



The ability to create replication tasks for specific repositories is a new feature for ePolicy Orchestrator 3.6.

- 13 If you selected **Replicate to the selected repositories**, then select the checkboxes next to the desired distributed repositories from the list.
- 14 Click **Finish**. Wait a moment while the task is created.

Once created, the task appears in the list of scheduled server tasks. The **Next Run Time** column displays the exact date and time when the task runs next, according to the schedule criteria you specified.

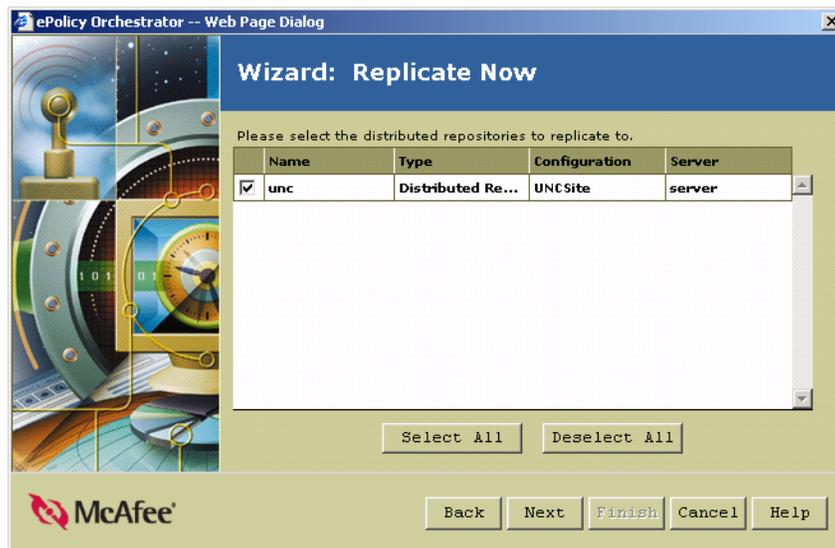
## Replicating to distributed repositories immediately

To replicate contents from the master repository to distributed repositories immediately:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, click **Replicate now**. The **Replicate Now** wizard appears.
- 3 Click **Next**.

- 4 Choose whether to replicate to all repositories, or to specific repositories.

**Figure 7-7 Replicate Now wizard**



If you are not sure which distributed repositories need to be updated, replicate to them all.



The ability to create replication tasks for specific repositories is a new feature for ePolicy Orchestrator 3.6.

- 5 Click **Next**, then select **Incremental replication** or **Full replication**.

If this is the first time you are replicating to a distributed repository, it is a full replication even if you select incremental replication.

- 6 Click **Finish** to begin the task. Replication time depends on the changes to the master repository and the number of distributed repositories to which you are replicating.
- 7 Select whether to jump to the task log after exiting the wizard, then click **Close**.

After replication is complete, you can initiate an immediate client update task so client systems in remote sites can get updates from the distributed repositories.

## Configuring agent policies to use appropriate distributed repository

Use the options on the **Repository** tab of the **ePO Agent 3.5.0 | Configuration** policy pages to customize how agents select distributed repositories.

- 1 On the **Repositories** tab in the **ePO Agent 3.5.0 | Configuration** policy pages, deselect **Inherit**.

**Figure 7-8 Repositories tab**

The screenshot shows the 'ePolicy Orchestrator Agent' configuration window with the 'Repositories' tab selected. The 'Inherit' checkbox is unchecked. Under 'Repository selection', 'Ping time' is selected. The 'Repository list' table contains three entries: 'ePO\_JBAILEY-WK6', 'unc', and 'NAIHttp', all with 'Enabled' states. Action buttons for 'Add...', 'Delete', and 'Edit...' are visible on the right.

Repository Description	Type	State
<input checked="" type="checkbox"/> ePO_JBAILEY-WK6	Global	Enabled
<input checked="" type="checkbox"/> unc	Global	Enabled
<input checked="" type="checkbox"/> NAIHttp	Fallback	Enabled

- 2 Select **Use ePO configured repositories**.
- 3 Under **Repository selection**, specify the method to sort repositories:
  - **Ping time** — Sends an ICMP ping to all repositories and sorts them by response time.
  - **Subnet value** — Compares the IP addresses of client systems and all repositories and sorts repositories based on how closely the bits match. The more closely the IP addresses resemble each other, the higher in the list the repository is placed.
  - **User defined list** — Selects repositories based on their order in the list.
- 4 All repositories appear in the **Repository list**. You can disable repositories by deselecting the box next to their name.
- 5 If you select **User defined list** in **Repository selection**, click **Move up** or **Move down** to specify the order in which you want client systems to select distributed repositories.
- 6 Click **Apply All** when finished.

## Using local distributed repositories that are not managed

Once created, you must manually update the unmanaged distributed repository with the contents of the master repository and configure the managed systems to go to the unmanaged repository for files.

To copy and paste contents from the master repository into the unmanaged distributed repository:

- 1 Copy all files and sub-directories in the master software repository folder from the server. By default, this is in the following location on your server:

```
C:\Program Files\Mcafee\ePO\3.6.0\DB\Software
```

- 2 Paste the copied files and subfolders in your distributed repository location on the distributed repository system.

To configure managed systems to use an unmanaged distributed repository:

- 1 In the console tree, select the site, group or system to use the unmanaged distributed repository.
- 2 In the details pane, select the **Policy** tab, then select **Agent | Configuration**.
- 3 Create a new named policy for this purpose, so that other Directory systems don't receive the instructions to use the unmanaged distributed repository.
- 4 Once the named policy is created and assigned, click the icon next to the policy name, then click the **Repositories** tab when the **Policy Settings** dialog box appears.
- 5 Deselect **Inherit** to enable configuration options.
- 6 Click **Add**.
- 7 In the **Repository Options** dialog box, type a name in the **Repository** text field. The name does not have to be the exact name of the repository location.
- 8 Under **Retrieve files from**, select the type of repository.
- 9 Under **repository configuration**, type the location you created using the appropriate syntax for the repository type.
- 10 Type a port number if you don't want to use the default port.
- 11 Configure authentication credentials as appropriate, if needed.
- 12 Click **OK** to save the new distributed repository.
- 13 At the top of the policy pages, click **Apply All** to save the policy settings.

The repository is added to the repository list. The type is **Local** to indicate it is not managed by ePolicy Orchestrator. When a non-managed repository is selected in the **Repository List**, the **Edit** and **Delete** buttons are enabled.



You cannot edit or delete managed distributed repositories the agent policy pages.

## Exporting the repository list to a file

Use this procedure to export the repository list (SITELIST.XML) file to a file for manual deployment to systems, or for import during the installation of supported products.

You must be a global administrator to export the repository list.

To export a repository list:

- 1 In the console tree, select **Repository | Software Repositories**.
- 2 On the **Master and Distributed Repositories** page, click **Export repository list**.
- 3 When the **Export repository list** wizard appears, click **Next**.
- 4 Type the path of the location to which you want to save the repository list, or click **Browse** to select a location, then click **Next**.
- 5 Click **Finish** to export the repository list to the location you specified.

Once you have exported the repository list to a file, you can import it during the installation of supported products. For instructions, see the installation guide for that product.

You can also distribute the repository list to managed systems, then apply the repository list to the agent. For more information, see [Agent installation command-line options on page 66](#).

## Importing a repository list file

To import a repository list file:

- 1 In the console tree, select **Repository | Software Repositories**.
- 2 On the **Master and Distributed Repositories** page, click **Import repository list**.
- 3 In the **Open** dialog box, browse to the saved SITEMGR.XML file and select it.

The repositories from the list are viewable from the **Master and Distributed Repositories** page.

- 4 Make changes to the repositories in this list as needed.

---

## Checking in engine, DAT and EXTRA.DAT updates manually

Some packages must be checked into the master repository manually.

To check packages into the master repository:

- 1 From your server, go to the McAfee update site and download the desired package, then save it to a temporary folder on server.
- 2 In the console tree, select **Repository**.
- 3 In the details pane under **AutoUpdate Tasks**, click **Check in package**. The **Check-in package** wizard appears.

- 4 Click **Next**.
- 5 Select the package type and click **Next**.
- 6 Type the full path or browse to and select the package that you saved in a temporary folder.
- 7 Click **Next** to view the package check-in summary information.
- 8 Click **Next** to configure the repository branch options.
- 9 Select the desired branch.
- 10 If you have older versions of McAfee products, such as VirusScan 4.5.1, deployed in your network, select **Support Legacy product update**.
- 11 Select **Move the existing package in 'current' branch to 'previous' branch**.
- 12 Click **Finish** to begin the check-in. Wait until the check-in completes.
- 13 Click **Close** when complete.

---

## Distributing DAT and engine files with client update tasks

If you are not using global updating, create scheduled client update tasks to run at a regular frequency, such as daily or weekly. When the client update task runs, managed systems are updated with the DAT and engine versions that have been most recently checked into the master repository.

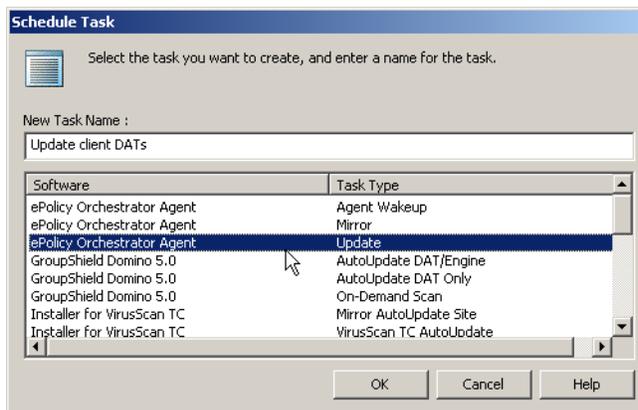
### Creating and scheduling a daily update task

Use this procedure to create and configure update tasks. This procedure describes configuring a daily update task to update DAT files only, but you can follow this procedure and adjust configuration to suit your own needs.

To create a scheduled client update task:

- 1 In the console tree, right-click **Directory**, then select **Schedule task**.
- 2 In the **Schedule Task** dialog box, type a name in the **New Task Name** field, such as `Daily client DAT update task`.

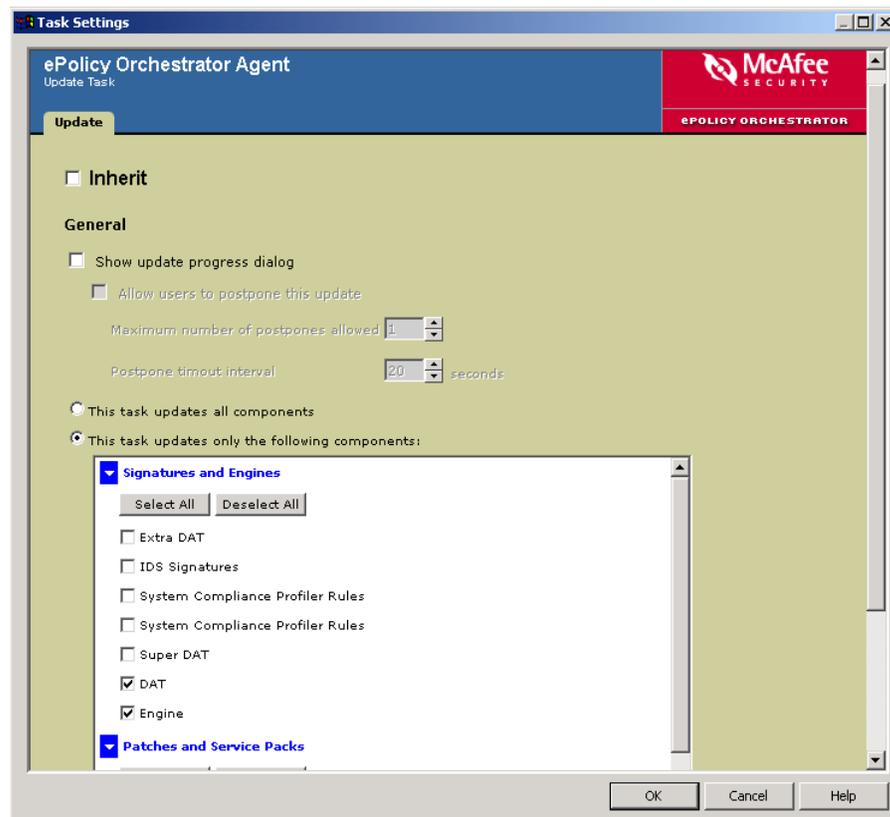
**Figure 7-9 Schedule Task dialog box**



- 3 In the software list, select **Agent | Update**, then click **OK**.
- 4 Refresh the console.  
By default, the task is scheduled to run daily at the current day and time and the **Enabled** flag is set to **False**.
- 5 Right-click the new task in the task list and select **Edit Task**.
- 6 Deselect **Inherit** under the **Schedule Settings** section of the **Scheduler** dialog box.
- 7 Select **Enable (specified task runs at specified time)**. The task does not run unless it is enabled.

- 8 Click **Settings**. The **Task Settings** dialog box appears.

Figure 7-10 Task Settings dialog box



- 9 On the **Task Settings** dialog box for the agent update task, deselect **Inherit**.
- 10 Leave the **Show update progress dialog** option deselected to hide updating on the managed system. McAfee recommends not allowing users to see and potentially interrupt updating.
- 11 Under **Only the following component check-ins trigger a global update**, select specific components that should be updated with the task.
- 12 Click the **Schedule** tab and deselect **Inherit**.
- 13 Set the **Schedule Task** option to run **Daily**.
- To run the task multiple times a day, click the **Advanced** button, select **Repeat Task**, then set the task to repeat as often as needed.
- 14 Click **OK** to close the **Task Settings** dialog box.
- 15 Click **OK** to close the **Scheduler**.

Agents receive the new update task information the next time they communicate with the server. The update task runs at the next occurrence of the scheduled day and time. Each system updates from the appropriate repository, depending on how the update policies for that client's agent are configured.

## Confirming that clients have updated to the latest DATs

You can use the console to confirm that the DAT and engine versions are installed on managed system are up-to-date.

To check the version of DAT files on managed systems:

- 1 In the console tree, select the desired system that has recently been updated.
- 2 In the details pane, select the **Properties** tab.
- 3 Select **VirusScan Enterprise 7.1 | General** to expand the list of general properties.
- 4 Check the **DAT Version** number. It should match the latest DAT version in your master software repository.

---

## Evaluating new DATs and engines before distribution

You may want to test DAT and engine files on a few systems before deploying them to your entire organization.

ePolicy Orchestrator provides three repository branches for this purpose.

Follow these steps to automate update testing using the Evaluation branch:

- 1 *Create a scheduled pull task to use the Evaluation branch.*
- 2 *Designate systems to update from the Evaluation branch.*
- 3 *Schedule a client update task for your evaluation group to update from the Evaluation branch.*
- 4 *Monitor the systems during the evaluation period.*
- 5 *Move the new DATs to the Current branch.*

## Create a scheduled pull task to use the Evaluation branch

Create a schedule pull task that copies updates into the Evaluation branch of your master repository. Schedule it to run after McAfee releases updated DAT files.

For details on specifying the evaluation branch when scheduling pull tasks, see [Scheduling a regular pull task on page 151](#).

## Designate systems to update from the Evaluation branch

Select systems in your Directory to serve as an evaluation group, and configure the updating agent policies for the systems to use only the Evaluation branch.

To configure systems to receive updates from the Evaluation branch:

- 1 In the console tree, select the desired site, group, or system.
- 2 In the details pane, select the **Policy** tab.
- 3 In the **Agent | Configuration** named policy, create a new named policy for this purpose.
- 4 Click the icon next to the policy name. The policy pages appear.

- 5 On the **Updating** tab, deselect **Inheritance**.
- 6 Under **Repository Branch Update Selection**, select **Evaluation** from each drop-down list to update all DAT and engine files only from the Evaluation branch.
- 7 Click **Apply All** to save the change.

The policies take affect the next time the agent calls into the server. The next time the agent updates, it retrieves them from the Evaluation branch.

## Schedule a client update task for your evaluation group to update from the Evaluation branch

Create a scheduled client update task for the evaluation systems that updates DATs and engines only from the Evaluation branch of your repository. Schedule it to run one or two hours after your scheduled pull task is scheduled to begin.

Creating the evaluation update task at the evaluation group level causes it to run only for that group.

To create an update task for your evaluation group:

- 1 In the console tree, right-click your evaluation group, then select **Schedule Tasks**.
- 2 In the **Schedule Task** dialog box, type a name, such as `Evaluation update`.
- 3 Select **Agent | Update** from the list of available tasks, then click **OK**.
- 4 In the details pane, select the **Tasks** tab. Your new update task should appear in the list of available tasks.
- 5 Schedule and enable the update task to run a short time after your scheduled evaluation pull task completes.

## Monitor the systems during the evaluation period

Monitor the systems in your evaluation group for several hours after they have updated with the new files.

When you are satisfied with their performance, distribute them to your entire network.

## Move the new DATs to the Current branch

Copy the files from the Evaluation branch to the Current branch of your master repository. Adding them to the Current repository branch makes them available to your client update task. The next time the update task runs, the new DAT files are distributed.

To move files from the Evaluation branch to the Current branch:

- 1 In the console tree, select **Repository**.
- 2 In the details pane under **AutoUpdate Tasks**, click **Manage packages**. The **Packages** page appears.
- 3 Scroll down the list until you find the files that are saved in your master repository.
- 4 Select the current files in the list, then click **Copy to previous** at the top of the table.

- 5 In the **Copy package** wizard, select **Support legacy product update** if you have older products deployed, such as VirusScan 4.5.1.
- 6 Click **Finish** to move the files.
- 7 Select the files in the Evaluation branch in the list.
- 8 Select **Copy to current**.
- 9 Click **Close** after the package is copied.

# 8

## Determining Compliance

### Limit vulnerabilities by maintaining minimum software versions, patches and service packs

Most outbreaks attack known vulnerabilities in common operating systems. Usually, these are vulnerabilities for which patches or service packs have been released.

Networks suffer outbreaks when operating systems and security software are not up-to-date on every system.

However, it is difficult to find such non-compliant systems and ensure that all systems are up-to-date with operating system and security software patches and service packs.

ePolicy Orchestrator 3.6 includes several features that help ensure that managed systems in your environment are compliant with your security policy.

---

## System Compliance Profiler

System Compliance Profiler includes these features:

- Microsoft patch compliance reporting.
- Customizable compliance assessment based on scans for specific files, registry entries, services and Microsoft patches.
- Downloadable rule templates.
- File and patch integrity verification (with MD5 “fingerprinting”).
- Graphical compliance reports with drill-down paths.

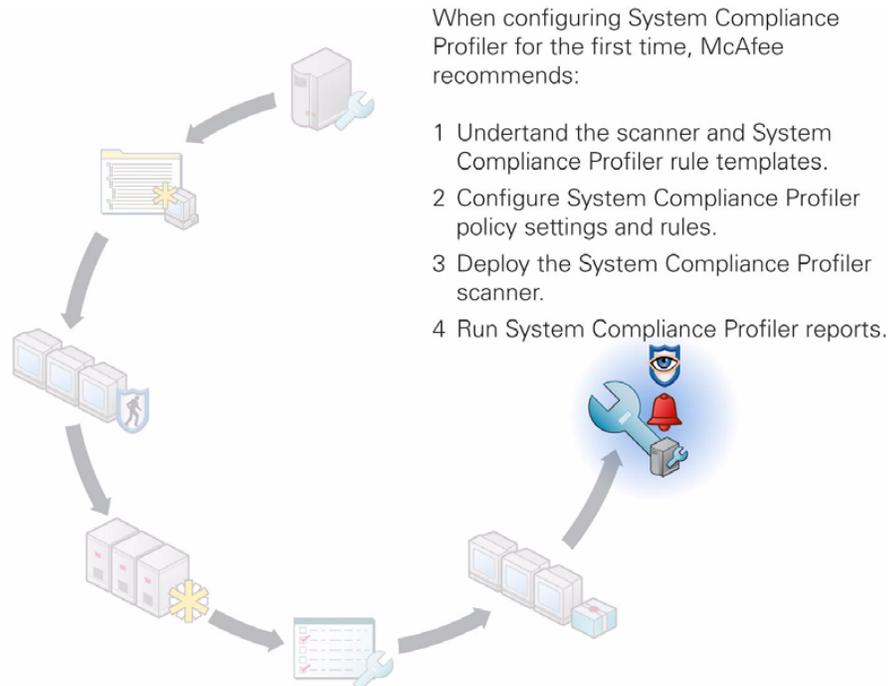
This section contains a brief introduction to the System Compliance Profiler. For more detail, refer to the *System Compliance Profiler 1.1 Configuration Guide* that is available on your installation CD or from the McAfee web site.

The System Compliance Profiler software scans remote systems to determine whether they comply with policies that you configure. These policies consist of rules that tell the software to look for a specific file, registry key, patch, or service on scanned systems. Systems that meet all of your rules are in compliance with your policies. Systems that do not meet rule criteria have rule violations.

Use System Compliance Profiler to create graphical and tabular reports that show which network systems do and do not comply with company policies.

System Compliance Profiler works by installing remote scanning software on each system that you want to monitor. This scanning software periodically scans for files, registry keys, patches, and services, and then sends the collected information to ePolicy Orchestrator. You can use System Compliance Profiler and ePolicy Orchestrator to run reports based on the collected data.

### Configuring System Compliance Profiler for the first time?



## Compliance Check server task

The Compliance Check server task allows you to schedule a task using one or more compliance rules that check your managed systems for compliance with specified:

- DAT version.
- Engine version.
- Agent version.
- VirusScan version.

The ability to create multiple rules allows you to configure separate rules (therefore, separate standards of compliance) for systems with different operating systems and for systems that have communicated with the ePolicy Orchestrator server within a given number of days.

For each rule you must define a threshold that, when crossed, generates an event and sends it to ePolicy Orchestrator Notifications. You can define the threshold as a percentage of target systems being non-compliant, or a specific number of the target systems being non-compliant. For example, you can define the rule to send an event when either 15% of the target systems are not compliant with the rule, or 50 systems are not compliant.



You must have a rule configured in ePolicy Orchestrator Notifications to send a message when a **Non-compliant computer detected** event is received in order for Notifications to send a message.

For more information and instructions, see [ePolicy Orchestrator Notifications on page 210](#).

#### To create a compliance task and the rules associated with it:

- 1 In the console tree, select the ePolicy Orchestrator server.
- 2 In the details pane, select the **Scheduled Tasks** tab.
- 3 Click **Create task**. The **Configure New Task** page appears.
- 4 Type a **Name** for the task.
- 5 Select **Compliance Check** from the **Task type** drop-down list.
- 6 Choose whether to enable or disable the task.
- 7 In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 8 The section under the **Task settings** section is named for the **Schedule type** you selected and allows you to configure its details. (For example, if you selected **Weekly** from the **Schedule type** drop-down list, you can choose the days of the week on which you want to run the task.) Define the settings as appropriate.
- 9 Under **Additional settings**, choose whether to run missed tasks, and how long (in minutes) to delay running a missed task, then click **Next** at the top of the page.

#### To configure compliance rules after creating the Compliance Check task:

- 1 Click **Create** under **Compliance Rules** on the **Edit Compliance Check Task** page. The **Add/Edit Compliance Rule** page appears.
- 2 Under **General Settings for this Rule**, type the desired **Rule name**.
- 3 Choose whether to generate a non-compliance event based on the **Percentage of target computers** or a **Specific number of target computers** and specify the threshold for your selection.
- 4 Under **Define Target Computers**, select whether to apply this task to systems running any operating systems, or to selected operating systems. (If you choose **Selected operating systems**, then select the desired operating systems from the list.)
- 5 Apply this rule to systems that have communicated with the ePolicy Orchestrator server within a specified number of days.
- 6 Under **Define Compliance**, select to define types of compliance you want this rule to apply:

- **DAT version** — Define DAT version compliance by specifying how many versions back you consider compliant.
- **Engine version** — Define engine version compliance by specifying how many versions back you consider compliant.
- **Agent version** — Define agent version compliance by specifying that the agent must be the latest version, or by specifying a specific version.
- **VirusScan version** — Define VirusScan Enterprise version compliance by specifying a specific version.



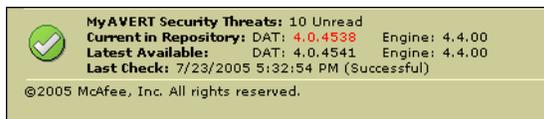
You can create one or more rules that each contain one or more of these types of compliance to run with this server task.

- 7 Click **Save** at the top of the page.
- 8 Repeat as necessary.
- 9 Create a rule in ePolicy Orchestrator Notifications to send a message to the desired individuals when such events are received. For information and instructions, see [ePolicy Orchestrator Notifications on page 210](#).

## MyAVERT Security Threats

The **Security Threats** data monitor (on the **General** tab in the details pane when the ePolicy Orchestrator server is selected in the console tree) informs you of the top ten medium-to-high-risk threats for corporate users. You no longer need to manually search for this information from the press (TV, radio, newspapers), informational web sites, mailing lists, or your peers. You are automatically notified of these threats from one single, trusted source: McAfee AVERT (Anti-virus and Vulnerability Emergency Response Team).

**Figure 8-1 The Security Threats data monitor**



**Protection Status and Risk Assessment** — You can easily determine whether the DAT and engine files in the Current branch of the master repository provide protection against the top ten threats and, if not, the highest risk level of any new threats.

 **Protection Available** — The DAT and engine files in the server repository already provide protection against all threats that are known to AVERT. To determine whether each managed computer is protected, run a “DAT Engine Coverage” report.

 **Protection Pending on Medium-to-Low Risk Threats** — The updated DAT file for threats assessed by AVERT as medium risk is pending. However, updated protection is available in a supplemental virus definition (EXTRA.DAT) file, which you can manually download if you need protection before the next full DAT file is available, such as in an outbreak scenario.

 **Protection Pending on High-Risk Threats** — The updated DAT file for threats assessed by AVERT as high risk is pending. However, updated protection is available in a supplemental virus definition (EXTRA.DAT) file, which you can manually download if you need protection before the next full DAT file is available, such as in an outbreak scenario.

**MyAVERT Security Threats** — Click **My AVERT Security Threats** to view details (such as risk level, discovery date, and detection type) about each threat. For instructions, see [Viewing and managing notifications on new threats on page 168](#).

**Unread** — The number of unread threat notifications is listed. Once you mark a notification as read, it is no longer counted here.

**Last Check** — You can view the last time that new threat notifications were retrieved from the AVERT web site and whether that task was successful.

## Viewing and managing notifications on new threats

You can mark threat notifications as read and delete them as the corresponding threats receive updated protection. Data is sorted by the date AVERT discovered the threat. In addition, you can click the threat name to go to the McAfee AVERT (Anti-virus and Vulnerability Emergency Response Team) web site and learn about each threat.



Each administrator views a Security Threats page that is unique to their account. When one administrator deletes, or marks threat notifications as read or unread, these actions are not represented in the table when another administrator account logs onto the ePolicy Orchestrator server.

Each reviewer views a Security Threats page that contains the superset of threat notifications. No reviewers can delete, or mark threat notifications as read or unread.

**1** In the console tree, select the ePolicy Orchestrator server.

- 2 In the details pane, select the **General** tab, then click **MyAVERT Security Threats**.

**Figure 8-2 Security Threats page**

Security Threats					
<a href="#">Back</a> <a href="#">Refresh</a> <a href="#">Delete</a> <a href="#">Mark as Read</a> <a href="#">Mark as Unread</a> <a href="#">Help</a>					
Threat	Protection	Risk	Discovery D...	Type	Status
W32/Zafi.d@MM	Protection Availa...	Medium	12/14/2004	Virus	Unread
W32/Bagle.af@MM	Protection Availa...	Medium	07/15/2004	Virus	Unread
W32/Bagle.ad@MM	Protection Availa...	Medium	07/04/2004	Virus	Unread
W32/Lovgate.ab...	Protection Availa...	Medium	05/14/2004	Virus	Unread
W32/Bagle.z@MM	Protection Availa...	Medium	04/26/2004	Virus	Unread
W32/Netsky.q@MM	Protection Availa...	Medium	03/28/2004	Virus	Unread
W32/Netsky.p@MM	Protection Availa...	Medium	03/21/2004	Internet Wo...	Unread

#### To mark threat notifications as read

Select unread notifications, then click **Mark as Read**. Notice that the notification text changes from bold to plain. When you mark notifications as read, they are no longer counted in the **Security Threats** data monitor.

#### To mark threat notifications as unread:

Select read notifications, then click **Mark as Unread**. Notice that the notification text changes from plain to bold.

#### To delete notifications:

Select notifications for threats for which protection is available, then click **Delete**. You cannot delete threat notifications for which an updated DAT file is still pending.

## Proxy settings

Using the MyAVERT Security Threats feature may require configuring proxy settings, depending on which operating system the ePolicy Orchestrator server is running. If the ePolicy Orchestrator sever connects to the Internet via a proxy server, you are using the proxy settings in Internet Explorer for the server, and the server is running one of these Microsoft operating systems, the proxy settings might be ignored:

- Windows 2000 Advanced Server, Service Pack 3 or 4
- Windows 2000 Professional, Service Pack 3 or 4
- Windows 2000 Server, Service Pack 3 or 4
- Windows XP, Service Pack 1
- Windows Server 2003

The ePolicy Orchestrator software relies on the Windows HTTP Services (WinHTTP) Proxy Configuration Tool (PROXYCFG.EXE) to use the proxy settings in Internet Explorer. This tool was not included in the operating systems listed above.

To resolve this issue in the long-term, McAfee recommends that you define the proxy settings used in Internet Explorer as custom proxy settings in ePolicy Orchestrator.

You can also obtain the WinHTTP Proxy Configuration Tool from Microsoft. At press time, information on obtaining and using this tool were available on the Microsoft web site:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;830605>

To use this tool to resolve this issue, do the following:

- 1** Enter proxy settings in Internet Explorer as needed.
- 2** Make sure that ePolicy Orchestrator is using these settings for the server.

At the command line on the ePolicy Orchestrator server, run the WinHTTP Proxy Configuration Tool and specify that WinHTTP applications, such as ePolicy Orchestrator use the current user's proxy settings for Internet Explorer:

```
proxycfg.exe -u
```

# 9

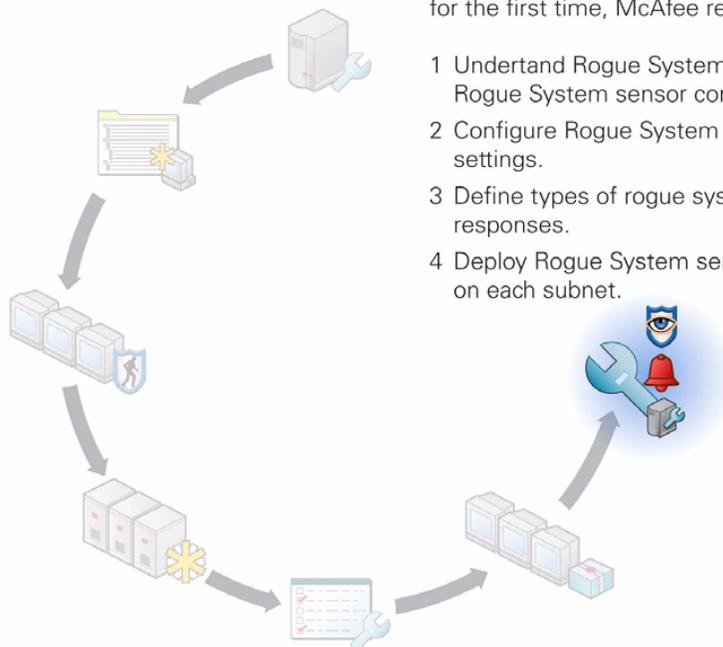
## Rogue System Detection

### Find and manage unknown systems in your network

Even though you already use ePolicy Orchestrator to manage your security products, your protection is only as good as your coverage. Deploying agents to the systems you know about in your network and keeping them up-to-date is only part of a comprehensive strategy. The next step is ensuring you cover each system that connects to your network.

In any managed network, there are inevitably a small number of systems that do not have an agent on them at any given time. These can be systems that frequently log onto and off from the network, including test servers, laptop systems, or wireless devices. Unprotected systems are often the weak spot of any security strategy, creating entry points by which viruses and other potentially harmful programs can access to your network.

#### Configuring Rogue System Detection for the first time?



When configuring Rogue System Detection for the first time, McAfee recommends to:

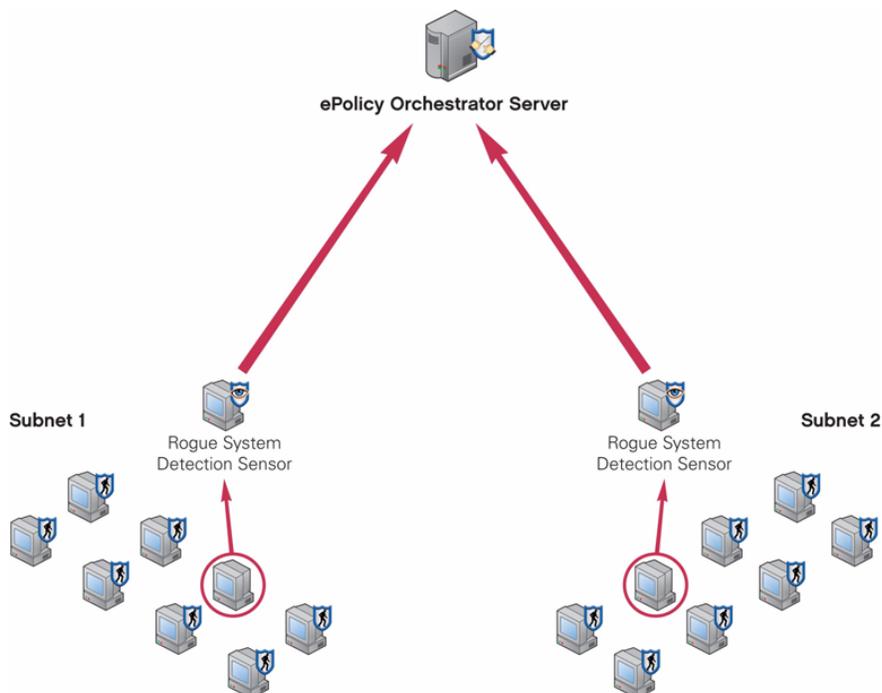
- 1 Understand Rogue System Detection and Rogue System sensor concepts.
- 2 Configure Rogue System sensor policy settings.
- 3 Define types of rogue systems and responses.
- 4 Deploy Rogue System sensors to systems on each subnet.

## About Rogue System Detection

Rogue System Detection helps you monitor all the systems on your network — not only the ones ePolicy Orchestrator manages already, but the rogue systems as well. A rogue system is any system that is not currently managed by an ePolicy Orchestrator agent, but should be.

Rogue System Detection provides real-time detection of rogue systems by means of a sensor placed on at least one system within each network broadcast segment (typically a subnet). The sensor listens to network broadcast messages and spots when a new system has connected to the network.

**Figure 9-1 Rogue system sensors detect systems without agents**



When the sensor detects a new system on the network, it sends a message to the ePolicy Orchestrator server. The server then checks whether the newly-identified system has an active agent installed and managed. If the new system is unknown to the ePolicy Orchestrator server, Rogue System Detection allows you to take remediation steps including alerting network and anti-virus administrators or automatically deploying an ePolicy Orchestrator agent to the system.

### The Rogue System sensor

The sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect systems, routers, printers, and other network devices connected to your network. The sensor gathers information about the devices it detects, and forwards the information to the ePolicy Orchestrator server.

The sensor is a small Win32 native executable application. Similarly with an ePolicy Orchestrator SuperAgent, you must have at least one sensor in each broadcast segment, usually the same as a network subnet, in your network. The sensor runs on any NT-based Windows operating system, such as Windows 2000, Windows XP, or Windows 2003.

## Passive listening to layer-2 traffic

To detect systems on the network, the sensor utilizes WinPCap, an open source packet capture library. Using WinPCap, the Rogue System sensor captures layer-2 broadcast packets sent by systems connected to the same network broadcast segment. The sensor listens passively to all layer-2 traffic for Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and IP traffic. The sensor is able to listen to the broadcast traffic of all devices on its broadcast segment.

The sensor does not actively probe the network to search for which devices are connected.



The sensor does not determine whether the system is a rogue system. It detects systems connected to the network and reports these detections back to the ePolicy Orchestrator server.

## Intelligent filtering of network traffic

The sensor implements intelligent filtering of network traffic to ignore unnecessary messages and capture only what it needs: Ethernet and IP broadcast traffic. By filtering out unicast traffic, which may contain non-local IP addresses, the sensor focuses only on devices that are part of the local network. For example, if a system on the network happens to be browsing McAfee, packets appear on the local network with the IP address belonging to mcafee.com. The sensor detects systems on your local network only, so it ignores all such unicast packets because their sources cannot be guaranteed to be a local system.

To optimize performance and minimize network traffic, the sensor is designed to limit its communication to the server by only relaying new system detections, and to ignore any re-detected systems for a user-configurable time. For example, the Rogue System sensor detects itself among the list of detected systems. If the sensor sent a message every time it detected a packet from itself, the result would be a network overloaded with sensor detection messages.

The sensor further filters on systems already detected:

- The sensor always reports any system the first time it is detected on the network.
- The sensor adds the MAC address of each detected system to the packet filter, so that it is not detected again.
- The sensor implements aging on the MAC filter so that after a time period, MAC addresses for systems that have already been detected are removed from the filter, causing those systems to be re-detected and reported to the server.

## Data gathering and communications to the server

Once the sensor detects a system located on the local network, it attempts to gather as much information about that system from the information contained in the network packet. The information gathered includes DNS name, operating system version, and NetBIOS information such as domain membership, system name, and the list of currently logged-in users.

All of the NetBIOS-related information gathered is subject to standard limitations of authorization and other limitations, as documented in the Microsoft management API.

The sensor packages the gathered information about the detected system into an XML message. It sends this message via secure HTTPS to the ePolicy Orchestrator server for processing. The server then queries the ePolicy Orchestrator database to determine whether the system is a rogue system.

To save bandwidth in large deployments, you can configure how often the sensors send detection messages to the server. You can configure the sensor to cache detection events for a given time period, such as one hour, and then send a single message containing all the events from that time period. For more information, see [Configuring sensor policy settings on page 177](#).

## Systems to host sensors

System on which the sensor is installed should be ones that are likely to remain on and connected to the network all the time, such as a server. If you don't have a server running in a given broadcast segment, deploy several sensors to several workstations to ensure that at least one of them is connected to the network at any time.

### Best practices information

To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor in each broadcast segment of your network. Installing more than one sensor in a broadcast segment does not create issues around duplicate messages — the server filters any duplicate detection messages. However, additional active sensors in each subnet results in traffic sent from each sensor to the server. While maintaining as many as five or ten sensors in a broadcast segment should not cause any bandwidth issues, you should not maintain more sensors in a broadcast segment than is necessary to guarantee that the broadcast segment is covered.

## Primary and inactive sensors

When deploying multiple sensors to the same subnet, you can configure how many are actively reporting to the server at any one time (three by default). These are the primary sensors. Any additional sensors you deploy are backups that remain inactive until the ePolicy Orchestrator server makes them become active.

At regular intervals, the ePolicy Orchestrator server changes primary sensors so that it is not dependant on any one sensor for too long. Also, if the primary sensor is disabled or stops responding, the ePolicy Orchestrator server automatically assigns a different sensor on that broadcast segment the role of primary sensor.

The **Subnet List** table on the **Subnets** tab of the Rogue System Detection interface allows you to view the subnets in your network on which you already have ePolicy Orchestrator agents. From here you can deploy sensors to systems.

## Configure sensor policy settings before deploying

Before you deploy sensors, you should configure the sensor policy settings to suit your needs. These needs are probably the same for all sensors in your environment. Most likely, you can configure sensor policy settings at the Directory root of the console tree and let them inherit throughout the Directory.

For more information, see [Configuring sensor policy settings on page 177](#).

## Machine status and rogue type

Machine status and rogue type are classifications ePolicy Orchestrator uses to determine which systems are rogue systems. Each detected system is listed in the **Machine List** table with a status and, if classified as a rogue system, a rogue type. These classifications are very useful for grouping systems in the **Machine List** table. You can also use status and rogue type as criteria for automatic responses.

For more information, see [Configuring automatic responses for specific events on page 200](#).

## Machine status for detected systems

Each detected system has a basic status of **Managed**, **Rogue**, **Exception**, or **Inactive**. This status is displayed in the **Status** column of the **Machine List** table.

**Table 9-1** Types of machine status

Machine Status	Description
<b>Managed</b>	A system that has an active agent installed and running. The vast majority of systems in the <b>Machine List</b> table should have this status.
<b>Rogue</b>	A system that does not have an agent on it.
<b>Exception</b>	A system you have identified as an exception. An exception is a piece of network equipment, such as a network router, switch, or printer, that you know does not require an agent.
<b>Inactive</b>	A system that is listed in the ePolicy Orchestrator database but which has not been detected by a rogue system sensor in a configurable time period. These are mostly likely systems that are shut down or disconnected from the network.

## Types of rogue systems

Systems with a status of **Rogue** or **Inactive** also are assigned a rogue type. These may be systems that are not listed in the database, but are also not necessarily true rogue systems at a given point in time. Rogue types allow you to define what exactly is a rogue system in your network.

For example, a new system may have just logged onto the network. This system had an agent installed with a network login script at this initial logon. Since the initial agent call to the server may take up to ten minutes, the rogue system sensor detects the system before the agent communicates with the server and is added to the database as a managed system. The system is classified as a rogue system, even though it is not really a rogue system because it already has an agent. If you configure automatic responses or automatic e-mail alerts for rogue detections, specifying a reasonable grace period using the **Rogue (Grace Period)** rogue type can help you minimize false positive detections.

The following table lists each rogue type and its description:

**Table 9-2 Types of rogue systems**

<b>Rogue Type</b>	<b>Description</b>
<b>No Agent</b>	The detected system has no agent installed. This is the most common rogue type.
<b>Grace Period</b>	<p>The detected system has no agent installed, but was detected within a user-configured time period, or grace period. This is useful if you have many systems that join and leave the network. It is also useful if you use login scripts to install the agent when new systems log onto the network. Using the grace period allows you to create a time buffer to avoid false positive rogue detections for systems that are not really rogue systems.</p> <p>The grace period is disabled by default, so all systems without agents are classified as <b>Rogue (No Agent)</b>. You might consider enabling the grace period if you are configuring automatic responses for the rogue detection event.</p>
<b>Inactive Agent</b>	The detected system has an agent installed, but it has not called into the server for some configurable period of days.
<b>Alien Agent</b>	<p>The detected system has an agent installed, but the agent does not report into your server. This can occur if your organization is large and you use multiple ePolicy Orchestrator servers to manage different parts of your network. Laptop users who may travel and log onto your network could have an alien agent. This rogue type is distinct as you probably would not want to take action on these systems as they are already managed. But since they are not managed by your server, you don't want them to be classified as managed either.</p> <p>To reduce false positive rogue detections, you can fine-tune automated responses to avoid pushing agents or sending e-mail alerts when alien agents are detected.</p>
<b>Managed</b>	For systems with a status of <b>Inactive</b> only. The system has not been detected by a sensor within a configured length of time, but when last detected it did have an agent.

## Subnet status

Each subnet listed in the **Subnet List** table on the **Subnets** tab receives a status of **Covered** if there is an active rogue system sensor installed on a system in that subnet. A subnet has an **Uncovered** status if there are no sensors present. You can click each subnet to view a list of all systems in the subnet that have an active agent installed.

## Distributing Rogue System sensors

The sensor reports only on detections occurring within its local broadcast segment. You must install at least one sensor per broadcast segment in your network for coverage.



Depending on your network configuration, a broadcast segment may or may not be the same as a subnet.

If your organization is large, installing sensors manually on individual systems throughout your network could require more of your time than you can afford. Although you can install sensors manually on managed systems, consider using ePolicy Orchestrator to deploy sensors to appropriate systems throughout your network.

Before distributing sensors, configure the settings on the **Rogue System Sensor** policy pages.

## Configuring sensor policy settings

You can configure policy settings for all sensors deployed by the server. This is similar to the managing policies for a deployed product like VirusScan Enterprise. The **Rogue System Sensor** policy pages are installed on the ePolicy Orchestrator server at installation.

Configure the sensor policy settings in the **Rogue System Sensor** policy pages, the same way you would for any managed security product. Policy settings you assign to higher levels of the Directory are inherited by lower-level groups or individual systems.

To configure sensor policy settings:

- 1 In the console tree, select **Directory**. To set policies at a lower level, select a site or group within the Directory.
- 2 In the details pane, select the **Policies** tab, then select **Rogue System Sensor | Configuration**.
- 3 Click the **Edit** button. If this is the first time you are configuring sensor policy settings, you must create a new named policy when prompted because the McAfee Default named policy is not editable. Name the policy as desired.
- 4 On the **General** tab of the **Rogue System Sensor** policy pages, deselect **Inherit**, then configure the options described in the following table as needed.

**Table 9-3 General tab**

Property	Description
Enable Rogue System Sensor	When selected, the sensor is enabled at installation and begins reporting detections to the server after the initial agent-server communication.  If you want to disable the sensor by stopping the sensor service on the client system, deselect this option. You can do this if you only want sensors to function for certain periods of time.
Server name or IP address	The name or IP address of the ePolicy Orchestrator server. When you install ePolicy Orchestrator, this value is set to the name of the system on which ePolicy Orchestrator is installed.

Table 9-3 General tab

Property	Description
Sensor-to-server communication port	<p>The port number used for sensor-to-server communication (8444 by default).</p> <p>If you change this sensor port number here, you must also change it in the SERVER.XML configuration file in the Tomcat subfolder of the ePolicy Orchestrator installation folder. For more information, see <a href="#">Changing sensor-to-server port number in SERVER.XML on page 188</a>.</p>
Minimum reporting interval for each detected host	<p>The length of time, in seconds, that property information for a particular system is cached with the sensor (3600 seconds by default).</p> <p>Use this setting to reduce network traffic by limiting the number of times the sensor reports on systems about which the sensor already knows. A given system likely sends network broadcast messages many times in an hour, and is detected by the sensor each time. But the system's status doesn't change that often, so the same information does not need to be reported to the server at each detection. To save network bandwidth, the sensor updates detection information once within this time period.</p>
Minimum sensor to server communication interval for primary sensors	<p>The length of time, in seconds, that the sensor waits before sending system detection events to the server (300 by default). If used, the sensor caches multiple detection events and sends them to the server together in a single batch message after each interval. When set to zero, the sensor forwards each detection event to the server immediately as a separate message.</p> <p>Use this setting to reduce network traffic by limiting the number of messages the sensor forwards to the server. Batching detection messages together reduces some of the message overhead of sending events separately.</p>
Minimum sensor-to-server communication interval for non-primary sensors	<p>The number of seconds that an inactive sensor should remain inactive before checking with the server to see if it should startup or stay inactive.</p> <p>Use this setting when you have multiple sensors deployed on the same broadcast segment as McAfee recommends. The server periodically switches which sensor is the primary sensor and which are inactive sensors.</p> <p>The difference between an inactive sensor and a disabled sensor is that an inactive sensor is running but does not report detections to the server. A disabled sensor, controlled by the <b>Enable Rogue System Sensor</b> policy setting, is one whose SENSOR.EXE service has been stopped by the agent.</p> <p>See the <b>Maximum number of primary sensors per subnet</b> feature in <a href="#">Configuring Rogue System Detection on page 185</a>.</p>

- 5 On the **Binding and Reporting** tab of the **Rogue System Sensor** policy pages, deselect **Inherit**, then configure the options described in the following table as desired.

**Table 9-4 Binding and Reporting tab**

Property	Description
Only listen on an adapter if its IP address is included on a network found during installation	<p>Forces the sensor to only report detections occurring in the local subnet. For example, if the sensor is installed on a system with IP address 192.168.13.100, then it reports only on detections that occur in the 192.168.13.0/24 subnet.</p> <p>Use this if the sensor is installed on a laptop that may move between subnets within your network or may move to different networks. Otherwise, the sensor reports detections in any of these other subnets. With this setting enabled, the sensor is active when the system is connected to the local subnet, but becomes inactive otherwise.</p>
Only listen on adapters whose IP addresses are included in the following networks	<p>If you install the sensor on a system with multiple network interface cards (NICs), specify the IP address range that includes the NIC to which you want the sensor to bind.</p> <p>The elements of the list are formatted in standard network address notation. For example, 192.168.13.0/24 indicates a subnet including systems with IP addresses 192.168.13.1 - 255 and a subnet mask of 255.255.255.0.</p>
Do not listen on adapters whose IP addresses are included in the following networks	<p>If you install the sensor on a system with multiple NICs, specify the IP address range for any NICs to which you do not want the sensor to bind.</p> <p>If a subnet address is included in both the included and excluded subnet lists, that subnet is excluded.</p>
Do not report systems whose IP address is outside of the sensor's network	<p>If selected, the sensor only reports detections to the server for systems that belong to the same network subnet as the system where the sensor is installed. If not selected, the sensor reports on all systems it detects regardless of which subnet they are a member.</p> <p>The sensor can detect systems within the same network broadcast segment. Often, a broadcast segment is the same as a network subnet. But this may not be the case if you have configured your network routers to not block IP broadcasts across subnets. If this is the case, manage your sensors by deploying one to each subnet and selecting this option to force the sensors to only report on their local subnet.</p>

- 6 Click **Apply All** when finished with each tab to save your changes, then click **Close**.

In most cases, McAfee recommends using the default policies. If, however, your specific network requires, you can change any of the policy settings as needed.

## Deploying Rogue System sensors

You deploy (send and install) Rogue System sensors from the **Subnet List**. You can only install sensors to managed computers (computers that are running an ePolicy Orchestrator agent).



In the future, network access sensors will be deployed from the **Subnet List**.

You can allow sensor host computers to be selected automatically based on specific criteria, or you can manually select them. As part of the sensor deployment, a **Rogue System Sensor Install** client task is created for the host computers. This task allows you to uninstall the sensor or upgrade it to a newer version.

- 1 In the console tree, select **Rogue System Detection**.
- 2 On the **Status** tab, click **Subnets**.
- 3 Select the desired uncovered subnets in the list, then click **Deploy Sensors**.
- 4 On the **Set Preferences** page in the **Deploy Sensors** wizard, chose **Select machines based on the criteria below** or **Let me select machines manually**, then specify the **Number of sensors to deploy per subnet**.

**Figure 9-2 Deploy Sensors: Set Preferences page**

- 5 If you chose **Select machines based on the criteria below**, move the desired selection criteria to **Selected criteria**, then click **Next**. Criteria are evaluated in the order in which they appear in this list.

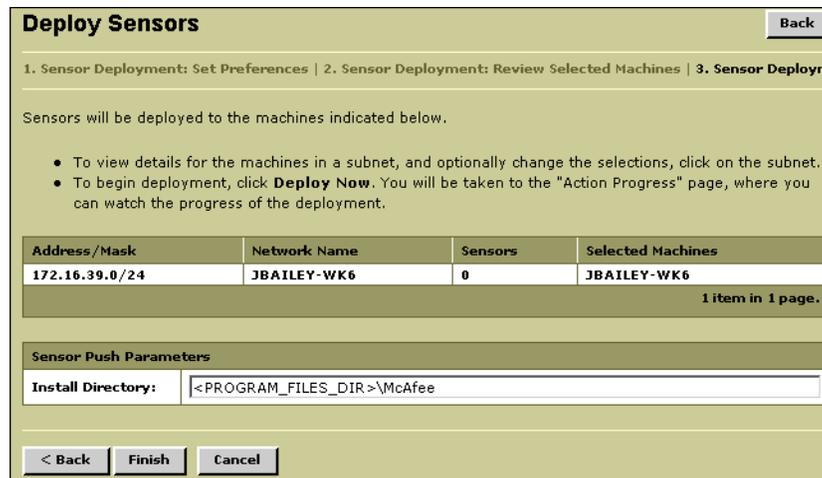
If you chose Let me select machines manually, click **Next**.

**Table 9-5 Automatic sensor deployment criteria**

Criteria	Description
<b>Most Recent ePO Agent Communication</b>	Most recent agent-server communications indicates a system is more likely to be connected and up-to-date at any given time.
<b>Server OS</b>	Servers are more likely than workstations to remain on and connected to the network at all times. Selecting this criterion can help ensure continuous coverage.
<b>Hostname</b>	ePolicy Orchestrator can select systems based on a text string you use in the DNS name. For example, if you add an "SRV" prefix to the names of your server systems, you could deploy a sensor to a system with "SRV" in its DNS name.  If you add <b>Hostname</b> to the <b>Selected criteria</b> list, type the text string that appears in your server DNS names in the <b>Hostname</b> text box.
<b>Most Memory</b>	Although the sensor is not a memory-intensive application, you can ensure resource efficiency by choosing the criterion.
<b>Fastest CPU</b>	Although the sensor is not a processor-intensive application, you can ensure resource efficiency by choosing the criterion.

- On the **Review Selected Machines** page, select the desired host computers, then click **Mark for Deployment**.
- On the **Review and Approve** page, accept the default installation location or type a different one in **Install Directory**.

**Figure 9-3 Sensor Deployment: Review and Approve page**



- Click **Finish** to send and install the sensor to the selected computers. The sensor deployment begins after the next agent-to-server communication. To initiate communication immediately, send an agent wakeup call.

The **Action Progress** page provides the status of the sensor deployment.

**Figure 9-4 Action Progress page**

<input type="checkbox"/>	Action	Action Status	Description	Start Time	End Time
<input type="checkbox"/>	Rogue System Sensor Install	In Progress	Installing sensor on system JBAILEY-WK6	2005-07-23 17:50:39.473	Not Available

## Installing the sensor manually

If you do not want to deploy sensors from the ePolicy Orchestrator console, you can perform the installation manually. To do so, you must be at the system you want to host the sensor. You must also be using an account that has administrative privileges on the system.

You can install the sensor either via a `SETUP.EXE` installation wizard or via the command line.

### Installing the sensor manually using SETUP.EXE

To manually install the Rogue System sensor:

- 1 Copy the entire contents of the sensor install folder to removable media or a shared network folder you can access from the systems to which you want to install the sensor. The sensor `SETUP.EXE` and other installation files are located in:

```
<Drive>:\program files\McAfee\epo\3.6.0\db\software\
current\SNOWCAP_1000\install\0409
```

- 2 At the system on which you want to install the sensor, access and double-click the sensor `SETUP.EXE` file.
- 3 Click **Next** in the wizard.
- 4 On the **Destination Folder** panel, specify an installation folder, then click **Next**. The default location is:

```
<system drive>:\Program Files\McAfee\Rogue System Detection Sensor.
```

- 5 On the **Rogue System Detection Server Information** panel, type the DNS name or IP address of the system hosting the ePolicy Orchestrator server into the **Server Host Name or IP address** text box.
- 6 Type the port number used by the Rogue System Detection server for secure HTTPS communication into the **Server Port Number** text box (8443 by default).



Be sure to specify the correct port number, especially if you configured the ePolicy Orchestrator server to use a port other than 8443 for this purpose.

- 7 Click **Next**. The **Ready to Install** panel appears.
- 8 Click **Next** again to begin the installation.
- 9 After the sensor installation is complete, click **Finish** to close the wizard.
- 10 Repeat the sensor installation steps for each desired system.

The sensor automatically installs and registers as an NT service on the client system, so it is not necessary to manually start the sensor after installation. The sensor begins detecting after the next agent-server communication. However, you can launch the sensor manually so that it displays in a command window on the client system. This can be useful for troubleshooting purposes. To do so, run `SENSOR.EXE` from the command line with the `--console` option to open the sensor in a DOS command dialog box.

## Installing the sensor manually using command lines

You can install the sensor by running `SETUP.EXE` from a command line.

Supported command-line options for the sensor are listed in the following table.

**Table 9-6 Sensor installation command-line options**

Switch	Sample value	Description
-s	N/A	Forces the installation to occur in silent mode.
-x	N/A	Uninstalls the sensor.
-h	MyServer	The host name or IP address of the ePolicy Orchestrator server.
-n	8444	The port number used by the server.
-d	C:\Program Files\mcafee	The installation folder to which the sensor is installed.

## Uninstalling the sensor

Occasionally, you may need to remove a sensor from a system. Make sure that you don't remove the only sensor in the broadcast segment. If you remove the only sensor in a broadcast segment, be sure to deploy one to another system.

You can uninstall the sensor with ePolicy Orchestrator, or manually at the client system.

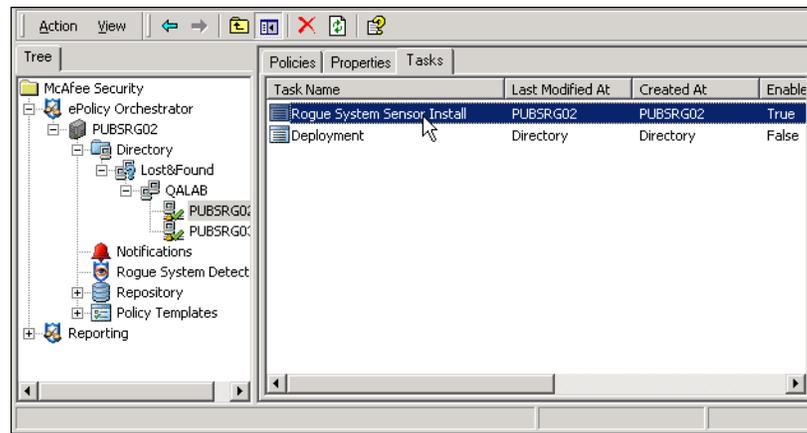
### Uninstalling the sensor with ePolicy Orchestrator

When you use ePolicy Orchestrator to deploy sensors to systems from the server, ePolicy Orchestrator creates a Rogue System Sensor Install task for those systems. You can use this task to remove the sensor, similarly to using the deployment task to remove security products from a client system.

To uninstall a sensor with the Rogue System Sensor Install task:

- 1 In the console tree, select the system from which you want to remove the sensor.
- 2 In the details pane of the console, select the **Tasks** tab, then double-click the **Rogue System Sensor Install** task.

**Figure 9-5 The Rogue System Sensor Install task**



- 3 In the **ePolicy Orchestrator Scheduler** dialog box, deselect **Inherit** and ensure that **Enable** is selected under **Schedule Settings**.
- 4 Click **Settings**. The **Task Settings** dialog box appears.
- 5 Deselect **Inherit** to enable task setting options.
- 6 Deselect **Force install sensor** and select **Force uninstall sensor**.
- 7 Click **OK** to save the changes and close the **Task Settings** dialog box.
- 8 Click **OK** to close the **ePolicy Orchestrator Scheduler** dialog box.

The sensor is uninstalled at the next agent-server communication.

## Uninstalling the sensor manually

You can uninstall the sensor at the client system using the **Add/Remove Programs** utility.

To uninstall a sensor manually:

- 1 Open the Windows **Control Panel** and select **Add/Remove Programs**.
- 2 In the **Add/Remove Programs Properties** dialog box, select **McAfee Rogue System Detection Sensor**, then click **Add/Remove**.
- 3 Click **Yes** when prompted to begin uninstalling the sensor.

## Uninstalling the sensor manually from the command line

You can uninstall the sensor from a command line. To do this, run `SETUP.EXE` from a command line, then specify the `-x` option to uninstall the sensor.



Specifying the `-x -s` command-line options together uninstalls the sensor in silent mode.

## Configuring Rogue System Detection

You can customize several features of Rogue System Detection on the **Configuration** tab. To do so:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab.
- 3 Configure the settings as desired. Descriptions of all options follow in this section.

Figure 9-6 Basic Configuration page

Basic Configuration	
<b>UI Related</b>	
Number of items to view per page:	<input type="text" value="15"/>
Sort machines by network subnet:	<input type="checkbox"/>
Auto Refresh delay:	<input checked="" type="checkbox"/> <input type="text" value="30"/> <input type="text" value="seconds"/>
Site administrators can edit e-mail contacts, responses, and external commands:	<input checked="" type="checkbox"/>
<b>E-mail alerting</b>	
Mail server:	<input type="text" value="mail-server"/>
From:	<input type="text" value="from@example.com"/>
<b>Machine Classification Parameters</b>	
Machine timeout:	<input type="text" value="3"/> <input type="text" value="days"/>
ePO agent timeout:	<input checked="" type="checkbox"/> <input type="text" value="7"/> <input type="text" value="days"/>

The following tables provide descriptions for all of the configurable options on this page.

**Table 9-7 UI-Related options**

Parameter	Default Value	Description
<b>Number of items to view per page</b>	15	The number of rows that appear on a single page in any of the Rogue System Detection tables.  While you can display hundreds of rows in a table if you wish, it may be easier to navigate the list if you keep the number to less than 20.
<b>Sort machines by network subnet</b>	Disabled	Enabling this feature ensures systems listed in the <b>Machine List</b> table are organized by subnet. Once enabled, sorting occurs within the subnet grouping only.
<b>Auto Refresh delay</b>	Enabled at 30 seconds	Automatically refreshes the Rogue System Detection tables at a configurable time period.  When auto refresh is enabled, the refresh status is listed as <b>Refresh (Auto)</b> above each table. If this is disabled, you must manually click <b>Refresh</b> above a table.
<b>Site administrators can edit e-mail contacts, responses, and external commands</b>	Enabled	Enabling this feature allows site administrators to edit the e-mail contacts list, the automatic responses associated with Rogue System Detection events, and the external commands associate with automatic responses.

**Table 9-8 E-mail Alerting options**

Parameter	Default Value	Description
<b>Mail server</b>	mail-server	The name of the e-mail server to use for the e-mail alert response.
<b>From</b>	from@example.com	The return e-mail address for the server that should appear in the <b>From</b> field of e-mail alert messages.

Table 9-9 Machine Classification Parameters options

Parameter	Default Value	Description
Machine timeout	3 days	<p>The amount of time since the last instance the system was detected by a Rogue System sensor before a system is listed as Inactive in the <b>Machine List</b> table. The default of three days allows for weekends, when users may shut down systems.</p> <p>This value can be configured in seconds, minutes, hours, or days.</p>
ePO agent timeout	7 days	<p>The amount of time after which an agent is considered inactive, if it has not called into the server. This affects whether a system is classified as a rogue or managed system. Managed systems whose agents have stopped responding for the configured time period, but are still detected on the network by sensors, are considered rogue systems.</p>
Find detected machines in ePO database by	MAC only	<p>When a detected system is processed, Rogue System Detection must try to find the system in the database. You can configure how it interrogates the database to find this.</p> <p>The options include:</p> <ul style="list-style-type: none"> <li>■ <b>MAC only</b></li> <li>■ <b>MAC first, try hostname if MAC fails</b></li> <li>■ <b>MAC first, try hostname (including domain) if MAC fails</b></li> </ul> <p>Use these selections when you have systems, such as laptops, that connect to the network by multiple methods (for example, Ethernet and a wireless card). These selections allow you to ensure such systems don't appear as other systems depending on the method of connection.</p> <p>However, using this parameter can also result in false positives. Selecting <b>MAC first, try hostname (including domain) if MAC fails</b> option can reduce such false positives.</p>
Rogue system grace period	Disabled	<p>The time period at which a rogue system exists in the <b>Rogue (In Grace Period)</b> status before being classified in the <b>Rogue (No Agent)</b> status. For more information, see <a href="#">Machine status and rogue type on page 175</a>.</p> <p>There can be a slight lag in time after the grace period expires, depending on the sensor reporting interval (60 minutes by default).</p>

**Table 9-10 Ports to check for an ePO agent**

Parameter	Default Value	Description
Agent port for this ePO server	8081	The port used for agent-server communication on the ePolicy Orchestrator server.
Additional ports to check for an agent	None	An administrator created list of additional ports on which to listen for agent communication.  Port numbers can be added or removed from this list.

**Table 9-11 Sensor Parameters**

Parameter	Default Value	Description
Sensor timeout	90 minutes	The period of time after which a non-communicating sensor is considered inactive.  For sensors that have not communicated to the server within the specified interval, the Rogue System Detection server updates their status in the <b>Subnet List to Inactive</b> .
Maximum number of primary sensors per subnet	Disabled	The maximum number of sensors that report to the server when there are multiple sensors deployed in the same broadcast segment. The server automatically chooses which sensors to use as primary sensors.  McAfee recommends having at least two primary sensors per subnet.
Maximum active time period for a primary sensor	12 hours	Rogue System Detection automatically changes the primary sensors at this interval. This avoids relying on any one sensor for too long.

## Changing sensor-to-server port number in SERVER.XML

If you change the sensor port number in the **Rogue System Sensor** policy pages, you must also change the port number in the Rogue System Detection SERVER.XML file on your ePolicy Orchestrator server, located in the `Tomcat` subfolder. If you change only the port number in the policy pages, the sensor is not able to communicate with the server. For more information, see [Configuring sensor policy settings on page 177](#).



There are several SERVER.XML configuration files in different subfolders on the server. Be sure you edit the one in the `Tomcat` subfolder only.

To change the port in the SERVER.XML file:

- 1 Browse to the SERVER.XML file. By default, this file is located in:

```
C:\Program Files\Common Files\McAfee\ePO\3.6.0\Tomcat\Conf
```

- 2 Open the file in a text editor.

- 3 Find the following section and change the port number as needed. The default port number is 8444.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8444 -->

<!-- This connector requires certificate auth and is used for sensor
communication -->

<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8444" minProcessors="5" maxProcessors="75" enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURIVValidationHack="false" disableUploadTimeout="true">

...

</Connector>
```

- 4 Save and close the SERVER.XML file.
- 5 Stop and start the Discovery and Notifications service on your ePolicy Orchestrator server.

---

## Viewing information about detected systems and deployed sensors

Rogue System Detection provides different views into the detected systems and subnets in your environment. This section discusses the locations of information and the information available from Rogue System Detection. Most of the information available is displayed in tables which function similarly to each other.

### Customizing table data in Rogue System Detection

Most of the information displayed in Rogue System Detection is in tables, such as the **Machine List** or **Subnet List** tables. These tables display data from the ePolicy Orchestrator database and have the following configurable features.

#### Filtering table data

Use the **Filter** drop-down list in the table toolbar to filter the table according to status. For example, you can filter the **Machine List** to show only rogue systems or only exception systems.

#### Custom filters

You can set customized filters for the **Machine List** and **Subnet List** tables to define which information is displayed in each. Create a custom filter if the available filters in the **Filter** drop-down list do not meet your needs.

Use the **Custom Filter** button to open the **Custom Filter** page. From here you can create conditions to apply to what appears in the table.

To set a custom filter for the **Machine List** or **Subnet List** table:

- 1 Click **Custom** at the top of the table.
- 2 The **Custom Filter** page lists the current custom filter conditions.

- 3 Add, change or delete conditions as needed.
- 4 Click **Filter** when finished to view the **Machine List** (or **Subnet List**) with the filters applied.



Although **Custom Filter** is selected in the **Filter** drop-down list at the top of the table, you can return to any of the other filtered views by selecting another filter. The custom filter settings are saved until you change them.

## Refreshing table data

Click **Refresh** to immediately refresh the table data. This is useful when performing tasks that cause data to change rapidly. For example, deploying a sensor to a new subnet can add many newly-detected systems to the ePolicy Orchestrator database.

By default, the tables refresh automatically at a configurable interval. You can disable this feature or change the refresh rate.

For more information, see [Configuring Rogue System Detection on page 185](#).

## Showing or hiding specific types of data

To show or hide specific types of data:

- 1 Click **Configure Table** to access the **Columns and Column Order** page for the table.
- 2 Select and move items between the **Available columns** and **Selected columns** lists to customize which columns appear in the table.
- 3 Use the **Up** and **Down** buttons to change the column display order; the first item in the **Selected Columns** list is in the first column of the table.

## Sorting a table by a column

Click any hyperlinked table heading, in blue font, to sort the table by that column.

## Monitoring systems and subnets

The **Machine List** and **Subnet List** tables provide a snapshot of your network coverage. After you have finished your initial deployment of sensors and configured the feature, most of your time dedicated to rogue systems is spent monitoring the **Machines** and **Subnets** tabs.

### Best practices information

Check these pages daily or several times a week to monitor the completeness of your coverage. Typical regular tasks might include deploying agents to new rogue systems and ensuring all your network broadcast segments have active sensors in them.

## Viewing coverage summary information

When you select Rogue System Detection in the console tree, the **Machine Summary** page of the **Machines** tab appears. This page shows a summary of your current Rogue System Detection coverage.

Figure 9-7 Machine Summary page

The screenshot shows the 'Machine Summary' page with a 'Back' button in the top right corner and a 'Refresh (Auto)' button in the top left. Below these are two tables. The first table, titled 'Machines', has three columns: category, count, and percentage. The second table, titled 'Subnets', also has three columns: category, count, and percentage.

Machines		
Rogue Machines	141	98%
Inactive Machines	0	0%
Managed Machines	2	1%
Exception Machines	0	0%
<b>Total Machines</b>	<b>143</b>	<b>100%</b>

Subnets		
Uncovered Subnets	1	50%
Covered Subnets	1	50%
<b>Total Subnets</b>	<b>2</b>	<b>100%</b>

The **Machine Summary** page provides a high-level summary of the status of the systems on your network and which network subnets have rogue system sensors installed in them. There are two tables on this page: **Machines** and **Subnets**.

The **Machines** table shows how many systems fall into each of four categories. You can click any row in the **Machine** table to see the complete list of all systems of the type that have been detected by rogue system sensors.

The four categories are:

- **Rogue Machines.** The number of rogue systems on your network. Rogue systems are systems that are not currently managed by ePolicy Orchestrator but should be. This number should be as close to zero as possible. In most cases, systems listed as rogue systems should have an agent deployed to them or be marked as an exception.
- **Exception Machines.** Number of systems that you have marked as exceptions. These are systems on your network that are not managed by ePolicy Orchestrator and do not need to be. These can be devices, such as routers, hubs, or printers, that do not require an ePolicy Orchestrator agent.
- **Managed Machines.** The number of systems on your network that currently have active agents running on them.
- **Inactive Machines.** Systems listed as inactive are those that have not been detected by a sensor in a user-configurable time period, by default three days. These are usually systems that have been shut down or are no longer connected to the network.

The **Subnets** table shows all the network subnets represented in the ePolicy Orchestrator database. These subnets are grouped into either:

- **Covered.** At least one active rogue system sensor is installed on a system located within this subnet.

- **Uncovered.** No active sensor is on any system within this subnet because no sensor was ever installed. A sensor was disabled or uninstalled, or all systems running sensors were shut down.

## Viewing the list of systems detected on your network

The **Machine List** page on the **Machines** tab displays a list of all systems on your network that have been detected by sensors.

Figure 9-8 Machine List table

<input type="checkbox"/>	Status	Friendly Name	IP	Last Detect Time
<input type="checkbox"/>	Managed	PUBSRG01	172.16.39.228	3/17/04 8:31:27 AM
<input type="checkbox"/>	Managed	PUBSRG02	172.16.39.164	3/17/04 8:21:00 AM
<input type="checkbox"/>	Rogue	QA-MWYMAN	172.16.39.48	3/17/04 8:31:29 AM
<input type="checkbox"/>	Rogue	QA-MWYMAN2	172.16.39.209	3/17/04 8:36:19 AM
<input type="checkbox"/>	Rogue	RIESCLIEN	172.16.39.212	3/17/04 9:01:36 AM
<input type="checkbox"/>	Rogue	RIESSERVER	172.16.39.57	3/17/04 8:57:22 AM
<input type="checkbox"/>	Rogue	RIESTEST3	172.16.39.171	3/17/04 8:46:16 AM
<input type="checkbox"/>	Rogue	RLI-EN-WIN2KSRV	172.16.39.116	3/17/04 8:42:28 AM
<input type="checkbox"/>	Rogue	RLI-EN-WINXPP	172.16.39.124	3/17/04 8:21:31 AM
<input type="checkbox"/>	Rogue	SHALEYDEV	172.16.39.219	3/17/04 8:18:08 AM

Each system has a status. Use the **Filter** drop-down list to filter which systems are displayed in the **Machine List** table. For example, to find out which systems do not have agents installed, set the filter so **Rogue** displays only rogue systems.

You can select systems in the list and perform manual actions on them, such as deploying an agent or adding the system to the Directory. To do this, select an action from the **Checked machines** drop-down.

For more information, see [Taking actions on detected rogue systems manually on page 196](#).

## Sorting systems in the Machine List table by address

You can sort the system list table to group machines by subnet address:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab.
- 3 Under **UI Related**, select **Sort machines by network subnet**.
- 4 Click **Apply**.

## Viewing details about specific detected systems

In the **Machine List** table, click any system to view its detailed information, which is stored in the ePolicy Orchestrator database. This includes operating system, IP address, and the network domains to which it belongs. It also includes its status and when it was last detected by a sensor.

In the **Comments** field, you can type notes about this system that are saved in the database.

Any of these fields can also be displayed in the **Machine List** table. Click **Configure Table** feature on the **Machine List** page to add any of these fields to the machine list table.

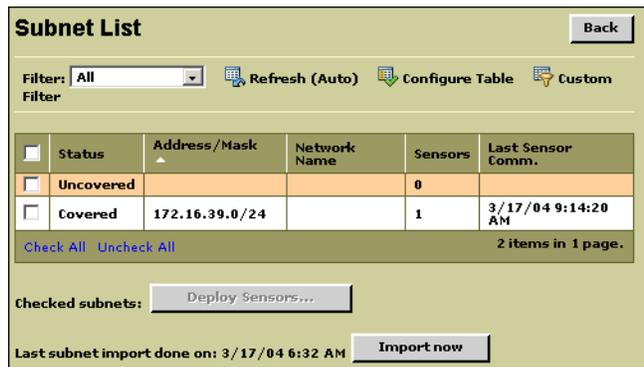
The **Events and Actions for this machine section** lists the event and action history for this system, including:

- Any ePolicy Orchestrator events that have occurred on this system, such as rogue system detected, sensor installed, or agent pushed.
- Any automatic or manual Rogue System Detection actions taken in response to events.

## Viewing your subnets

The **Subnet List** page shows all network subnets represented in your ePolicy Orchestrator database, which records where you have agents deployed.

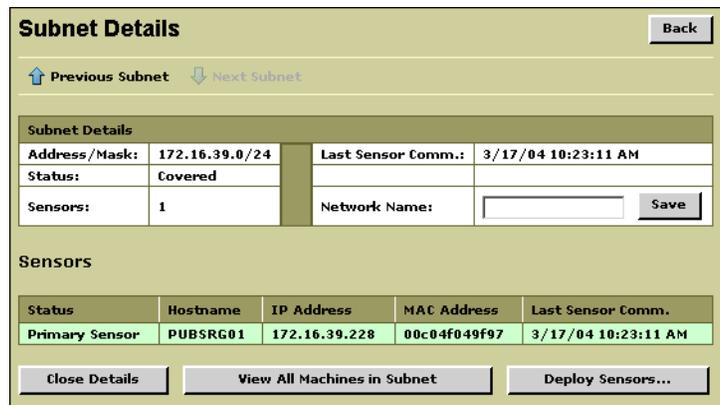
Figure 9-9 Subnet List page



From this page, you can:

- View the further details of any listed subnet by clicking it, including which systems in the subnet have installed sensors currently.

Figure 9-10 Subnet details



- Deploy sensors to uncovered subnets. If a subnet is listed as **Uncovered**, deploy a sensor to it by selecting the corresponding checkbox, then clicking **Deploy Sensors**. For more information, see [Distributing Rogue System sensors on page 177](#).

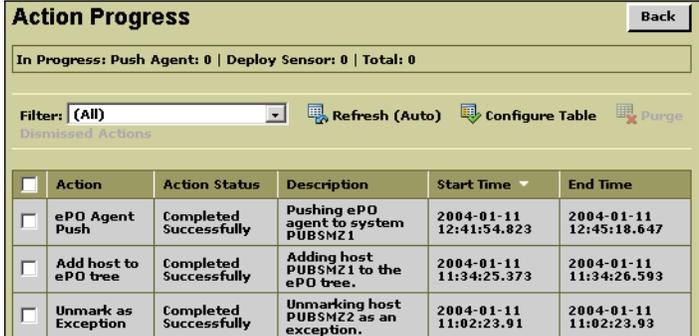
## Viewing status of actions taken and event history

Rogue System Detection allows you to check the history of events that have occurred. Also, you can view the status of actions you have taken, such as manually deploying an agent or sensor.

### Viewing the status of in-progress actions

You can confirm that the server is actually implementing your manual and automatic responses, such as deploying agents to rogue systems, by viewing the **Action Progress** page of the **Events** tab. The table lists all recent actions taken by the Rogue System Detection server, including both manual and automatic responses. After you have initiated a response, such as deploying a sensor to a specific system, that response is added to the table.

Figure 9-11 Action Progress page



Action Progress <span style="float: right;">Back</span>					
In Progress: Push Agent: 0   Deploy Sensor: 0   Total: 0					
Filter: (All) <span style="float: right;">Refresh (Auto) Configure Table Purge</span>					
Dismissed Actions					
<input type="checkbox"/>	Action	Action Status	Description	Start Time	End Time
<input type="checkbox"/>	ePO Agent Push	Completed Successfully	Pushing ePO agent to system PUBSMZ1	2004-01-11 12:41:54.823	2004-01-11 12:45:18.647
<input type="checkbox"/>	Add host to ePO tree	Completed Successfully	Adding host PUBSMZ1 to the ePO tree.	2004-01-11 11:34:25.373	2004-01-11 11:34:26.593
<input type="checkbox"/>	Unmark as Exception	Completed Successfully	Unmarking host PUBSMZ2 as an exception.	2004-01-11 11:02:23.91	2004-01-11 11:02:23.93

The **Action Status** column indicates whether the response is complete or still in progress. The response is in progress until the **Action Status** column displays **Completed** and the **End Time** column is populated with the date and time that the action was completed.

While a response is in progress, you must refresh the page to see whether the status has changed and the action has been completed. To do this, click **Refresh**.

Click any action listed in the **Action Progress** table to view more detailed information on that action.

### Viewing Rogue System Detection event history

The **Event History** table on the **Events** tab lists the recent Rogue System Detection server events that have occurred. As with any Rogue System Detection table, you can sort the table on any row, filter the table by event types, or click individual rows to view more detailed information on each event.

The events that the Rogue System Detection server can generate are:

- Rogue Machine Detection.** A sensor has detected a system that is not in the ePolicy Orchestrator database, indicating that the system does not have an agent installed.

- **User Request.** Any manual action taken by a user through the Rogue System Detection interface, such as marking systems as exceptions or adding systems to the Directory. Click these events in the **Event History** table to view details for the event, which show the specific action taken.
- **Subnet Uncovered.** A subnet that was covered by one or more Rogue System sensors is now uncovered again. This can occur if the sensors have been uninstalled or stopped. This event occurs only once the first time that the covered subnet becomes uncovered.
- **Agent Push Failed.** You deployed an agent to a rogue system from the **Machine List** page, but the agent failed to install successfully.
- **Sensor Push Failed.** You deployed a sensor to a system from the **Subnet List** page, but the sensor failed to install successfully.
- **Dismissed Events.** Events that you have removed from the **Event History** table. Note that dismissed events are only removed from the table and not from the database.

### Viewing details of a particular event

Click any event listed in the **Event History** table to view more detailed information, including any automatic responses associated with it.

### Dismissing old events to filter the Event History table

If the table becomes too large, you can remove old or unimportant events no longer requiring attention from the **Event History** table. To do this:

- 1 Select the checkboxes of desired events.
- 2 Click **Dismiss**.

Dismissed events are removed from the **Event History** table, but remain in the database so you can use them in queries and reports.

### Purging dismissed events from the database

If your database grows too large with dismissed events, you can purge selected dismissed events. This removes them from the database. You can only purge events that have already been dismissed.

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Events** tab, then click **Event History**.
- 3 Select **Dismissed Events** from the **Filter** drop-down list.
- 4 Click **Purge Dismissed**.



Purging events removes them from the database permanently, making them unavailable to reports or queries. Event history can provide very valuable information in troubleshooting problems with specific systems or subnets. Therefore, purge dismissed events only if you are certain the event information is no longer needed or if your database grows so large that it causes performance problems.

### Viewing event information in other locations

You can view additional detailed information on a particular action taken as part of an automatic response by clicking that action listed in the **Action Progress** page on the **Events** tab.

Also, you can view the event history for a particular system by clicking that system in the **Machine List** table. The **Events and Actions for this machine** table at the bottom of the page lists all events that have occurred for this system which are still in the database.

## Taking actions on detected rogue systems manually

You can perform actions on one or more systems listed in the **Machine List** table. For example, you may want to push an agent to a detected rogue system or mark systems for later action. In addition to these manual actions, you can configure automatic responses that can be initiated by a detection event.

For more information, see [Configuring automatic responses for specific events on page 200](#).

The following table lists the manual actions you can take on selected systems in the **Machine List** table. Some of these are covered in greater detail in following sections.

**Table 9-12 Available manual actions**

Action	Description
<b>Add to ePO tree</b>	Adds a system node to a <b>Rogue System</b> site in the Directory. You can place the systems into an appropriate site or group manually after it is added to this site.
<b>Mark for Action</b>	Marks the detected system as a system still needing action. For more information, see <a href="#">Marking specific systems for later action on page 198</a> .
<b>Mark as Exception</b>	Marks selected system as a machine that does not require an agent. For example, routers and printers. For more information, see <a href="#">Marking systems as exceptions on page 199</a> .
<b>Push ePO Agent</b>	Instructs the server to deploy an agent to the selected system. For more information, see <a href="#">Deploying agents to rogue systems on page 197</a> .
<b>Query ePO agent</b>	Queries the detected system to ascertain whether there is an agent installed on it. This query is required when using the <b>Alien Agent</b> rogue type. For more information, see <a href="#">Machine status and rogue type on page 175</a> .  Consider creating an automatic response that uses this action if you have multiple servers in your network. If travellers from other parts of your organization frequently log onto your network, they appear as rogue systems even if they have an agent from another server. For more information, see <a href="#">Configuring automatic responses for specific events on page 200</a> .
<b>Remove Host</b>	Hides the detected system in the <b>Machine List</b> table but does not delete it from the database.
<b>Unmark for Action</b>	Unmarks systems that you have already marked for action.
<b>Unmark as Exception</b>	Unmarks systems that you have already marked as exceptions.

## Deploying agents to rogue systems

One of the most important features of Rogue System Detection is the ability to deploy agents easily to newly-detected rogue systems. You can do this from the **Machine List** table. Once the agent is installed, ePolicy Orchestrator adds the systems to the Directory. If you are using IP filtering, the system is automatically added to the correct site or group. For more information, see [Deploying the agent when adding systems to the Directory on page 43](#).

Depending on your network, you may or may not be able to distribute agents to client systems with this method. For more information, see [Distributing agents on page 76](#).

To deploy agents from the **Machine List** table:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Machines** tab, then click **List** to display the **Machine List** table.
- 3 Select the checkbox of the desired system in the table.
- 4 In the **Checked machines** drop-down list, select **Push ePO Agent**, then click **Apply**.

Figure 9-12 Machine List page

<input type="checkbox"/>	Status	Friendly Name	IP	Last Detect Time
<input type="checkbox"/>	Rogue	PS-PRINCE	172.16.39.111	3/17/04 10:32:57 AM
<input checked="" type="checkbox"/>	Rogue	PUBSMZ1	172.16.39.23	3/17/04 11:17:17 AM
<input type="checkbox"/>	Rogue	PUBSMZ2	172.16.39.187	3/17/04 11:19:06 AM
<input type="checkbox"/>	Rogue	QA-MWYMAN	172.16.39.48	3/17/04 10:37:44 AM
<input type="checkbox"/>	Rogue	QA-MWYMAN2	172.16.39.209	3/17/04 10:42:20 AM
<input type="checkbox"/>	Rogue	RIESCLIENT	172.16.39.212	3/17/04 11:12:32 AM
<input type="checkbox"/>	Rogue	RIESSERVER	172.16.39.57	3/17/04 11:09:31 AM
<input type="checkbox"/>	Rogue	RIESTEST3	172.16.39.171	3/17/04 10:51:37 AM
<input type="checkbox"/>	Rogue	RLI-EN-WIN2KSRV	172.16.39.116	3/17/04 10:50:51 AM
<input type="checkbox"/>	Rogue	RLI-EN-WINXPP	172.16.39.124	3/17/04 10:45:29 AM

- 5 On the **Push Agent** page, modify the default installation configuration as desired.

Figure 9-13 Configure agent installation parameters for deployment

**Push Agent** Back

Agent version: ePO Agent 3.5.0 for Windows

Agent install configuration

Suppress agent installation GUI :

Installation path : <SYSTEM\_DRIVE>\ePOAgent

System Drive: C: ePOAgent

Credentials for agent push

Use ePO credentials :

User account (domain\user) :

Password :

The following table describes the settings on the **Push Agent** page:

**Table 9-13 Push Agent page settings**

Parameter	Description
<b>Agent version</b>	A drop-down list displaying the agent installation packages you have checked into your master software repository.
<b>Suppress agent installation GUI</b>	Deselecting this checkbox (not recommended) displays the agent installation on the client systems.
<b>Installation path</b>	The agent installation folder. By default this is C:\Program Files\McAfee.
<b>Credentials for agent push</b>	Make sure that the credentials you specify have domain administrator rights in the target system's network domain and also local administrator rights to the target system.

**6** Click **OK** to begin the agent deployment.

After clicking **OK**, the **Action Progress** page of the **Events** tab appears. The action is listed in the table and the **End Time** field is empty. When the agent installation is complete and the agent has called into the server, the **End Time** value is populated.

The status for the target system in the **Machine List** table changes from **Rogue** to **Managed** when the system is redetected.

After the agent-server communication, the server adds the system to the Directory.

## Adding systems to the Directory

You can add systems listed in the **Machine List** table to the Directory. New systems are added to a **Rogue Systems** site, from which you can move them manually or use IP sorting to move them automatically to the appropriate site or group.

To add systems to the Directory:

- 1** In the console tree, select **Rogue System Detection**.
- 2** In the details pane, select the **Machines** tab, then click **List** to display the **Machine List** table.
- 3** Select the checkboxes of the desired systems in the table.
- 4** Select **Add to ePO tree** from the **Checked machines** drop-down list, then click **Apply**.

After clicking **OK**, the **Response Progress** page of the **Events** tab appears, which contains a new entry for the system you have just added to the Directory. The system is added to a **Rogue Systems** site beneath the **Lost&Found** site in the Directory.

## Marking specific systems for later action

In some cases, you may not want to do anything to a particular system immediately.

To mark a system for later action:

- 1** In the console tree, select **Rogue System Detection**.
- 2** In the details pane, select the **Machines** tab, then click **List** to display the **Machine List** table.
- 3** Select the checkboxes of the desired systems in the table.

- 4 Select **Mark for Action** from the **Checked machines** drop-down list, then click **Apply**.

The system's entry in the **Machine List** table displays a red exclamation point icon in the **Action** column.

## Marking systems as exceptions

Some of the systems that sensors detect, such as network switches, routers, or printers, do not require agents and therefore are not rogue systems. You can mark these systems as exceptions to indicate they are not managed by ePolicy Orchestrator but are also not rogue systems. You can sort or filter the **Machine List** table to hide these systems so you can focus on true rogue systems.

You can also configure rules for automatic responses to classify certain systems as exceptions.

For more information, see [Configuring automatic responses for specific events on page 200](#).

### Marking specific systems as exceptions

You can mark a system in the **Machine List** table as an exception if it has a status of either **Rogue** or **Inactive**. Systems with a **Managed** status already have an agent installed, and therefore, are never going to be exceptions.

To mark a specific system as an exception:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Machines** tab, then click **List** to display the **Machine List** table.
- 3 Select the checkboxes of the desired systems in the table.
- 4 From the **Checked machines** drop-down list, select **Mark as Exception**, then click **Apply**.
- 5 Refresh the **Machine List** to see that the state for the selected system has been changed to **Exception**.

### Importing and exporting exceptions using an XML file

To prevent the need to re-create the exceptions list if you must reinstall the ePolicy Orchestrator server, you can save your exceptions list to an XML file. The exceptions list preserves your exceptions information so you can re-import it easily when needed.

#### Exporting the exceptions list

Exporting your current list of exception systems to an XML file includes all systems from your **Machine List** table that you have marked as exceptions. To export your current list of exceptions to an XML file:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab, then select **Basic Configuration**.
- 3 Click **Export** under **Exceptions List Import / Export** at the bottom of the page.

The exported XML exceptions list appears in a new Internet Explorer browser window. You can save this XML file to a secure location so that you can re-import it later.

**Import the exceptions list file**

You can also re-import an exceptions list. When imported, the exception list overwrites all data for those systems that are listed in the exception list. When you do this, be aware that the exception list overwrites information for the **Machine List** table. For example, if Machine A is listed in your current database as a **Rogue**, but in your exported exception list as an exception, when you import the exception list the status of Machine A changes to **Exception**.

To import an exported exception list XML file:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab, then select **Basic Configuration**.
- 3 Under **Exceptions List Import / Export** at the bottom of the page, type the full path and file name into the text box or browse to the exceptions list XML file on your hard drive, then click **Import**.
- 4 Go to the **Machine List** and refresh your browser to see the newly imported exception data reflected in the table.

---

## Configuring automatic responses for specific events

You can configure automatic responses so that ePolicy Orchestrator responds automatically to the Rogue System Detection events. There are two specific Rogue System Detection events for which you can configure automatic responses:

- **Rogue Machine Detected.** A new system not already found in the ePolicy Orchestrator database.
- **Subnet Uncovered.** A subnet in your network that does not have a rogue system sensor installed.

You can also configure responses for any event.

An automatic response can contain one or more of the actions described in the following table. For example, if you configure a response to deploy an ePolicy Orchestrator agent to newly-detected systems, you may also want to send an e-mail to administrators to follow up on the agent installation.

**Table 9-14 Actions available for automatic responses**

Action	Description
Add to ePO tree	Adds the system to a <b>Rogue System</b> site within the Directory. After the system is added to this site, you can move the system to an appropriate location manually.
Mark for Action	Marks the detected system as a system still needing action. For more information, see <a href="#">Marking specific systems for later action on page 198</a> .

**Table 9-14 Actions available for automatic responses**

Action	Description
<b>Mark as Exception</b>	<p>Marks selected system as a machine that does not require an agent. For example, routers and printers. For more information, see <a href="#">Marking specific systems as exceptions on page 199</a>.</p> <p>For example, in your organization you may reserve a range of IP addresses within each subnet for network equipment such as routers, switches, and printers. You can create an automatic response to mark such equipment as exceptions and add a condition to initiate the response only if the detected system's IP address falls within a certain range. Or, maybe you use certain vendors for network equipment that are always different from your vendors for server or workstation systems. In this case, you can use the <b>OUI Org</b> condition to initiate an automatic response to mark systems as exceptions if the system's MAC address contains a specific vendor code.</p>
<b>Push ePO Agent</b>	Instructs the server to deploy an agent to the selected system. For more information, see <a href="#">Deploying agents to rogue systems on page 197</a> .
<b>Query ePO agent</b>	<p>Queries the detected system to ascertain whether there is an agent installed on it. This query is required when using the <b>Alien Agent</b> rogue type. For more information, see <a href="#">Machine status and rogue type on page 175</a>.</p> <p>Consider creating an automatic response that uses this action if you have multiple servers in your network. If travellers from other parts of your organization frequently log onto your network, they appear as rogue systems even if they have an agent from another server installed. For more information, see <a href="#">Configuring automatic responses for specific events on page 200</a>.</p>
<b>Remove Host</b>	Hides the detected system in the <b>Machine List</b> table but does not delete it from the database.
<b>Send E-mail</b>	<p>Sends a pre-configured e-mail message to pre-configured recipients.</p> <p>See <a href="#">Configuring automatic e-mail alerts on page 201</a>.</p>
<b>Send ePO Server Event</b>	Forwards Rogue System Detection and Subnet Uncovered events to the server. This is required if you plan to use Notifications to automatically send e-mail alerts for Rogue System Detection events.
<b>Unmark for Action</b>	Unmarks systems that you have already marked for action.
<b>Unmark as Exception</b>	Unmarks systems that you have already marked as exceptions.

## Configuring automatic e-mail alerts

One of the most common automated tasks used is to have the Rogue System Detection server send an e-mail alert when sensors detect new rogue systems on the network. This is a fast and easy way to alert you or other network administrators of potentially unmanaged systems so you can take appropriate remediation.

You can configure e-mail alerts for Rogue System Detection events in two ways. You can configure the automatic response to send e-mail alerts in the Rogue System Detection interface, or you can configure Notifications to handle messages for these events.



Configure all your e-mail alert messages in Notifications if you want to send all Rogue System Detection events to the same address(es). Configure e-mail notifications in the Rogue System Detection interface if you want more granularity in defining recipients of rogue detection e-mail alerts.

There are benefits to using each of these features for this purpose:

#### Automatic Response

- More domain-specific information.
- Tokens that provide more Rogue System Detection-specific information.
- Information can be sent based on specified **Conditions**.

#### Notification

- Centralized alerting for all events types.
- Throttling and aggregation of messages.
- Ability to send SNMP traps as well as e-mail messages.



For instructions to use Notifications to send e-mail alerts for Rogue System Detection events, see [Configuring Rogue System Detection for Notifications](#) on page 207.

## Configuring e-mail alerts in Rogue System Detection

There is more flexibility with your e-mail alerts in Rogue System Detection than in Notifications. You can use the Conditions feature on the **Add or Edit Automatic Response** page to create separate e-mail alerts for different criteria. For example, if you have different IT personnel responsible for different parts of your network or for different types of systems, such as workstations or servers, you can create separate, targeted e-mail alerts that go to different people depending on the IP address. Or you can send an e-mail alert for a newly-detected server to the IT team that is responsible for servers.

To configure an automatic response to send an e-mail alert, perform the following tasks:

- 1 [Configuring Rogue System Detection to use your e-mail server.](#)
- 2 [Adding recipients to the automatic response contact list.](#)
- 3 [Creating an automatic e-mail response.](#)

### Configuring Rogue System Detection to use your e-mail server

If you have not done so already, specify an e-mail server on your network that Rogue System Detection should use to sending e-mail alerts. Rogue System Detection communicates with the e-mail server via SMTP over TCP/IP.

The ePolicy Orchestrator server can send SMTP messages to the e-mail server as long as it can “see” the e-mail server on the network. To test this connectivity, use a ping command from the ePolicy Orchestrator server to the e-mail server. Depending on your e-mail server configuration, there may be additional requirements. For example, ePolicy Orchestrator may need to reside in the same domain as the e-mail server. Consult your network documentation to troubleshoot any connection issues between your ePolicy Orchestrator server and e-mail server.

To configure Rogue System Detection to use an SMTP e-mail server:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab, then select **Basic Configuration**.
- 3 Under **E-mail alerting**, type the name of your e-mail server in the **Mail server** text box.
- 4 Type a valid return address in the **From** text field.

This must be a valid e-mail address. E-mail alerts that cannot be delivered are returned to this address. You may need to access this e-mail account occasionally to troubleshoot or track undelivered Rogue System Detection e-mail alerts.

- 5 At the bottom of the **Basic Configuration** page, click **Apply** to save the change.

### Adding recipients to the automatic response contact list

Manage the list of recipients for rogue detection e-mail alerts from the **E-mail Contacts** table. Before creating an automatic response to send e-mail alerts, be sure to add any desired recipients to the **E-mail Contacts** table.

You must add a separate contact for each e-mail address to which you might send e-mail alerts. If you want to send some e-mail alerts to many recipients, create a distribution list on your e-mail server and then create a Rogue System Detection e-mail contact for that address instead.

E-mail contacts added in either Rogue System Detection or Notifications are available in both.

To add a new e-mail contact for a Rogue System Detection alert:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab, then select **E-mail Contacts**.
- 3 Click **Add Contact** above the list of current contacts.
- 4 Type a name or short description for the new contact in the **Name** text box.
- 5 Type the e-mail address for the contact into the **E-mail address** text box. Make sure you type the complete and correct e-mail address, such as `MyEmail@example.com`.
- 6 Click **OK**.

## Creating an automatic e-mail response

Once you have configured Rogue System Detection to use your e-mail server and created one or more e-mail contacts to which to send e-mail alerts, you can create the automated e-mail response.



To configure Notifications to send notification e-mail messages based on Rogue System Detection events. For more information, see [Chapter 10, ePolicy Orchestrator Notifications](#).

To create an automated e-mail response for this event:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Responses** tab, then click **Add Automatic Response**.

**Figure 9-14 Create an automatic e-mail response**

Property	Comparison	Value	Delete

- 3 Type a short description of the response in the **Name** field. This name appears in the list of available automatic responses in the **Automatic Responses** table.
- 4 From the **Event** drop-down list, select **Rogue Machine Detected**.
- 5 Make sure **Enabled** is selected. This allows the response to happen automatically every time a Rogue System Detection event occurs.
- 6 To add conditions, select **Add Condition** and then configure the property and its value.  
You can add one or more conditions that must be met before the automatic response occurs. For example, you may want to perform this action only if the detected rogue system is located in a specific subnet or IP address range, or only if the system is running a particular version of Windows.
- 7 Under **Actions**, select **Send E-mail** from the **Method** drop-down list.
- 8 Select a recipient from the **To** drop-down list of available recipients. If the address you want is not available in the list, you must first add it to the contact list. For more information, see [Adding recipients to the automatic response contact list on page 203](#).
- 9 Type your e-mail message in the **Subject** and **Body** fields.

You can include tokens in your e-mail by selecting them from the **Insert Variable** drop-down list and inserting them in the e-mail subject or body. Tokens represent information such as IP address, subnet location, and operating system of any new rogue systems that are detected. Rogue System Detection dynamically populates these tokens with real data about the detected system.

**10** To send e-mails to multiple addresses, add an additional response for each contact to which you want to send an e-mail. To do this, click **Add Action** and repeat [Step 7](#) through [Step 9](#), for each additional contact.

**11** Click **OK** to save the new automatic response.

The new automatic response is enabled once it has been added to the response list. The next time that the event associated with the response occurs, Rogue System Detection initiates the configured response.

## Using command-line executables in automatic responses

You can run any command-line executables to gather additional information about detected systems. You can run these executables as part of an automatic response to a detected rogue system or uncovered subnet event, or you can run them manually. To run command-line executables, they must be installed on the ePolicy Orchestrator server.

You can run command-line executables only as part of an automatic response, as described in this section.

Two common executables you may want to use are listed below.

### **NMAP.EXE Network Mapper**

NMAP (Network Mapper) is a free, open-source utility for performing security audits of individual systems and entire networks. Features include network-wide ping sweep, port scan, and operating system detection. An advantage of NMAP is the information returned — it can identify operating system type and other information about non-Windows systems. The sensor can identify operating system type only for Windows-based systems. This more specific information provided by NMAP is placed into the appropriate host field.

For more information, see <http://www.insecure.org/nmap>.

### **NSLOOKUP.EXE**

NSLOOKUP.EXE is a simple utility that comes with Windows and looks up information on specific systems using the DNS name server. Use this utility when the sensor is unable to resolve DNS name information for certain systems. For example, you can create an automatic event with a condition that tests if the DNS name field of a detected system is blank, then run NSLOOKUP.EXE to see if the DNS server has the system name.

This command-line tool is installed on Windows systems if you have the TCP/IP protocol installed, typically installed in the `System32` folder.

## Configuring an executable for an automatic response

To configure a command-line executable for use with an automatic response, perform the following tasks, in order:

- 1 *Making a registered executable available to Rogue System Detection.*
- 2 *Configuring the executable command-line options.*
- 3 *Using the command-line option in an automatic response.*

See the following sections for more details on each of these steps.

### Making a registered executable available to Rogue System Detection

Before you can configure a command-line tool for an automatic response, you must register it with Rogue System Detection. Registering ensures that only the executable applications you want are available, and allows you to make the executable available for other ePolicy Orchestrator administrators.

To register an executable:

- 1 Install the executable, if it is not already, on the system hosting your ePolicy Orchestrator server.
- 2 In the console tree, select **Rogue System Detection**.
- 3 In the details pane, select the **Configuration** tab, then select **External Commands**.
- 4 On the **External Commands** page, select **Add Registered Executable**.
- 5 On the **Add or Edit Registered Executable** page, type a descriptive name for the executable in the **Name** field.
- 6 Type the full path or browse to the location of the .EXE file for this executable.
- 7 Click **OK**.

The executable is added to the list of available registered executables. It is also available for you to configure command-line options under the **Command Lines** section of the **External Commands** page.

### Configuring the executable command-line options

Once you have registered an executable, you can configure command-line options for it. To do this:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Configuration** tab, then select **External Commands**.
- 3 On the **External Commands** page, select **Add Command Line**.
- 4 On the **Add or Edit Command Line** page, type a descriptive name for the command in the **Name** field.
- 5 Select the executable to use for this command-line option from the drop-down list of registered executables that are available to Rogue System Detection.

6 Type arguments into the **Arguments** field. Consult the documentation for the relevant executable to make sure you use the correct syntax. Optionally, you can include a number of system tokens. These are available in the **Variables** drop-down list.

7 Click **Add** when finished.

The command-line option is added to the list of available **Command Lines**. It is also available in the **Method** drop-down list on the **Add or Edit Automatic Response** page, for you to include it as an action as part of an automatic response.

### Using the command-line option in an automatic response

Once configured, the registered command-line option is available in the **Method** drop-down list on the **Add or Edit Automatic Response** page. You can configure automatic responses that can run the executable.

Results of run executables are viewable on the **Machine Details** and on the **Action Progress** page of the **Events** tab. You can click the list items to drill down to more detailed information.

---

## Configuring Rogue System Detection for Notifications

You can configure Notifications to send messages based on certain events from Rogue System Detection.

To configure notification messages you must perform the following tasks, in order:

- 1 [Configuring an automatic response to send ePO server events.](#)
- 2 [Creating a notification rule based on Rogue System Detection events.](#)

## Configuring an automatic response to send ePO server events

To configure an automatic response to send ePO server events:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Responses** tab.
- 3 Click **Add Automatic Response**. The **Add or Edit Automatic Response** page appears.
- 4 Specify a **Name** for the automatic response. For example, **Send event to Notification**.
- 5 Select an event type from the **Event** drop-down list for which to configure the automatic response. We recommend selecting **Any Event**.



Rogue System Detection can only send two events to Notifications: **Rogue Machine Detected** and **Subnet Uncovered**. Selecting **Any Event** forwards either type to Notifications.

- 6 Add any desired conditions.
- 7 In the **Actions** section under **Method**, change the default method to **Send ePO Server Event**.
- 8 Click **OK**.

## Creating a notification rule based on Rogue System Detection events

Create a notification rule to send notification messages based on Rogue System Detection events. For instructions to create notification rules, see [Creating and editing rules](#).



Notifications can only send notification messages (regarding Rogue System Detection) based on server events.

When creating a notification rule for Rogue System Detection events, you must:

- Select **ePO Server** from the **Products** list on the **Set Filters** page.
- Select either **New Rogue System detected** or **Subnet has become unmonitored by Rogue System Sensor**.

McAfee recommends utilizing the aggregation and throttling features for all rules.

## Rogue System sensor command-line options

You can run command-line options from the client system. The following table lists the run-time command-line options for the sensor.

**Table 9-15 Sensor runtime command line options**

Switch	Description
--help	Prints the help screen listing available command-line options.
--install	Registers the sensor with the Windows Service Control Manager (SCM).
--uninstall	Unregisters the sensor with the Windows Service Control Manager.
--version	Prints the version of the sensor and exits.
--server "[server name]" or "[IP address]"	Overrides the ServerName configuration setting in the registry that you specified during installation.  <b>Note:</b> This parameter only takes affect when running in command-line mode, which requires the --console command line switch as well.  Sample syntax:  <code>sensor.exe --server "MyServerName" --console</code>
--port "[server port]"	Overrides the ServerPort configuration setting in the registry that you specified during installation.  <b>Note:</b> This parameter only takes affect when running in command-line mode, which requires the --console option.  Sample syntax:  <code>sensor.exe --port "8081" --console</code>
--console	Forces the sensor to run as a normal command-line executable; otherwise it must be run as an NT service.

---

## Frequently asked questions

### **Is the sensor deployed automatically when I install the server?**

No, you must initiate sensor deployment. Basically, the sensor is treated like any other managed security product by ePolicy Orchestrator.

### **Will events from the sensor cause agents to be deployed automatically?**

By default, no; the sensor is configured to monitor and alert you to new rogues or subnets. However, you can configure an automatic response for the server to deploy agents when specific events are received from the sensor.

### **What happens when a sensor is deployed – in terms of agents and managed products getting installed?**

Sensor deployment does not affect the installation of agents and other managed products. However, from the ePolicy Orchestrator console, the sensor can only be deployed to a system that already has an agent.

The sensor is treated by ePolicy Orchestrator as a managed product.

### **What happens when the system where the sensor is installed changes subnets?**

Occasionally, you may need to move a system on which a sensor is installed from one broadcast segment to another. For example, this can happen when such a system is a laptop that may connect to different broadcast segments at different times.

The sensor correctly recognizes when its location has changed and reports this change to the server. If the system running the sensor changes broadcast segments, this is reflected immediately in the **Subnet List** table. If you deploy a sensor to a system that may change subnets, such as a laptop, make sure you deploy another sensor to cover that subnet.

For more information, see [Viewing your subnets on page 193](#).

# 10

## ePolicy Orchestrator Notifications

### Configure rules to alert you to events on your network

The ePolicy Orchestrator Notifications feature can alert you to any events that occur on the managed systems in your environment or on the ePolicy Orchestrator server itself. You can configure rules in ePolicy Orchestrator to send e-mail, SMS, or text pager messages (or SNMP traps), as well as run external commands, when specific events are received and processed by the ePolicy Orchestrator server. The ability to specify the event categories that generate a notification message and the frequencies with which notifications are sent are highly configurable.



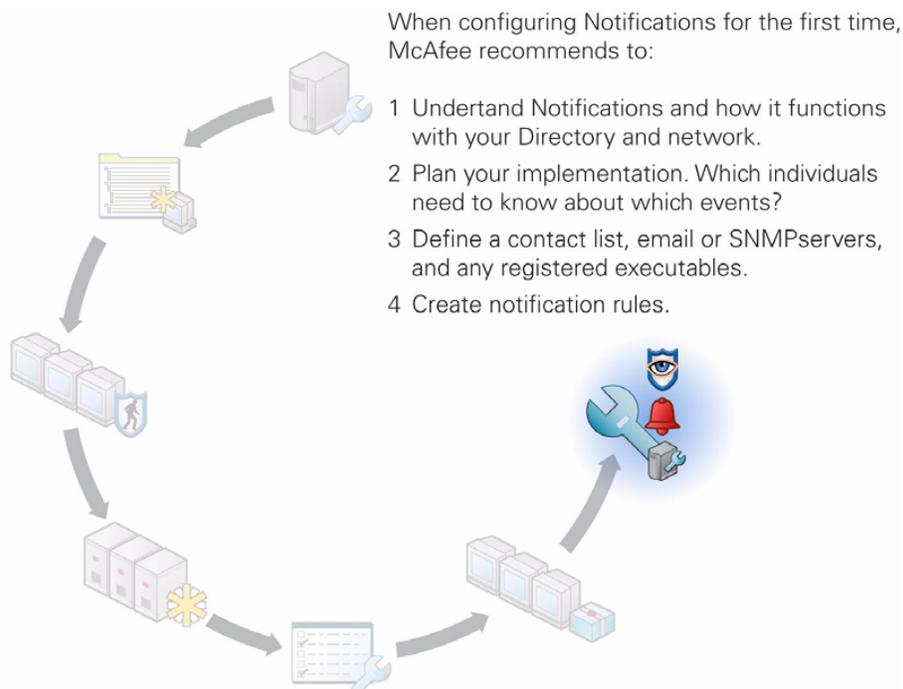
For a list of specific products and ePolicy Orchestrator components for which you can configure notifications, see [Product and component list on page 228](#).

This feature is designed to notify specific individuals when the conditions of a rule are met. These can include:

- Detection of a virus or other potentially unwanted program by your anti-virus software product. Although almost any anti-virus software product is supported, events from VirusScan Enterprise 8.0i include the IP address of the source attacker so that you can isolate the system infecting the rest of your environment.
- Outbreak situations. For example, 1000 virus detected events are received within five minutes.
- Compliance events from McAfee System Compliance Profiler. For example, systems are found that are not current with the latest Microsoft patches.
- High-level compliance of ePolicy Orchestrator server events. For example, a replication task did not complete.
- Detection of rogue systems.

This feature also allows you to configure notification rules to execute command lines and launch registered executables when the specified conditions are met.

### Configuring Notifications for the first time?



## About Notifications

Before you plan the implementation of Notifications, you should understand how this feature works with ePolicy Orchestrator and its Directory.



This feature does not follow the inheritance model of policy enforcement.

When events occur on systems in your environment, they are delivered to the ePolicy Orchestrator server, and the notification rules (associated with the group or site that contains the affected systems and each parent above it) are applied to the events. If the conditions of any such rule are met, a notification message is sent, or an external command is run, per the rule's configurations.

This design allows you to configure independent rules at the different levels of the Directory. These rules can have different:

- Thresholds used to send a notification message. For example, a site administrator wants to be notified if viruses are detected on 100 systems within 10 minutes on the site, but a global administrator does not want to be notified unless viruses are detected on 1000 systems within the same amount of time within the entire environment.
- Recipients for the notification message. For example, a site administrator wants to receive a notification message only if a specified number of virus detection events occur within the site. Or, a global administrator wants each site administrator to receive a notification message if a specified number of virus detection events occur within the entire Directory.

## Throttling and aggregation

You can configure when notification messages are sent by setting thresholds based on *aggregation* and *throttling*.

### Aggregation

Use aggregation to determine the thresholds of events at which the rule sends a notification message. For example, you can configure the same rule to send a notification message when the ePolicy Orchestrator server receives 100 virus detection events from different systems within an hour *and* whenever it has received 1000 virus detection events altogether from any system.

### Throttling

Once you have configured the rule to notify you of a possible outbreak situation, you may want to use throttling to ensure you do not get too many notification messages. If you are administering a large network, then you may be receiving tens of thousands of events during an hour, creating thousands of notification messages based on such a rule. ePolicy Orchestrator Notifications allows you to throttle the number of notification messages you receive based on a single rule. For example, you can specify in this same rule that you don't want to receive more than one notification message in an hour.

For instructions, see [Creating and editing rules on page 220](#).

## Notification rules and Directory scenarios

To show how this feature functions with the Directory, two scenarios are used.

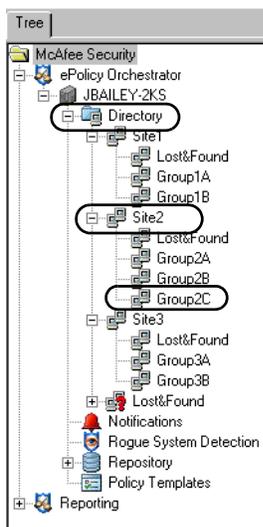
For both scenarios, we can assume that each group, site, and the Directory root of the console tree has a similar rule configured. Each rule is configured to send a notification message when 100 virus infection events have been received from any product within 60 minutes. For reference purposes, each rule is named **VirusDetected\_<node name>**, where <nodename> is the name of the node as it appears in the Directory (for example, **VirusDetected\_Group2c**).

## Scenario one

For this scenario, 100 virus infections are detected in Goup2C within 60 minutes in a single day.

Conditions of the rules **VirusDetected\_Group2C**, **VirusDetected\_Site2**, and **VirusDetected\_Directory** are met, sending notification messages (or launching registered executables) per the rules' configurations.

Figure 10-1 Console tree

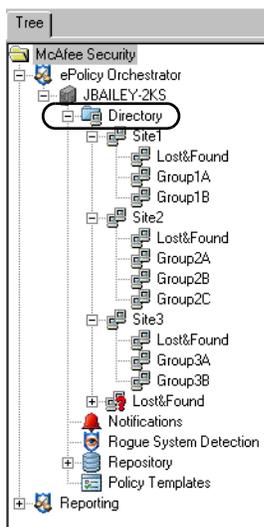


## Scenario two

For this scenario, 50 virus infections are detected in **Group2C** and 50 virus infections are detected in **Group3B** within 60 minutes in a single day.

Conditions of the **VirusDetected\_Directory** rule are met, sending notification messages (or launching registered executables) per the rules' configurations. This the only rule that can be applied to all 100 events.

**Figure 10-2 Console tree**



## Default rules

ePolicy Orchestrator provides six default rules that you can enable for immediate use while you learn more about the feature.



Once enabled, the default rules send notification e-mail messages to the e-mail address you provided on the **Set E-mail Address** panel of the installation wizard.

You can edit any of the default rules as necessary.

Before enabling any of the default rules:

- Specify the e-mail server from which the notification messages are sent. For more information, see [Basic configurations of Notifications on page 217](#).
- Ensure the recipient e-mail address is the one you want to receive e-mail messages. For more information, see [E-mail contacts list on page 218](#).

The default rules are described in [Table 10-1](#):

**Table 10-1 Default notification rules**

Rule name	Associated events	Configurations
Daily unknown product notification	Any events from any unknown products.	Sends a notification message at most, once a day.
Daily unknown category notification	Any event of an unknown category.	Sends a notification message at most, once a day.

**Table 10-1 Default notification rules**

Rule name	Associated events	Configurations
Virus detected and not removed	<b>Virus Detected and Not Removed</b> events from any product.	Sends a notification message: <ul style="list-style-type: none"> <li>■ When the number of events exceeds 1000 within an hour.</li> <li>■ At most, once every two hours.</li> <li>■ With the source system IP address, actual threat names, and actual product information, if available.</li> </ul>
Virus detected heuristics and not removed	<b>Virus Detected (Heuristics) and Not Removed</b> events from any product.	Sends a notification message: <ul style="list-style-type: none"> <li>■ When the number of events exceeds 1000 within an hour.</li> <li>■ At most, once every two hours.</li> <li>■ With the source system IP address, actual threat names, and actual product information, if available.</li> </ul>
Repository update or replication failed		Sends a notification message when any events are received.
Non-compliant computer detected	<b>Non-compliant Computer Detected</b> events.	Sends a notification message: <ul style="list-style-type: none"> <li>■ When any events are received.</li> <li>■ Once per each rule of the Compliance Check server task. (This task sends one event per each of the four rules associated with the Compliance Check server task.)</li> </ul>

## Determining when events are forwarded

The ePolicy Orchestrator server receives notifications from the Common Management Agent (CMA). You must configure its policy pages to forward events either immediately to the ePolicy Orchestrator server or only at agent-to-server communication intervals.

If you choose to have events sent immediately (as set by default in ePolicy Orchestrator Agent 3.5.0 McAfee Default policy), the agent forwards all events as soon as they are received. If you want all events sent to the ePolicy Orchestrator server immediately so that they can be processed by Notifications when the events occur, configure the agent to send them immediately.

If you choose not to have events sent immediately, the agent only forwards events immediately that are designated by the issuing product as high priority. Other events are only sent at the agent-to-server communication intervals.

If the currently applied named policy is not set for immediate uploading of events, either edit the currently applied named policy or create a new named policy for the **ePO Agent 3.5.0 | Configuration** policy pages. This setting is configured on the **Events** tab of these policy pages.

---

## Determining which events are forwarded

Along with being able to determine when events are forwarded to the server, you can also select which events are forwarded.



If you choose not to select which events are forwarded, all events are forwarded. This is the default setting.

To select which events are forwarded immediately:

- 1 In the console tree, select the desired ePolicy Orchestrator database server under **Reporting** and log onto it.
- 2 Select **Events** in the console tree under the database server.
- 3 Select the **Filtering** tab in the details pane.
- 4 Select **Send only the selected events to ePO** on the **Filtering** tab.
- 5 Select the desired events in the list and click **Apply**.

---

## Planning

Before creating rules that send notifications, you can save time by planning:

- The types of events (both product and server) that could generate and send a notification message in your environment. For more information, see [Product and component list on page 228](#).
- Who should receive which notifications. For example, it may not be necessary to notify the site administrator of site B about a failed replication in site A, but you may want all site administrators to know that an infected file was discovered in site A.
- Which types and levels of thresholds you want to set for each rule. For example, you may not want to receive an e-mail message every time an infected file is detected during an outbreak. Instead, you can choose to have such an e-mail message sent — at most — once every five minutes, regardless of how often that server is receiving the event.
- Which command lines or registered executables you want to run when the conditions of a rule are met.

---

## Configuring Notifications

To use this feature, you need to configure:

- [Basic configurations of Notifications on page 217](#) — The **Basic Configurations** interface allows you to specify some interface configurations and an e-mail server from which to send notification messages.
- [E-mail contacts list on page 218](#) — This is the list from which you select recipients of notification messages.

- [SNMP servers on page 219](#) — You can specify a list of SNMP servers to use while creating rules. You can configure rules to send SNMP traps to SNMP servers when the conditions are met for a rule to initiate a notification message.
- [Configuring external commands on page 219](#) — You can specify a list of external commands to run when the conditions of a rule are met.

## Basic configurations of Notifications

If you have not yet implemented the feature, or if you want to make modifications to it, you can set some basic configurations. Here, you can specify some interface configurations, which rules and notification messages site administrators and reviewers can view, and an e-mail server from which to send notification messages.

- 1 In the console tree, select **Notifications**.
- 2 Select the **Configuration** tab in the details pane, then click **Basic Configuration**.

Figure 10-3 Basic Configuration page

- 3 Under **UI Related**, configure the following, as desired:
  - **Number of items to view per page** — This setting defines how many items display at one time. When there are more items than the quantity you specify here, a **Next** button appears on the page to allow you to navigate through the items in sets of this size.
  - **Auto Refresh delay** — Enable this feature by selecting the checkbox, then type the number of seconds you want the system to wait between automatic refreshes of database tables.
  - **Site administrators/reviewers can view Directory rules/notifications** — If selected, site administrators and reviewers can view global rules and notifications. If deselected, site administrators can only view site rules and notifications, and cannot filter them.



Site administrators can not edit global rules.

- **Site administrators can edit E-mail Contacts, SNMP servers, and External Commands** — If selected, site administrators can edit the other areas of the **Configuration** tab.
- 4 Under **E-mail Server**, type:
- The name of the **Mail server**.
  - The e-mail address you want to appear in the **From** line of the notification message.



This e-mail address does not have to be the same address from which the notification message is sent. This is an address to populate the **From** line only — it can be any text that matches the format of an e-mail address.

- 5 Click **OK**.

## E-mail contacts list

The e-mail contacts list expedites rule creation by defining a list of e-mail addresses that can be reused.



Creating a contact list is not necessary, but you may find it convenient.

To configure the e-mail contacts list:

- 1 In the console tree, select **Notifications**.
- 2 In the details pane, select the **Configuration** tab, then click **E-mail Contacts**. This page allows you to specify the e-mail addresses of individuals you want to receive notifications of events.

**Figure 10-4 Add or Edit E-mail Message page**

- 3 Click **Add Contact**, and type the name of the recipient and the recipient's e-mail address, then click **OK**. Repeat as necessary.

## SNMP servers

You can configure ePolicy Orchestrator Notifications to send SNMP (Simple Network Management Protocol) traps to your SNMP server. This allows you to receive SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment. Before using this feature, you must add your SNMP servers to Notifications, and import the .MIB files.



You do not need to make other configurations or start any services to configure this feature.

### Adding SNMP servers

To be able to receive an SNMP trap, you must add the server's information to ePolicy Orchestrator so that ePolicy Orchestrator knows where to send the trap.

To add an SNMP server:

- 1 In the console tree, select **Notifications**.
- 2 Select the **Configuration** tab in the details pane, then click **SNMP Servers**. The **SNMP Servers** page appears displaying a list of the SNMP servers currently added.
- 3 Click **Add SNMP Server**, type the **Name** and the **Server address** of the desired SNMP server, then click **OK**.



If you are editing an already added SNMP server, click the server in the list and the settings of this server appear.

### Deleting an SNMP server from Notifications

To delete an SNMP server from Notifications, click the **X** button in the **Delete** column next to the desired SNMP server in the list.

### Importing .MIB files

If you are setting up rules to send notification messages to an SNMP server via an SNMP trap, you must import the NAICOMPLETE.MIB file. This file is located at:

```
\Program files\mcafee\ePO\3.6.0\MIB
```

This file allows your network management program to decode the data in the SNMP traps sent by Notifications into meaningful text.

For instructions on importing and implementing .MIB files, see the product documentation for your network management program.

## Configuring external commands

You can configure notification rules to execute an external command when the rule is initiated. You must first add the registered executable before adding the command line that references the executable.



You can only configure registered executables on the server. You cannot configure registered executables from a remote console.

You can configure a list of external commands which you can select from when creating or editing rules.



Before configuring the list of external commands, you should place the external commands to the location on your system to which the rules can point.

To create the external commands list:

- 1 In the console tree, select **Notifications**.
- 2 Select the **Configuration** tab in the details pane, then click **External Commands**. The **External Commands** page appears displaying two lists: The **Command Lines** and **Registered Executables** lists.
- 3 To add a command line, click **Add Command Line**. The **Add or Edit Command Line** page appears.

To add a registered executable, click **Add Registered Executable**. The **Add or Edit Registered Executable** page appears.



You can configure multiple command lines that reference a single registered executable.

- 4 Type a **Name** for the external command.
- 5 Type or **Browse** to the external command you want the rule to execute when initiated.
- 6 Click **OK** to add the external command to the list.
- 7 Repeat [Step 3](#) through [Step 6](#) as necessary.



You can add the command lines to rules when you create or edit them.

## Creating and editing rules

Rules allow you to define when, how, and to whom, notifications are sent.



Notification rules do not have a dependency order.

Creating or editing a rule is a several step process:

- 1 [Describing the rule on page 221](#).
- 2 [Setting filters for the rule on page 222](#).
- 3 [Setting thresholds of the rule on page 223](#).
- 4 [Configuring the notifications for the rule on page 224](#).

## Describing the rule

The **Describe Rule** page allows you to:

- Define the Directory, site, or group to which the rule applies.
- Name and describe the rule.
- Set a priority for the notification message.

To begin creating or editing a rule:

- 1 In the console tree, select **Notifications**.
- 2 In the details pane, select the **Rules** tab.
- 3 To create a new rule, click **Add rule**. The **Add or Edit Notification Rule** wizard appears.

**Figure 10-5 Describe Rule page**

To edit an existing rule, click the desired rule in the **Notification Rules** list. The **Add or Edit Notification Rule** wizard appears. The pages of the wizard are filled by default with the specifics of the selected rule.

- 4 On the **Describe Rule** panel, click **Browse** to select the Directory or a desired site or group of the console tree to which the rule applies.
- 5 Type the desired **Rule Name**.



Rule names on each server must be unique. For example, if one site administrator creates a rule named **Emergency Alert**, no other administrator (site or global) can create a rule with the same name.

- 6 Type a **Description** of the rule, if desired. This should be something that clearly distinguishes this rule from other rules.

- 7 Set the priority of the rule to **High**, **Medium**, or **Low**.



The priority of the rule is used to set a flag on an e-mail message in the recipient's Inbox. For example, selecting **High** places a red exclamation mark next to the notification e-mail message, and selecting **Low** places a blue, down-facing arrow next to the notification e-mail message. The priority does not affect the rule or event processing in any way.

- 8 Click **Next**.

## Setting filters for the rule

On the **Set Filters** page:

- 1 Select the **Products** whose events initiate this rule.

Figure 10-6 Set Filters page

**Add or Edit Notification Rule** Back

1. Describe Rule | 2. **Set Filters** | 3. Set Thresholds | 4. Create Notifications | 5. View Summary

For notification rule: **VirusScan 8.0i event!**

Select the types of events that will trigger this rule.  
Use Shift-click and Ctrl-click to select multiple products or categories.

Operating systems:  Workstation  Server  Unknown

Products:  Products selected below  Any product

1 selected

ThreatScan	Select All
Unknown Product	Deselect All
Virus	
VirusScan	
VirusScan PDA	
WebShield	

Categories:  Categories selected below  Any category

Any selected

Access Protection rule violation detected and blocked	Select All
Access Protection rule violation detected and NOT blocked	Deselect All
Buffer Overflow detected and blocked	
Buffer Overflow detected and NOT blocked	
Intrusion detected	
Normal operation	

Threat or rule name: (Any)

- 2 Select **Categories** of events that initiate this rule.



Both the **Products** and **Categories** selections must be true for the rule to initiate and send a notification. For example, if you select **VirusScan** and **Virus detected but NOT cleaned**, the rule does not send a message for a Dr. Ahn **Virus detected but NOT cleaned** event.

If only the event category is important, then select **Any product**.

3 In **Threat name**, define the pattern matching the threat comparison to use.

- a Select an operator from the drop-down list.
- b Type any text for the operator to act on.

For example, if you want to use the name of a virus. Select **Contains** as the operator, then type **nimda** in the text box, then events are scanned for any line of text that contains **nimda**.



If you choose to filter on a threat name, the **Products**, **Categories**, and the **Threat name** selections must all be true for the rule to send a notification message.

4 Click **Next**.

## Setting thresholds of the rule

The **Set Thresholds** page allows you to define when the rule initiates a notification message.

On the **Set Thresholds** page:

- 1 Define whether to send a notification for every event, or a notification per multiple events within a defined amount of time. If you choose the latter, define this amount of time in minutes, days, or weeks.

Figure 10-7 Set Thresholds page

**Add or Edit Notification Rule**

1. Describe Rule | 2. Set Filters | 3. **Set Thresholds** | 4. Create Notifications | 5. View Summary

**For notification rule: VirusScan 8.0i event!**

You can use aggregation and throttling to limit the number of notifications you receive. Each sends a single notification that summarizes multiple events.

**Aggregation:**  Send a notification for every event

Send a notification for multiple events within: 5 Minutes

When the number of affected computers is at least: 100

or

When the number of events is at least: 1000

**Throttling:**  At most, send notification every: 1 Hours

< Back   Next >   Cancel

2 If you selected **For multiple events within**, you can choose to send a notification when the specified conditions met. These conditions can include:

- When the number of affected systems is at least a defined number of systems.
- When the number of events is at least a defined number of events.

- Either (by selecting both options).



You can select *one* or *both* options. For example, you can set the rule to send a notification if the number of affected systems exceeds 300, *or when* the number of events exceeds 3000, whichever threshold is crossed first.

- 3 If desired, select **At most, send notification every** to choose an amount of time that must be passed before this rule can send notification messages again. The amount of time can be defined in minutes, hours, or days.
- 4 Click **Next**.

## Configuring the notifications for the rule

You can configure the message, the size of the message depending on the target, the type of message, and the recipients of the message.

On the **Create Notifications** page:

- 1 If you want the notification message to be sent as an e-mail, SMS, or text pager message, click **Add E-mail Message** to select a type of notification message to add.
  - **Standard E-mail** — Create a subject line and body message to send to an individual via e-mail message.
  - **SMS** — Define a brief message to send to a specified cell phone with SMS functionality.
  - **Text Pager** — Define a brief message to send to a specified pager.

If you want the notification message to be sent as an SNMP trap, click **Add SNMP Trap**, then select the desired SNMP server and the variables to include in the trap:

- a Select the desired **SNMP server** from the drop-down list.
- b Select the **Variables to include** in the SNMP trap. These include:
 

■ Notification rule name	■ Rule site
■ Rule defined at	■ Selected products
■ Selected categories	■ Selected threat or rule name
■ First event time	■ Event IDs
■ Event descriptions	■ Actual number of computers
■ Actual number of events	■ Actual products
■ Actual categories	■ Actual threat or rule names
■ Source computers	■ Affected computer IP addresses
■ Affected computer name	■ Time notification sent
■ Affected objects	■ Event descriptions



Some events do not include this information. If a selection you made is not represented, the information was not available in the event file.

- c Click **Save**.
- 2 Choose the desired address from the drop-down list or type a different one.
- 3 Type the **Subject** line and **Body** text of the notification e-mail message.



If you select **SMS** you can only enter the text message in the **Subject** text box. If you select **Text Pager**, you can only enter the text message in the **Body** text box.

- 4 If desired, select a variable to insert from the **Insert variable** drop-down list, then click **Subject** or **Body** to place the variable in those lines, respectively, of the notification message. Repeat as necessary.

These variables include:

- |                           |                                  |
|---------------------------|----------------------------------|
| ■ Notification rule name  | ■ Rule site                      |
| ■ Rule defined at         | ■ Selected products              |
| ■ Selected categories     | ■ Selected threat or rule name   |
| ■ First event time        | ■ Event IDs                      |
| ■ Event descriptions      | ■ Actual number of computers     |
| ■ Actual number of events | ■ Actual products                |
| ■ Actual categories       | ■ Actual threat or rule names    |
| ■ Source computers        | ■ Affected computer IP addresses |
| ■ Affected computer name  | ■ Time notification sent         |
| ■ Affected objects        | ■ Event descriptions             |



Some events do not include this information. If a selection you made is not represented, the information was not available in the event file.

- 5 Repeat [Step 1](#) through [Step 4](#) as necessary.
- 6 Click **Save**.
- 7 Click **Add External Command** on the **Add or Edit Notification Rule** page.
- 8 Select an external command from the **External command** drop-down list.
- 9 Click **Save**.
- 10 Repeat [Step 7](#) through [Step 9](#) as necessary.
- 11 Click **Next** and review the rule, select **Enable this rule** if desired, then click **Finish**.

---

## Viewing the history of Notifications

This feature allows you to view the history of notifications sent. You can view a collective summary of all notifications sent, by product or category, or a list of all the specific notifications sent.

### Notification summary

The **Notification Summary** page allows you to view a summary of the number of notifications sent by product or category:

- 1 In the console tree, select **Notifications**.
- 2 Select the **Log** tab, then click **Summary**.
- 3 Select the **Time** by which you want to limit the **Notification Summary** data. These include:
  - **All Times**
  - **Last Hour**
  - **Last 8 Hours**
  - **Last Day**
  - **Last Week**
- 4 Select the **Site** for which you want to limit the **Notification Summary** data. You can select individual sites or **All** sites.



If the global administrator has not allowed reviewers and site administrators to view all notifications and rules, site administrators and site reviewers are limited to viewing only notifications and rules for their sites.

- 5 In **Group by**, select **Product**, **Category**, **Priority**, or **Rule name** from the drop-down list, and the quantity of notifications sent for the **Group by** selection.

### Notification list

The **Notification List** page allows you to view a list of all notifications sent. This list can be sorted by the data of any column by clicking the column title.

- 1 In the console tree, select **Notifications** under the desired **Directory** in the console tree.
- 2 Select the **Log** tab, then click **List**.
- 3 Click any column title (for example, **Notification Type**) to sort the list by that column.



If the global administrator has not selected to allow reviewers and site administrators to view all notifications and rules, site administrators and reviewers are limited to viewing only notifications and rules for their sites.

## Notification details

Click any notification from the **Notification List** page to view its details, including:

- Time notification sent
- Rule priority
- First event time
- Actual number of events
- Number of computers
- Affected computer IP addresses
- Affected computer names
- Source computers
- Notification status
- Notification type
- Event IDs
- Affected objects
- Notification rule name
- Rule site
- Rule defined at
- Actual products
- Selected products
- Actual categories
- Selected categories
- Actual threat or rule names
- Selected threat or rule names
- Message subject
- Event descriptions
- Additional information

## Using custom filters

Custom filters provide flexibility to view the notification list. By defining a filter, you can choose to have specific notification log items included or excluded from those displayed.

ePolicy Orchestrator Notifications allows you to create multiple conditions on which to filter the **Notification List**.

You can filter notification log items based on:

- Sites.
- Received products.
- Actual event categories.
- Priority of the notification message.
- Rule names.

To create a custom filter:

- 1 In the console tree, select **Notifications**.
- 2 Select the **Log** tab, then **List** in the details pane.
- 3 Click **Custom Filter**. The **Custom Filter** page appears.
- 4 Click **Add Condition**.
- 5 Choose to filter the list by:

- **Site** — Select **Site** from the **Property** drop-down list, **is** or **is not** from the **Comparison** drop-down list, then the site name from the **Value** drop-down list.
  - **Actual products** — Select **Actual products** from the **Property** drop-down list, **contains** or **does not contain** from the **Comparison** drop-down list, then the product you want to filter from the **Value** drop-down list.
  - **Actual categories** — Select **Actual categories** from the **Property** drop-down list, **contains** or **does not contain** from the **Comparison** drop-down list, then the event category you want to filter from the **Value** drop-down list.
  - **Priority** — Select **Priority** from the **Property** drop-down list, **is** or **is not** from the **Comparison** drop-down list, then the notification priority you want to filter from the **Value** drop-down list.
  - **Rule name** — Select **Rule name** from the **Property** drop-down list, **is** or **is not** from the **Comparison** drop-down list, then the rule name you want to filter from the **Value** drop-down list.
- 6 Repeat [Step 4](#) and [Step 5](#) as needed until all conditions by which you want to filter the list are represented.
- 7 Click **Filter**. The **Notification List** page reappears showing the filtered list.

## Product and component list

You can configure rules to generate notification messages for specific event categories for specific products and components. This is a list of products and components for which you can configure rules and a list of all possible event categories.

- Dr. Ahn
- Desktop Firewall
- Entercept
- ePO Server
- ePO Agent
- GroupShield Domino
- GroupShield Exchange
- System Compliance Profiler
- Symantec NAV
- NetShield
- NetShield for NetWare
- PortalShield
- Stinger
- ThreatScan
- Unknown product
- Virex
- VirusScan
- VirusScan PDA
- WebShield
- LinuxShield

Event categories for which rules can be configured:

- Access Protection rule violation detected and blocked
- Access Protection rule violation detected and NOT blocked
- Banned content or file detected and NOT removed
- Banned content or file detected and removed
- Computer placed in quarantine mode
- E-mail content filtered or blocked
- Encrypted/corrupted file detected and removed
- Firewall rule triggered
- Virus detected (heuristic) and NOT removed
- Virus detected (heuristic) and removed
- Unwanted program detected (heuristic) and NOT removed
- Unwanted program detected (heuristic) and removed
- Intrusion detected
- System Compliance Profiler rule violation
- Non-compliant computer detected
- Normal operation
- On-access scan disabled
- Policy enforcement failed
- Repository update or replication failed
- Virus detected and removed
- Scan cancelled
- Scan line item results
- Software deployment failed
- Software deployment succeeded
- Software failure or error
- Spam detected and handled
- Unknown category
- Unwanted program detected and NOT removed
- Unwanted program detected and removed
- Update/upgrade failed
- Update/upgrade succeeded
- Virus detected and NOT removed

---

## Frequently asked questions

**If I set up a notification rule for virus detections, do I have to receive a notification message for each event received during an outbreak.**

No. You can configure rules so that a notification can be sent only once per specified quantity of events within a specified amount of time, or sent at a maximum of once in a given time amount of time.

**Can I create a rule that generates notifications to multiple recipients?**

Yes. You can enter multiple e-mail addresses for recipients in the **Add or Edit Notification Rule** wizard.

**Can I create a rule that generates notifications in multiple notification formats?**

Yes. Notifications for ePolicy Orchestrator supports any combination of the following notification targets for each rule:

- E-mail (including standard SMTP, SMS, and text pager).
- SNMP servers (via SNMP v1 traps).
- Any external tool installed on the ePolicy Orchestrator server.

# Glossary

**agent AutoUpgrade**

The act of automatically upgrading the agent whenever a newer version is available on the server.

**agent host**

See *client computer*.

**agent installation package**

The Setup program and all other files needed to install the agent.

**agent language packages**

The set of files that need to be distributed to client computers to view the agent user interface in languages other than English.

**Agent Monitor**

The agent user interface that appears optionally on managed computers. It allows you to run tasks immediately that are normally initiated by the agent at predefined intervals.

**agent wakeup call**

The ability to initiate agent-to-server communication from the server-side.

See also *SuperAgent wakeup call*.

**agent**

See *ePolicy Orchestrator agent*.

**agent-server communication**

Any communication that occurs between agents and the server where agents and server exchange data. Typically, the agent initiates all communication with the server.

**agent-to-server communications interval (ASCI)**

The time period between predefined agent-server communication.

**Alert Manager**

McAfee alert notification utility that can be configured to use various notification methods when it receives an alert, such as a pager message or e-mail message. The utility allows you to select which events, such as a virus detection, initiate alert messages.

**anti-virus policy**

See *policy*.

**ASCI**

See *agent-to-server communication interval*.

**AutoUpdate**

The automatic program in McAfee products that updates that software program with the latest virus definition (DAT) files and scanning engine.

**AutoUpgrade**

The automatic program that upgrades McAfee products to the latest available version. It also provides the ability to update products with the latest virus definition (DAT) files and scanning engine.

**AVERT**

Anti-virus & Vulnerability Emergency Response Team, a division of McAfee, Inc.; an anti-virus 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.

**backdoor**

A planned security breach in an application that can allow unauthorized access to data.

**binary (Setup) files**

The Setup program and all other files needed to install products.

**branch**

Locations on the master repository that allow you to store and distribute different versions of selected updates, including Current, Previous, and Evaluation.

See also *selective updating*.

**brute force**

A hacking method used to find passwords or encryption keys by trying every possible combination of characters until the code is broken.

**camping out**

A hacking technique of breaking into a system and finding a safe place from which to monitor the system, store information, or re-enter the system at a later time.

**check in, checking in**

The process of adding files to the master repository.

**clean, cleaning**

An action taken by the scanner when it detects a *virus*, a *Trojan horse* or a *worm*. The cleaning action can include removing the virus from a file and restoring the file to usability; removing references to the virus from system files, system .INI files, and the registry; ending the process generated by the virus; deleting a macro or a Microsoft Visual Basic script that is infecting a file; deleting a file if it is a Trojan horse or a worm; renaming a file that cannot be cleaned.

**client computer**

A computer on which the agent is installed.

**client tasks**

Tasks that are executed on the client-side of the software.

**common framework**

The architecture that allows different McAfee products to share the common components and code, which are the Scheduler, AutoUpdate, and the agent.

**complete properties**

The entire set of properties being exchanged during agent-to-server communication.

See also *incremental properties*.

**computers**

In the console tree, the physical computers on the network to be managed via ePolicy Orchestrator. Computers can be added under existing sites or groups in the Directory.

**configuration settings**

See *policy*.

**console tree item**

The individual icons in the console tree of the console.

**console tree**

The contents of the **Tree** tab in the left pane of the console; it shows the items that are available in the console.

**custom agent installation package**

An agent installation package that uses the user credentials you provide to perform the installation, instead of those of the currently logged on user.

**DAT files**

Virus definition files, sometimes referred to as signature files, that allow the anti-virus software to detect and handle viruses and related potentially unwanted code embedded in files.

See also *EXTRA.DAT file*, *incremental DAT files*, and *SuperDAT*.

**DB Merge Tool (AVIDB\_MERGE\_TOOL.EXE)**

A program that combines data from multiple databases into a new or existing database. The resulting merged database can be used for reporting purposes only.

**denial-of-service attack (DoS)**

A means of attack, an intrusion against a computer, server or network that disrupts the ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.

**details pane**

The right pane of the console, which shows details of the currently selected console tree item.

**Directory**

In the console tree, the list of all computers to be managed via ePolicy Orchestrator; the link to the primary interfaces for managing these computers.

**distributed software repositories**

A collection of web sites or computers located across the network in such a way as to provide bandwidth-efficient access to client computers. Distributed software repositories store the files that client computers need to install supported products and updates to these products.

See also *fallback repository*, *global distributed repository*, *local distributed repository*, *master repository*, *mirror distributed repository*, *source repository*, and *SuperAgent distributed repository*.

**download site**

The McAfee web site from which you retrieve product or DAT updates.

See also *update site*.

**EICAR test file**

European Institute of Computer Anti-Virus Research has developed a file consisting of a string of characters that can be used to test the proper installation and operation of anti-virus software.

**enforce, enforcement**

The act of applying predefined settings on client computers at predetermined intervals.

**ePolicy Orchestrator agent**

A program that performs background tasks on managed computers, mediates all requests between the server and the anti-virus and security products on these computers, and reports back to the server to indicate the status of these tasks.

**ePolicy Orchestrator console**

The user interface of the software that is used to remotely control and monitor managed computers.

See also *ePolicy Orchestrator remote console*.

**ePolicy Orchestrator database server**

The computer that hosts the database. This can be the same computer on which the server is installed or a separate computer.

**ePolicy Orchestrator database**

The database that stores all data received by the server from agents and all settings made on the server itself.

See also *ePolicy Orchestrator database server*.

**ePolicy Orchestrator remote console**

The ePolicy Orchestrator user interface when it is installed on a separate computer from the server.

See also *ePolicy Orchestrator console*.

**ePolicy Orchestrator server**

The back-end component of the software.

**error reporting utility**

A utility specifically designed to track and log failures in the McAfee software on your system. The information that is obtained can be used to help analyze problems.

**events**

Data exchanged during agent-to-server communication that includes information about each managed computer (for example, hardware and software) and its managed products (for example, specific policy settings and the product version number).

**EXTRA.DAT file**

Supplemental virus definition file that is created in response to an outbreak of a new virus or a new variant of an existing virus.

See also *DAT files*, *incremental DAT files*, and *SUPERDAT*.

**fallback repository**

A type of distributed software repository used in the event that client computers cannot contact any of their predefined distributed repositories. Typically, another source repository is defined as the fallback repository.

See also *replicate*, *replication*.

**force install, force uninstall**

See *product deployment client task*.

**FRAMEPKG.EXE**

See *agent installation package*.

**full properties**

All properties that can be exchanged during agent-to-server communication.

See also *minimal properties*.

**full replication**

The act of copying all files from the master repository to distributed software repositories regardless of their contents.

See also *incremental replication*.

**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 use by only the global administrator.

Compare to *global reviewer*, *site administrator*, *site reviewer*.

**global distributed repository**

A distributed software repository that can be automatically kept current with the contents of the master repository.

See also *replicate*, *replication*.

**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 *global administrator*, *site administrator*, *site reviewer*.

**global updating**

A method for deploying product updates as soon as the files are checked into the master repository without user intervention. Files are immediately replicated to all SuperAgent and global distributed repositories; the server sends a wakeup call to all SuperAgents; SuperAgents send a broadcast wakeup call to all agents in the same subnet; then all client computers retrieve the updated files from the nearest repository.

**group**

In the console tree, a logical collection of entities assembled for ease of management. Groups can contain other groups or computers, and can be assigned IP address ranges or IP subnet masks to allow sorting computers by IP address. If you create a group by importing a Windows NT domain, you can automatically send the agent installation package to all imported computers in the domain.

**heuristic analysis, heuristics**

A method of scanning that looks for patterns or activities that are virus-like, to detect new or previously undetected viruses.

**host, host computer**

See *client computer*.

**HotFix releases (now Patches)**

Intermediate releases of the product that fix specific issues.

**immediate event forwarding**

The act of immediately sending events of a specific severity or higher to the server once a predefined number of events are available. This communication is done outside of other agent-to-server communication.

**inactive agent**

Any agent that has not communicated with the server within a specified time period.

**incremental DAT files**

New virus definitions that supplement the virus definitions currently installed, and are available for up to 15 weeks. Allows the update utility to download only the newest dat files rather than the entire DAT file set.

See also *DAT files*, *EXTRA.DAT file* and *SUPERDAT*.

**incremental properties**

Only those properties that have changed since the last agent-to-server communication.

See also *complete properties*, *properties*.

**incremental replication**

The act of copying only those files on the master repository that differ from the contents of each distributed software repository.

See also *full replication*.

**incremental virus definition (DAT) files**

See *incremental DAT files*

**inherit, inheritance**

The act of applying the settings defined for an item within a hierarchy from the item above it.

**item**

See *console tree item*.

**joke program**

A non-replicating program that may alarm or annoy an end user, but does not do any actual harm to files or data.

**local distributed repository**

A type of distributed software repository whose content is manually updated and is not updated by ePolicy Orchestrator.

**log file**

A record of the activities of a component of McAfee anti-virus software. Log files record the actions taken during an installation or during the scanning or updating tasks.

See also *events*.

**Lost&Found group**

A group used to temporarily store computers whose appropriate location in the **Directory** cannot be determined.

**macro virus**

A malicious macro — a saved set of instructions created to automate tasks within certain applications or systems — that can be executed inadvertently, causing damage or replicating itself.

**managed products**

Anti-virus and security products that are being managed from ePolicy Orchestrator.

**mass mailer virus**

Viruses such as Melissa and Bubbleboy that propagate themselves rapidly using e-mail services.

**master repository**

A type of distributed software repository whose contents acts as the standard for all other distributed repositories. Typically, the master repository contents are defined from a combination of the source repository contents and additional files added to the master repository manually.

See also *pull*; *replicate*, *replication*.

**merged databases**

Two or more databases that have been combined into a single database, used for reporting purposes only.

**minimal properties**

A subset of the full properties that can be exchanged during agent-to-server communication.

See also *full properties*.

**mirror distributed repository**

A type of distributed software repository whose content is automatically updated by mirroring the contents of another distributed repository, instead of by replicating the contents of the master repository.

See also *distributed software repositories*; *master repository*; *mirror*, *mirroring*; *replicate*, *replication*.

**Named policy**

A collection of policy settings that can be assigned independent of the Directory structure.

**NAP file**

The file extension used to designate McAfee software program files that are installed in the software repository for ePolicy Orchestrator to manage.

**node**

See *console tree item*.

**on-access scanning**

An examination of files in use to determine if they contain a virus or other potentially unwanted code. It can take place whenever a file is read from the disk and/or written to the disk.

Compare to *on-demand scanning*.

**on-demand scanning**

A scheduled examination of selected files to determine if a virus or other potentially unwanted code is present. It can take place immediately, at a future scheduled time, or at regularly scheduled intervals.

Compare to *on-access scanning*.

**package catalog file**

A file that contains details about each update package, including the name of the product for which the update is intended, language version, and any installation dependencies.

**Patch releases (previously HotFix release)**

Intermediate releases of the product that address specific issues.

**ping attack**

The method of overwhelming a network with `ping` commands.

**ping of death**

A hacking technique used to cause a *denial-of-service* by sending a large ICMP packet to a target. As the target is attempting to reassemble the packet, the size of the packet overflows the buffer and can cause the target to reboot or freeze.

**policy enforcement interval**

The time period during which the agent enforces the settings it has received from the server. Because these settings are enforced locally, this interval does not require any bandwidth.

**policy files**

Set of policy settings for one or more products that are saved to the local drive of the server, but cannot be accessed via a remote console.

See also *policy templates*.

**policy pages**

Part of the console; they allow you to set policies and create scheduled tasks for products, and are stored on individual servers (they are not added to the master repository). Also referred to as NAP files.

**policy**

The configuration settings of managed product that are defined and managed from ePolicy Orchestrator.

**port scanning**

A hacking technique used to check TCP/IP ports to reveal which services are available in order to plan an exploit involving those services, and to determine the operating system of a particular computer.

**potentially unwanted program**

A programs that performs some unauthorized (and often harmful or undesirable) act such as viruses, worms, and Trojan horses.

**product deployment client task**

A scheduled task for deploying all products currently checked into the master repository at once. It enables you to schedule product installation and removal during off-peak hours or during the policy enforcement interval.

**properties**

Data exchanged during agent-to-server communication that includes information about each managed computer (for example, hardware and software) and its managed products (for example, specific policy settings and the 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**

Enforced isolation of a file or folder — for example, to prevent infection by a virus or to isolate a spam e-mail message — until action can be taken to clean or remove the item.

**remote console**

See *ePolicy Orchestrator console*.

**replicate, replication**

The act of copying files from the master repository to other distributed software repositories.

See also *full replication*, *incremental replication*.

**repository list (SITELIST.XML)**

The SITELIST.XML file that is used by those McAfee security products that include the AutoUpdate program; it is used to access distributed repositories and retrieve packages.

**Repository**

The location that stores policy pages used to manage products.

**scan, scanning**

An examination of files to determine if a virus or other potentially unwanted code is present.

See *on-access scanning* and *on-demand scanning*.

**selective updating**

The ability to specify which version of updates you want client computers to retrieve from distributed software repositories.

See also *branch*.

**Server Configuration (CFGNAIMS.EXE) program**

The program that changes the SQL Server user account information in ePolicy Orchestrator when you make changes to the SQL Server user account in another program; for example, SQL Server Enterprise Manager.

**server events**

Activity on the server that is recorded by the Windows Event Viewer. This information is not stored in the database, so is not available for reporting purposes.

**server tasks**

Tasks that can be executed on the server-side of the software.

**signature files**

See *DAT files*.

**silent installation**

An installation method that installs a software package onto a computer silently, without need for user intervention.

**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 *global reviewer*, *global administrator*, *site reviewer*.

**site**

In the console tree, a logical collection of entities assembled for ease of management. Sites can contain groups or computers, and can be organized by IP address range, IP subnet mask, location, department, and others.

**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 *global administrator*, *global reviewer*, *site administrator*.

**SITELIST.XML**

See *repository list*.

**Smurf attack**

A *denial-of-service* attack that floods its targets with replies to ICMP echo (*ping*) requests. A smurf attack sends *ping* requests to Internet broadcast addresses, which forward the requests to as many as 255 hosts on a subnet. The return address of the *ping* request is spoofed to the address of the attack target. All hosts receiving the *ping* requests reply to the attack target, flooding it with replies.

**source repository**

A type of distributed software repository from which the master repository retrieves files. Typically, the source repository is the McAfee web site or another master repository.

See also *pull*.

**spoofing**

Forging something, such as an IP address, to hide one's location and identity.

**Status Monitor**

See *Agent Monitor*.

**SuperDAT**

A utility that installs updated virus definition (SDAT\*.EXE) files and, when necessary, upgrades the scanning engine.

See also *DAT files*, *EXTRA.DAT file*, and *incremental DAT files*.

**SuperAgent distributed repository**

A type of distributed software repository that takes advantage of the HTTP capabilities of the SuperAgent to create a repository without the use of a dedicated server to host it.

See also *replicate*, *replication*.

**SuperAgent wakeup call**

The ability to prompt each SuperAgent and all agents in the same subnet to contact the server when needed, rather than waiting for the next agent-to-server communication interval (ASCI).

See also *agent wakeup call*.

**SuperAgent**

A type of agent for Windows with the ability to send wakeup calls to all agents in the same subnet.

See also *global updating*, *SuperAgent wakeup calls*, *SuperAgent distributed repositories*.

**SuperDAT (SDAT\*.EXE) files**

A standard application that you can double-click to start from within Microsoft Windows. The Microsoft version of the Installer includes a wizard that provides instructions in a series of panels.

**SuperDAT Package Installer**

An installation program that upgrades McAfee software programs. It automatically shuts down any active scans, services, or other memory-resident components that could interfere with the upgrade, then copies new files to their proper locations so that your software can use them immediately.

**supplemental virus definition file**

See *EXTRA.DAT file*.

**SYN flood**

A hacking technique used to cause a *denial-of-service*.

**task**

An activity (both one-time such as *on-demand scanning*, and routine such as *updating*) that is scheduled to occur at a specific time, or at specified intervals.

Compare to *policy*.

See *client tasks*, *server tasks*.

**Trojan horse**

A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan horses are not technically viruses, because they do not replicate.

**unmanaged products**

Anti-virus and security products that are not being managed via ePolicy Orchestrator.

**update package**

Package files from McAfee that provide updates to a product. All packages are considered product updates with the exception of the product binary (Setup) files.

**update site**

The repository from which you retrieve product or DAT updates.

See also *download site*.

**updating**

The process of installing updates to existing products or upgrading to new versions of products.

**UTC time**

Coordinated Universal Time (UTC). This refers to time on the zero or Greenwich meridian.

**virus definition (DAT) files**

See *DAT files*.

**virus**

A program that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.

**virus-scanning engine**

The mechanism that drives the scanning process.

**worm**

A virus that spreads by creating duplicates of itself on other drives, systems, or networks.

# Index

## A

- accounts (*See* user accounts)
- Active Directory
  - discovery, 50
  - discovery task, 50
- adding
  - user accounts, 26
  - WebShield appliances to the Directory, 49
- administrator accounts (*See* user accounts)
- agent
  - activity log, 93
  - command-line options, 96
  - deployment, 77
  - deployment requirements, 77
  - distributing, using third-party deployment tools, 85
  - events, 215
  - installation command-line options, 66
  - installation, using search feature to send agent install, 59
  - interface, 94
  - introduction, 11
  - log, 69
  - policies, 155
  - properties, 92
  - selective updating policies, 162
  - uninstalling, 88 to 89
  - upgrading from 2.5.1, 86
  - upgrading from 3.x, 87
  - wakeup call, 89
- agent deployment, 49, 61
  - with ePolicy Orchestrator, 76
- Agent Monitor, 94
- agent wakeup call, 89
  - using search feature to send, 59
  - with client task, 90
- aggregating notifications, 202, 212
- appliances, adding WebShield, 49

- audience for this manual, 17
- AVERT security headquarters
  - contacting, 20
  - DAT file notification service, 20
  - WebImmune, 20

## B

- bandwidth usage
  - product deployment improvements, 12 to 14
- beta program, contacting, 20

## C

- checking in packages, 146
- client tasks, 115
  - agent wakeup call, 90
  - scheduling, 135
  - update, 158
  - VirusScan Enterprise on-demand scan, 134
- compliance check, 164
  - server task, 165
- computer names
  - finding duplicates in the Directory, 59
- configuring
  - external commands, 219
  - notifications, 216
- console (*See* ePolicy Orchestrator software)
- console tree items
  - organizing the Directory, 60
  - WebShield appliances, 49
- consulting services, 20
- contacting McAfee, 19
- creating
  - notification rule based on Rogue System Detection events, 208
- customer service, contacting, 20

## D

- DAT file, 157
  - and engine update, 158
  - daily update, 158
  - evaluating, 161

- McAfee update web site, 20
- update notification service, 20

## DAT file updating, 99, 161

- from source repository, 108
- in master repository, 105
- with client task, 158

## definition of terms (*See* Glossary)

## deleting

- computers from the Directory, 59

## deploying products, 140

## deployment

- improvement in bandwidth usage, 12 to 14

## devices, adding WebShield appliances, 49

## Directory

- Active Directory discovery, 50
- add computers, 198
- creating, 34
- Directory Search, 59
- importing a computer from a domain, 42, 46
- importing from Active Directory, 40
- inheritance, 35
- IP filters, 49, 55
- IP integrity check, 56
- IP sorting, 57
- search feature to delete computers, 59
- synchronizing with NT domains, 54
- updating domains, 54

## Directory, creating

- about, 35
- from NT domain, 41

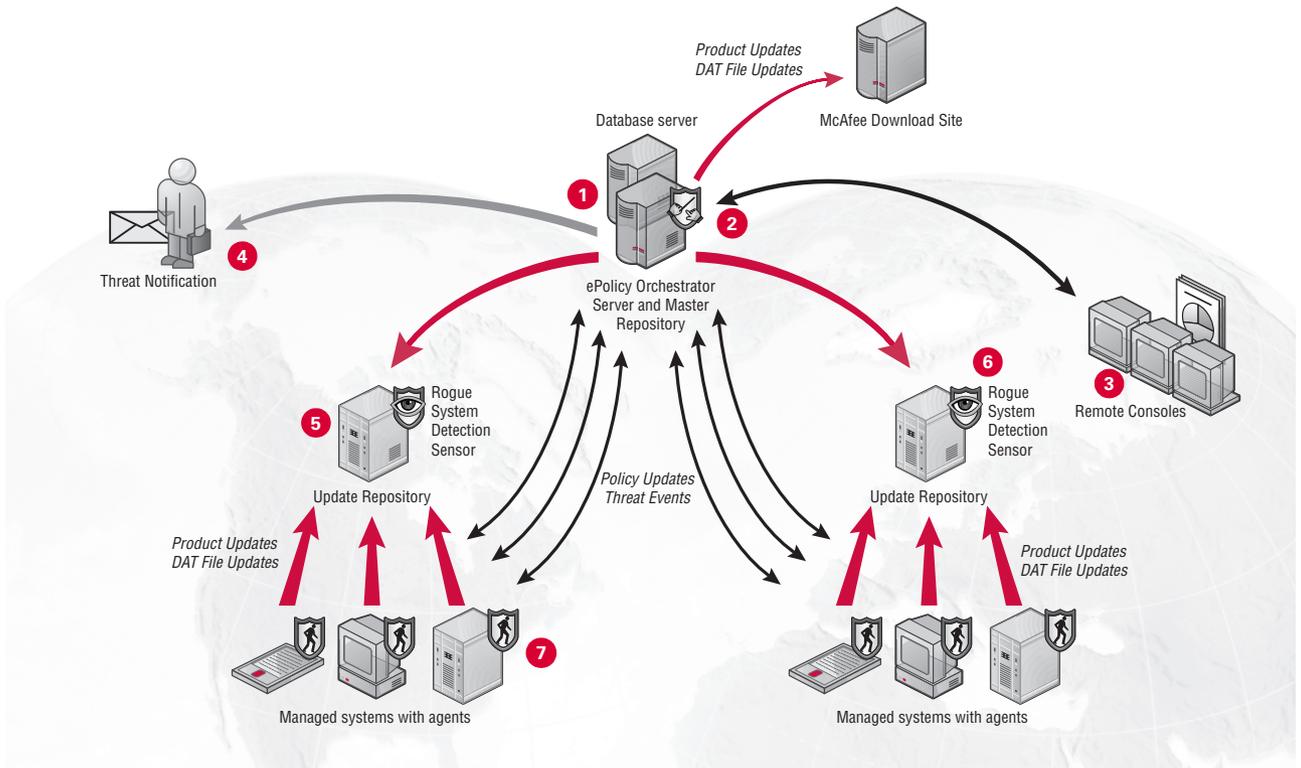
## distributed repositories

- about, 163
- local, 156
- nonmanaged, 156
- replicating to, 152 to 153, 163

## documentation for the product, 19

- domain synchronization, manual, 54
- download web site, 20
- duplicate computer names, finding in the Directory, 59
- E**
- e-mail contact, 218
- e-mail notifications, 201
- engine updating, 99
  - from source repository, 108
  - in master repository, 105
- ePolicy Orchestrator server, 21
  - events, 31
  - logging off, 22
  - logging on, 22
  - logging onto additional, 22
  - server tasks, 30
  - settings, 29
  - version, 33
- ePolicy Orchestrator software
  - console, introduction, 11
  - new features, 11
- events, 215
  - virus detection, 211 to 212
- exporting
  - repository list to a file, 157
- F**
- fallback repository (*See* repository)
- FAQ (frequently asked questions), 209, 229
- feature comparison, 12 to 14
- features, new in this release, 11
  - selective updating, 14
  - System Compliance Profiler, 12
- G**
- getting information, 19
  - list of contacts, 19
- global updating
  - new features, 12 to 14
  - selective updating, 162
- glossary, 231
- groups, 55
- I**
- importing a computer
  - from a domain, 42, 46
- inheritance, 35
  - resetting, 133
- installation (*See* Installation Guide)
- integrity check, IP address, 55
- IP address, checking integrity, 55
- IP filters, Directory, 55
- IP integrity check, 56
- IP management
  - sorting computers by, 58
- IP sorting, 57
- L**
- local distributed repositories, 156
- Locale IDs, 67
- M**
- Machine Summary page, 191
- manuals for the product, 19
- master repository
  - pulling from source repository, 149, 151 to 152
  - replicating to distributed repositories, 152 to 153, 163
- McAfee University, contacting, 20
- moving items in the Directory
  - via search feature, 59
- N**
- NAP package, 116
  - checking in, 148
  - defined, 236
- new features, 11
  - global updating, 12 to 14
- nodes (*See* console tree items)
- notification service, DAT updates, 20
- notifications, 166 to 167, 202, 204, 207 to 208, 210, 212, 215 to 217, 219, 227
  - aggregation, 202, 212
  - configuring, 216
  - configuring notifications, 217
  - default rules, 214
  - history, 226
  - how they work, 211
  - notification list, 226 to 228
  - rules, 212, 220
  - summary, 226
  - throttling, 202, 212
- NT domains
  - importing to Directory, 41
  - synchronizing with Directory, 54
- O**
- on-site training, 20
- overview
  - ePolicy Orchestrator servers, 21
  - ePolicy Orchestrator software, 10
- selective updating, 14
- P**
- packages
  - checking in, 146
  - dependencies, 140
  - ordering, 140
- policies, 116
  - about, 116
  - exporting and importing, 121
  - importing from a template, 130
  - resetting inheritance, 133
- policy pages (NAP), 116
- PrimeSupport, 19
- product deployment package
  - checking in, 146
- product information
  - documentation, 19
  - resources, 19
  - training, 20
- products
  - deploying, 137
  - deploying with ePolicy Orchestrator, 148
- properties for products, 92
- proxy server, 151
- Pull Now task, initiating, 152
- R**
- remote console
  - corporate intranet, 65
- removing
  - user accounts, 27
- Replicate Now task, 153
- replication of repositories, 163
- replication tasks, 152
  - initiating, 153
- repository
  - about, 100
  - branches, 105, 161
  - creating, 110
  - distributed repository, 86
    - nonmanaged, 156
  - fallback, changing, 108
  - replication, 152 to 153, 163
  - source repository, 108, 149, 151 to 152
- repository list
  - exporting to a file, 157
- Repository Pull task, 149, 151
- Repository Replication server tasks, 152
- resources for information, 19

- Rogue System Detection, 28, 171 to 174, 177, 182 to 189, 191, 193 to 195, 197 to 198, 200 to 209
  - about, 172
  - action
    - status, 194
  - action status, 207
  - action types, 196
  - automatic e-mail notifications, 201
  - automatic response
    - status, 194
    - using an executable in, 206
  - automatic responses, 200, 205
  - customize server, 185
  - customizing, 185
  - dealing with new rogues, 196
  - event history, 194, 207
  - interface, 177
  - Machine Summary, 191
  - sensor-to-server communication, 188
  - server, 172, 174, 177, 182, 188, 194, 201, 209
  - using with notification, 207
- Rogue system sensor
  - about, 172
  - managing, 193
  - policies, 177
- rogue system sensor
  - deploying, 61, 182
  - installing manually, 182
  - uninstalling, 183
- S**
- sample virus, submitting, 20
- scheduling
  - Repository Pull task, 149, 151
  - repository replication, 152
- search
  - feature, using to delete computers, 59
  - for computers in the Directory, 59
- Security certificate
  - installing, 23
- security certificate, 23
- security headquarters, contacting AVERT, 20
- selective updating
  - overview, 14
- server events, 31
- servers
  - introduction, 10
  - printing events, 32
  - tasks, scheduling Repository Replication, 152
- service portal, PrimeSupport, 19
- SITELIST.XML file
  - enabling the agent, 84
- sites
  - IP filter, 55
- SNMP, 217, 219
- sorting computers using IP management settings, 58
- source repositories, 108
  - adding, 109
  - changing, 108
  - pulling from, 149, 151 to 152
- SuperAgent
  - defined, 239
  - deploying, 61
- synchronizing domains, 54
- System Compliance Profiler, 120, 164 to 165, 210, 229
- T**
- tasks
  - Pull Now, 152
  - Update Domain Directory, 54
- technical support
  - contact information, 19
- throttling notifications, 202, 212
- training web site, 20
- U**
- Update Domain Directory task, 54
- updating
  - DAT file, 158
  - domains, 54
  - global, new features, 12 to 14
- upgrading
  - agent, 87
  - web site, 20
- user accounts, 24
  - adding and editing, 26
  - removing, 27
  - site administrators, 25
- using this guide, 15
- utilities
  - Agent Monitor, 94
- V**
- Virus Information Library, 20
- virus, submitting a sample
  - web site, 20
- VirusScan Enterprise
  - deploying, 137
  - deploying with ePolicy Orchestrator, 148
  - detection events, 211 to 212
  - on-demand scan, 134
- policies, 115
- W**
- WebImmune, 20
- WebShield appliance, 49
- wizard
  - Add repository, 109
  - Check-in package, 147, 157
  - Export repository list, 157



## Enterprise scalable, system security management

- 1 ePolicy Orchestrator server** — The center of your managed environment. The server delivers security policy, controls updates, processes events, and serves tasks for all managed systems.
- 2 Master repository** — The central location for all McAfee product updates and signatures, which are then provided to the managed systems using distributed repositories and ePolicy Orchestrator agents.
- 3 Remote consoles** — The access point to the ePolicy Orchestrator server and reports from another system. From a remote console, you can configure policies, create or edit tasks, and run reports.
- 4 Threat notification** — An alert message based on threat and compliance events in your environment. ePolicy Orchestrator can alert you immediately to any such events in your environment via standard e-mail, text pager, SMS, or SNMP trap.
- 5 Distributed repository** — Repositories, distributed throughout your environment, provide managed systems easy access to pull DAT files, product updates, and product installations. Depending on how your network is configured, you may want to set up HTTP, FTP, or UNC share distributed repositories, or create an update repository on each subnet by converting an agent into a SuperAgent repository.
- 6 Rogue System Detection (RSD) sensor** — The sensor resides on one system per subnet and notifies you when a rogue system enters the environment. It can then initiate an automatic response, such as deploying an agent to that system.
- 7 ePolicy Orchestrator agent** — A vehicle of information and enforcement between the ePolicy Orchestrator server and each system. The agent retrieves updates, ensures task implementation, enforces policy and forwards events for each managed system.

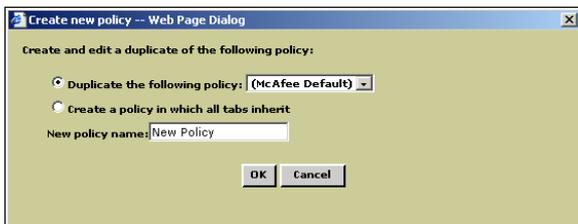
# Creating and assigning policies

Manage policy assignments from both the **Assign Policies** and **Policy Catalog** pages. These pages allow you to create and assign policies to multiple, independent Directory nodes.

## Creating policies in the Policy Catalog

To create a policy:

- 1 In the console tree, select **Policy Catalog**. All existing policies are available in the details pane, grouped under products.
- 2 Click  next to the desired product name to expose the policy categories.
- 3 Click  next to the desired policy category to expose the named policies in that category.
- 4 Click **Define new policy** under the last policy for the category. The **Create new policy** dialog box appears.



- 5 To base your new policy on an existing policy, select the named policy you want to duplicate from the **Duplicate the following policy** drop-down list.  
To create a policy in which all tabs inherit from the parent node, select **Create a policy in which all tabs inherit**.
- 6 Type a name for the new policy in the **New policy name** field, then click **OK**. The **Policy Settings** dialog box appears with the policy pages.
- 7 Deselect **Inherit** on the desired tabs (if selected), edit the selections as needed, then click **Apply**.
- 8 Click **Close**.

## Creating policies on the Assign Policies page

When you create a policy on this page, the new named policy is assigned to the node selected in the console tree.

- 1 In the console tree, select the desired node of the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies are available in the details pane, grouped under products by category.
- 3 Click  next to the desired product name to expose the specific named policies assigned to the node.

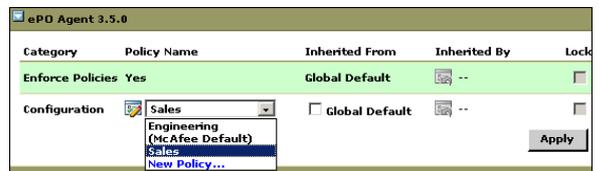
- 4 Locate the desired policy category for which you want to create a new policy, then click **Edit**.
- 5 Select **New Policy** from the drop-down list under **Policy Name**. The **Create new policy** dialog box appears.
- 6 To base your new policy on an existing policy, select the named policy you want to duplicate from the **Duplicate the following policy** drop-down list.  
To create a policy in which all tabs inherit from the parent node, select **Create a policy in which all tabs inherit**.
- 7 Type a name for the new policy in the **New policy name** field, then click **OK**. The **Policy Settings** dialog box appears with the policy pages.
- 8 Deselect **Inherit** on the desired tabs (if selected), edit the selections as needed, then click **Apply**.
- 9 Click **Close**.

The modifications are enforced on each system on each system the policy is assigned on the next agent-server-communication.

## Assigning existing named policies

You can assign named policies to any Directory node to which you have rights (unless another policy is assigned and locked). When policies are assigned to a node, all child nodes apply any policy settings they are configured to inherit.

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies, grouped under products by category, are available in the details pane.
- 3 Click  next to the desired product name to expose the specific named policies assigned to the node.
- 4 Locate the desired policy category for which you want to assign a named policy, then click **Edit**.
- 5 Select the desired policy from the **Policy Name** drop-down list.



- 6 Click **Apply**. All child nodes that were inheriting policy settings of the previous assignment now inherit the same settings from the new assignment.

# Viewing information on policy assignment and inheritance

Policy management with ePolicy Orchestrator 3.6 provides access to information about the policy assignments in your environment, allowing you to troubleshoot problems quickly.

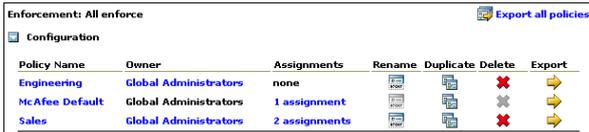
Within a couple of clicks, you can find the:

- Assignments of any policy — See a list of nodes where a policy has been assigned. (This is a list of nodes on which the policy has been assigned, not a list of all systems that inherit the assignment.)
- Inheritance of any assignments — See from which parent node a child node inherits a policy, and a list of child nodes whose inheritance for the policy has been disabled.

## Viewing the assignments of a policy

ePolicy Orchestrator allows you to view the Directory node to which a policy is assigned. This list shows the assignments only not each system that inherits the policy. For example, if a policy is assigned to one group node, **1 assignment** appears, regardless of the number systems within the group.

- 1 In the console tree, select **Policy Catalog**. All created policies, are available in the details pane, grouped under products by category.
- 2 Click  next to a product name to expose its policy categories.
- 3 Click  next to a policy category to expose the named policies associated with that category.
- 4 Under **Assignments** on the row of the desired named policy, click the blue text that indicates the number of nodes to which the policy is assigned (for example, **6 assignments**).



Policy Name	Owner	Assignments	Rename	Duplicate	Delete	Export
Engineering	Global Administrators	none				
McAfee Default	Global Administrators	1 assignment				
Sales	Global Administrators	2 assignments				

- 5 On the **View assignments** page, each node to which the policy is assigned appears with its **Node Name** and **Node Type**.
- 6 Click the node name to see its **Assign Policies** page.

## Finding assignments with enforcement disabled

From the **Policy Catalog** page, you can easily view where policy assignments are unenforced per product category.

To view assignments where policy enforcement is disabled:

- 1 In the console tree, select **Policy Catalog**.
- 2 In the details pane, select the desired policy category.
- 3 Above the category name, click the blue text next to **Enforcement**, which indicates the number of assignments where enforcement is disabled. The **View assignments where policy enforcement is disabled** page appears.
- 4 Click a node in the list to open its **Assign Policies** page.

## Viewing inheritance information

You can quickly see from which parent node a policy is inherited and which child nodes have a policy's inheritance disabled. This allows you to view both directions of inheritance.

### Viewing from which parent node a policy is inherited

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies are available in the details pane, grouped under products.
- 3 Click  next to a product name to expose the specific named policies assigned to the node.
- 4 On the desired policy row under **Inherited From**, the name of the node from which the policy is inherited appears.

### Viewing and resetting broken inheritance

To view where policy inheritance is broken below a specific node:

- 1 In the console tree, select the desired node in the Directory.
- 2 In the details pane, select the **Policies** tab. All assigned policies are available in the details pane, grouped under products.
- 3 Click  next to a product name to expose the specific named policies assigned to the node.
- 4 On the desired policy row under **Inherited By**, the number of nodes to which this policy's inheritance is broken appears.



Category	Policy Name	Inherited From	Inherited By	Lock	Edit Row
Enforce Policies	Yes	Global Default	 all inherit	<input type="checkbox"/>	
Configuration	Sales	--	 3 don't inherit	<input type="checkbox"/>	

This is the number of child nodes to which a different named policy is assigned, not the number of systems that do not inherit the policy. For example, if only one group node does not inherit the policy, **1 doesn't inherit** appears, regardless of the number of systems within the group.

- 5 Click the blue text indicating the number of child nodes that do not inherit. The **View broken inheritance** page appears with a list of the names of these nodes.
- 6 To reset the inheritance of any of these nodes, select the checkbox next the node name, then click **Reset Inheritance**.

# Copying and exporting policies

ePolicy Orchestrator 3.6 allows you to copy and paste policy assignments between Directory nodes, and export and import policies between ePolicy Orchestrator servers.

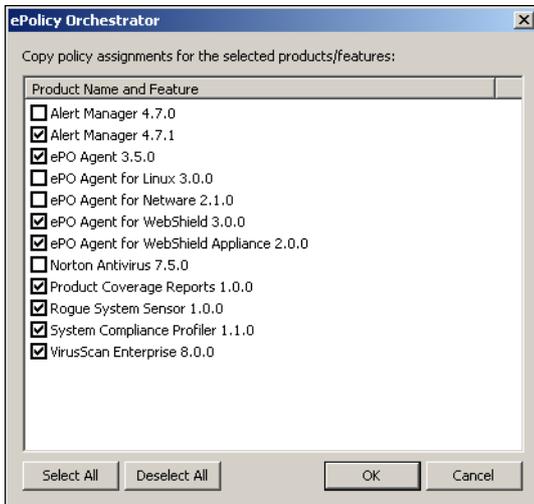
To copy policy assignments between Directory nodes, use the copy and paste assignment features on the **Assign Policies** page.

To export policies between ePolicy Orchestrator servers, use the export and import policy features on the **Policy Catalog** page.

## Copying and pasting policy assignments

If you want a site, group, or system to use the same policy assignments as another site, group, or system, then copy and paste the desired policy assignments from the original.

- 1 In the console tree, select the Directory node whose policy assignments you want to copy.
- 2 In the details pane, click **Copy policy assignments**.
- 3 Select the desired products or features for which you want to copy policy assignments from the selected node, then click **OK**.



- 4 In the console tree, select the target node.
- 5 In the details pane, select **Paste policy assignments**.
- 6 Confirm the replacement of assignments as prompted.

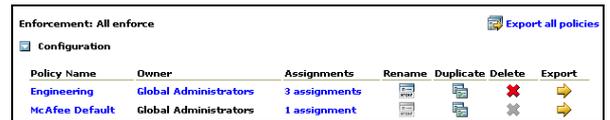
 Changing the settings of a policy at any location, affects each location the policy is assigned.

## Exporting policies from a server

To share named policies between servers, you can export the named policy, or policies, to a policy XML file from the **Policy Catalog** page of the source server, then import it to the **Policy Catalog** page on the target server.

- 1 In the console tree, select **Policy Catalog**.
- 2 To export an individual policy, click  next to the desired product, select the desired named policy, then click **Export**.

To export all policies for a product, click  next to the desired product, then click **Export all policies**.

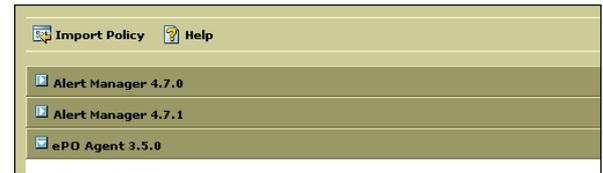


- 3 Name and save the policy XML file to the desired location in the file system. Ensure that this location is accessible to the target ePolicy Orchestrator server.

## Importing policies to a server

To import a policy XML file:

- 1 In the console tree, select **Policy Catalog**.
- 2 In the details pane, click **Import Policy**.



- 3 Browse to and select the desired policy XML file, then click **OK**. The imported policies appear in the appropriate location of the **Policy Catalog** page.

# Replicating selective content to specified repositories

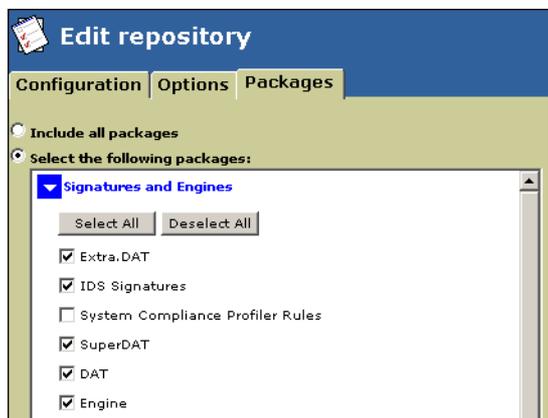
Three new replication features improve performance and decrease bandwidth usage:

- Server-side replication — Replication now occurs on the ePolicy Orchestrator server, improving performance up to 300%.
- Selective content replication — When creating or editing distributed repositories, choose which packages you want to replicate to the distributed repository to optimize bandwidth usage.
- Repository selection — When creating or editing replication tasks, choose which distributed repositories are included in the task to optimize bandwidth usage.

## Selecting content to replicate per repository

When creating or editing distributed repositories, choose which types of content are replicated to a specific distributed repository:

- 1 In the console tree, select **Repository | Software Repositories** to display the list of all configured repositories.
- 2 Select the desired distributed repository, then click **Edit**.
- 3 Change the package selection options as needed.



- 4 Click **OK**.



Ensure that all packages required by any managed system that uses this repository are selected. Managed systems go to one repository for all packages — if an expected package type is not present in the repository, the entire task fails. This feature is designed to ensure that packages used by a few systems only (for example, gateway products) are not replicated throughout your entire environment.

## Selecting repositories when creating a replication task

When creating a replication task, specify the distributed repositories to which the task applies:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Schedule replication tasks** to open the **Configure Server Tasks** page.
- 3 Select **Create task** to open the **Configure New Task** page, then type a **Name**, such as `Daily Distributed Repository Replication task`.
- 4 Select **Repository Replication** from the **Task type** drop-down list, then select **Yes** next to **Enable Task**.
- 5 In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 6 The section under the **Task settings** section is named for the **Schedule type** you selected and allows you to configure its details. Define these settings as appropriate.
- 7 Under **Additional settings**, choose whether to run missed tasks, and how long (in minutes) to delay a missed task, then click **Next**.



If you are using a source repository to update your master repository, schedule your replication task at least five minutes after your scheduled pull task begins. The replication task will wait to run until the pull task completes.

- 8 Select **Incremental replication** or **Full replication**. (In most cases, **Incremental replication** is recommended.)
- 9 Select either **Replicate to all the repositories** or **Replicate to the selected repositories**.

<input type="checkbox"/>	Name	Type	Server
<input checked="" type="checkbox"/>	Repository 1	UNC:Site	Server 1
<input type="checkbox"/>	Repository 2	UNC:Site	Server 2

If you selected **Replicate to the selected repositories**, then select the checkboxes next to the desired distributed repositories from the list.

- 10 Click **Finish**. Wait a moment while the task is created.

# Using ePolicy Orchestrator documentation

The ePolicy Orchestrator documentation set provides you with the information you need during each phase of product implementation, from evaluating the product to maintaining an existing implementation.

## Evaluating ePolicy Orchestrator

When determining how ePolicy Orchestrator can benefit your company, use the *ePolicy Orchestrator 3.6 Walkthrough Guide* in your lab environment.

This guide includes:

- Procedures on preparing for, installing and deploying software in a test environment.
- Conceptual information about each component of the product.
- Best practices information.

## Installing ePolicy Orchestrator

Use the *ePolicy Orchestrator 3.6 Installation Guide* and *Release Notes* before, during, and immediately after the installation.

The *ePolicy Orchestrator 3.6 Installation Guide* includes:

- Information and instructions to prepare for the database and product installation in a production environment.
- Installation and upgrade instructions.
- Clustering instructions, for use with Microsoft Clustering Services.

The *Release Notes* includes:

- Known issues in the current release.
- Issues resolved since the last release.
- Last-minute changes to the product or its documentation.

## Setting up your environment for management

Use the *ePolicy Orchestrator 3.6 Product Guide*, *ePolicy Orchestrator 3.6 Reporting Guide*, and the managed product configuration guides to bring your systems and security products under management.

The *ePolicy Orchestrator 3.6 Product Guide* includes:

- Procedures on setting up and customizing the software in your environment.
- Detailed information about the options in the product.

The *ePolicy Orchestrator 3.6 Reporting Guide* includes:

- Procedures on running reports.
- Reference information for each report and query template that ships with ePolicy Orchestrator 3.6.

The managed product configuration guides (from the documentation sets of managed McAfee products) include:

- Procedures for managing and deploying the product with ePolicy Orchestrator.
- Information on any product-specific ePolicy Orchestrator reports.

## Maintaining ePolicy Orchestrator

Use the Help file, the *ePolicy Orchestrator 3.6 Quick Reference Card*, or the KnowledgeBase for your day-to-day use of the product.

The Help file includes:

- Procedures on maintaining the software.
- Reference information.
- Maintenance tool information.
- Database maintenance information.
- All information found in the product guide and reporting guide.

The ePolicy Orchestrator 3.6 Quick Reference Card includes detailed instructions for both common and infrequent, but important tasks.

The KnowledgeBase includes:

- Supplemental product information.
- Workarounds to known issues.

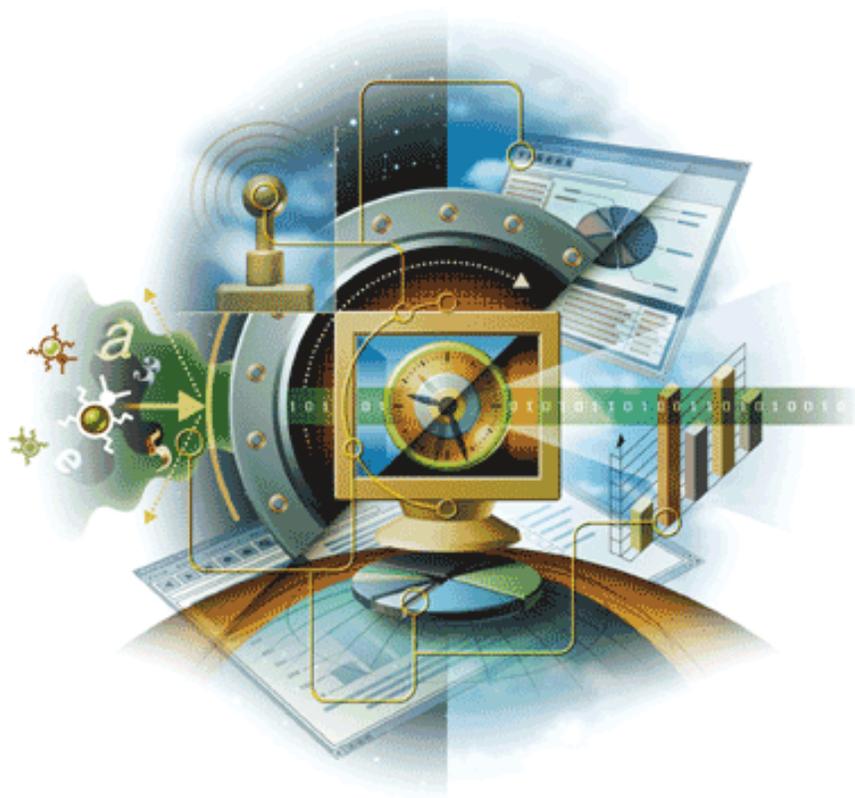
Use this link to access the Knowledge Base:

<https://mysupport.nai.com>

# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6



**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

**McAfee®**



# ePolicy Orchestrator®

Deploy and manage security products and network systems

version 3.6

**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

---

**McAfee®**

## COPYRIGHT

Copyright © 2005 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, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE 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 WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

### 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 pro+34vide 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](http://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/Æ Optimizer/Æ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In/Æ Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In/Æ 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](http://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 <[rsse@engelschall.com](mailto:rsse@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 ([gregor@cs.rpi.edu](mailto:gregor@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](mailto: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](mailto: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.

## PATENT INFORMATION

Protected by US Patents 6,470,384; 6,493,756; 6,496,875; 6,553,377; 6,553,378.

# Contents

<b>1</b>	<b>Reporting</b>	<b>4</b>
	About pre-defined reports in ePolicy Orchestrator . . . . .	4
	About reporting . . . . .	5
	Crystal Reports 8.5 . . . . .	6
	Authentication and user accounts . . . . .	6
	Getting started with reporting . . . . .	7
	Specifying global reporting options . . . . .	7
	Limiting report and query results by client system . . . . .	8
	Running and working with reports . . . . .	8
	Running reports . . . . .	9
	Working with reports in the report window . . . . .	15
	Queries . . . . .	19
	Running queries . . . . .	19
	Report repository maintenance . . . . .	20
	Saving customized report selections as report templates . . . . .	20
	Adding a custom report template . . . . .	21
	Modifying report templates . . . . .	21
	Deleting report templates . . . . .	21
	Creating report groups . . . . .	21
	Deleting report groups . . . . .	22
	Adding report templates from new products to the report repository . . . . .	22
	Query repository maintenance . . . . .	23
	Adding custom query templates . . . . .	23
	Modifying query templates . . . . .	24
	Deleting query templates . . . . .	25
	Creating query groups . . . . .	25
	Deleting query groups . . . . .	25
<b>2</b>	<b>ePolicy Orchestrator Databases and Reports</b>	<b>26</b>
	About ePolicy Orchestrator databases . . . . .	26
	Working with user accounts and events . . . . .	26
	Logging onto and off from ePolicy Orchestrator database servers . . . . .	26
	Defining which events are stored in the database . . . . .	29
	Reporting and multiple databases . . . . .	30
	Merging ePolicy Orchestrator databases . . . . .	30
	Importing events into the database . . . . .	35
<b>3</b>	<b>Report and Query Templates</b>	<b>37</b>
	Anti-Virus report templates . . . . .	37
	Coverage report templates . . . . .	37
	Infection report templates . . . . .	46
	Anti-Virus Coverage and Infection subreports . . . . .	59
	Rogue System Detection report templates . . . . .	59
	Intercept report templates . . . . .	60
	System Compliance Profiler report templates . . . . .	62
	Computer query templates . . . . .	63
	Events query templates . . . . .	65
	Installations query templates . . . . .	67

# 1

## Reporting

The ePolicy Orchestrator software includes enterprise-wide reporting functionality. You can produce a wide range of useful reports and queries from events and properties that are sent by the agent to the ePolicy Orchestrator server, and stored in the ePolicy Orchestrator database.

The ePolicy Orchestrator software includes many predefined report and query templates. These templates are stored in the report repository and query repository (accessed under **Reporting** in the console tree). You can use any template found here to create reports and queries using data on any database server. For information, see [Report and Query Templates on page 37](#).

You can produce reports and queries for a group of selected client systems. You can also limit report results by product or system criteria; for example, product name, product version number, or operating system. You can export reports into a variety of file formats, including HTML and Microsoft Excel.

ePolicy Orchestrator reports allow you to:

- Set a directory filter to gather only the information that you want to view. When setting this filter you can choose which Directory segment is included in the report.
- Set a data filter, by using logical operators, to define precise filters on the data returned by the report.
- Generate graphical reports from the information in the database, and filter the reports as desired. You can print the reports and export them for use in other software.
- Conduct queries of computers, events, and installations.

---

### About pre-defined reports in ePolicy Orchestrator

The ePolicy Orchestrator agents on the client systems send useful information to the server. This information is stored in the reports database. You can run reports and queries against this stored information.

More than 40 pre-defined reports come with ePolicy Orchestrator, and they fall into two main categories: Coverage reports and Infection reports. In addition to the reports that are available through ePolicy Orchestrator, you can also create your own report templates with the help of Crystal Reports 8.5.

### Report repository contains all report templates

The report repository contains both the pre-defined reports and queries that come with ePolicy Orchestrator and any custom reports and queries you create yourself.

You have the flexibility to organize and maintain the report repository to suit your needs. You can add reports that you exported as report templates (for example, to save custom selections made when generating a report) or add custom report templates. You can also organize report templates in logical groupings. For example, you can group reports that you run daily, weekly, and monthly under report groups with the same name.

### Coverage reports show completeness of ePolicy Orchestrator deployment

Using coverage reports, you can easily view anti-virus policy compliance. Coverage reports provide snapshots of the protection that is currently active on your systems. These reports are based on the system and product property information stored in the server's database.

Examples of coverage information include which anti-virus product has been deployed and which version of DAT and engine files are installed on which client systems. Compliance reports can help illustrate issues graphically that you have with your ePolicy Orchestrator coverage, such as getting DAT file updates to particular systems. Generate these reports and review them frequently to find areas where you can improve your ePolicy Orchestrator coverage.

### Infection reports show which viruses have been detected

Infection reports, by contrast, alert you to actual virus detections that occur in your network. These reports list which systems have the most virus detections (for example, e-mail servers running GroupShield or the Internet gateway running WebShield). They list which specific viruses are being detected, and which actions were taken by the anti-virus software deployed in your network.

### View summary information and drill down to detail

Another benefit of ePolicy Orchestrator is the ability to receive both summary and detailed information from the same report.

Summary reports are useful to remind people in your organization that ePolicy Orchestrator is doing its job. After you have ePolicy Orchestrator fully deployed for several months, generate a *Top 10 Detected Viruses* report. You may be surprised to learn how many viruses are routinely detected, and cleaned or removed.

### Control access and filter results

You can control how much report information is visible to different ePolicy Orchestrator users; for example, global administrators or site administrators. Site administrators and site reviewers can only report on those client systems in sites to which they have permissions.

---

## About reporting

Before using ePolicy Orchestrator software's reporting functionality, you should understand:

- [Crystal Reports 8.5 on page 6.](#)
- [Authentication and user accounts on page 6.](#)

## Crystal Reports 8.5

ePolicy Orchestrator 3.6 software uses Business Objects Crystal Reports 8.5 to generate reports from data stored in the ePolicy Orchestrator database. ePolicy Orchestrator comes with over 40 pre-defined reports to cover a variety of scenarios. If these do not meet your needs, you can use Crystal Reports to write your own reports. To create custom reports, see the Crystal Reports documentation.

For a list of the reports provided with ePolicy Orchestrator 3.6, see [Report and Query Templates on page 37](#).

## Authentication and user accounts

The ePolicy Orchestrator software provides enterprise-wide reporting capabilities. The ePolicy Orchestrator databases store the information that you define to include in the reports and queries.

Before using these features, it is important that you understand how certain settings or situations affect which data is reported.

### Database authentication

The authentication mode that you use to log on to ePolicy Orchestrator database servers affects whether you can limit, remove, import, or repair events in the ePolicy Orchestrator database.

When using SQL authentication:

- The DBO database role is created automatically during the installation.
- This database role is assigned to the default SQL user account (sa), and contains all of the permissions needed to access ePolicy Orchestrator databases and to limit, remove, import, or repair events.

When using NT authentication, local administrators on the database server have all permissions needed to access ePolicy Orchestrator databases and remove events. But not permissions to filter, import, or repair events.

### ePolicy Orchestrator authentication and working with events

If you use ePolicy Orchestrator authentication:

- Global administrators can view and change all options on all tabs available from Events under Reporting | ePO Databases | <DATABASE SERVER> in the console tree.
- Other users can only view this information.

If you use SQL authentication or Windows NT authentication, all users can view and change options only on the Removal tab available from Events under Reporting | ePO Databases | <DATABASE SERVER> in the console tree.

### User accounts and the data that appears in reports

When you remove systems from the Directory, the events associated with them remain in the ePolicy Orchestrator database.

Site administrators and site reviewers can only report on those client systems in sites to which they have rights.

---

## Getting started with reporting

Before generating reports, you can make configurations to limit the data retrieved. Some reporting settings affect ePolicy Orchestrator database servers, and all reports and queries. Review these settings before you run reports and queries to ensure that the desired data is displayed.

## Specifying global reporting options

Typically, you must log on to database servers every time you start the software. If using Windows NT or SQL authentication to log on to database servers, you can save the logon information for all database servers, so that you do not need to manually log on to them.



You can save logon information for individual database servers.

To specify settings that affect all ePolicy Orchestrator database servers, reports, and queries:

- 1 In the console tree, right-click **Reporting**, then select **Options**. The **Reporting** dialog box appears.
- 2 Select **Add local machine to server list if ePO server is detected** to add a local database server under **ePO Databases** every time you start the software.
- 3 Select **Encrypt and save passwords between sessions** to save logon information for all database servers using Windows NT or SQL authentication.



If you select **Encrypt and save passwords between sessions**, be sure to password-protect all database servers. Otherwise, other users might be able to gain direct access to them via the ePolicy Orchestrator console.

- 4 Accept the default **Query time-out** (600 seconds) or specify a different value to determine when to interrupt attempts to return report or query results. If you are experiencing network delays or time-out messages (for example, SQL time-out messages), increase this value.
- 5 Accept the default **Login time-out** (10 seconds) or specify a different value to determine when to interrupt attempts to log on to the database. If you are experiencing network delays or time-out messages (for example, SQL time-out messages), increase this value.
- 6 Specify whether to display event information in infection reports in local time as reported on the client system (**Local**), or in Greenwich mean time (**GMT**) under **Select Reporting Time**.
- 7 Click **OK** when done.

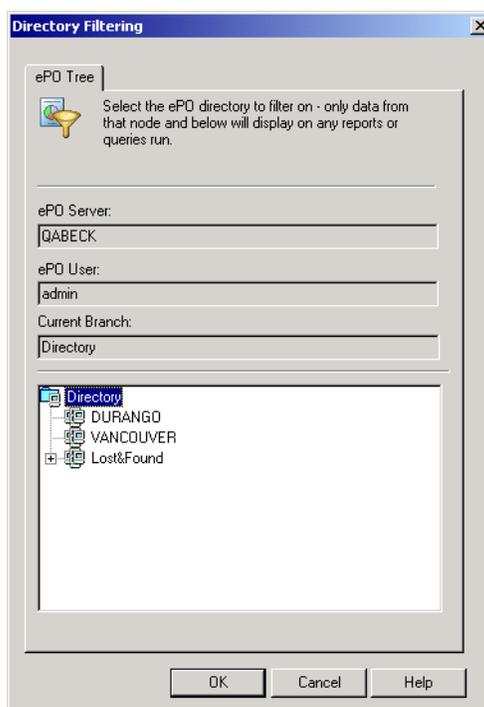
## Limiting report and query results by client system

You can limit the results of reports and queries by client systems under a selected site or group, and all groups and systems underneath it. For example, if the Directory is organized by functional group, you might want to produce separate reports and queries for each department.

To limit the results of reports and queries to client systems under a selected site or group, and all groups and systems underneath it:

- 1 In the console tree, right-click the desired database server, then select **Set Directory Filter**. The **Directory Filtering** dialog box appears.

**Figure 1-1 Directory Filtering dialog box**



- 2 Select the desired site or group for which you want to generate reports and queries.
- 3 Verify that the desired site or group appears in **Current Branch**, then click **OK**.

---

## Running and working with reports

You can control the data that appears on reports. You can define the version number of virus definition files, virus scanning engines, and supported products that need to be installed on client systems for them to be considered compliant, based on your company's anti-virus and security program. You can also limit the results of reports by selected product criteria. (For example, computer name, operating system, virus name, or action taken on infected files.)

Once the results of a report appear, you can then perform a number of functions on the data. You can view details on desired report data (for example, to determine which client systems do not have a compliant version of VirusScan installed on them). Some reports even provide links to other reports, called subreports, that provide data related to the current report. You can also print reports or export report data into a variety of file formats, including HTML and Microsoft Excel.

This section contains the following topics:

- [Running reports on page 9.](#)
- [Working with reports in the report window on page 15.](#)

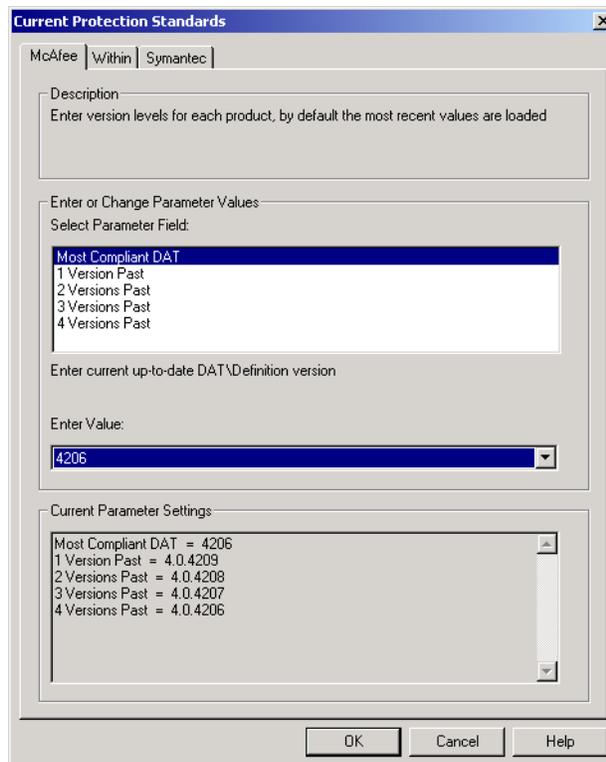
## Running reports

You can create reports using data in the selected ePolicy Orchestrator database. You can also save the selections you make in the **Enter Report Inputs** and **Report Data Filter** dialog boxes for future use. For instructions, see [Using the Saved Settings tab on page 13](#) and [Saving customized report selections as report templates on page 20](#), respectively.

To run a report:

- 1 In the console tree, select the desired report under **Reporting | ePO Databases | <database server> | Reports**.
- 2 If the **Current Protection Standards** dialog box appears, specify the version numbers of virus definition files or the virus scanning engine on which to report.

**Figure 1-2 Current Protection Standards dialog box**



- 3 If the **Enter Report Inputs** dialog box appears, make selections on any of the tabs that may appear:



Which tabs appear depends on which report is selected.

- Rules tab — See [Using the Rules tab on page 11](#).
  - Layout tab — See [Using the Layout tab on page 11](#).
  - Data Grouping tab — See [Using the Data Grouping tab on page 12](#).
  - Within tab — See [Using the Within tab on page 12](#).
  - Saved Settings tab — See [Using the Saved Settings tab on page 13](#).
- 4 To limit the results of the report by product criteria, click **Yes** when asked whether you want to set a data filter for the report. The **Report Data Filter** dialog box appears:

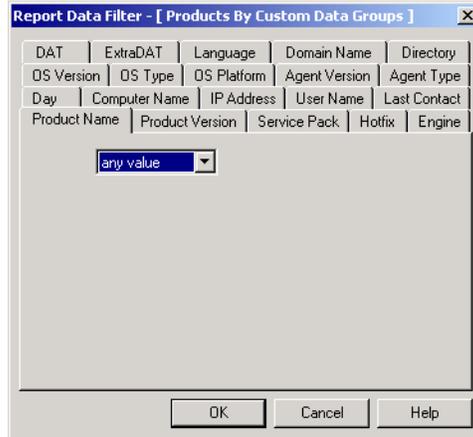


For a list of criteria for all predefined reports, see [Criteria used to limit report results on page 14](#).

- a Select the tab (for example, **Product Version**) that corresponds to the criterion for which you want to limit the report results.
- b Select an operator (for example, **any value**, **equal to**, **one of**, and others) in the condition drop-down list.
- c Further refine the condition:
  - If you select **greater than** or **less than**, select **or equal to** as needed.
  - If you select any operator other than **any value**, select **Not** to exclude the specified values.
  - If you select **between**, select or type the beginning and ending range of values.
  - If you select **equal to**, **less than**, or **greater than**, select or type the desired data field.
  - If you select **one of**, **starting with**, or **like**, select or type the desired data field, then click **Add** to include that value in the data list.
- d Repeat [Step a](#) through [Step c](#) for each desired criterion.
- e Click **OK** when done. The **Data Filter Criteria** dialog box appears.
- f To display the SQL statement that represents the product criteria you defined in the **Report Data Filter** dialog box on the report, select **Show On Report**. Use this statement to highlight that the report is based on a subset of the data in the database.

- g Click Yes. The main section of the desired report appears in the report window.

**Figure 1-3 Report Data Filter dialog box**



- 5 View report details. For instructions, see [Viewing the details of report data on page 17](#).

## Using the Rules tab

Create rules that define what compliance means in your company on the **Rules** tab of the input dialog box. These rules define the cutoff criteria for data that appears on selected reports. In other words, the data that does not meet the rules you specify is the data that appears on the report. For example, if you define the 2.5 version of the agent as being compliant, data for client systems with the 2.0, 1.1, or 1.0 version of the agent appear on the report.

To define compliance rules for the report:

- 1 In **Select Parameter Field**, select the desired item. A definition of the selected item appears under **Select Parameter Field**.
- 2 In **Enter Value**, select or type the cutoff value. The current settings appear under **Current Parameter Settings**.
- 3 Repeat [Step 1](#) and [Step 2](#) to define rules for each item listed in **Select Parameter Field**.



To modify a setting, select the desired item in **Select Parameter Field**, then select or type a different value in **Enter Value**.

To delete a settings, select the desired item in **Select Parameter Field**, then clear the value in **Enter Value**.

- 4 Click **OK** when you have finished making selections on the tabs.

## Using the Layout tab

You can select the type of chart for the report on the **Layout** tab of the input dialog box. In addition, you can specify how data is retrieved. This affects the speed that report results are returned and whether you can view report details or related report data. It also allows you to select a printable version of the report.

To specify viewing and printing options for the report:

- 1 Select **Chart Type** in **Select Parameter Field**, then select the desired chart type in **Enter Value**. The current settings appear under **Current Parameter Settings**.
- 2 To specify how data is retrieved, select **Layout** in **Select Parameter Field**, then select the desired option in **Enter Value**. The current settings appear under **Current Parameter Settings**.
  - **Drilldown (subreports)** — Allows you to view report details and related report data by clicking data in reports.
  - **Fast Drilldown (no subreports)** — Allows you to view report details only by clicking data in reports. We recommend using this option for the best performance running reports from remote consoles.
  - **No Drilldowns (Printable)** — Returns all report details, but without links. This allows you to print all pages of the report.



To change a setting, select the desired item in **Select Parameter Field**, then select or type a different value in **Enter Value**.

To delete a settings, select the desired item in **Select Parameter Field**, then clear the value in **Enter Value**.

- 3 Click **OK** when you have finished making selections on the tabs.

## Using the Data Grouping tab

You can group data in up to four different levels on the **Data Grouping** tab of the input dialog box.

To define how data is grouped on the report:

- 1 In **Select Parameter Field**, select the desired item (**First Group**, **Second Group**, **Third Group**, or **Fourth Group**). A definition of the selected item appears under **Select Parameter Field**.
- 2 In **Enter Value**, select the desired data value. The current settings appear under **Current Parameter Settings**.
- 3 Repeat [Step 1](#) and [Step 2](#) for each level of report details that you want to appear on the report.



To change a setting, select the desired item in **Select Parameter Field**, then select or type a different value in **Enter Value**.

To delete a settings, select the desired item in **Select Parameter Field**, then clear the value in **Enter Value**.

- 4 Click **OK** when you have finished making selections on the present tabs.

## Using the Within tab

You can limit the results of selected reports to data recorded within the time period you specify on the **Within** tab of the input dialog box. For example, within the last three days. Also, use this tab to limit the results of selected reports by custom data groups; for example, within anti-virus products only.

To limit the results of the report to a time period or data group:

- 1 To specify a static time period, select the item labeled **Date** in **Select Parameter Field**; for example, **Agent Connection Date**. A definition of the selected item appears under **Select Parameter Field**.

To specify a relative time period, select the item labeled **Rule** in **Select Parameter Field**; for example, **Agent Connection Rule**. A definition of the selected item appears under **Select Parameter Field**.

- 2 In **Enter Value**, select the desired time period. The current settings appear under **Current Parameter Settings**.



To change a setting, select the desired item in **Select Parameter Field**, then select or type a different value in **Enter Value**.

To delete a settings, select the desired item in **Select Parameter Field**, then clear the value in **Enter Value**.

- 3 Click **OK** when you have finished making selections on the present tabs.

## Using the Saved Settings tab

This tab allows you to:

- Save the selections you made in the **Enter Report Inputs** dialog box for future use. See [Saving settings for later use](#).
- Apply saved report input settings. See [Reusing saved settings on page 13](#).
- Duplicate and editing saved settings. See [Duplicating and editing saved settings on page 14](#).
- Delete saved settings. [Deleting saved settings on page 14](#).

## Saving settings for later use

To save settings for later use:

- 1 In **Select Parameter Field**, select **Save**.
- 2 Type a descriptive name in **Enter Value**, type a descriptive name for the report input settings. The current settings appear under **Current Parameter Settings**.
- 3 Make changes as needed.
- 4 Click **OK** when you have finished making selections on the present tabs.

## Reusing saved settings

To reuse saved settings:

- 1 In **Select Parameter Field**, select **Open**.
- 2 In **Enter Value**, select the desired report settings. The current report settings appear under **Current Parameter Settings**.
- 3 Make changes as needed.
- 4 Click **OK** when you have finished making selections on the present tabs.

### Duplicating and editing saved settings

To save settings based on already saved settings:

- 1 In **Select Parameter Field**, select **Open**.
- 2 In **Enter Value**, select the desired report settings.
- 3 Make changes as needed.
- 4 Click the **Saved Settings** tab.
- 5 In **Select Parameter Field**, select **Save As**.
- 6 In **Enter Value**, select the same report settings you selected in [Step 4](#). The current report settings appear under **Current Parameter Settings**.
- 7 Click **OK** when you have finished making selections on the present tabs.

### Deleting saved settings

To delete saved settings:

- 1 In **Select Parameter Field**, select **Delete**.
- 2 In **Enter Value**, select the desired report input settings you want to delete.
- 3 Click **OK** when you have finished making selections on the present tabs.

### Criteria used to limit report results

You can limit the data that appears on selected reports by the computer, infection, or product criteria you specify in the **Report Data Filter** dialog box. For example, you might want to view only coverage information about VirusScan Enterprise 8.0i.

The criteria vary depending on the report. Criteria for all predefined reports are:

- **Action** — Limits results by the action taken by anti-virus product upon detection.
- **Agent Type** — Limits results by agents, SuperAgents, or SuperAgent distributed repositories.
- **Agent Version** — Limits results by agent version number.
- **Computer Name** — Limits results by client system name.
- **DAT** — Limits results by the virus definition file version number.
- **Date Time** — Limits results by the date and time of events.
- **Day** — Limits results by day. Use this format YYYY-MM-DD (year-month-day); for example, 2003-04-23.
- **Directory** — Limits results to the systems in the selected site or group under the **Directory**. Data for groups and systems under the selected site or group are not included on the report.
- **Domain Name** — Limits results by Windows NT domain name.
- **Engine** — Limits results by the virus scanning engine version number.
- **Extra DAT** — Limits results by the supplemental virus definition (EXTRA.DAT) file version number.

- **File Name** — Limits results based on the name and location of infected files.
- **HotFix** — Limits results by HotFix release number.
- **IP Address** — Limits results using the IP address of client systems.
- **Language** — Limits results by language version.
- **Last Contact** — Limits results by the date and time that the agent communicated with the ePolicy Orchestrator server.
- **Month** — Limits results by month. Use this format YYYY-MONTH (year-month); for example, 2003-April.
- **OS Platform** — Limits results by platform; for example, Server or Workstation.
- **OS Type** — Limits results by operating system name.
- **OS Version** — Limits results by operating system version number.
- **Product Name** — Limits results by product.
- **Product Version** — Limits results by product version number.
- **Quarter** — Limits results by quarter. Use this format YYYY-Q (year-quarter); for example, 2003-2.
- **Rule Name** — Limits results by content rule.
- **Rule Type** — Limits results by content rule type; for example, content scanning.
- **Server** — Limits results by WebShield appliance name.
- **Service Pack** — Limits results by service pack release number.
- **Severity** — Limits results by event severity. The severity levels in order from most to least severe are **Critical**, **Major**, **Minor**, **Warning**, and **Informational**.
- **Spam Source** — Limits results by the portion of the e-mail message that contains the offending content; for example, header, subject, or body.
- **Spammer** — Limits results by the e-mail address of the spammer.
- **Task Name** — Limits results by the scanning task that resolved the infection; for example, on-demand scan or on-access scan.
- **User Name** — Limits results using the user name logged on to the client system.
- **Virus Name** — Limits results by the virus name.
- **Virus Subtype** — Limits results by virus subtype.
- **Virus Type** — Limits result by virus type; for example, Trojan Horse.
- **Week** — Limits results by week. Use this format YYYY-WW (year-week); for example, 2003-17.
- **Year** — Limits results by year.

## Working with reports in the report window

The results of reports appear in the report window. Use the report window exclusively to work with generated reports, including viewing details of report data, printing reports, and exporting report data. For this reason, it is important to understand the components in the report window before you begin working with reports.

## The report window components

The report window provides the following components:

**Preview tab** — When selected, displays the main section of the report.

**Group tab** — When selected, displays the corresponding group section of the report.

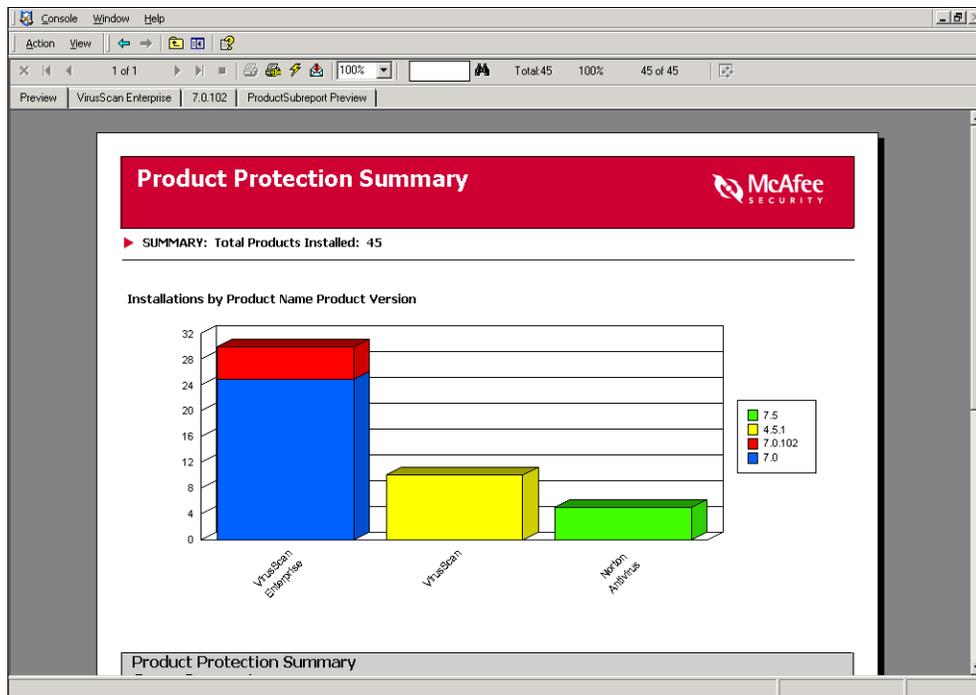
**Details tabs** — When selected, displays the corresponding details section of the report.

**Subreport tabs** — When selected, displays the corresponding subreport.

**Report sections** — Displays summary-level data (main section), group-level data (group section), detailed data (details section), or related data (subreport).

**Report toolbar** — Provides access to common reporting tasks. For more information, see [The report toolbar on page 16](#).

Figure 1-4 Report window components



## The report toolbar

The report toolbar is one of the main components of the report window. The buttons on this toolbar are:

Click this...



To...

Close the active details section of the report.



Go to the first page in the selected section of the report.

	Go to the previous page in the selected section of the report.
1 of 2	Display the current page number and the total number of pages in the selected section of the report.
	Go to the next page in the selected section of the report.
	Go to the last page in the selected section of the report.
	Stop updating the report with data.
	Print the selected section of the report.
	Set printing preferences.
	Update the current report with data that has been saved into the ePolicy Orchestrator database since you initially ran the report. Available only when you select the <b>Preview</b> tab.
	Export the selected section of the report in a variety of file formats.
<input data-bbox="480 1037 609 1083" type="text" value="3.0.0"/>	Specify the words or phrases that you want to find in the selected section of the report.
	Locate specified words or phrases in a selected section of the report.
100%	Display the percentage of records that were relevant to the report.
62 of 62	Display the number of relevant records in relation to the total number of records in the database.
	Start Crystal Analysis. This is available only when this application is installed.

## Viewing the details of report data

To view details of report data:



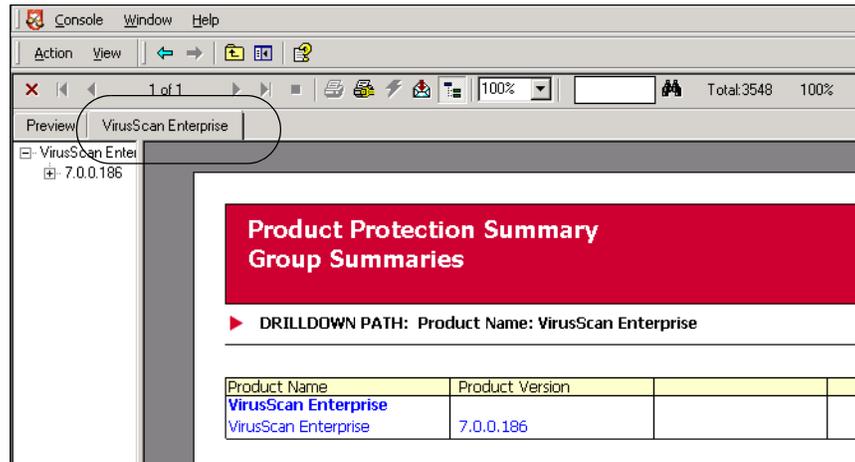
For a list of detailed data available in each report, see [Report and Query Templates on page 37](#).

- 1 Run the report. For instructions, see [Running reports on page 9](#). The main section of the desired report appears in the report window.
- 2 Click any blue text to drill down for more detailed information.

- To view the group-level report data, double-click the desired data. The group-level data appears in the report window. A group tab for the selected data also appears and allows you to move between sections of the report.

In the following example, when you double-click **VirusScan Enterprise** in the main section of the report, the corresponding group section appears in the report window and the **VirusScan Enterprise** group tab also appears.

**Figure 1-5 Viewing group-level report data**



- Repeat [Step 3](#) to view more group-level report data.  
If no additional data is listed, you've reached the details section of the report for the selected data.
- To continue viewing details on report data, click the **Preview** tab or a groups tab, then repeat [Step 3](#) to view details on other data.
- To view related report data, click the subreport icons or links that appear in selected report.

## Printing reports

To print the selected section of the report:

- Run the report. For instructions, see [Running reports on page 9](#).
- To set printing preferences, click the **Printer Setup** button on the report toolbar. The **Print Setup** dialog box appears. For instructions on setting printing preferences, see printing-related topics in the Microsoft Windows Help file.
- To print the selected section of the report, click the **Print** button on the report toolbar.

## Exporting report data to other formats

You can export reports to many number standard formats. Distributing reports or making them available for viewing is an important part of ongoing ePolicy Orchestrator administration. For example, you can post a daily summary report on DAT compliance to a corporate web site, or distribute a weekly PDF report detailing virus infection and security information to important individuals in your organization to help remediate problems.

Some common export formats are:

- Adobe Acrobat PDF
- HTML
- Crystal Reports (RPT)
- Rich Text and Microsoft Word.
- Microsoft Excel

Use this procedure to export the selected section of the report in a variety of file formats.

- 1 Run the report. For instructions, see [Running reports on page 9](#).
- 2 Click the **Export** button on the report toolbar. The **Export** dialog box appears.
- 3 Select the desired **Format**.
- 4 Click **OK**. The **Choose Export File** dialog box appears.
- 5 Specify the name and location of the file, then click **Save**.

---

## Queries

Queries provide a specific, single view. A query can be either a group summary or a detailed view. Queries run faster than reports but do not support all the functionality of the reports.

Queries display data in a raw tabular form. They support Directory filtering and the creation of new user SQL queries. They do not support data filtering, drilling down into details, and the subreport features of reports.

In addition to the predefined queries that are available, you can create your own custom queries. In addition, you can refresh query data or go to specific rows in a query.

## Running queries

To create queries using data in the selected ePolicy Orchestrator database:

- 1 Log on to the desired ePolicy Orchestrator database server.
- 2 To limit the results to the client systems in a selected site or group, set a query filter. For instructions, see [Limiting report and query results by client system on page 8](#).
- 3 In the console tree under **Reporting | ePO Databases | <DATABASE SERVER> | Queries | <QUERY GROUP>**, right-click **<QUERY>**, then select **Run**. Results of the query appear in the details pane.
- 4 To go to a specific row in the query:
  - a Right-click anywhere in the query, then select **Row**. The **Go to Row** dialog box appears.
  - b Type or select the **Row number**, then click **OK**.

- 5 To refresh the data in the query, right-click anywhere in the query and select **Run**.



You can copy and paste query results into other applications; for example, Microsoft Excel.

---

## Report repository maintenance

You have the flexibility to organize and maintain the report repository however it best suits your needs. You can add reports that you exported as report templates (for example to save custom selections you made when you ran the report) or add custom report templates. You can also organize report templates in logical groupings. For example, you can group reports that you run daily, weekly, and monthly under report groups with the same name.

### Saving customized report selections as report templates

Use this procedure to save the selections you made in the **Current Protection Standards**, **Enter Report Inputs**, and **Report Data Filter** dialog boxes as a report template.



This procedure is the only method with which you can save the selections you made in the **Current Protection Standards** and **Report Data Filter** dialog boxes for future use.

You can save the selections you made in the **Enter Report Inputs** dialog box at the same time that you make them. For instructions, see [Using the Saved Settings tab on page 13](#).

- 1 Run the desired report.
- 2 Click the **Export** button on the report toolbar. The **Export** dialog box appears.
- 3 Select **Crystal Reports (RPT)**.
- 4 Click **OK**. The **Choose Export File** dialog box appears.
- 5 Specify the name of the file and a new folder in the report repository where you want to store it temporarily, then click **Save**.
- 6 Copy the **REPORTS.INI** and **REPORTS\_0409.INI** files from the **Coverage** folder to the location in the report repository to which you exported the report template file.
- 7 Edit the **REPORTS.INI** file in the new folder:
  - a Remove all entries except the entry of the newly exported report.
  - b Comment out the **RptReportFileDir** parameter (by adding a semicolon at the start of the line).
  - c If you do not want the **Enter Report Inputs** or **Report Data Filter** dialog boxes to appear, comment out the **ConfigurationDLL** parameter (by adding a semicolon at the start of the line).
  - d If desired, change the name and description parameters.



Leave the **SectionName** and **RptReportFileName** parameters the same as the exported reports file name.

## Adding a custom report template

To add report templates to the desired report group in the report repository under **Reporting** in the console tree:

- 1 In the console tree, right-click the desired report group under **Report Repository** (for example, **Anti-Virus**), then select **Add report template**. The **New Report Definition** dialog box appears.



If you need to create an appropriate report group for the template you want to add, see [Creating report groups on page 21](#).

- 2 Type the **Name of the Report** as you want it to appear in the console tree.
- 3 Type the path of the desired report template (.RPT) file in **Report file**, or click >> to browse to and select one.
- 4 Type a literal **Description** of the report.
- 5 If you are adding a custom report template that requires external files, click **Add** to include them under **Report Components**.



The predefined report templates do not use external files.

- 6 Click **OK**. The report template appears in the report repository. The report appears under **Reporting | ePO Databases | <DATABASE SERVER>** the next time you log on to a database server.

## Modifying report templates

To modify existing report templates:

- 1 In the console tree under **Report Repository**, select the desired report template. The **Report Definition** dialog box appears.
- 2 Click **Organize** to open the **Organize Report** dialog box.
- 3 Change the **Name of the Report** as needed.
- 4 Specify a different **Report file** as needed.
- 5 Change the **Description** as needed.
- 6 Click **OK** when done.

## Deleting report templates

To permanently delete report templates from the report repository that you no longer want to use to create reports, right-click the desired report template in the console tree under **Report Repository**, then select **Remove**.

## Creating report groups

To create report groups for better organization of the report repository:

- 1 In the console tree, right-click **Report Repository** or the desired report group within which you want to create the new report group, then select **New report group**. The **New Report Group** dialog box appears.
- 2 Enter the name for the new group, then click **OK**. The new group appears in the console tree.

## Deleting report groups

To permanently delete report groups and all of the report templates stored in them from the report repository, right-click the desired report group in the report repository, then select **Remove**.

## Adding report templates from new products to the report repository

If you decide to deploy and manage a new McAfee product to your environment that is released after ePolicy Orchestrator 3.6, you can add report templates to the report repository that come bundled in the reporting NAP file.

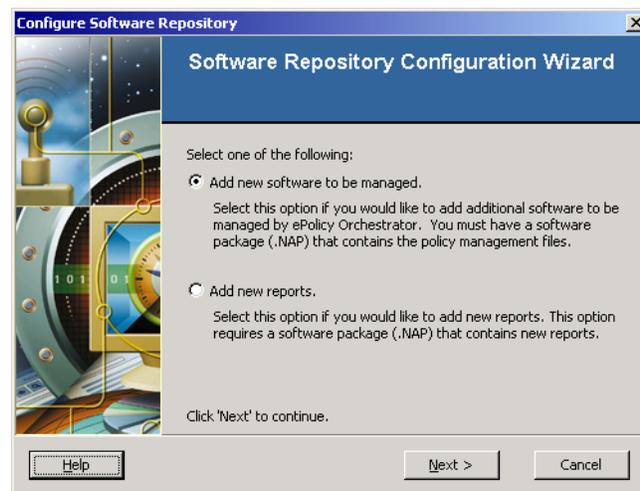
To add report templates from a NAP file to the report repository:

- 1 In the console tree, right-click **Repository**, then select **Configure Repository**. The **Software Repository Configuration Wizard** appears.



Although you right-click **Repository** to initiate this task, the report template is added to the report repository and not the software repository.

**Figure 1-6 Software Repository Configuration Wizard**



- 2 Select **Add new reports**, then click **Next**. The **Select a Software Package** dialog box appears.
- 3 Select the desired language version reporting NAP file of the product, then click **Open**. The file is uncompressed, then the individual files are added to the report repository on the ePolicy Orchestrator server.

- Log back onto the ePolicy Orchestrator database to download the reports into the report repository.



You must use ePolicy Orchestrator authentication or NT authentication to download the reports.

## Query repository maintenance

You can organize the query repository to suit your needs, or add custom query templates.

### Adding custom query templates

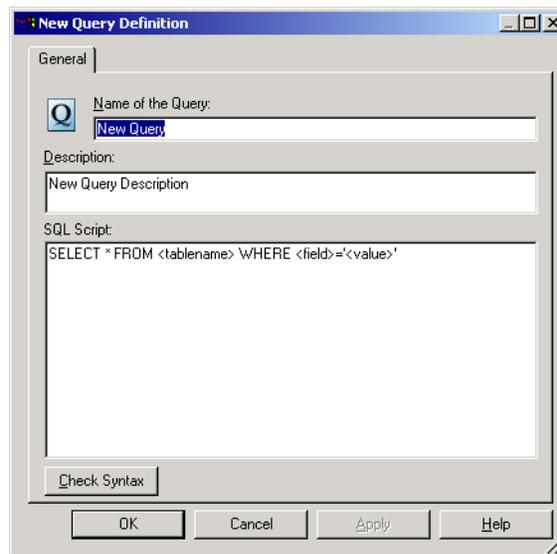
To add custom query templates to the desired query group in the query repository:

- In the console tree, right-click the desired query group under **Query Repository**, then select **Add query template**. The **New Query Definition** dialog box appears.



If you need to create a new query group in which to add the new query, see [Creating query groups on page 25](#).

**Figure 1-7 New Query Definition dialog box**



- Type the **Name of the Query** as you want it to appear in the console tree.
- Type a literal **Description** of the query.
- In **SQL Script**, type the SQL statement of the query that you want to add.



You can only specify one select statement. This statement cannot execute stored procedures or use a union clause.

- To verify the syntax of the **SQL Script**:

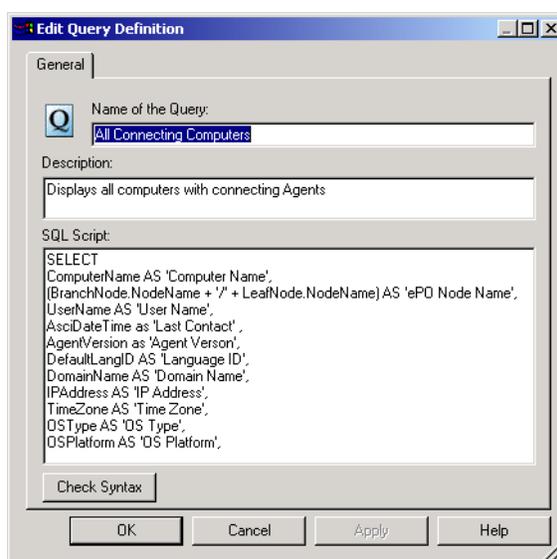
- a Click **Check Syntax**. If you are currently logged onto more than one database server, the **Choose Server** dialog box appears.
  - b Select the desired database server, then click **OK**.
- 6 Click **OK** when done. The query template appears in the query repository.

## Modifying query templates

To modify existing query templates:

- 1 Click the desired query template under **Query Repository**. The **Query Definition** dialog box appears in the details pane.
- 2 Click **Edit** to open the **Edit Query Definition** dialog box.

**Figure 1-8 Edit Query Definition dialog box**



- 3 Change the **Name of the Query** as needed.
- 4 Change the **Description** of the query as needed.
- 5 In **SQL Script**, change the SQL statement of the query as needed.



You can only specify one select statement. This statement cannot execute stored procedures or use an union clause.

- 6 To verify the syntax of the **SQL Script**, do the following:
  - a Click **Check Syntax**. If you are currently logged on to more than one database server, the **Choose Server** dialog box appears.
  - b Select the desired database server, then click **OK**.
- 7 Click **OK** when done.

## Deleting query templates

To permanently delete query templates from the query repository that you no longer want to use to create queries, right-click the desired query template in the in the query repository, then select **Remove**.

## Creating query groups

To better organize the query repository, you can create query groups. To add query groups to the query repository:

- 1** In the console tree, right-click **Query Repository** or the desired query group in which to store query templates, then select **New query group**. The **New Query Group** dialog box appears.
- 2** Enter the name for the new group, then click **OK**. The new group appears in the console tree.

## Deleting query groups

To permanently delete a query group and all of the query templates stored in it, from the query repository, right-click the desired query group, then select **Remove**.

# 2 ePolicy Orchestrator Databases and Reports

You can use either Microsoft Data Engine or Microsoft SQL Server as your ePolicy Orchestrator database server. Whichever you use, your ePolicy Orchestrator databases require some management. Database servers can reside on the same system as the ePolicy Orchestrator server or on a separate system. You can work with multiple databases within the same console session.

You can use a combination of tools to maintain ePolicy Orchestrator databases. You must use a slightly different set of tools depending on whether you are using a Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) or SQL Server database as the ePolicy Orchestrator database. Note that you can use Microsoft SQL Server Enterprise Manager to maintain both MSDE and SQL Server databases.

---

## About ePolicy Orchestrator databases

Once your ePolicy Orchestrator databases are installed, you need to be able to understand and perform some basic tasks, and configure which events are going to be stored for efficient reporting.

## Working with user accounts and events

The ePolicy Orchestrator administrator account that you use to log on to ePolicy Orchestrator database servers determines the tasks you can perform, and the data on which you can report.

Only the global administrator can:

- Limit events.
- Import events.
- Repair events.
- Delete events.

Site administrators can only view events.

## Logging onto and off from ePolicy Orchestrator database servers

Before you can run reports or queries, you need to log on to the ePolicy Orchestrator database server that contains the data on which you want to report.

You can be logged on to multiple database servers at once. Note that you log on to database servers separately from the ePolicy Orchestrator server itself. You can also log off or remove database servers from the console tree as needed.

## Logging onto ePolicy Orchestrator database servers

Typically, you must log onto database servers every time you start ePolicy Orchestrator. If you are using Windows NT or SQL authentication to log on to database servers, you can save the logon information for individual database servers, as well as all database servers. For instructions, see [Specifying global reporting options on page 7](#).

Depending on whether the desired ePolicy Orchestrator database server already appears in the console tree, you need to complete different steps to log on to it.



If the ePolicy Orchestrator database resides on the same system as the ePolicy Orchestrator server, the database server appears automatically in the console tree.

In the console tree, ePolicy Orchestrator database server names are displayed in the format: `database_name(authenticated_server_name)`

The name within parentheses is the name of the server to which you authenticate, which is not necessarily the server on which the database is housed.

## Logging onto database servers that appear in the console tree

To log onto an ePolicy Orchestrator database server that already appears in the console tree under **Reporting | ePO Databases**:

- 1 In the console tree under **Reporting | ePO Databases**, right-click the desired database server, then select **Connect**. The **ePO Database Login** dialog box appears.
- 2 If **Connection Information** items do not appear in this dialog box, click **Options** to display them. They allow you to select the authentication mode.
- 3 Under **Connection Information**, select the **Authentication Type** to verify the authenticity of the logon information. Depending on the **Authentication Type** you chose, make the necessary selections:
  - Type the **User name** and **Password** of the account type selected.
  - Type the **Domain** name.
  - Type the **HTTPS port number** that corresponds to the ePolicy Orchestrator server as entered during the installation
  - To save the logon information for the selected database server, select **Save connection information and do not prompt again**.



This option is available for SQL and NT authentication only.

If you select **Save connection information and do not prompt again**, be sure to password-protect the corresponding database server. Otherwise, users might be able to gain direct access to it via the ePolicy Orchestrator console.

- 4 Click **OK** to connect to the specified database server using the logon information provided.

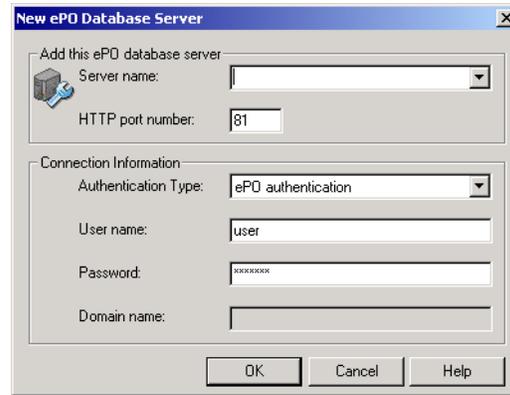
## Logging onto ePolicy Orchestrator database servers that do not appear in the console tree

You can add multiple database servers to the console tree, which enables you to work with more than one database server in the same session.

To add and log onto an ePolicy Orchestrator database server:

- 1 In the console tree under **Reporting**, right-click **ePO Databases**, then select **Add new server**. The **New ePO Database Server** dialog box appears.

**Figure 2-1 New ePO Database Server dialog box**



- 2 Select the **Authentication Type** to verify the authenticity of the logon information.



If you log on to a database server with ePolicy Orchestrator authentication, you have access to all of the **Events** tabs: **Filtering**, **Removal**, **Import**, **Repair**. If you log on to a remote database server with any other type of authentication, you only have access to the **Removal** tab of **Events**. To check your authentication type, see the **Access Type** column in the details pane when you select the ePolicy Orchestrator database under Reporting of the console tree.

- 3 In **Server name**, type or select the name of the database server to which you want to connect. To select the local server, type or select **local**.
- 4 Make selections based on the **Authentication Type** you chose in [Step 2](#):
  - Type the **User name** and **Password** of the account type selected.
  - Type the **Domain** name.
  - Type the **HTTP port number** that corresponds to the ePolicy Orchestrator server as entered during the installation
  - To save the logon information for the selected database server, select **Save connection information and do not prompt again**.



This option is available for SQL and NT authentication only.

If you select **Save connection information and do not prompt again**, be sure to password-protect the corresponding database server. Otherwise, users might be able to gain direct access to it via the ePolicy Orchestrator console.

- 5 Click **OK** to connect to the specified database server using the logon information provided.

## Logging off from ePolicy Orchestrator database servers

To log off the selected ePolicy Orchestrator database server, but leave its icon in the console tree, right-click the desired database server in the console tree under **Reporting | ePO Databases**, then select **Disconnect**.

## Removing ePolicy Orchestrator database servers

To log off from the selected ePolicy Orchestrator database server (if a connection currently exists) and remove its icon from the console tree:

- 1 In the console tree under **Reporting | ePO Databases**, right-click <DATABASE SERVER>, then select **Remove**.
- 2 To clear the saved logon information:
  - a Exit the software.
  - b Log onto the desired database server. Be sure to deselect **Save connection information and do not prompt again**.



Once you clear the logon information, log onto the database server every time you start the software.

## Defining which events are stored in the database

ePolicy Orchestrator databases store events from managed systems and appliances. ePolicy Orchestrator allows you to define, by filtering, which events you want stored in the ePolicy Orchestrator database for reporting purposes.

Because service events (for example, starting or stopping software) are numerous, they are not collected by default. McAfee recommends that you accept the default selections to reduce the size of the database.



You must be a global administrator to limit events. Other users can only view these settings.

To specify the events to be stored in the database:

- 1 Log on to the desired ePolicy Orchestrator database server using ePolicy Orchestrator authentication and a global administrator user account.
- 2 In the console tree under **Reporting | ePO Databases | <DATABASE SERVER>**, select **Events**. The **Filtering**, **Import**, **Repair**, and **Removal** tabs appear in the details pane.
- 3 On the **Filtering** tab, select **Send only the selected events to ePO**, then select checkboxes that correspond to events that you want to collect.

The severity icons of events are listed in order of severity below:

-  Informational
-  Warning
-  Minor
-  Major
-  Critical

- 4 To collect all events, select **Do not filter events (send all events)**.
- 5 Click **Apply** to save the current entries. Your selections take affect at the next agent-server communication.

---

## Reporting and multiple databases

Although you can log onto multiple ePolicy Orchestrator database servers at once, reports and queries can only display data from a single ePolicy Orchestrator database at a time, unless you:

- Merge two or more ePolicy Orchestrator databases. This is useful when the databases were created using version 3.0 or later. For instructions, see [Merging ePolicy Orchestrator databases on page 30](#).
- Import events from one ePolicy Orchestrator database into another. This is useful if the databases were created with versions of the software previous to version 3.0. [Importing events into the database on page 35](#).

## Merging ePolicy Orchestrator databases

To create reports or queries that combine data from multiple databases, you can merge them into a new or existing database. This allows you to create reports and queries that contain data for all of the databases that you merge together:

### Creating merged databases

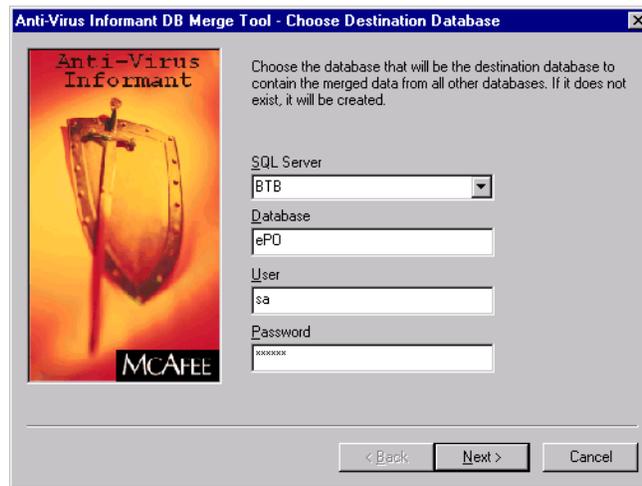
You can merge multiple ePolicy Orchestrator databases into a new or existing database. You can also save the settings you make in the DB Merge Tool to a merge settings text file so that you can run the program later, using the database merge settings you define here. Use this if you merge the same ePolicy Orchestrator databases on a routine basis.

To merge multiple ePolicy Orchestrator databases into a new or existing database:

- 1 Double-click the DB Merge Tool (AVIDB\_MERGE\_TOOL.EXE) file. The default location is:

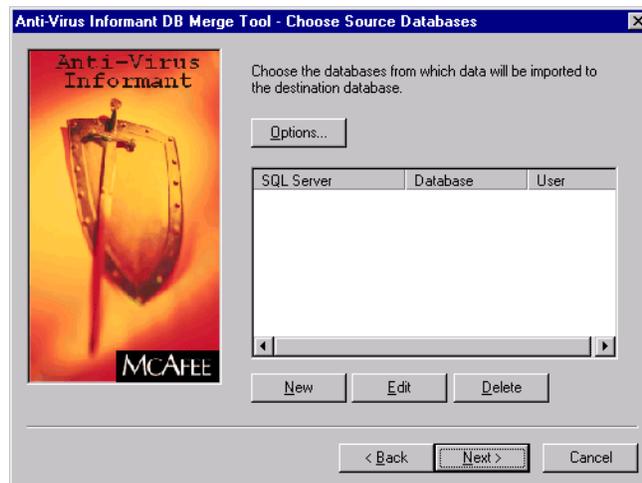
c:\program files\mcafee\epo\3.6.0\avi

**Figure 2-2 Choose Destination Database dialog box**



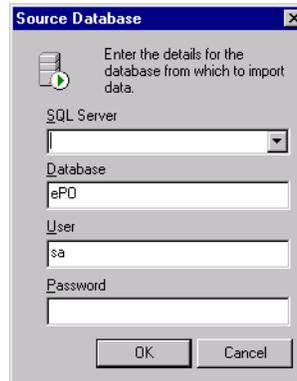
- 2 In the Choose Destination Database dialog box, select or type the name of the SQL Server (database server) and Database into which you want to merge databases.
- 3 Type the User name and Password of an administrator user account on the database server you specify, then click Next. The Choose Source Databases dialog box appears.

**Figure 2-3 Choose Source Databases dialog box**



- Click **New** to open the **Source Database** dialog box to specify the databases that you want to merge.

**Figure 2-4 Source Database dialog box**

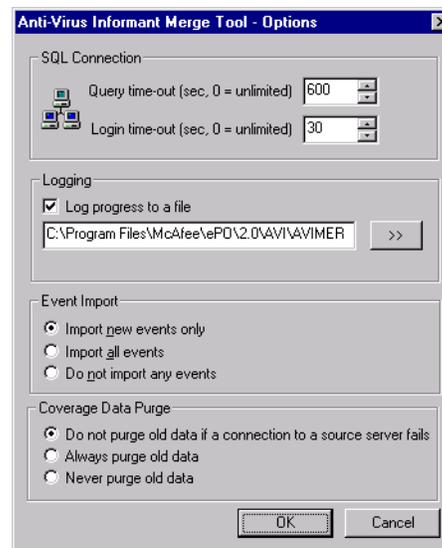


- Select or type the name of the **SQL Server** (database server) and **Database**, then type the **User** name and **Password** of an administrator user account on the database server you specify.
- Click **OK** to save the current entries and return to the **Choose Source Databases** dialog box.
- Repeat [Step 4](#) through [Step 6](#) for each desired database.
- Click **Options** to open the **Merge Tool - Options** dialog box to specify merge settings for all of the databases that are being merged.



If you are merging databases into an existing database, these settings do not affect that database.

**Figure 2-5 Merge Tool - Options dialog box**



- a Accept the default **Query time-out** (600 seconds) or specify a different amount of time to interrupt attempts to return report or query results.
- b Accept the default **Login time-out** (10 seconds) or specify a different amount of time to interrupt attempts to log on to the database.
- c To save entries about the merge process to a log file, select **Log progress to a file**, then specify the path of the merge log (AVIMERGE.LOG) file. If you select an existing file, entries are appended to the end of it. The default location is:

```
c:\program files\mcafee\epo\3.6.0\avi
```

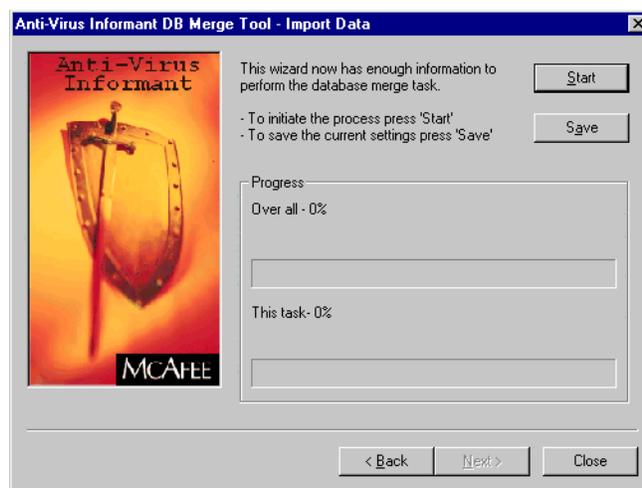
- d Under **Event Import**, specify whether to include events in the destination database.



McAfee recommends deleting events from the destination database before using the **Import all events** option to avoid creating duplicate events in the destination database.

- e Under **Coverage Data Purge**, specify whether to include system and product properties in the destination database.
- f Click **OK** to save the current entries and return to the **Choose Source Databases** dialog box.
- g Click **Next** to open the **Import Data** dialog box.

**Figure 2-6 Import Data dialog box**



- 9 If you want to save these settings for reuse:
  - a Click **Save** to open the **Save As** dialog box.
  - b Specify a path and name of the merge settings file (for example, C:\PROGRAM FILES\MCAFFEE\EPO\3.6.0\AVI\SETTINGS.TXT).
  - c Click **Save** to return to the **Import Data** dialog box.
- 10 Click **Start** to begin the merge process.

If you chose **Import new events only**, you can stop the merge process any time by clicking **Cancel**.

- 11 Click **Close** when complete.



If the merge process could not connect to a server, the merge database is not created.

## Merging databases with a merge settings file

You can merge ePolicy Orchestrator databases together using predefined database merge settings. After you create a merge settings text file, you can use it, as needed, with one of the following methods.

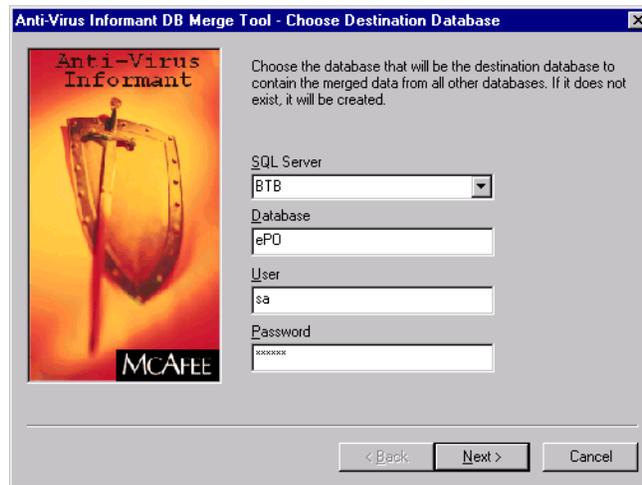
### Merging databases with a merge settings file using the drag-and-drop operation

To drag the merge settings file that contains predefined database merge settings to the application window:

- 1 Start the DB Merge Tool (AVIDB\_MERGE\_TOOL.EXE). The default location is:

```
c:\program files\mcafee\epo\3.6.0\avi
```

**Figure 2-7 Choose Destination Database dialog box**



- 2 In Windows Explorer, locate the desired Merge Settings (.TXT) file.
- 3 Drag the desired merge settings file to the **Choose Destination Database** dialog box.
- 4 Make any changes as needed.
- 5 In the **Import Data** dialog box, click **Start** to begin the merge process.
- 6 Click **Close**.

### Merging databases with the merge settings file from the command line

To run the DB Merge Tool from the command line using the merge settings file:

- 1 At the command line, type the path of the DB Merge Tool (AVIDB\_MERGE\_TOOL.EXE) followed by the path of the merge settings text file.

For example, if the program and merge settings file are in the default location, type the following:

```
C:\PROGRAM FILES\MCAFEE\EPO\3\AVI\AVIDB_MERGE_TOOL.EXE C:\PROGRAM FILES\MCAFEE\EPO\3.6.0\AVI\SETTINGS.TXT
```

- 2 Make any changes as needed.
- 3 In the **Import Data** dialog box, click **Start** to begin the merge process.
- 4 Click **Close**.

### Merging databases in the background using the merge settings file

You might find this helpful if you want to use a third-party scheduling tool to schedule the merge process. To merge ePolicy Orchestrator databases in the background using the merge settings file:

- 1 At the command line, type the path of the DB Merge Tool (AVIDB\_MERGE\_TOOL.EXE), type the silent parameter to run the program in the background, followed by the path of the merge settings file.

For example, if the program and merge settings file are in the default location, type the following:

```
C:\PROGRAM FILES\MCAFEE\EPO\3.6.0\AVI\AVIDB_MERGE_TOOL.EXE /SILENT C:\PROGRAM FILES\MCAFEE\EPO\3.6.0\AVI\SETTINGS.TXT
```

- 2 An **Anti-Virus Informant DB Merge Tool - Choose Destination Database** icon appears on the taskbar to indicate that the merge process is running.

## Importing events into the database

You can import events from another ePolicy Orchestrator database into the current one, so that the selected events are available for reporting purposes.



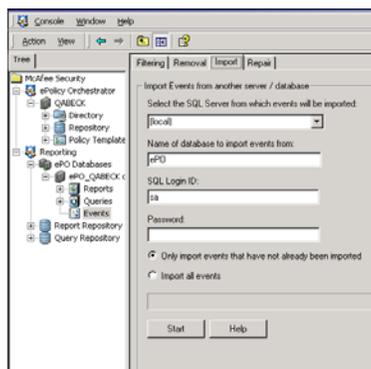
You must be a global administrator to import events.

To import events from one ePolicy Orchestrator database into another:

- 1 Back up both databases.
- 2 Log onto the desired ePolicy Orchestrator database server using ePolicy Orchestrator authentication and a global administrator user account.
- 3 In the console tree under **Reporting | ePO Databases | <DATABASE SERVER>**, select **Events**. The **Filtering**, **Import**, **Repair**, and **Removal** tabs appear in the details pane.

- 4 Click the **Import** tab.

**Figure 2-8 Import tab**



- 5 In **Select the SQL Server from which events will be imported**, select or type the name of the SQL server that contains the database from which you want to import events.
- 6 In **Name of database to import events from**, accept the default database server name, or type the name of a different database server from which you want to import events.
- 7 Type the **SQL Login ID** and **Password** of an administrator account on the selected database.
- 8 Select either **Only import events that have not already been imported** or **Import all events**.



Be aware that the **Import all events** option might add duplicate events into the database.

- 9 Click **Start** to import events from the selected database into the current one.
- 10 Repair events.

# 3

## Report and Query Templates

The ePolicy Orchestrator software includes a number of predefined report and query templates. These templates and any custom templates you provide are stored in the Report Repository and query repository, (available under **Reporting** in the console tree). Any template found here can be used to create reports and queries using the data on any ePolicy Orchestrator database server.

The purpose of each report and query template is described in the following sections. Depending on which products you have checked into the Repository, you may see additional templates that are not described here. For information on them, see the product-specific configuration guide.

---

### Anti-Virus report templates

Anti-virus report templates are divided into two categories:

- [Coverage report templates on page 37.](#)
- [Infection report templates on page 46.](#)

### Coverage report templates

There are predefined coverage report templates under **Reporting | Anti-Virus | Coverage**.

#### Agent to Server Connection Info report template

Specify the time period that defines an inactive agent, then view report data in a pie chart format that categorizes your systems as:

- **Current** — Systems with agents that have called into the server within the user-defined time period. Also referred to as *active agents*.
- **Late** — Systems with agents that have not called into the server within the user-defined time period. Also referred to as *inactive agents*.
- **No Agent** — Systems without agents.

You can view historical data for systems using the Tasks, Policies, Update, and Infection subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 59](#).

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab in the **Enter Reports Input** dialog box:

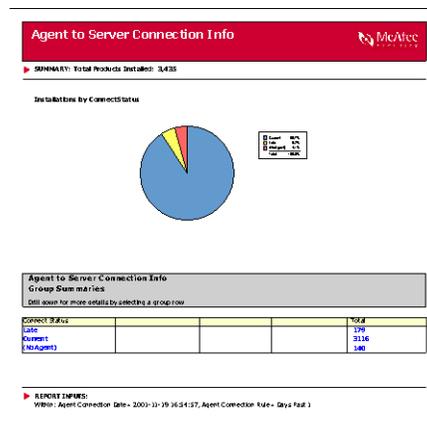
- **Agent Connection Date** — Specifies a cutoff date and time that defines an inactive agent. Agents that have not communicated with the server since the date you specify are reported as inactive (late).
- **Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) that defines an inactive agent.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

### Sample report

**Figure 3-1 Sample Agent to Server Connection Info report**



## Agent Versions report template

View the versions of ePolicy Orchestrator agents, SuperAgents, and SuperAgent distributed repositories that are currently in use on client systems, in a bar chart format. Use this report for an overall view of how up-to-date the agents are on client systems.



Legacy agents are not fully functional in ePolicy Orchestrator 3.6. For full agent functionality, you must upgrade to agent version 3.5. Check the versions of agents in your environment.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Compliance Issues report template

View all compliance issues on systems that violate the compliance rules you specify. You can also view systems with unresolved detections. In addition, you can view historical data for systems using the **Tasks**, **Policies**, **Update**, **Infection**, and **Compliance History** subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 59](#).

Compliance violations are grouped into these categories:

- Inactive agents.
- No agent.
- No anti-virus protection.
- Out-of-date agent.
- Out-of-date virus definition (DAT) files.
- Out-of-date virus scanning engine.
- Out-of-date anti-virus products.
- Unresolved infections.

### Rules

Use the **Product Version Rules** tab in the **Enter Reports Input** dialog box to define compliance rules for this report. Specify the minimum version number of the following that meets your compliance requirements. The report includes data for systems with older versions installed.

- The ePolicy Orchestrator agent.
- Supported products.
- McAfee virus definition (DAT) files.
- McAfee virus scanning engine.
- Symantec virus definition files.
- Symantec engine.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (**Enter Reports Input** dialog box):

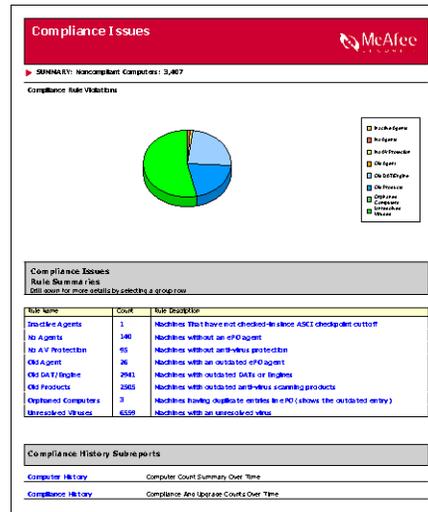
- **Late Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Late Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since the time period you specify appear on the report.
- **Recent Infection Date** — Specifies a cutoff date and time for unresolved infection events. Events created after this date and time appear on the report.
- **Recent Infection Rule** — Specifies a relative time period (for example, **Current Week**) for unresolved infection events. Events created after the time period you specify appear on the report.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Sample report

Figure 3-2 Sample Compliance Issues report



## Compliance Summary report template

Use this report to view a one-page summary of compliance and infection resolution by product. By default, this report uses the same compliance rules you defined for the Compliance Issues report.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (Enter Reports Input dialog box):

- **Recent Infection Date** — Specifies a cutoff date and time for unresolved infection events. Events created after this date and time appear on the report.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## DAT/Definition Deployment Summary report template

Use this report to view the versions of McAfee and Symantec virus definition files that are currently in use on client systems, in a pie chart format. You can also use this report for an overall view of how up-to-date your anti-virus protection is across client systems, and to determine which client systems need to be updated with the most current virus definition files. In addition, you can view historical data for systems using the Tasks, Policies, Update, Infection, and Compliance History subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 59](#).

A variation of this report is included in the predefined settings of the Products By Custom Data Groups report. For more information, see [Products By Custom Data Groups report template on page 44](#).

The versions of virus definition files are grouped into these categories:

- Current or newer.
- One version out-of-date.

- Two versions out-of-date.
- Three versions out-of-date.
- Four versions out-of-date.
- Five or more versions out-of-date.
- Unprotected (no virus definition file present).

**Rules**

Use the McAfee tab (Current Protection Standards dialog box) to define compliance rules for this report. Specify up to five version numbers of McAfee or Symantec virus definition files that meet your compliance requirements. Systems with older versions of virus definition files are reported as non-compliant.

**Within**

You can limit the report results to data recorded within the time period you specify on the **Within** tab (Current Protection Standards dialog box):

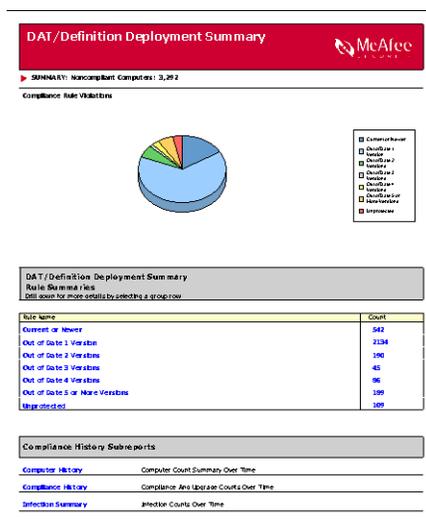
- **Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since the time period you specify appear on the report.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Sample report**

**Figure 3-3 Sample DAT/Definition Deployment Summary report**



## DAT Engine Coverage report template

Use this report to view the versions of McAfee and Symantec virus definition files and virus scanning engines that are currently in use on client systems, in a pie chart format. You can use this report for an overall view of how up-to-date your anti-virus protection is across client systems, and to determine which client systems need to be updated with the most current virus definition files or engine. In addition, you can view historical data for systems using the Tasks, Policies, Update, Infection, and other subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 59](#).

A variation of this report is included in the predefined settings of the Products By Custom Data Groups report. For more information, see [Products By Custom Data Groups report template on page 44](#).

The versions of virus definition files and engines are grouped into these categories:

- Current or newer.
- DAT out-of-date.
- Engine out-of-date.
- Both out-of-date.
- Unprotected (no virus definition file or engine present).

### Rules

Use the McAfee tab (Current Protection Standards dialog box) to define compliance rules for this report. Specify the version numbers of McAfee or Symantec virus definition files or the virus scanning engine that meet your compliance requirements. Systems with older versions of virus definition files or engines are reported as non-compliant.

### Within

You can limit the report results to data recorded within the time period you specify on the Within tab (Current Protection Standards dialog box):

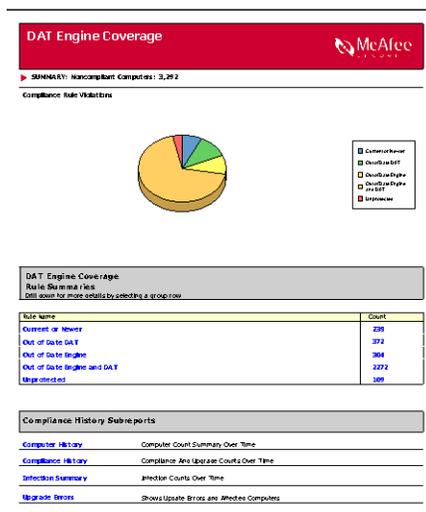
- **Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Agent Connection Rule** — Specifies a relative time period (for example, Current Week) for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since the time period you specify appear on the report.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

Sample report

Figure 3-4 Sample DAT Engine Coverage report



Engine Deployment Summary report template

Use this report to view the versions of McAfee and Symantec virus scanning engines that are currently in use on client systems, in a pie chart format. You can use this report for an overall view of how up-to-date your anti-virus protection is across client systems, and to determine which client systems need to be updated with the most current engine. In addition, you can view historical data for systems using the Tasks, Policies, Update, Infection, and other subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 59](#).

A variation of this report is included in the predefined settings of the Products By Custom Data Groups report. For more information, see [Products By Custom Data Groups report template on page 44](#).

The versions of the virus scanning engine are grouped into these categories:

- Current or newer.
- One version out-of-date.
- Two versions out-of-date.
- Three or more versions out-of-date.
- Unprotected (no engine present).

Rules

Use the McAfee tab (Current Protection Standards dialog box) to define compliance rules for this report. Specify up to three version numbers of the McAfee or Symantec engine that meet your compliance requirements. Systems with older versions of engines installed on them are reported as non-compliant.

Within

You can limit the report results to data recorded within the time period you specify on the Within tab (Current Protection Standards dialog box):

- **Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) for agent communication. Data for systems with agents that have not communicated with the ePolicy Orchestrator server since the time period you specify appear on the report.

#### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

### Active Directory Links report template

Use this report to view the links between your ePolicy Orchestrator Directory sites and your Active Directory containers. This report displays the ePolicy Orchestrator Directory segment, the container to which it is linked in Active Directory, the time the LDAP server was last updated, and any exceptions that are associated with the link.

#### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

### Product Protection Summary report template

Use this report to compare product version numbers for McAfee products, Norton AntiVirus products, all versions of non-compliant anti-virus products, and systems without any anti-virus protection software or an agent, in a stacked column chart format. In addition to systems without any anti-virus protection software, client systems that are using anti-virus products that the software does not currently support (for example, Trend OfficeScan) are reported in this report as if no anti-virus protection software were present.

This report lists the product versions and service pack or patch applied. This data is provided for all managed products that report this data via the agent.

A variation of this report is included in the predefined settings of the Products By Custom Data Groups report. For more information, see [Products By Custom Data Groups report template on page 44](#).

#### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

### Products By Custom Data Groups report template

Use this report to define custom settings for coverage reports, then save them for future use.

#### Group by

You can specify how data is grouped on this report on the **Data Groupings** tab (Enter **Reports Input** dialog box). You can group data in up to four different levels.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (**Enter Reports Input** dialog box):

- **Agent Connection Date** — Specifies a cutoff date and time for agent communication. Systems that have communicated with the server after this date are categorized as current; those that haven't communicated since this date are categorized as late.
- **Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) for agent communication. Systems that have communicated with the server after this date are categorized as current; those that haven't communicated since this date are categorized as late. This rule is saved as the default the next time the report runs.
- **Connection Status** — Specifies whether to include data for all systems, current systems only, or late systems only.
- **Product Type** — Specifies the type of products to include on the report. You can select the agent only, all products, anti-virus products only, or security products only. This rule is saved as the default the next time the report runs.

### Saved Settings

You can save the selections you make in the **Enter Report Inputs** dialog box for future use. The next time that you run that report, you can apply the report input settings that you saved, then change or delete them as needed.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Product Updates By Custom Event Groups report template

Use this report to define custom settings for reports on product updates, then save them for future use. You can use these reports to focus on product updates, update history and distributed software repositories.

### Group by

You can specify how data is grouped on this report on the **Data Groupings** tab (**Enter Reports Input** dialog box). You can group data in up to four different levels.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (**Enter Reports Input** dialog box):

- **Product Upgrade Date** — Specifies a cutoff date and time for product update events. Events created after this date and time appear on the report.
- **Product Upgrade Rule** — Specifies a relative time period (for example, **Current Week**) for product update events. Events created after the time period you specify appear on the report.

### Saved Settings

You can save the selections you make in the **Enter Report Inputs** dialog box for future use. The next time that you run that report, you can apply the report input settings that you saved, then change or delete them as needed.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Infection report templates

The anti-virus infection report templates are divided among three categories: Action Summaries, Detections, Top Tens, and WebShield.

### Action Summary By Top 10 Files Resolved report

Use this report to view the ten most frequently infected files that have been successfully resolved by the scanning engine. Data is grouped by file name, action taken, and infection name.

**Witin**

You can limit the report results to data recorded within the time period you specify on the **Within** tab (**Enter Reports Input** dialog box):

- **Event Date** — Specifies a cutoff date and time for product update events. Events created after this date and time appear on the report.
- **Event Rule** — Specifies a relative time period (for example, **Current Week**) for product update events. Events created after the time period you specify appear on the report.
- **Layout** — Specifies drilldown and printing properties.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

### Action Summary By Top 10 Files Unresolved report

Use this report to view the ten most frequently infected files that have been resolved unsuccessfully by the scanning engine. Data is grouped by file name, action taken, and infection name.

**Within**

You can limit the report results to data recorded within the time period you specify on the **Within** tab (**Enter Reports Input** dialog box):

- **Event Date** — Specifies a cutoff date and time for product update events. Events created after this date and time appear on the report.
- **Event Rule** — Specifies a relative time period (for example, **Current Week**) for product update events. Events created after the time period you specify appear on the report.
- **Layout** — Specifies drilldown and printing properties.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Action Summary By Top 10 Viruses report

Use this report to view the actions performed on the ten most frequently detected viruses, in a stacked bar chart format. It provides an indication of the most common viruses that are being detected by your organization, and the actions that were performed to prevent them from infecting your organization. Data is grouped by infection name, action taken, and product version number.

A variation of this report is included in the predefined settings of the Infections By Custom Data Groups report. For more information, see [Infections By Custom Data Groups report template on page 48](#).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Action Summary report template

Use this report to view the actions performed when viruses were detected by supported anti-virus protection products, in a pie chart format. It provides a good overall view of the detection activity across your organization, and can indicate the effectiveness of your current anti-virus setup. Data is grouped by infection name, action taken, and product version number.

A variation of this report is included in the predefined settings of the Infections By Custom Data Groups report. For more information, see [Infections By Custom Data Groups report template on page 48](#).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Infection History report template

Use this report for a complete view of virus infection activity over time, and to see the relationship between virus infections, action taken, users, and files.

You can view report details on year, month, week, and day. The details sections for year, month, and week shows the same information as the main report section. The details section for day shows the date and time that the virus infection was detected, user name, engine version number, virus definition file version number, virus name, action taken, and the name and location of the infected file.

You can click the virus name to access the AVERT web site for a description of that virus.

A variation of this report is included in the predefined settings of the Infections By Custom Data Groups report. For more information, see [Infections By Custom Data Groups report template on page 48](#).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Infections By Custom Data Groups report template

Use this report to define custom settings for infection reports and save them for future use. Use these reports to focus on infection events and service events (for example, starting or stopping software) events.

### Group by

You can specify how data is grouped and summarized on this report on the **Data Groupings** tab (**Enter Reports Input** dialog box). You can group data in up to four different levels.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (**Enter Reports Input** dialog box):

- **Event Date** — Shows only events occurring after the listed date.
- **Event Rule** — Shows only events occurring after the listed date.
- **Event Type** — Allows you to specify the type of event to retrieve:
  - **All** — Shows all events; both infections and operational.
  - **Infections**
  - **Infection-cleaned**
  - **Infection-deleted**
  - **Infection-moved**
  - **Infection-Unresolved** (for example, clean error, move error, etc.)
  - **Non Infection**
  - **Buffer overflow** — For VirusScan Enterprise 8.0i only.
  - **Unwanted programs** — For VirusScan Enterprise 8.0i only.

### Saved Settings

You can save the selections you make in the **Enter Report Inputs** dialog box for future use. The next time that you run that report, you can apply the report input settings that you saved, then change or delete them as needed.

A number of predefined settings are provided for you:

- **Action summary for last 4 weeks** — Provides the same data as the Action Summary report, but provides data over the past four weeks.
- **Events by severity - all events** — Lists event descriptions by severity.
- **Events by severity - noninfection events** — Lists non-infection operational event descriptions by severity.
- **Infection History** — Provides the same data as the Infection History report. It is provided here as a base for you to customize as desired.
- **Infections by Task Type** — Provides an infection summary by scan task type.
- **Infections over last 24 hours** — Provides the same data as the Number Of Infections For the Past 24 Hours report. It is provided here as a base for you to customize as desired.

- **Monthly infections by product** — This report replaces the Number Of Infections Detected Monthly report from previous versions of the software, but groups data by product name. Use this report to view detected infections for each calendar month. It allows you to compare monthly infection levels.
- **Monthly infections by virus name** — This report replaces the Number Of Infections Detected Monthly report from previous versions of the software, but groups data by virus name. Use this report to view detected infections for each calendar month. It allows you to compare monthly infection levels.
- **Virus actions over last 4 weeks** — This report replaces the Action Summary for Current Month report from previous versions of the software, but provides data over the previous four weeks. Use this report to view all actions performed over the previous four weeks by anti-virus products when viruses were detected. It provides a good overall view of the detection activity across your organization.
- **Viruses found over last 7 days** — Provides the same data as the Viruses Detected report, but provides data on all detected viruses over the last seven days.
- **Weekly infections by product over last 4 weeks** — This report replaces the Infections Detected By Product For The Last 4 Weeks report from previous versions of the software. Use this report to view detected infections by anti-virus product over the past 28 days. It allows you to compare the anti-virus products across your organization, and identify common entry methods (for example, e-mail messages or removable media) for viruses.
- **Weekly infections by virusname** — This report replaces the Infections Detected By Product For The Last 4 Weeks report from previous versions of the software, but groups data by virus name. Use this report to view detected infections by anti-virus product over the past 28 days. It allows you to compare the anti-virus products across your organization, and identify common entry methods (for example, e-mail messages or floppy disks) for viruses.

#### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

### Number Of Infections Detected By Product For Current Quarter (3D Bars) report template

Use this report to view a three-dimensional bar chart of the detected infections for each of the anti-virus products on your systems for the current quarter. It allows you to compare the detection levels of the anti-virus products over the three months.

The current quarter is measured as the current calendar quarter, and not as a fixed number of days from the time that the report is generated. Therefore, generating this report in the first month of a quarter only shows information for that month. The quarters are January–March, April–June, July–September, October–December.

Drill down within a product to view virus counts by product name followed by virus name, then the detailed list of occurrences for that product and virus.

#### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Number Of Infections Detected Monthly Showing Viruses report template

Use this report to view the detected infections for each month, with a breakdown of the individual levels for each virus. It allows you to view the monthly infection levels, with extra details on the individual viruses.

The months are measured as calendar months, not as a fixed number of days from the time that the report is generated.

Drill down within a virus name to view virus counts by product version, followed by Product Version, then the detailed list of occurrences for that month, product, and virus.

A variation of this report is included in the predefined settings of the Infections By Custom Data Groups report. For more information, see [Infections By Custom Data Groups report template on page 48](#).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Number Of Infections For the Past 24 Hours report template

Use this report to view the detected infections in the last 24 hours, with a breakdown of the individual levels for each product. Data is grouped by product version number.

A variation of this report is included in the predefined settings of the Infections By Custom Data Groups report. For more information, see [Infections By Custom Data Groups report template on page 48](#).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Outbreaks — Weekly History report template

Use this report to view historical data on detected infections within an outbreak for each week in a quarter, in a three-dimensional bar chart format.

The report allows the user to enter an outbreak definition. An historic outbreak is defined as occurring over at least a minimum number of distinct systems or distinct files infected within the timeframe of a week.

### Outbreak Rules

You can define an outbreak as a situation where a specified number of systems or files are infected:

- **Minimum Machines Infected** — Specify the minimum number of infected machines for a situation to be considered an outbreak.
- **Minimum Files Infected** — Specify the minimum number of infected files for a situation to be considered an outbreak.

### Saved Settings

You can save the selections you make in the **Enter Report Inputs** dialog box for future use. The next time that you run that report, you can apply the report input settings that you saved, then change or delete them as needed.

A number of predefined settings are provided:

- **Open** — Opens a set of input settings saved previously.
- **Save** — Saves the current input settings to an existing name.
- **Save As** — Saves the current input settings to a user-specified name.
- **Delete** — Deletes a set of input settings saved previously.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Outbreaks — Current report template

Use this report to view detected infections within an outbreak, in a three-dimensional bar chart format.

This report defines outbreaks within a shorter time span than a week. It is designed to show outbreaks that have occurred recently over a narrower time span than the weekly outbreak history report. An outbreak can be defined in terms of hours. A current outbreak is defined as occurring over a minimum number of distinct system (x) or distinct files (y) infected within a timeframe specified in hours (z). In others words, an outbreak is said to have occurred if x distinct systems or y distinct files have been infected by the same virus within z hours.

### Outbreak Rules

You can define an outbreak as a situation where a specified number of systems or files are infected:

- **Minimum Machines Infected** — Specify the minimum number of infected systems for a situation to be considered an outbreak.
- **Minimum Files Infected** — Specify the minimum number of infected files for a situation to be considered an outbreak.
- **Hour Range** — Specify the maximum number hours over which infections occur to be considered an outbreak.

### Saved Settings

You can save the selections you make in the **Enter Report Inputs** dialog box for future use. The next time that you run that report, you can apply the report input settings that you saved, then change or delete them as needed.

A number of predefined settings are provided:

- **Open** — Opens a set of input settings saved previously.
- **Save** — Saves the current input settings to an existing name.
- **Save As** — Saves the current input settings to a user-specified name.
- **Delete** — Deletes a set of input settings saved previously.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (Enter Reports Input dialog box):

- **Start Date** — Specify the date after which to search for outbreaks.
- **Outbreak Start Date Rule** — Shows outbreaks having occurred within a selected number of past weeks or months, up to one year.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Product Events By Severity report template

Use this report to view events by severity. Data is grouped by severity and event description.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Number Of Infections From Removable Media report template

Use this report to view a pie chart of the number of detected viruses from a removable media source such as a floppy drive. Specify the drive letter (default is a:), the report number then shows the number coming from that drive versus those from other sources.

Use this report to also show infections of specific types of files. The input dialog box allows you to enter any file name substring and it searches for infections on the matching files.

Drill down within a rule number to view the detailed list of occurrences for that given media type.

### Media Rules

Use these parameters to scan infected files for an input string. These are used to identify viruses infecting a removable drive and to search for infections of specific file types:

- **Filename string** — Specify the removable drive letter or file name substring.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Security Summary report template

Use this report to view a one-page summary of detections by McAfee anti-virus products, intrusions detected by McAfee Desktop Firewall, and security vulnerabilities reported by McAfee ThreatScan.

**Within**

Selects how data returned by the server is limited:

- **Recent Infection Date** — Specify a date and time after which infections are considered recent.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Virus Type report template**

Use this report to see what types of viruses have infected the enterprise. This report shows the number of virus infections by virus type, in pie chart format.

You can view report details by virus type, virus subtype, and virus name.

For definitions of virus types (for example, trojan horse), see the Virus Glossary on the AVERT web site:

<http://www.mcafee.com/na/common/avert/avert-research-center/virus-glossary.asp#m>

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Viruses Detected report template**

Use this report to view the number of virus infections for the top ten viruses by year, in a stacked bar chart format. You can view details on virus name, quarter, month, week, and day.

You can click the AVERT link next to each virus name to access the AVERT web site for a description of that virus.

A variation of this report is included in the predefined settings of the Infections By Custom Data Groups report. For more information, see [Infections By Custom Data Groups report template on page 48](#).

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Top 10 Detected Viruses report template**

Use this report to view a pie chart of the ten most detected viruses. The segment sizes are proportional to how often the viruses were detected. It allows you to identify the most common viruses that are being detected by your organization.

Drill down within a virus name to view virus counts by product version, then the detailed list of occurrences for that product and virus.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Top 10 Infected Files report template

Use this report to view the ten most infected files, in pie chart format. It allows you to identify the most common infected files that are being accessed by your organization.

Drill down within files to view counts by virus name, product name, and product version number, then the detailed list of occurrences for that file, product, and virus.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (Enter Reports Input dialog box):

- **Event Date** — Specifies a cutoff date and time for product update events. Events created after this date and time appear on the report.
- **Event Rule** — Specifies a relative time period (for example, **Current Week**) for product update events. Events created after the time period you specify appear on the report.
- **Layout** — Specifies drilldown and printing properties.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Top 10 Infected Machines report template

Use this report to view the ten most infected client systems, in pie chart format. It allows you to identify the most common systems within your organization that are attempting to access infected files. You may want to investigate how the systems are being used and the external information sources that are being accessed (possible sources for the infections).

Drill down within systems to view counts by virus name and computer name, then the detailed list of occurrences for that system, product, and virus.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (Enter Reports Input dialog box):

- **Event Date** — Specifies a cutoff date and time for product update events. Events created after this date and time appear on the report.
- **Event Rule** — Specifies a relative time period (for example, **Current Week**) for product update events. Events created after the time period you specify appear on the report.
- **Layout** — Specifies drilldown and printing properties.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Top 10 Infected Users report template

Use this report to view the ten most infected users, in pie chart format. It allows you to identify the most common users within your organization who are attempting to access infected files. You may want to investigate how they are using their systems and the external information sources that they are accessing (possible sources for the infections).

Drill down within users to view counts by virus name and user name, then the detailed list of occurrences for that user, product, and virus.

### Within

You can limit the report results to data recorded within the time period you specify on the **Within** tab (Enter Reports Input dialog box):

- **Event Date** — Specifies a cutoff date and time for product update events. Events created after this date and time appear on the report.
- **Event Rule** — Specifies a relative time period (for example, **Current Week**) for product update events. Events created after the time period you specify appear on the report.
- **Layout** — Specifies drilldown and printing properties.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Content Filter Report By Rule template

Use this report to view the number of times each content rule was initiated for the quarter, in pie chart format.

You can view report details by month, week, and day. The details section of this report shows the event date and time, WebShield appliance name (WebShield), WebShield appliance IP address, blocked spam addresses (User Name), action taken, and portion of the e-mail message that contained the offending content (Message Part).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Content Filter Report By Rule And Time template

Use this report to view the number of times each content rule was initiated over the quarter, in a line chart format. You can view report details by month, week, and day.

The details section of this report shows the event date and time, WebShield appliance name (WebShield), WebShield appliance IP address, blocked spam addresses (User Name), action taken, and portion of the e-mail message that contained the offending content (Message Part).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Content Filter Report Rules Triggered template

Use this report to view the number of times individual users initiated a content rule by month, in a stacked bar chart format.

You can view report details by system name, month, week, and content rule. The details section of this report shows the event date and time, WebShield appliance IP address, blocked spam addresses (User Name), action taken, and portion of the e-mail message that contained the offending content (Message Part).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Content Scanning Detections By Appliance report template

Use this report to view the number of broken content rules by WebShield appliance for the current quarter, in a bar chart format.

You can view report details by broken content rule. The details section of this report shows the event date and time, portion of the e-mail message that contained the offending content (Affected Area), and e-mail address of the sender (User Name).

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Infection History report template (WebShield)

Use this report for a complete view of virus infection activity over time, and to see the relationship between virus infections, action taken, users, and files. You can view report details by year, month, week, and day.

The main section of this report shows the following information:

- Number of virus infections by year (bar chart at the top of page 1).
- Top ten virus infections and the corresponding action taken (stacked bar chart at the bottom of page 1 on the left side).
- Top ten users and the viruses that infected them (stacked bar chart at the bottom of page 1 on the right side).
- Number of times each type of action taken was made (bar chart on the left side of page 2).
- Top ten files and the action taken on them (stacked bar chart on the right side of page 2).

The details section shows the event date and time, e-mail address or IP address of the user responsible for initiating the event (User Name), scanning engine version number, virus definition (DAT) file version number, virus name, action taken, and portion of the e-mail message that contained the offending content or name of the infected file (File Name).

You can click the virus name to access the AVERT web site for a description of that virus.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Spam Detections By Appliance report template**

Use this report to view the number of broken spam rules by WebShield appliance for the current quarter, in a bar chart format.

The details section of this report shows the event date and time, spam rule name, IP address of the spam source, and e-mail address of the sender (User Name).

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Top Ten Spammers report template**

Use this report to view the number of broken spam rules by the top ten users for the current quarter, in a bar chart format.

The details section of this report shows the event date and time, spam rule name, IP address of the spam source, and e-mail address of the sender (User Name).

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**URLs Blocked report template**

Use this report to view the number of blocked Uniform Resource Locators (URL) by WebShield appliance for the year, in a stacked bar chart format. You can view report details by quarter, month, week, and day.

The details section of this report shows the event date and time, WebShield appliance IP address (IP Address), IP address of the source that initiated the event (Offending IP), action taken, and the URL that initiated the event (Blocked URL).

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Virus Detections By Appliance report template**

Use this report to view the number of detected virus infections by WebShield appliance, in a pie chart format. You can view report details on virus name.

The details section of this report shows the event date and time, e-mail address of sender or IP address of source that initiated the event (User Name), scanning engine version number, virus definition (DAT) file version number, action taken, and name of the infected file.

You can click a virus name to access the AVERT web site for a description and other information about that virus.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Virus Detections Timing report template**

Use this report to view the number of detected virus infections by the hour for the year, in a bar chart format. Use this report to determine if virus infections are concentrated during a specific time of day.

The details section of this report shows the event date and time, user name, scanning engine version number, virus definition (DAT) file version number, virus name, action taken, and name of the infected file.

You can click a virus name to access the AVERT web site for a description and other information about that virus.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Virus Type report template (WebShield)**

Use this report to view the number of virus infections by virus type, in a bar chart format. You can view report details on virus type, virus subtype, virus name, and product name. Use this report to see what types of viruses have infected the enterprise.

The details section of this report shows the event date and time, name of the WebShield Appliance item in the **Directory** and – if a report filter has been applied – group name in the **Directory** (Computer Name/Group), WebShield appliance IP address, virus definition (DAT) file version number, scanning engine version number, action taken, and name of the infected file.

For definitions of virus types (for example, Trojan horse), see the Virus Glossary on the AVERT web site:

<http://www.mcafee2b.com/naicommon/avert/avert-research-center/virus-glossary.asp#m>

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

**Viruses Detected report template (WebShield)**

Use this report to view the number of virus infections for the top ten viruses by year, in a stacked bar chart format. You can view report details on virus name, quarter, month, week, and day.

The details section of this report shows the event date and time, WebShield appliance name (Computer Name), virus definition (DAT) file version number, scanning engine version number, action taken, and name of the infected file.

You can click each virus name to access the AVERT web site for a description and other information about that virus.

**Limit report results**

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

---

## Anti-Virus Coverage and Infection subreports

Most coverage reports and several infection reports include links to subreports that provide historical data on systems, compliance, upgrades, and infections and detailed data on policies, tasks, updates, and infections.

**Computer History subreport**

Use this subreport to compare compliant versus non-compliant systems over time.

**Compliance History subreport**

Use this subreport to view the percentage of compliant systems over time.

**Infection History subreport**

Use this subreport to view the infection history on client systems.

**Infection Summary subreport**

Use this subreport to compare detected and unresolved infections and to view the number of infected systems over time.

**Policy subreport**

Use this subreport to view the policy settings on client systems.

**Task subreport**

Use this subreport to view the tasks scheduled on client systems.

**Update Errors subreport**

Use this subreport to view client system messages related to updating.

**Upgrade History subreport**

Use this subreport to view the product upgrade history of client systems.

---

## Rogue System Detection report templates

There are four Rogue System Detection report templates provided for your use.

## Rogues Detected by Subnet report template

Use this report to view the number of rogue systems detected per subnet.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Sensor Coverage report template

Use this report to view known monitored subnets and known unmonitored subnets.



This report does not show information regarding any unknown subnets.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Rogue Type Summary

Use this report to view a summary of all rogue systems categorized by rogue type.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

## Rogues Detected by Time report template

Use this report to view the number of rogues systems detected over a period of time.

### Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 14](#).

---

## Intercept report templates

There are seven Intercept report templates provided for your use.

### Intercept Agent Details

Use this report to view the current details (in a column chart format) of the Intercept agents in your environment. Details include:

- Agent machine name
- Version
- Type
- Host IPS state-mode
- Network IPS state-mode

- Firewall state-mode

### Intercept Agent State

Use this report to view the details of the state of the Intercept agents in your environment. The details are represented in two pie charts. Details include:

- Agent IPS status/operating mode
- Firewall status/operating mode

### Intercept Agent Type

Use this report to view the distribution of types of Intercept agents across your environment. The distribution details are represented in a pie chart. Details include:

### Intercept IPS Events Details

Use this report to view historical details of Intercept IPS events. The details are represented in a bar chart. Details include:

- Incident time
- Recording time
- Machine name
- Agent install type
- Signature name
- Reaction
- Operating mode
- Remote IP address
- Process name
- Operating system user

### Intercept Firewall Event Details

Use this report to view historical details of Intercept firewall events. The details are represented in a bar chart. Details include:

- Incident time
- Recording time
- Agent machine name
- Firewall rule name
- Reaction
- Operating mode
- Process name
- Protocol
- Local service

- Remote service
- Local IP address
- Remote IP address

### Top 10 Attacked Machines — IPS

Use this report to view a bar chart of the top 10 attacked machines and their corresponding IPS security event count.

### Top 10 Attacked Machines — Firewall

Use this report to view a bar chart of the top 10 attacked machines and their corresponding firewall event count.

---

## System Compliance Profiler report templates

There are five System Compliance Profiler report templates provided for your use:



For complete information about System Compliance Profiler and reporting, see the System Compliance Profiler documentation.

### Historical Summary by Severity

Use this report to view information about all detected rule violations by severity level over a period of time. This data displays in both a bar chart and summary table.

You can drill down and view more specific:

- Severity details — Provides a list of the groups that contain rule violations for a specific severity level. Also, indicates how many violations each group registered.
- Group details — Provides a list of rules violated within a specific group, and the number of times each rule was violated.
- Rule details — Provides detailed information on a specific rule, indicating which systems violated it, and when.

### Compliance & Non-Compliance Summary

Use this report to view the number of scanned systems that are:

- Compliant with System Compliance Profiler rules.
- Not compliant with one or more rules.
- 'Unknown' (either because they have not run a scan yet, or because they have not run the most recent scan).

This information is displayed in both a pie chart and a summary table.

You can drill down and view more specific data on:

- Non-compliant computers — Provides a list of systems that contributed to the percentage of non-compliant systems.

- Computer details — Provides information on a specific system and a list of groups containing rule violations.
- Group details — Provides information on a specific group and a list of violated rules, the time these were detected, and the associated severity levels.

### Non-compliance by Computer Name

Use this report to view how many rules each non-compliant system violates. The table lists each scanned system's host name and IP address.

You can drill down and view more specific data on:

- Computer summary — Provides system information for a specific system, and a list of the groups that have rule violations.
- Rule violation details — Provides a list of the rules violated within a specific group, as well as when these violations occurred, and at what severity level.

### Non-Compliance Summary by Group

Use this report to view how many violations System Compliance Profiler found for each of your rule groups. The information is presented in both tabular and bar graph formats.

You can drill down and view more specific data on:

- Group details — Provides a list of the rules violated within a specific group, as well as when these violations occurred, and at what severity level.
- Computer summary — Provides a list of systems that violated a specific rule.
- Violation time details — Provides system information for a specific system, and the time when it violated the selected rule.

### Non-Compliance Summary by Severity

Use this report to view how many rule violations System Compliance Profiler found for each rule severity level. The information is presented in both tabular and bar graph formats.

You can drill down to view more specific data on:

- Severity details — Provides a list of groups that contributed to the total number of violations at a specific severity level.
- Group details — Provides a list of the rules violated within a specific group, and a count of how many systems violated each rule.
- Rule details — Provides detailed information on a specific rule, indicating which systems violated it, and their general system information.

---

## Computer query templates

The system queries provide information on the systems in your organization:

- [All Connecting Computers query template on page 64.](#)
- [Hourly ASCII Count query template on page 64.](#)

- [Computers With No Protection query template on page 64.](#)
- [Computers By Language query template on page 64.](#)
- [Computers By OS Type query template on page 64.](#)
- [Computers By Timezone query template on page 64.](#)
- [Computers By ePONode query template on page 65.](#)
- [Count Of All Connecting Computers query template on page 65.](#)
- [OS Summary query template on page 65.](#)

### All Connecting Computers query template

Use this query to view the system properties of all client systems with agents that have connected to the ePolicy Orchestrator server, sorted by system name.

### Hourly ASCII Count query template

Use this query to view connections made during agent-to-server communication intervals (ASCII) by the hour. Use this query to identify throughput bottlenecks.

### Computers With No Protection query template

Use this query to view properties of all systems without any supported anti-virus protection software, sorted by each system's location in the **Directory** (ePONodeName). In addition to systems without any supported anti-virus protection software, client systems that are using anti-virus products that ePolicy Orchestrator does not currently detect (for example, Trend OfficeScan) are reported in this query as if no anti-virus protection software were present.

### Computers By Language query template

Use this query to view properties of all systems, sorted by language and each system's location in the **Directory** (ePONodeName). Because this query provides the locale settings of client systems, you can use it to determine which language version of products to deploy to them.

### Computers By OS Type query template

Use this query to view properties of all systems, sorted by operating system platform, version and type. Because this query provides operating system information of client systems, you can use it to determine whether they meet the minimum requirements for products before you deploy them.

### Computers By Timezone query template

Use this query to view properties of all systems, sorted by time zone and each system's location in the **Directory** (ePONodeName). Because this query identifies the time zone in which client systems are operating, you can use it to determine the best time to schedule tasks and other operations that affect network traffic.

### Computers By ePONode query template

Use this query to view properties of all systems sorted by their location in the Directory (ePONodeName).

### Count Of All Connecting Computers query template

Use this query to view the total number of systems that are connected and whose properties are stored in the ePolicy Orchestrator database.

### OS Summary query template

Use this query to view the number of operating systems installed on client systems. Use with the **Computers by OS Type** query to view outdated software and upgrade requirements.

---

## Events query templates

The event queries provide information on events. These queries are based on events stored in the ePolicy Orchestrator database. McAfee recommends that you configure the alert filter for the database before generating any queries, so that your future queries do not include any surplus information.

- [All Scanning Events query template on page 66.](#)
- [All Scanning Events By ePONode query template on page 66.](#)
- [All Non-Compliance Events on page 66.](#)
- [All Product Update Events query template on page 66.](#)
- [All Replication Failures on page 66.](#)
- [All ePO Server Events on page 66.](#)
- [Count Of All Scanning Events query template on page 66.](#)
- [Count Of All Product Update Events query template on page 66.](#)
- [Count of All Infections query template on page 66.](#)
- [Scanning Event Summary query template on page 66.](#)
- [First Virus Occurrence query template on page 66.](#)
- [Summary of Past Outbreak Events query template on page 67.](#)
- [Upgrade Summary query template on page 67.](#)
- [Upgrade Summary by Date query template on page 67.](#)
- [Server Task Log query template on page 67.](#)
- [All Infections query template on page 67.](#)
- [All Infections By Virus Name query template on page 67.](#)

### All Scanning Events query template

Use this query to view all events generated when files are scanned on client systems, sorted by date and time.

### All Scanning Events By ePONode query template

Use this query to view all events generated when files are scanned on client system, sorted by its location in the Directory (ePONodeName).

### All Non-Compliance Events

Use this query to view all non-compliance events generated by the ePolicy Orchestrator server.

### All Product Update Events query template

Use this query to view all events generated when product updates are installed on client system, sorted by date and time.

### All Replication Failures

Use this query to view all events generated when repository replication fails.

### All ePO Server Events

Use this query to view all events generated by the ePolicy Orchestrator server.

### Count Of All Scanning Events query template

Use this query to view the total number of events generated when files are scanned on client systems.

### Count Of All Product Update Events query template

Use this query to view the total number of events generated when product updates are installed on client system.

### Count of All Infections query template

Use this query to view the total number of events.

### Scanning Event Summary query template

Use this query to view events generated when files are scanned on client systems and their descriptions, sorted by severity. You might find this query helpful to optimize event filtering.

### First Virus Occurrence query template

Use this query to view when and where infections first entered the network.

### Summary of Past Outbreak Events query template

Use this query to view a summary of outbreaks starting from the most recent.

### Upgrade Summary query template

Use this query to view a summary of updating activity including repository name (SITE NAME) and package type (UPGRADE TYPE).

### Upgrade Summary by Date query template

Use this query to view a summary of updating activity by date.

### Server Task Log query template

Use this query to view the server task log.

### All Infections query template

Use this query to view all infection events, sorted by the event date and time.

### All Infections By Virus Name query template

Use this query to view all infection events, sorted by virus name.

---

## Installations query templates

The installation queries provide information on the anti-virus products installed on client systems. These queries are based on the system and product properties stored in the ePolicy Orchestrator database.

- [All AV Installations by Last Contact query template on page 67.](#)
- [All Installations query template on page 67.](#)
- [All Installations By ePONode query template on page 68.](#)
- [Compliance Summary query template on page 68.](#)
- [Count Of All AV Installations query template on page 68.](#)
- [Count Of All Installations query template on page 68.](#)

### All AV Installations by Last Contact query template

Use this query to view all anti-virus product installations and system properties, sorted by the date that agents last communicated with the ePolicy Orchestrator server. You might find this query useful in viewing the properties received during the most recent agent-to-server communication.

### All Installations query template

Use this query to view all installations (anti-virus scanners and support products), sorted by product and each system's location in the Directory (ePONodeName).

### All Installations By ePONode query template

Use this query to view all installations (anti-virus scanners and support products), sorted by each system's location in the **Directory** (ePONodeName) and product.

### Compliance Summary query template

Use this query to view systems without anti-virus protection, unresolved infections, and non-compliant products, etc.

### Count Of All AV Installations query template

Use this query to view the total number of anti-virus product installations.

### Count Of All Installations query template

Use this query to view the total number of product installations.

# Index

## A

- Action summary
  - by top 10 viruses report, [47](#)
- adding
  - custom report templates, [21](#)
  - your own queries, [23](#)
- Agent versions report, [38](#)
- agent-to-server communication interval (See ASCII)
- ASCII (agent-to-server communication interval)
  - connection interval report, [37](#)

## C

- compliance reports
  - Product Protection Summary, [44](#)
- configuring
  - report filter, [8](#)
- creating
  - SQL queries, [19](#)
  - your own SQL query tables, [23](#)

## D

- DAT file
  - deployment summary report, [40](#)
  - engine coverage report, [42](#)

## E

- Engine deployment summary report, [43](#)
- exporting
  - report data to other formats, [18](#)

## F

- filter, for reports, [8](#)

## G

- generating
  - SQL queries, [19](#)
  - your own custom query tables, [23](#)

## N

- number of infections detected

- monthly showing viruses report, [50](#)

## P

- printing a report, [18](#)
- Product Protection Summary report, [44](#)

## Q

- queries, ?? to [19](#)
  - SQL, [19](#)
  - templates, [63](#) to [68](#)
- query results, copy and paste, [19](#)

## R

- release features
  - Product Protection Summary report, [44](#)
- report filter, setting, [8](#)
- reporting
  - options, specifying, [7](#)
- reports
  - about, [4](#)
  - Action Summary By Top 10 Files Resolved, [46](#)
  - exporting data to other formats, [18](#)
  - printing, [18](#)
  - Product Protection Summary, [44](#)
  - regenerating, [18](#)
  - specifying options, [7](#)
  - templates, [46](#) to [68](#)

## S

- SQL
  - queries, generating, [19](#)

## T

- templates
  - report and query, [37](#) to [68](#)
- Top 10 reports
  - detected viruses report, [53](#)
  - infected files bar report, [54](#)
  - infected machines bar report, [54](#)
  - infected users bar report, [55](#)





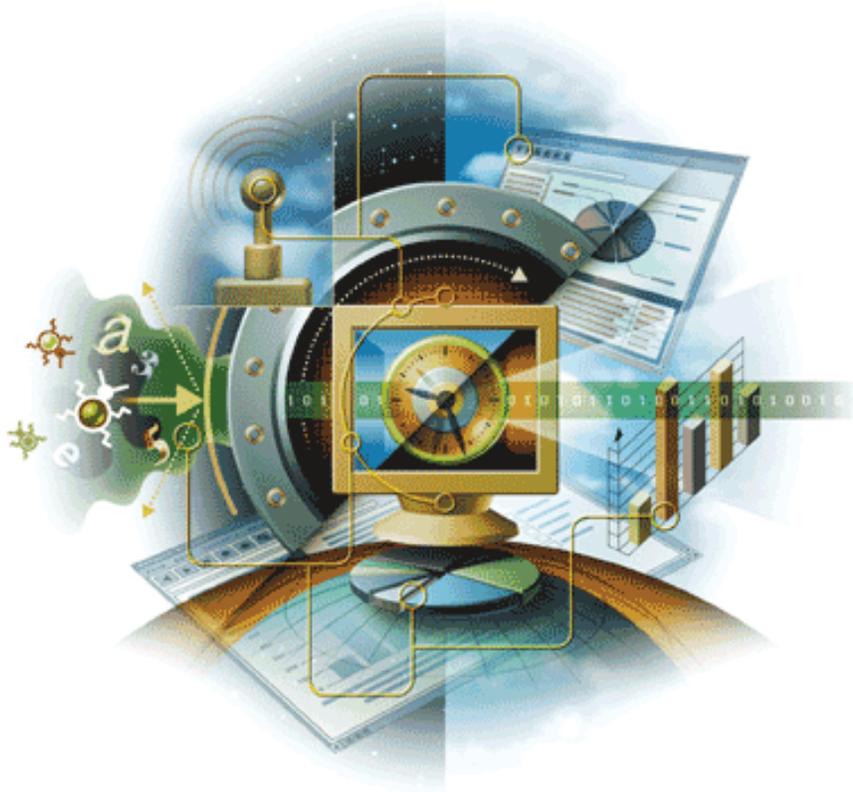
Copyright © 2005 McAfee, Inc. All Rights Reserved.

**McAfee<sup>®</sup>**

[mcafee.com](http://mcafee.com)

# ePolicy Orchestrator®

A product overview and quick set up in a test environment  
version 3.6



## McAfee® System Protection

Industry-leading intrusion prevention solutions

**McAfee®**



# ePolicy Orchestrator®

A product overview and quick set up in a test environment  
version 3.6

**McAfee®**  
System Protection

Industry-leading intrusion prevention solutions

---

**McAfee®**

## COPYRIGHT

Copyright © 2005 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 WEB SITE 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 pro+34vide 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](http://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/Æ Optimizer/Æ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In/Æ Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In/Æ 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](http://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](mailto: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 ([gregor@cs.rpi.edu](mailto:gregor@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](mailto: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](mailto: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.

## PATENT INFORMATION

Protected by US Patents 6,470,384; 6,493,756; 6,496,875; 6,553,377; 6,553,378.

# Contents

## Walkthrough

<b>1</b>	<b>Introduction</b>	<b>6</b>
	Components of ePolicy Orchestrator.....	6
	Policy, properties, and events .....	9
	Policies.....	9
	Properties .....	9
	Events .....	9
	Tasks, services, and accounts.....	10
	Other times when credentials are needed .....	11
	Minimum requirements .....	11
<b>2</b>	<b>Installing or Upgrading the Server</b>	<b>12</b>
	Installing for the first time .....	12
	Pre-installation preparation .....	13
	Information to have during installation .....	13
	Upgrading from a previous version .....	15
	Preparation .....	15
	Information to have during the upgrade .....	16
	Upgrading issues .....	17
<b>3</b>	<b>Organizing the Directory and Repositories</b>	<b>18</b>
	ePolicy Orchestrator Directory: concepts and roles .....	18
	About ePolicy Orchestrator roles.....	19
	Organizing the Directory .....	21
	Environmental borders.....	22
	IP address filters and sorting .....	23
	Repositories.....	25
	Source repository .....	25
	Fallback repository .....	25
	Master repository .....	25
	Distributed repository.....	26
<b>4</b>	<b>Deploying the Agent and Products</b>	<b>28</b>
	ePolicy Orchestrator agent.....	28
	About the ePolicy Orchestrator agent.....	28
	Agent installation folder.....	28
	Agent language packages .....	29
	The agent installation package .....	29
	Agent-server communication .....	31
	SuperAgents and broadcast wakeup calls .....	32
	Agent activity logs .....	34
	Distributing agents .....	34
	Deploying the agent from ePolicy Orchestrator.....	35
	Installing the agent with login scripts.....	37
	Installing the agent manually .....	38
	Enabling the agent on unmanaged McAfee products.....	38
	Including the agent on an image.....	39

	Distributing the agent using other deployment products . . . . .	39
	Distributing the agent to WebShield appliances and Novell NetWare servers 39	
	About deploying packages . . . . .	40
	Package signing and security . . . . .	41
	Legacy product support . . . . .	42
	Package ordering and dependencies . . . . .	42
	About deploying and updating products . . . . .	42
	Product deployment and updating process . . . . .	42
	Deployment task . . . . .	43
	Update tasks . . . . .	43
	Global updating . . . . .	44
	Pull tasks . . . . .	45
	Replication tasks . . . . .	46
	Repository selection . . . . .	46
	Repository selection by agents . . . . .	47
	Selective updating . . . . .	47
	About the SITELIST.XML repository list . . . . .	47
	Checking in product deployment packages manually . . . . .	48
	Configuring the deployment task to install products on client systems . . . .	49
<b>5</b>	<b>Rogue System Detection</b>	<b>52</b>
	The Rogue System sensor . . . . .	52
	Machine status and rogue type . . . . .	55
	Subnet status . . . . .	56
	Distributing Rogue System sensors . . . . .	57
	Deploying Rogue System sensors . . . . .	57
	Installing the sensor manually . . . . .	58
	Taking actions on detected rogue systems manually . . . . .	58
	Configuring automatic responses for specific events . . . . .	59
<b>6</b>	<b>ePolicy Orchestrator Notifications</b>	<b>61</b>
	About Notifications . . . . .	61
	Throttling and aggregation . . . . .	62
	Notification rules and Directory scenarios . . . . .	63
	Determining when events are forwarded . . . . .	64
	Determining which events are forwarded . . . . .	65
	Planning . . . . .	65
	Rules . . . . .	66
	Configuring ePolicy Orchestrator Notifications . . . . .	66
	Default rules . . . . .	66
	Creating rules . . . . .	67
	Viewing the history of Notifications . . . . .	67
	Notification summary . . . . .	68
	Notification list . . . . .	68
	Product and component list . . . . .	70
<b>7</b>	<b>Outbreaks</b>	<b>72</b>
	Tasks to do on a daily or weekly basis to stay prepared . . . . .	72
	Server and client tasks you should schedule to run regularly . . . . .	72
	Checklist — Are you prepared for an outbreak? . . . . .	74
	Other methods to recognize an outbreak . . . . .	74
	Network utilization key indicators . . . . .	74
	E-mail utilization key indicators . . . . .	75
	Virus detection events . . . . .	75
	Checklist — You think an outbreak is occurring . . . . .	75

## Lab Evaluation

<b>8</b>	<b>Installing and setting up</b>	<b>78</b>
	Setting up a lab environment .....	79
	Add systems to your Directory .....	85
	Organize systems into groups for servers and workstations .....	89
	Configure the agent policy settings before deployment .....	91
	Deploy agents .....	92
	Installing agent manually on client systems .....	94
	Add VirusScan Enterprise to the master repository .....	95
	Pull updates from McAfee source repository .....	96
	Create a distributed repository .....	98
	Create a shared folder on the system to use as a repository .....	98
	Add the distributed repository to the ePolicy Orchestrator server .....	99
	Replicate master repository data to distributed repository .....	101
	Configure remote sites to use the distributed repository .....	101
	Schedule a pull task to update master repository daily .....	109
	Schedule a replication task to update your distributed repository .....	110
	Schedule a client update task to update DATs daily .....	110
	Use SuperAgents to wake up all agents on the network .....	111
	Convert an agent on each subnet into a SuperAgent .....	112
	Enable global updating on ePolicy Orchestrator server .....	113
<b>9</b>	<b>Advanced Feature Evaluations</b>	<b>114</b>
	ePolicy Orchestrator Notification .....	114
	Rogue System Detection .....	118



## SECTION 1

# Walkthrough

This section provides a walkthrough of conceptual and best practices information.

---

*Introduction*

*Installing or Upgrading the Server*

*Organizing the Directory and Repositories*

*Deploying the Agent and Products*

*Rogue System Detection*

*ePolicy Orchestrator Notifications*

*Outbreaks*

# 1

## Introduction

ePolicy Orchestrator 3.6 is a powerful tool that allows you to manage security policy, assess and enforce policy, identify and take actions on rogue systems, and notify you of certain events that occur, all across your entire network.

- *Components of ePolicy Orchestrator.*
- *Policy, properties, and events*
- *Tasks, services, and accounts*

---

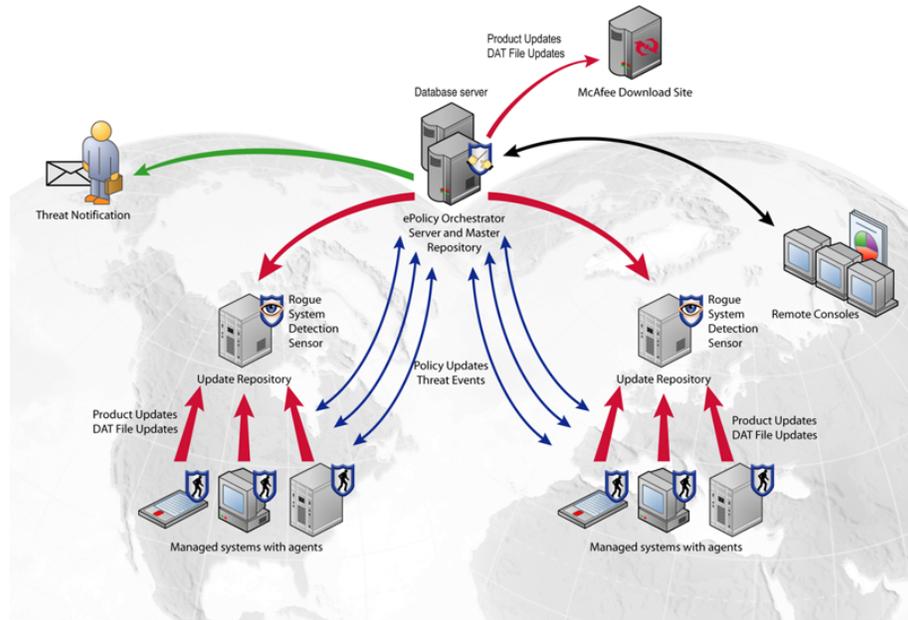
### Components of ePolicy Orchestrator

ePolicy Orchestrator is made up of several components that can reside on systems across your network:

- *ePolicy Orchestrator server.*
- *Database server.*
- *ePolicy Orchestrator consoles.*
- *ePolicy Orchestrator agent.*
- *Rogue System Detection (RSD) sensor.*
- *Master repository.*

- [Update repositories.](#)

**Figure 1-1 ePolicy Orchestrator on your network**



**ePolicy Orchestrator server**

The center of your managed environment. One server can manage up to 250,000 systems, but you may be restricted by your bandwidth and other considerations. For example, network obstacles like firewalls and proxy servers, geographic locations of sites, and security divisions within your organization.

The server:

- Delivers security policies.
- Controls product and DAT file updates.
- Processes events and serves tasks for all managed systems.
- Provides the mechanism for agent communication.
- Controls data access to and from the ePolicy Orchestrator database.

The ePolicy Orchestrator server should be hosted on a dedicated server. Typically, the ePolicy Orchestrator server is accessed via remote ePolicy Orchestrator consoles (installed on other systems), although it can be accessed from a local console as well.

For information on server sizing, see the *ePolicy Orchestrator 3.6 Hardware Sizing and Bandwidth Usage White Paper*.

**Database server**

ePolicy Orchestrator uses a back-end database to store data, which is represented in the console tree of the user interface. The database contains information from each managed system.

The reporting and query features of ePolicy Orchestrator (accessed through the consoles) allow you to view this data in ways you can customize.

### ePolicy Orchestrator consoles

You can have multiple consoles installed on your network. One resides on the ePolicy Orchestrator server itself as a local console, and you can install as many as you like remotely throughout your network.

Typically, you will want one that is accessible to anyone in your environment who needs to access the ePolicy Orchestrator server. For example, you would want all administrators to be able to access the ePolicy Orchestrator server from a console to perform their management tasks. You can assign roles with different rights and permissions to users.

### ePolicy Orchestrator agent

The agent is a vehicle of information and enforcement between the ePolicy Orchestrator and each managed system. For each of the managed systems, the agent:

- Retrieves updates.
- Executes scheduled tasks.
- Enforces policies.
- Forwards properties and events to the server.

Every system you want to manage must have this component installed.

### Rogue System Detection (RSD) sensor

Sensors can reside on one or more systems per subnet. The active sensor notifies you when a rogue system (a system without an ePolicy Orchestrator agent) enters the environment, and can then initiate a user-defined automatic response on that system, such as deploying an agent to it.

Sensors “listen” to all broadcast layer 2 communications on the subnets. Although you can deploy multiple sensors to a subnet, only one is listening at a time. This allows a minimum of network activity, and ensures one sensor is always listening per subnet.

### Master repository

The master repository exists on the ePolicy Orchestrator server and is the central location for all McAfee product updates. The master repository goes to the McAfee Download Site (source repository) at defined times to retrieve all available updates and signatures. The master repository contains a copy of the contents of the McAfee Download Site that can be accessed by the various update repositories in your organization.

### Update repositories

Update repositories are distributed throughout your environment, providing easy access for managed systems to pull DAT files, product updates, and product installations. Depending on how your network is configured, you may want to set up different types of repositories. You can create HTTP, FTP, and UNC share distributed repositories anywhere on your network, or you can create an update repository per subnet by converting an agent on each subnet into a SuperAgent repository.

---

## Policy, properties, and events

Two main purposes of ePolicy Orchestrator are to enforce policies on the managed systems, and to receive and process properties and events from all of the managed systems.

### Policies

A policy is a set of software configurations. The set of options differs depending on the product and system you are managing. For example, a policy for VirusScan Enterprise includes the configuration options for the On-Access Scanner and the On-Demand Scanner. You can set these configuration options differently for different systems.

Policies are the security product configurations that you want to ensure each site, group, or individual systems have. Policies are enforced during the policy enforcement interval. This interval is set to five minutes by default. Therefore, anytime an end user changes the settings on the system, the settings are returned to those set in the policy within five minutes.

New to version 3.6 is the ability to create named policies, that you can assign to independent locations of the Directory.

### Properties

Properties are collected from each system by the installed agent. These include:

- System information (system name, memory available, etc.).
- Information from installed ePolicy Orchestrator-managed security products (for example, VirusScan Enterprise).

### Events

When a threat or compliance issue on a system is recognized by an installed and managed security product, an event file is created by the product that the agent delivers to the server to be processed. These events are processed and stored in the database.

Events are processed by event parser and applied to the notification rules or ePolicy Orchestrator Notifications. Notifications is a feature that allows you to configure rules to alert you to events in your network.

If the event triggers a notification rule, any of the following can happen depending on the rule's configurations:

- Notification messages are sent to specified recipients.
- Actions, such as agent deployment, can be taken against the system.
- Specified registered executables can be launched.

## Tasks, services, and accounts

Several tasks and services of ePolicy Orchestrator require authentication with specific accounts to complete.

This information is useful if you encounter issues with the following tasks.

Task	Service	Account
Logging onto the server	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	ePolicy Orchestrator server account.
Deploying agents	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	Local system account.
Upgrading agents	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	Local system account on client system.
Replicating UNC share distributed repositories	McAfee ePolicy Orchestrator 3.6.0 Application Server (TOMCAT.EXE)	Local system account.
Replicating FTP distributed repositories	McAfee ePolicy Orchestrator 3.6.0 Application Server (TOMCAT.EXE)	Local system account.
Replicating HTTP distributed repositories	McAfee ePolicy Orchestrator 3.6.0 Application Server (TOMCAT.EXE)	Local system account.
Replicating SuperAgent repositories	McAfee Framework Service	ePolicy Orchestrator server account. (Then the local system account installs them.)
Accessing ePolicy Orchestrator Notification	McAfee ePolicy Orchestrator 3.6.0 Application Server (TOMCAT.EXE)	Local system account.
Reporting (with an Authentication Type of ePO Authentication)	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	ePolicy Orchestrator server account. (This account is used to validate the user, then the NT or SQL account is used.)
Reporting (with an Authentication Type of SQL authentication)	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	SQL account.
Reporting (with an Authentication Type of NT Authentication)	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	NT account.
Reporting (with an Authentication Type of Currently logged on user)	McAfee ePolicy Orchestrator 3.6.0 Server (NAIMSRV.DLL)	Account of the currently logged in user. (This account is used to validate the user, then the NT or SQL account is used.)
Parsing events	McAfee ePolicy Orchestrator 3.6.0 Event Parser (EVENTPARSER.EXE)	Local system account.



If the local system account's rights are diminished, installations on client systems of the agent or security products may fail on client systems.

## Other times when credentials are needed

While performing various tasks in ePolicy Orchestrator, you may be required to provide user credentials.

**Table 1-1 Tasks and credentials**

Task	Credentials	Location stored
Logging on to Active Directory containers (set in <b>Active Directory Import</b> wizard)	Active Directory administrator credentials (for each container that is mapped to the ePolicy Orchestrator <b>Directory</b> ). These credentials are stored to run as a task.	If the Active Directory Discovery task is launched manually, it runs as the Microsoft Management Console.  If the task runs as scheduled, it runs as adi.exe using the stored credentials from an encrypted file.
Deploying agents from the ePolicy Orchestrator console by manually specifying the user name and password.	Credentials with administrator rights to the desired systems.	Stored in the encrypted CONSOLE.INI file.

## Minimum requirements

The following are minimum hardware and software requirements for the ePolicy Orchestrator 3.6 server.



These are the minimum requirements. The number of systems you plan to manage as well as network considerations impact the hardware specifications your solution requires. For more information on hardware sizing, see the *ePolicy Orchestrator 3.6 Hardware Sizing and Bandwidth Usage White Paper*.

**Table 1-2 Hardware and software minimum requirements**

Hardware	Software and Network
500MB free disk space (first-time installation); 1GB (upgrade); 2GB recommended.	Windows 2000 Advanced Server with SP 3 or later, Windows 2000 Server with SP 3 or later, Windows Server 2003 Enterprise, Windows Server 2003 Standard, or Windows Server 2003 Web operating systems.
512MB RAM	Microsoft Internet Explorer version 6.0 or later.
Intel Pentium II-class processor or higher; 450MHZ or higher	Trust relationship with the primary domain controller (PDC).
1024x768, 256-color, VGA monitor	User must have administrator rights on the server.
100MHZ or higher NIC	Static IP address recommended
NTFS partition (recommended)	

# 2

## Installing or Upgrading the Server

Whether you are installing ePolicy Orchestrator 3.6 as a new installation or upgrading from prior versions you must understand the minimum system requirements, preparation tasks on your network, and which pieces of information to take to the installation or upgrade.

Information on hardware sizing and bandwidth usage are located in the *Hardware Sizing and Bandwidth Usage White Paper*.

---

### Installing for the first time

Installing or upgrading the ePolicy Orchestrator server is straight forward, using a standard installation wizard. However, before running the installation wizard it is important that you perform certain tasks and have certain pieces of information at hand.



Complete instructions on installing ePolicy Orchestrator are located in the *ePolicy Orchestrator 3.6 Installation Guide*.

This section covers:

- [Pre-installation preparation](#).
- [Information to have during installation](#).

## Pre-installation preparation

Before installing ePolicy Orchestrator 3.6, complete the following tasks:

- Determine what database you are going to use. ePolicy Orchestrator includes the Microsoft SQL Database Engine (MSDE) 2000 (Service Pack 3) database which can be used for all of the reporting and data storage needs. This database has a storage limit of 2GB. This means that a standard installation and configuration of ePolicy Orchestrator 3.6 can record approximately 12 months of data for 10,000 client systems.

If the standard database does not meet your needs, utilize a Microsoft SQL Server 2000 database.



McAfee recommends that a dedicated server is used for the database if you are managing more than 2,000 client systems.

- Update both the ePolicy Orchestrator server system and the ePolicy Orchestrator database server system with the latest Microsoft security updates.
- Install and/or update the anti-virus software on the ePolicy Orchestrator server and database server systems and scan for viruses.
- Install and/or update firewall software on the ePolicy Orchestrator server system. (For example, Desktop Firewall 8.5.)
- Notify the network staff of the ports you intend to use for HTTP communications via ePolicy Orchestrator.

## Information to have during installation

Have the following information with you during installation, some of which may take some careful planning:

- *Server password.*
- *Database server.*
- *Ports you want to use.*
- *E-mail address for Notifications.*

### Server password

During the installation wizard, you are asked to provide a password for the Administrator account to access the ePolicy Orchestrator server. Use a password that is memorable and contains a combination of alpha- and numeric-characters.



Special characters (for example, %, <, >, and &) are not supported in passwords.

### Database server

During the installation wizard, you are asked to select the MSDE 2000 database, or use an already installed database server on the local system or remote (MSDE 2000, or SQL Server 2000).

Consider before installing:

- If you are going to use a database other than the MSDE 2000 provided with ePolicy Orchestrator, you should install the database software before installing ePolicy Orchestrator.
- If you are planning on managing more than 2,000 systems, use a dedicated server with Microsoft SQL Server 2000 with Service Pack 3 for the database.

### Ports you want to use

As ePolicy Orchestrator runs, there is considerable communication between the server and the other components. During the installation wizard, you must designate the ports that the server uses for this communication. Although defaults are provided, we recommend that you consider strongly the ports that you will assign to the different types of communication.

Once ePolicy Orchestrator is installed, you cannot change some of these assignments through the ePolicy Orchestrator console without uninstalling the software.

Make sure that the ports you assign are not already assigned to other products.

- **Agent-to-Server communication port** — This is the port the agent uses to communicate with the server. The default port is **80**. This port cannot be changed after installation.



McAfee strongly recommends that you change this to another port due to potential conflicts in many environments. For example, to **82**.

- **Console-to-Server communication port** — This is the port the console uses to communicate with the server. The default port is **81**. This port can be changed after installation.



McAfee strongly recommends that you change this to another port due to potential conflicts in some environments. For example, to **83**. This port cannot be changed after installation.

- **Agent Wake-Up communication port** — This is the port used to send agent wakeup calls. The default port is **8081**. This port can be changed after installation.
- **Agent Broadcast communication port** — This is the port used to send SuperAgent wakeup calls. The default port is **8082**. This port can be changed after installation.
- **Event Parser-to-Server communication port** — This is the port used by Rogue System Detection and ePolicy Orchestrator Notifications for non-SSL user interface communication and non-SSL sensor communication. The default port is **8080**. This port cannot be changed after installation.
- **Console-to-Application Server communication port** — This is the port used by Rogue System Detection and ePolicy Orchestrator Notifications for SSL user interface communication and SSL sensor communication. The default port is **8443**. This port cannot be changed after installation.
- **Sensor-to-Server communication port** — The port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL. The default port is **8444**. This port cannot be changed after installation.

### E-mail address for Notifications

If you want to use the default rules of the ePolicy Orchestrator Notifications feature, you can provide an e-mail address on the **Set E-mail Address** panel of the installation wizard to which you want to receive notification messages when you enable any of the default rules.

This allows you to use the feature upon implementation, while you are still learning about it.



The e-mail address can be added or changed after installation.

For complete information and procedures to install ePolicy Orchestrator 3.6, see the *ePolicy Orchestrator 3.6 Installation Guide*.

---

## Upgrading from a previous version

You can upgrade or migrate to ePolicy Orchestrator 3.6 if you are currently using:

- ePolicy Orchestrator 3.0.2 or later.
- Protection Pilot 1.0 or later.
- Evaluation versions of ePolicy Orchestrator 3.6.



You cannot upgrade from beta versions of the software.

This section provides information on:

- [Preparation](#).
- [Information to have during the upgrade](#).
- [Upgrading issues](#).

## Preparation

Before upgrading to ePolicy Orchestrator 3.6 complete the following tasks:

- Upgrade the database software if it does not meet the minimum requirements.
- Update both the ePolicy Orchestrator server system and the ePolicy Orchestrator database server system with the latest Microsoft security updates. (Specifically, be sure to install Service Pack 3 on all MSDE and SQL Server 2000 databases.)
- Install and/or update the anti-virus software on the ePolicy Orchestrator server system and scan for viruses.
- Install and/or update firewall software on the server system. (For example, Desktop Firewall 8.5.)
- Notify the network staff of the ports you intend to use for HTTP communications via ePolicy Orchestrator.

## Information to have during the upgrade

Have the following information with you during the upgrade, some of which may take some careful planning:

- [Ports you want to use.](#)
- [E-mail address for Notifications.](#)

### Ports you want to use

As ePolicy Orchestrator runs, there is considerable communication between the server and the other components. During the installation wizard, you must designate the ports that the server uses for this communication. Although defaults are provided, we recommend that you consider strongly the ports that you will assign to the different types of communication.

Once ePolicy Orchestrator is installed, you cannot change some of these assignments through the ePolicy Orchestrator console without uninstalling the software.

Make sure that the ports you assign are not already assigned to other products.

- **Agent-to-Server communication port** — This is the port the agent uses to communicate with the server. The default port is **80**. This port cannot be changed after installation.



McAfee strongly recommends that you change this to another port due to potential conflicts in many environments. For example, to **82**.

- **Console-to-Server communication port** — This is the port the console uses to communicate with the server. The default port is **81**. This port can be changed after installation.



McAfee strongly recommends that you change this to another port due to potential conflicts in some environments. For example, to **83**. This port cannot be changed after installation.

- **Agent Wake-Up communication port** — This is the port used to send agent wakeup calls. The default port is **8081**. This port can be changed after installation.
- **Agent Broadcast communication port** — This is the port used to send SuperAgent wakeup calls. The default port is **8082**. This port can be changed after installation.
- **Event Parser-to-Server communication port** — This is the port used by Rogue System Detection and ePolicy Orchestrator Notifications for non-SSL user interface communication and non-SSL sensor communication. The default port is **8080**. This port cannot be changed after installation.
- **Console-to-Application Server communication port** — This is the port used by Rogue System Detection and ePolicy Orchestrator Notifications for SSL user interface communication and SSL sensor communication. The default port is **8443**. This port cannot be changed after installation.
- **Sensor-to-Server communication port** — The port used by the Rogue System sensor to report host-detected messages to the Rogue System Detection server using SSL. The default port is **8444**. This port cannot be changed after installation.

### E-mail address for Notifications

To use the default rules of the ePolicy Orchestrator Notifications feature, you can provide an e-mail address on the **Set E-mail Address** panel of the installation wizard to which you want to receive notification messages when you enable any of the default rules.

This allows you to use the feature upon implementation, while you are still learning about it.



The e-mail address can be added or changed after installation.

For complete information and procedures to upgrade to ePolicy Orchestrator 3.6, see the *ePolicy Orchestrator 3.6 Installation Guide*.

## Upgrading issues

If your agents are not upgrading to version 3.5 agents, and you're running VirusScan 7.0.0 on those systems, you may need to physically go to these systems and perform the following steps:

- 1 Stop any of the following processes that are running: `NAPRDMGR.EXE`, `FRMWORKSERVICE.EXE`, or `UPDATERUI.EXE`.
- 2 Force uninstall the agent by running `FRMINST.EXE /FORCEUNINSTALL` from the command line. (`FRMINST.EXE` is located in the Common Framework installation directory.)
- 3 Go back to the ePolicy Orchestrator server and deploy an agent to the system.

# 3

## Organizing the Directory and Repositories

The ePolicy Orchestrator software requires you to configure and set up several components. Although extensive, the configurations allow you to customize the product specifically for your environment. Carefully planning the implementation of your ePolicy Orchestrator solution is essential before installing the software.

You should consider how your:

- Directory should be organized.
- The client systems should receive their updates.

This chapter contains the following sections:

- *ePolicy Orchestrator Directory: concepts and roles.*
- *Repositories.*

---

### ePolicy Orchestrator Directory: concepts and roles

The Directory allows you to combine systems into sites and groups. Combining systems with similar properties or requirements allows you to manage policies for these groupings in one place, rather than having to set policies for individual systems. It can also make visually browsing your Directory much easier.

Before discussing Directory organization further, it is important to define some terms:

#### **Directory**

The Directory contains all your managed network systems that you are managing with ePolicy Orchestrator. It is possible to add all the systems to be managed by ePolicy Orchestrator into one site in the Directory. However, this flat unorganized list makes setting specific policies for different systems very difficult. Therefore, organizing the systems in smaller units within the Directory is essential.

#### **Sites**

A site is a first-level group immediately under the Directory root of the console tree. Systems contained within a site can be organized into groups. Sites can contain groups and individual systems.

#### **Groups**

A group is a secondary grouping beneath a site. It can contain more groups (sub-groups) and individual systems, but a group cannot contain a site.

### Lost&Found groups

Lost&Found groups store system names whose locations could not be determined by the ePolicy Orchestrator server. The administrator (with appropriate rights) must move the systems in Lost&Found groups to the appropriate place in the Directory to manage them. Each site has a Lost&Found group, and the Directory has a global Lost&Found group.

### Inheritance

Inheritance is an important property that makes policy administration simpler. Because of inheritance, child nodes in the Directory hierarchy inherit policies that have been set at their parent nodes. For example:

- Policies set at the Directory level are inherited by sites.
- Site policies are inherited by groups and individual systems within that site.
- Group policies are inherited by sub-groups or individual systems within that group.

Inheritance is enabled by default for all sites, groups and individual systems that you add to your Directory. This allows you to set policies and schedule scan tasks in fewer places.

However, inheritance can be turned off at any location of the Directory to allow for customization.



Let inheritance do the work for you. While you can assign security policies and schedule client on-demand scans or DAT file update tasks at any node of the Directory, consider setting policies at the highest-level node possible. If you do, you'll have fewer changes to make. Avoid setting policies at the individual system level if possible.

## About ePolicy Orchestrator roles

If you plan to have multiple people administer ePolicy Orchestrator in your environment, you can create multiple user accounts in the console. Fellow administrators can use these accounts to log onto the server.

The different types of user accounts include:

- [Global administrator](#).
- [Site administrators on page 20](#).
- [Global reviewers on page 21](#).
- [Site reviewers on page 21](#).

### Global administrator

Global administrators have read and write permissions and rights to all operations. When you install the server and console, a global administrator account with the user name `admin` is created.

You can create additional global administrator accounts for other people who need global administrative rights to all aspects of the console.

Global administrators can use the console to deploy agents and security products, change agent or product policies, create and run client tasks for updating DAT files or performing on-demand scans for any node in any site in the Directory. In addition, only global administrators can perform certain server-based functions.

Only global administrators can perform the following repository management functions:

- Define, edit, or remove source and fallback repositories.
- Create, change, or delete global distributed repositories.
- Export or import the repository list from the server.
- Schedule or perform pull tasks to update the Master Repository
- Schedule or perform replication tasks to update distributed repositories
- Check packages into the master repository, move packages between branches, or delete packages from the master repository.

Only global administrators can perform the following server management functions:

- Change server settings and work with server events.
- Schedule Synchronize Domains server tasks.
- Verify the integrity of IP management settings, or change site-level IP subnet masks.
- Add and delete user accounts.
- View and change all options on all tabs in the **Events** dialog box, if using ePolicy Orchestrator authentication.
- Import events into ePolicy Orchestrator databases and limit events that are stored there.
- Create, rename, or delete sites.

## Site administrators

Site administrators have read, write, and delete permissions and rights to all operations (except those restricted to global administrator user accounts) for one or more products, and one or more sites in the Directory.

Site administrators can use the console to deploy agents and security products, change agent or product policies, create and run client tasks for all groups or systems within their sites in the Directory (for products to which they have permissions). Site administrators can also run reports, but the reports show only data on systems located within their sites. The site administrator is able to see, but not change, other sites in the Directory.

### Best practices information

Create site administrator accounts if you have a very decentralized network with no single global administrator account or where different local administrators have local control over their parts of the network. For example, your organization may have sites located in different cities or countries, and these sites may have local IT or network administrators with rights to install and manage software on systems in that part of the network.

You can also create site administrator accounts if you have administrators who you want to only have ePolicy Orchestrator permissions to specific products.

## Global reviewers

Global reviewers can view, but not edit, all settings in the console (except for Rogue System Detection), including property settings, policy, and task settings for all nodes in the Directory. Global reviewers can also run enterprise-wide and site-specific reports.

## Site reviewers

Site reviewers can only view settings and run reports for specified products within specified sites of the Directory.

## Organizing the Directory

The Directory is a hierarchical tree structure that allows you to group your systems within units called *sites* and *groups*. Grouping systems with similar properties or requirements into these units allows you to manage policies for collections of systems in one place, rather than having to set policies for each system separately.

As part of the planning process, consider the best way to divide systems into sites and groups prior to building the Directory.

### Sites

A site is a primary-level unit immediately under the Directory root in the console tree. Traits of sites include:

- Sites can only be created by global administrators.
- A site can include both groups and systems.
- Sites (and their groups and systems) are administered by a global administrator or by a site administrator who has ownership of the specific site. (Site administrators have administrative rights only over the sites to which ownership has been assigned.)
- Each site contains a Lost&Found group; a temporary container for systems for which ePolicy Orchestrator wasn't able to automatically place in the correct location within the site.

### Groups

A group is a secondary-level (or subsequent level) unit of the Directory. Traits of groups include:

- Groups can be created by global administrators, or the site administrator of the site to which the group belongs.
- A group can include both groups and systems.
- Groups are administered by a global administrator or by the site administrator of the site to which the group belongs.
- Groups do not contain a Lost&Found group.

## Lost&Found groups

The Directory root and each site includes a Lost&Found group. Depending on the methods you use to create and maintain Directory segments, the server uses different characteristics to determine where to place systems within the Directory. Lost&Found groups store systems whose locations could not be determined by the server.

### Best practices information

If you delete systems from the Directory, you also need to uninstall the agent from these systems. Otherwise, these systems continue to appear in the Lost&Found group because the agent continues to communicate to the server.

## Environmental borders

How you implement ePolicy Orchestrator and organize the systems for management depends significantly on the borders that exist in your network. Borders influence the organization of the Directory differently than the organization of your network topology.

McAfee recommends evaluating the following borders in your network and organization, and whether they must be taken into consideration when defining the organization of your Directory.

### Topological

Your network is already defined by domains or Active Directory containers. The better organized your network environment, the easier it is to create and use the Directory.

### Geographical

If your organization includes facilities in multiple geographic locations, even on multiple continents, this must be taken into consideration when building your Directory. Available bandwidth and administrative roles must be considered when your organization has multiple locations.

Managing security is a constant balance between protection and performance. Organize your Directory to make the best use of limited network bandwidth. Consider how the server connects to all the parts of your network, especially remote locations that are often connected by slower WAN or VPN connections, instead of faster LAN connections. You may want to set updating and agent-to-server communication policies differently for these remote sites to minimize network traffic over slower WAN or VPN connections.

Grouping systems first by geography provides several advantages for setting policies:

- You can set update policies for the site or group so that all systems update from one or more distributed software repositories located nearby.
- If sites are located in other countries, you can deploy language-specific versions of the agent or security software to these systems at once.
- You can configure the update and product deployment policies for these systems once.
- You can schedule tasks to run at off-peak hours.

## Political

Many large networks are divided because different individuals or groups are responsible for managing various portions of the network. Sometimes these borders do not coincide with the topological or geographical borders. Who you want to access and manage the various segments of the Directory can affect how you structure it.

## Functional

Some networks are divided by the roles of the groups and individuals using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you may need to organize the Directory by functionality if different groups of users require different policies.

Different business groups may run different kinds of software that require special anti-virus or security policies. For example, you may want to arrange your e-mail exchange servers or SQL database servers into a group and set specific exclusions for VirusScan Enterprise on-access scanning.

When planning, focus on the access individuals require or have to the ePolicy Orchestrator server or nodes, and the borders you must accommodate.

## IP address filters and sorting

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. If these organizational units reflect your needs to organize systems for policy management, consider using them to create your Directory structure by setting IP address filters for sites and groups. ePolicy Orchestrator provides tools, such as an IP sorting task that can automatically place systems in the correct site or group according to IP address. This can be a very powerful tool for automatically populating your Directory and making sure systems stay in the intended locations.

If you use IP filters, you must set the IP filtering properties at each level of the Directory properly. Know that:

- To set an IP filter for a group, you must also set IP filters in parent groups or sites.
- The IP ranges specified in lower-level groups must be a subset of the IP range of the parent.
- IP filters cannot overlap between different groups. Each IP range or subnet mask in a given site or group must cover a unique set of IP addresses that cannot be contained in other filter settings in other sites or groups.

After creating groups and setting your IP filters, run an IP integrity check task to make sure your IP filter hierarchy is valid. This task alerts you if there are any conflicts or overlaps between IP filters for different sites or groups.

You can assign IP ranges or IP subnet mask values to sites and groups as you create them, or add or edit them at any time later.

### IP filtering for the first time

When the agent calls into the server for the first time, the system is placed in the Directory location to which it has been assigned. The server searches for the appropriate site whose IP mask or range matches the agent's IP address.

Automatically populating the Directory with this method is the result of an algorithm that uses both IP filters you create and domain information for the NT domain to which the new system belongs.



Be careful if you have sites or groups in your Directory with the same name as NT domains. The domain name search rule takes precedence over the IP group rule.

If you want the system to populate the appropriate location, create the IP group under the site or group associated with the domain, or do not create the domain group under the site.

The server uses the following search algorithm to place systems in the Directory based on the criteria in this order:

**1 Site IP filter** — If a site with a matching IP filter is found, the system is placed in that site based on the criteria in this order:

- a** In a group named the same as the NT domain to which the system belongs.
- b** In a group with a matching IP filter.



If no group match for IP address or domain name is found, the system is placed in the Lost&Found group of the site.

**2 Site Domain name** — If no site is found with a matching IP filter, the server searches for a site with the same name as the NT domain to which the system belongs. If such a site is found, the server searches for a group with a matching IP filter and places the system within. If no group is found, the system is placed in the Lost&Found group of the site.

**3 No site IP filter or domain name match is found** — If the server cannot find an IP or domain name match in any site, the server adds the system to the global Lost&Found.

### Best practices information

This feature is useful when not using ePolicy Orchestrator to deploy agents to systems on your network. If you use another distribution method, the agent is installed on the system before the system is added to the Directory. After the agent installs and calls into the server for the first time, ePolicy Orchestrator adds it to the Directory. If you set IP filters for the sites and groups, the system is added to the appropriate location. Otherwise, it is added to the Lost&Found group and you must move it manually to the appropriate group. Especially in a large network, using IP filters to get the system in the right location can save time.



Automatic IP address sorting does not apply to systems that you add to the Directory using Active Directory integration.

---

## Reposities

Before implementing the ePolicy Orchestrator software, you should decide the type of update repositories to use, and how they should be organized.

### Source repository

The source repository provides all updates for your master repository. The default source repository for clean installations is the McAfee FTP update site (FtpSite), but you can change the source repository or even configure multiple source repositories if you require. McAfee recommends using the McAfee HTTP (HttpSite) or FTP (FTPSite) update sites as your source repository.



You can download updates manually and check them into your master repository. However, using a source repository automates this process.

McAfee posts software updates to these sites regularly. For example, DAT files are posted daily. Update your master repository with updates as they are available.

Use pull tasks to copy source repository contents to the master repository.

The McAfee update sites provide virus definition (DAT) and scanning engine file updates (SCP templates and Spam rules are also available if the corresponding managed products are in the master repository as well). All other packages and updates must be checked into the master repository manually.

### Fallback repository

The fallback repository is a repository from which managed systems can retrieve updates when their usual repositories are not accessible. For example, when network outages or virus outbreaks occur, accessing your established update infrastructure may be difficult. Therefore, managed systems can remain up-to-date in such situations. The default fallback repository is the McAfee HTTP download site (HTTPSite) for clean installations, upgrades keep the designated repository. You can only define one fallback repository.

Source repositories can be used as a fallback repository, but fallback repositories cannot be created manually.

### Master repository

The master software repository maintains the latest versions of security software and updates for your environment. This repository is the source of software and updates for the rest of your environment. There is only one master repository for each ePolicy Orchestrator server.

The master repository is configured when installed. However, you must ensure that proxy server settings are configured correctly. By default, ePolicy Orchestrator uses Microsoft Internet Explorer proxy settings.

## Distributed repository

Distributed repositories host copies of your master repository contents (although you can restrict which files get copied from the master repository to each of the distributed repository). Consider using distributed repositories and placing them throughout your network strategically to ensure managed systems are updated while network traffic is minimized, especially across slow connections.

As you update your master repository, ePolicy Orchestrator replicates the contents to the distributed repositories, instead of to each system.

A large organization can have multiple locations with limited bandwidth connections between them. Distributed repositories limit updating traffic across low-bandwidth connections. If you create a distributed repository in the remote location and configure the systems within the remote location to update from this distributed repository, the updates are copied across the slow connection only once — to the distributed repository — instead of once to each system in the remote location.

### Systems to use for distributed repositories

Use an existing server to host the distributed repository. Although you do not need to use a dedicated server, the server should be large enough for the desired systems to connect for updates. Servers are better than workstations because they are more likely to be running all the time.

### Types of distributed repositories

ePolicy Orchestrator supports four different types of distributed repositories. Consider your environment and needs when determining which type of distributed repository to use. You are not limited to using one type, and may have the need to use several, depending on the nature of your network.

#### SuperAgent repositories

Use systems hosting SuperAgents as distributed repositories. If global updating is enabled, SuperAgent repositories update managed systems automatically as soon as selected updates and packages are checked into the master repository. You do not need to spend additional time creating and configuring repositories or the update tasks.



McAfee recommends using SuperAgent repositories and global updating together to ensure your managed environment is up-to-date.

SuperAgent repositories have several advantages over other types of distributed repositories:

- Folder locations are created automatically on the host system before adding the repository to the repository list.
- File sharing is enabled automatically on the SuperAgent repository folder.
- SuperAgent repositories don't require replication or updating credentials.



Although SuperAgent broadcast wakeup call functionality requires a SuperAgent in each broadcast segment which contains managed systems, this is not a requirement for SuperAgent repository functionality. Managed systems only need to "see" the system hosting the repository.

SuperAgents and global updating use a proprietary protocol, SPIPE.

### FTP repositories

If you are unable to use SuperAgent repositories, you can use an existing FTP server to host a distributed repository. Use your existing FTP server software such as Microsoft Internet Information Services (IIS) to create a new folder and site location for the distributed repository. See your web server documentation for details to create a site.

### HTTP repositories

If you are unable to use SuperAgent repositories, you can use an existing HTTP server to host a distributed repository. Use your existing HTTP server software such as Microsoft Internet Information Services (IIS) to create a new folder and site location for the distributed repository. See your web server documentation for details to create a site.

### UNC share repositories

If you are unable to utilize SuperAgent repositories, create a UNC shared folder to host a distributed repository on an existing server. Be sure to enable sharing across the network for the folder so that the ePolicy Orchestrator server can copy files to it.

### Unmanaged repositories

If you are unable to use managed distributed repositories, ePolicy Orchestrator administrators can create and maintain distributed repositories that are not managed by ePolicy Orchestrator.

If a distributed repository is not managed, a local administrator must keep the repository up-to-date manually.

Once the distributed repository is created, you can use ePolicy Orchestrator to configure managed systems of a specific Directory site or group to update from it.



McAfee recommends that you manage all distributed repositories through ePolicy Orchestrator. Managing distributed repositories with ePolicy Orchestrator and using global updating, or scheduled replication tasks frequently ensures your managed environment is up-to-date. Only use non-managed distributed repositories if your network or organizational policy do not allow managed repositories.

# 4

## Deploying the Agent and Products

Once the ePolicy Orchestrator server and consoles are installed, you must deploy certain core components and security products in order to manage your systems.

---

### ePolicy Orchestrator agent

The agent is the distributed component of ePolicy Orchestrator that must be installed on each system in your network that you want to manage. SuperAgents are agents that have been enabled to distribute broadcast wakeup calls. SuperAgents can also be used as repositories from which to distribute products and product updates.

The agent collects and sends information among the server, update repositories, managed systems, and products. Systems cannot be managed without an installed agent.

Due to the variety of network environments, McAfee provides several methods for you to get the agent on to the systems you want to manage.

### About the ePolicy Orchestrator agent

Consider the following topics when planning to distribute agents:

- [Agent installation folder on page 28.](#)
- [Agent language packages on page 29.](#)
- [The agent installation package on page 29.](#)
- [Agent-server communication on page 31.](#)
- [SuperAgents and broadcast wakeup calls on page 32.](#)

### Agent installation folder

The location of the agent installation folder depends on whether the agent is located on managed systems or the server.

- On the server, the agent is installed in this location:

```
<system_drive>\program files\common files\mcafee\common framework
```

- On the client system, if the agent was installed as part of another product installation or deployed from the console to the system, it is installed by default in this location:

```
<system_drive>\program files\mcafee\common framework
```

- On the client system, if you are upgrading the agent from version 2.5.1, the new agent is also installed after the existing agent is uninstalled, by default in this location:

```
<system_drive>\program files\network associates\common framework
```



Once the agent has been installed, you cannot change its installation directory without first uninstalling it.

## Agent language packages

Agent installation packages, both default and custom, install in English. To use other language versions of the agent on the systems you want to manage, you must check the desired agent language packages into the master repository.

Each agent language package includes only those files needed to display the user interface for that language. Agent language packages can be replicated to distributed repositories.

After the initial ASCII, the agent retrieves the new package that corresponds to the in-use locale and applies it. In this way, the agent retrieves only language packages for the locales being used on each managed system.



The agent software continues to appear in the current language until the new language package has been applied.

Multiple language packages can be stored on managed systems at the same time to allow users to switch between available languages by changing the locale. If a locale is selected for which a language package is not available locally, the agent software appears in English.

Agent language packages are available for these languages:

- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English
- French (Standard)
- German (Standard)
- Italian
- Japanese
- Korean
- Polish
- Spanish (Traditional Sort)
- Swedish

## The agent installation package

The FRAMEPKG.EXE file is created when you install the server. It is a customized installation package for agents that report to your server. The agent installation package contains the server name, its IP address, ASCII port number, and other information that allows the agent to communicate with the server.

By default, the agent installation package is installed in this location:

```
C:\PROGRAM_FILES\MCAFEE\EPO\3.6.0\DB\SOFTWARE\CURRENT\
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

This is the installation package that the ePolicy Orchestrator server uses to deploy agents.

The default agent installation package contains no embedded user credentials. When executed on the system, the installation uses the account of the currently logged-on user.

## Custom agent installation packages

If you use a distribution method other than ePolicy Orchestrator software's own deployment capabilities (such as login scripts or third-party deployment software), you must create a custom agent installation package (FRAMEPKG.EXE) with embedded administrator credentials if users do not have local administrator permissions. The user account credentials you embed are used to install the agent.



Microsoft Windows XP Service Pack 2 and later operating systems do not allow embedded administrator credentials until the package file name has been added to the exception list of the Windows firewall.

To create a custom agent installation package:

- 1 In the console tree, select the server.
- 2 In the details pane, select the **General** tab, then click **Agent Installation Package Creation Wizard**.
- 3 Click **Next**. The **User Credentials** dialog box appears.

**Figure 4-1 Agent Installation Package Creation wizard — User Credentials**

- 4 Type the **User Name** (<DOMAIN>\<USER>) and **Password** you want to embed in the package, then click **Next**.
- 5 On the **Install Directory** dialog box, click **Browse** and select the location to which you want to save the custom agent installation package.

- 6 Click **Next**. The **Create Package** dialog box appears, showing the progress of the creation.
- 7 Click **Next**, then **Finish**.

You can distribute the custom installation package file as needed.

If you plan to deploy the custom installation package with ePolicy Orchestrator, check the package into your master repository.

## Agent-server communication

During agent-server communication, the agent and server exchange information using SPIPE, a proprietary network protocol used by ePolicy Orchestrator for secure network transmissions. At each communication, the agent collects its current system properties and events, then sends them to the server. The server sends any new or changed policies, tasks, and repository list to the agent. The agent then enforces the new policies locally on the managed system.

Agent and server communication can be initiated in three ways:

- [Agent-to-server-communication interval](#).
- [Agent-server communication after agent startup on page 32](#).
- [Wakeup calls on page 32](#).

### Agent-to-server-communication interval

The agent-to-server-communication interval (ASCI) is set on the **General** tab of the **ePO Agent 3.5.0** policy pages. This setting determines how often the agent calls into the server for data exchange and updated instructions. By default, the ASCI is set to 60 minutes. With this setting, the agent checks into the server once every hour. This is a configurable setting on the agent policy pages.

#### Best practices information

When considering whether to leave this policy setting at the default, or to modify it, you must consider your organization's threat response requirements, available bandwidth, and the hardware hosting the server. Be aware that ASCI communication can generate significant network traffic, especially in a large network. In such a case, you probably have agents in remote sites connecting to the server over slower network connections. For these agents, you may want to set a less frequent ASCI. The following table lists general ASCI recommendations for several common network connection speeds.

**Table 4-1 General recommended ASCI settings**

Network Size	Recommended ASCI
Gigabit LAN	60 minutes
100MB LAN	60 minutes
WAN	360 minutes
* Dial-up or RAS	360 minutes
10MB LAN	180 minutes
Wireless LAN	150 minutes
* When you connect to a corporate intranet via dial-up or RAS, the agent communicates to the ePolicy Orchestrator server when the connection is detected.	



For complete information on balancing bandwidth, server hardware, and ASCI, see the *ePolicy Orchestrator 3.6 Hardware Sizing and Bandwidth Usage* white paper.

## Agent-server communication after agent startup

After the installation, or if the agent service is stopped and restarted, the agent calls into the server at a randomized interval within ten minutes. The second and subsequent ASCI after startup occurs with the ASCI set in the agent policy (60 minutes by default).

You can force the agent to communicate to the server immediately after the installation by running the CMDAGENT.EXE with the `/P` command-line option.

## Wakeup calls

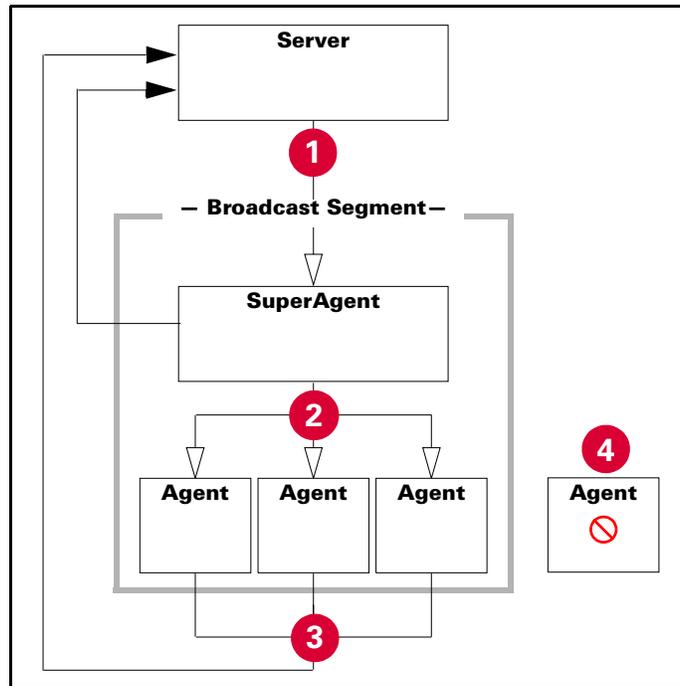
When you send a wakeup call from the server to agents in your environment, the agents are prompted to call into the server. Wakeup calls can be sent manually or scheduled as a task and are useful when you have made policy changes or checked in updates to the master repository that you want to be applied to the managed systems sooner than when the ASCI may occur.

## SuperAgents and broadcast wakeup calls

If you plan to use agent wakeup calls in your network to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent. SuperAgents distribute the agent wakeup call's bandwidth impact, minimizing network traffic. Depending on your network environment, you may find SuperAgent wakeup calls to be a more resource-efficient method of prompting agents to call in, than relying on the server to send wakeup calls to all agents.

Instead of sending agent wakeup calls from the server to every agent, the server sends the SuperAgent wakeup call to SuperAgents in the selected Directory segment. When SuperAgents receive this wakeup call, they send broadcast wakeup calls to all the agents in their network broadcast segments. This reduces network traffic, which is beneficial in large networks where ePolicy Orchestrator may manage agents in remote sites over lower-speed WAN or VPN connections.

**Figure 4-2 Broadcast wakeup calls**



- 1 Server sends a wakeup call to all SuperAgents.
- 2 SuperAgents send a broadcast wakeup call to all agents in the same broadcast segment.
- 3 All agents (regular agents and SuperAgents) exchange data with the server.
- 4 Any agents without an operating SuperAgent on its subnet are not be prompted to communicate with the server.

#### Best practices information

To deploy the right number of SuperAgents to the right locations, first analyze the divisions of broadcast segments in your environment and select a system (preferably a server) to host the SuperAgent. Any agents that do not have a SuperAgent in the local broadcast segment do not receive the broadcast wakeup call. Similar to the regular agent wakeup call, the SuperAgent wakeup call utilizes the SPIPE protocol.

Ensure that the agent wakeup port (8081 by default) is not blocked by your firewall.

## Agent activity logs

The agent log files are useful when determining agent status or troubleshooting problems. There are two log files that record agent activity, both are located in the agent installation folders on the managed system running Windows 95, Windows 98, or Windows NT systems. On managed systems running Windows 2000, Windows 2003, and Windows XP, these files are located in the `Common Framework` folder (within `Documents and Settings`):

- Agent activity log

The agent activity log is an XML file named `AGENT_<SYSTEM>.XML` where `<SYSTEM>` is the NetBIOS name of the system on which the agent is installed. This log file records agent activity related to such things as policy enforcement, agent-to-server communication, and event forwarding. You can define a size limit of this log file.

You can configure the level of logging of agent activity on the **Logging** tab of the **ePO Agent 3.5.0 | Configuration** policy pages.

- Detailed agent activity log

The detailed agent activity log (`AGENT_<SYSTEM>.LOG`) file contains troubleshooting message in addition to the content of the agent activity log. This file has a 1MB size limit. When this log file reaches 1MB, a backup copy is made (`AGENT_<COMPUTER>_BACKUP.LOG`).

## Distributing agents

Due to the variety of scenarios and requirements of different environments, there are several methods you can use to distribute the agent to the systems you want to manage. Before using any of these methods, you should consider each.

The following table details the advantages and disadvantages of the different methods to distribute the agent.

**Table 4-2 Advantages and disadvantages of agent distribution methods**

Method	Advantages	Disadvantages
Deploying agents while creating Directory	By deploying the agent automatically while creating the sites and groups of the Directory, you don't have to complete any additional steps.	If you are creating sites by importing large NT domains or Active Directory containers, too much network traffic may be generated for your network resources.
Deploying agents from ePolicy Orchestrator	This is an efficient method for distributing the agent.	You must embed user credentials with administrator rights to the desired systems. Also, you must ensure that systems running Microsoft XP Service Pack 2, have File and Printer sharing added to the firewall exceptions list.
Using login scripts	This is an efficient method for an environment where systems log onto the network frequently. You do the work once, and the agent is deployed automatically.	Systems that don't log onto the network frequently, may not be running the most up-to-date agent.

**Table 4-2 Advantages and disadvantages of agent distribution methods**

Method	Advantages	Disadvantages
Installing manually	This is an efficient method if you are not using ePolicy Orchestrator to deploy the agent, or if you have many Windows 95 and Windows 98 systems and do not want to enable file and print sharing on them.	This is not a time-efficient method if you have many systems.
Including the agent on an image	Installing the agent as part of an image prevents the bandwidth impact that other forms of distribution can incur. This method also reduces the overhead by integrating the task into another one that must occur.	If you do not use images consistently, this method would not be efficient to ensure coverage.
Enabling the agent on unmanaged McAfee products	Enabling an agent that is already on the client system rather than deploying the 1.5MB package, can save significant bandwidth and time.	The disabled agent may be out-of-date and require you run the deployment task to upgrade the agent to the current release.  You cannot change the agent installation folder without uninstalling and reinstalling the agent — agents that you enable may be located in a different folder than agents that you deploy in your network by some other method.

- [Deploying the agent from ePolicy Orchestrator](#)
- [Installing the agent with login scripts](#)
- [Installing the agent manually](#)
- [Enabling the agent on unmanaged McAfee products](#)
- [Including the agent on an image](#)
- [Distributing the agent using other deployment products](#)
- [Distributing the agent to WebShield appliances and Novell NetWare servers](#)

## Deploying the agent from ePolicy Orchestrator

You can use ePolicy Orchestrator to deploy agents to your systems. This method uses Windows NT push technology.

### When to use this method

This is a desirable method to install agents if you already have large sections of your Directory populated. This is an efficient method if you were able to build Directory segments by importing domains or Active Directory containers.

### Requirements

To use this method, several requirements must be met, including:

- Systems to which you want to deploy the agent must already be added to the Directory.

For information and instruction, see [Chapter 3, Creating a Directory of Managed Systems](#) in the product guide.



If you have not yet created the Directory, you can send the agent installation package to systems at the same time that you are adding sites, groups, and systems to the Directory.

However, McAfee does not recommend this procedure if you are creating your Directory by importing large NT domains or Active Directory containers. This can generate too much network traffic.

- Specify domain administrator credentials.

Domain administrator rights are required to access the default `Admin$` shared folder on the desired systems. The ePolicy Orchestrator server service requires access to this shared folder in order to install agents and other software.

- Verify the ePolicy Orchestrator server can communicate with the desired systems.

Before beginning a large agent deployment, use ping commands to verify that the server can communicate with a few systems in each segment of your network to which you want to deploy agents.

If the targeted systems respond to the ping, then ePolicy Orchestrator can communicate with them.



The ability to successfully use ping commands from the ePolicy Orchestrator to the managed systems is not required for the agent to communicate with the server after the agent is installed. This is only a useful test for determining if you can deploy agents from the server to them.

- Verify that the `Admin$` share folders on the desired systems are accessible from the server.

This test also confirms your administrator credentials, because you cannot access remote `Admin$` shares without administrator rights.

To access `Admin$` shares on desired systems from the ePolicy Orchestrator server:

- a Select **Start | Run**.
- b Type the path to the client `Admin$` share by specifying either the system name or IP address.

If the systems are properly connected over the network, your credentials have sufficient rights, and the `Admin$` shared folder is present, you should see a **Windows Explorer** dialog box.

- Ensure file and print sharing is enabled. (This is disabled by default on Windows 95, Windows 98, and Windows ME systems.)

In addition, if you have systems in your network running these operating systems, you must make sure they can be managed by ePolicy Orchestrator. By default, these systems do not allow ePolicy Orchestrator administration. To enable these systems for ePolicy Orchestrator administration, download `VCREDIST.EXE` and `DCOM 1.3` updates from the Microsoft web site and install them on each client as required.

- Ensure network access is enabled on Windows XP Home systems.

To deploy the agent from the ePolicy Orchestrator console or install a custom agent installation package on systems running Windows XP Home, you must enable network access.

To enable network access on systems running Windows XP Home:

- a** Select **Start | Control Panel**.
- b** Click **Performance and Maintenance**.
- c** Click **Administrative Tools**.
- d** Select **Local Security Policy**. The **Local Security Settings** application window appears.
- e** In the console tree under **Security Settings | Local Policies**, select **Security Options**. The available policies appear in the details pane.
- f** Select **Network access: Sharing and security model for local accounts** to open the **Network access** dialog box.
- g** Select **Classic - local user authenticate as themselves**, then click **OK**. Local users are able to authenticate and access resources on the system from the network.

## Installing the agent with login scripts

Using network login scripts is a very reliable and popular way to make sure that every system logging onto your network is running an agent. You can create a login script to call a batch file that checks if the agent is installed on systems attempting to log onto the network. If no agent is present, the batch file can install the agent before allowing the system to log on. Within ten minutes of being installed, the agent calls into the server for updated policies, and the system is added to the Directory.

### When to use this method

This is a desirable method to use when:

- You assigned IP sorting filters or NT domain names when creating the segments of your Directory.
- You already have a managed environment and you want to ensure that new systems logging onto the network become managed as a result.
- You already have a managed environment and you want to ensure systems are running a current version of the agent.

### Best practices information

McAfee recommends that you first create segments of your Directory that use either network domain names or IP address filters that add the expected systems to the desired sites and groups when the agents call into the server for the first time automatically. If you don't, all systems are added to the Lost&Found group and you must move them later manually.

Especially when distributing agents to systems in a very large network, creating a Directory that uses some automated sorting method *before* installing agents with login script can save valuable time.

The details of the login script used to install the agent can vary, depending on your needs. Consult your operating system documentation for more details on how to write login scripts.

## Installing the agent manually

A simple way to install the agent is to run the installer directly from the desired system.

### When to use this method

This is a desirable method to install agents in the following circumstances:

- Your organization requires that software is installed on systems manually.
- You intend to use ePolicy Orchestrator for policy management only.
- You have systems running Windows 95, Windows 98, or Windows ME and do not want to enable file and print sharing on them.
- You assigned IP sorting filters or NT domain names when creating the segments of your Directory.

You can install the agent on the system, or distribute the FRAMEPKG.EXE installer to users in your organization and have them run the installation program themselves.

After the agent is installed, it calls into the server and adds the new system to the Directory.

Having assigned IP sorting filters or NT domain names to the desired Directory segments saves valuable time.

## Enabling the agent on unmanaged McAfee products

Before purchasing ePolicy Orchestrator, you may have already been using McAfee products in your network. Some of the more recent McAfee products that use the AutoUpdate updater, such as VirusScan Enterprise, install with the agent in a disabled state. When you want to start managing these products with ePolicy Orchestrator, you do not need to install the agent on these systems. Instead, you can simply enable the agent that is already on the system.

Enabling the agent in this way, rather than re-deploying the 1.5MB agent installation package to each system, can save significant network bandwidth when you have many systems with disabled agents on the network.



You cannot change the agent installation folder without uninstalling and reinstalling the agent. Agents that you enable may be in a different folder location than agents that you deploy in your network using another method.

Having assigned IP sorting filters or NT domain names to the desired Directory segments saves valuable time.

You must copy the SITELIST.XML repository list file from the ePolicy Orchestrator server to the desired systems. The repository list contains network address information the agent requires to call into the server after installing.

To enable the agent on unmanaged systems running a McAfee product with a disabled agent:

- 1 Export the repository list (SITELIST.XML) from the ePolicy Orchestrator server and copy it to a temporary folder on the system, such as C:\TEMP
- 2 Run the following command line on the desired system:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

/SITEINFO is the location of the SITELIST.XML file that you exported.

Reference the SITELIST.XML file in the temporary folder. By default, the FRMINST.EXE file is installed in the following location:

```
c:\program files\mcafee\common framework
```



Such products were most likely installed with an older version of the agent. These agents are *not* automatically upgraded to the latest agent version that is on the ePolicy Orchestrator server. To upgrade the agent, you should also enable and run the deployment task to install the new agent on the managed system.

## Including the agent on an image

You can install the ePolicy Orchestrator agent on systems used to create common images for your environment. The first time the user logs into a system built using a common image that includes the agent, the system is assigned a unique ID called a *global unique identifier* (GUID).



Before creating an image for this purpose, remove the agent GUID registry value from the agent registry key. A GUID is regenerated on the first ASCII with the ePolicy Orchestrator server.

### When to use this method

This is a desirable method to use when:

- Your organization uses standard installation images for new systems.
- You may not have access to systems in some portions of your environment except when they are brought in for repair.

For instructions, see the documentation for your preferred image-creation product.

## Distributing the agent using other deployment products

You may already use other network deployment products in your organization to deploy software. You can use many of these tools, such as Microsoft Systems Management Server (SMS), IBM Tivoli, or Novell ZENworks, to deploy agents. Configure your deployment tool of choice to distribute the FRAMEPKG.EXE agent installation package located on your ePolicy Orchestrator server.

For instructions, see the documentation of the desired deployment tool.

## Distributing the agent to WebShield appliances and Novell NetWare servers

You cannot use ePolicy Orchestrator to deploy agents to WebShield appliances or Novell NetWare servers. Instead, use a method such as a login script or manual installation.



These systems require different agents, which can be downloaded from the McAfee web site. These agent installation packages are not installed on the ePolicy Orchestrator server by default.

See your product documentation for specific details.

## About deploying packages

The ePolicy Orchestrator deployment infrastructure supports deploying products and ePolicy Orchestrator components.

Each McAfee product that ePolicy Orchestrator can deploy provides a product deployment package (PKG.CATALOG.Z) file. ePolicy Orchestrator can deploy these packages to any of your managed systems, once they are checked into the master repository. The package catalog file contains the product installation files, which are compressed in a secure format.

PKG.CATALOG.Z files are used for both virus definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. McAfee recommends configuring policy settings before deploying the product to network systems, this can save time and ensure that your systems are protected as desired as soon as possible.

Global administrators can check these package types into the master repository with pull tasks, or manually:

**Table 4-3 Supported packaged types**

Package type	Description	Origination
Virus definition (DAT) files. File type: PKG.CATALOG.Z	The regular, daily DAT files released by McAfee.	FTPSite and HttpSite update sites, and the McAfee web site.  Use a pull task to download DAT files directly into the master repository, or download and check them into the master repository manually.
Scanning engine. File type: PKG.CATALOG.Z	The updated scanning engine for McAfee anti-virus products, such as VirusScan Enterprise. Engines are usually updated once or twice a year.	FTPSite and HttpSite update sites, and the McAfee web site.  Use a pull task to download engine files directly into the master repository, or download and check them into the master repository manually.
SuperDAT (SDAT.EXE) files. File type: SDAT.EXE	The SuperDAT files contain both DAT and engine files in one update package.  If bandwidth is a concern, McAfee recommends updating DAT and engine files separately.	McAfee web site.  Download and check SuperDAT files into the master repository manually.

Table 4-3 Supported packaged types

Package type	Description	Origination
Supplemental virus definition (EXTRA.DAT) files. File type: EXTRA.DAT	The EXTRA.DAT files address one or a few specific viruses that have appeared since the last DAT file was posted. If the threat has a high severity, distribute the EXTRA.DAT immediately, rather than wait until that signature is added to the next DAT file.  EXTRA.DAT files are from the McAfee web site. You can distribute them through ePolicy Orchestrator.  Pull tasks do not retrieve EXTRA.DAT files.	McAfee web site.  Download and check supplemental virus definition files into the master repository manually.
Product deployment packages. File type: PKGCATALOG.Z	A product deployment package contains the installation software of a McAfee product.	Product CD or downloaded product ZIP file.  Check product deployment packages into the master repository manually. For a specific location, see the <i>Configuration Guide</i> for the product.  Only the ePolicy Orchestrator agent and System Compliance Profiler deployment packages are checked into the master repository as part of the ePolicy Orchestrator server installation.
Agent installation package. File type: PKGCATALOG.Z	An agent installation package contains the installation software for the ePolicy Orchestrator agent.	Master repository — checked in at installation.  For future versions of the agent, you must check agent installation packages into the master repository manually.
Agent language packages. File type: PKGCATALOG.Z	An agent language package contains files necessary to display agent information in a local language.	Master repository — checked in at installation.  For future versions of the agent, you must check agent language packages into the master repository manually.

## Package signing and security

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

You are notified when you check in packages that are not signed by McAfee. If you are confident of the content and validity of the package, continue with the check-in. These packages are secured in the same manner described above, but are signed by ePolicy Orchestrator when they are checked in.

Using digital signatures guarantees that packages originated from McAfee or were checked in by you, and that they have not been tampered with or corrupted. The agent only trusts package catalog files signed by ePolicy Orchestrator or McAfee. This protects your network from receiving packages from unsigned or untrusted sources.

## Legacy product support

Older products use a flat directory structure in conjunction with the AutoUpdate and AutoUpgrade client tasks to install product updates. New products that take advantage of AutoUpdate 7.0 use a hierarchal directory structure and the update task to install product updates.

If the update location you specify in the AutoUpdate or AutoUpgrade task settings is a distributed repository managed by ePolicy Orchestrator, you must enable legacy product support when you check the corresponding package into the master repository. Doing so copies the packages into both directory structures, enabling you to support legacy products.

## Package ordering and dependencies

If one product update is dependent on another, you must check their packages into the master repository in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them back in, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.

---

## About deploying and updating products

The ePolicy Orchestrator repository infrastructure allows you to deploy products and update packages to your managed systems from a central location. Although the same repositories are used, there are differences.

**Table 4-4 Comparison of product deployment and update packages**

Product deployment packages	Update packages
Must be manually checked into the master repository.	DAT and engine update packages can be copied from the source repository automatically with a pull task. Most other update packages must be checked into the master repository manually.
Can be replicated to the distributed repositories and installed on managed systems with global updating.	Can be replicated to the distributed repositories and installed on managed systems <i>automatically</i> with global updating.
If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.	If not implementing global updating for product updating, an <i>Update task</i> must be configured and scheduled for managed systems to retrieve the package.

## Product deployment and updating process

The high-level process for distributing DAT and engine update packages follows:

- 1 Check the update package into the master repository with a pull task or manually.

- 2 If using global updating, nothing else is necessary provided global updating has been configured and enabled.  
  
If not using global updating, use a replication task to copy the contents of the master repository to the distributed repositories.
- 3 If not using global updating, create and schedule an update or deployment task for agents to retrieve and install the update on managed systems.

## Deployment task

Once you have checked in the product deployment package, you can use the deployment task to install the product on managed systems. The deployment task is a unique client task created automatically when ePolicy Orchestrator installs. It installs any product that is deployable through ePolicy Orchestrator and has been checked into the master repository.

### Best practices information

You can run the product deployment task at any site, group, or individual system. When deciding how to stage your product deployment, McAfee recommends considering the size of the package and the available bandwidth between the master or distributed repositories and the managed systems. In addition to potentially overwhelming the ePolicy Orchestrator server or your network, deploying products to many systems can make troubleshooting problems complicated.

Consider a phased roll-out to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred client systems at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

If you chose to deploy server-based McAfee products, deploy them to specific systems, rather than groups or sites.

## Update tasks

Once an update package has been checked into the master repository and replicated to the distributed repositories, the agents on the managed systems still need to know when to go to the distributed repositories for updates. This is unnecessary if you are using global updating.

You can create and configure client update tasks to control when and how managed systems receive update packages. If you are not using global updating, creating these client update tasks are the only way you can control client updating with ePolicy Orchestrator.

If you are using global updating, a client update task is unnecessary, although you can create a daily client update task for redundancy.

## Considerations when creating client update tasks

Consider the following when scheduling client update tasks:

- Create a task to update DAT and engine files daily at the highest level of the Directory that is inherited by all systems. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact of all systems updating at the same time. Also, for large networks with offices in different time zones, running the task at the local system time on the managed system, rather than at the same time for all systems, helps balance network load.
- Schedule the update task at least an hour after the scheduled replication task, if you are using scheduled replication tasks.
- Run update tasks for DAT and engine files at least once a day. Managed systems can be logged off from the network and miss the scheduled task; running the task frequently ensures these systems receive the update.
- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one update task to update only DAT files, then create another to update both DAT and engine files weekly or monthly — engine packages are released less frequently.
- Create and schedule additional update tasks for products that do not use the agent for Windows.
- Use the **Run missed task** option. This can be useful if systems are logged off from the network at the scheduled update time, ensuring they update after logging onto the network.

## Global updating

McAfee recommends using global updating with your updating strategy. Global updating automates replication to your distributed repositories and updating managed systems. Replication and update tasks are not required. Checking contents into your master repository initiates a global update. The entire process should complete within an hour in most environments.

Additionally, you can specify which packages and updates initiate a global update. However, when you only specify that certain content initiates a global update, ensure that you create a replication task to distribute content that was not selected to initiate a global update.



When using global updating, McAfee recommends scheduling a regular pull task (to update the master repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, network traffic over the updating time period is increased.

## Global updating process

Global updating updates your environment within an hour in most environments using the following steps:

- 1 Contents are checked into the master repository.
- 2 Contents of the master repository are replicated automatically to the distributed repositories.

- 3 A SuperAgent wakeup call with the SITESTAT.XML file is broadcast to all agents. This file lists the contents of the master repository. If a package the managed systems requires is in the list, the agent goes to a distributed repository to get the package.
- 4 All agents go to their local distributed repositories for new updates.

## Requirements

The following requirements must be met to implement global updating:

- A SuperAgent is installed on each broadcast segment. Managed systems cannot receive a SuperAgent wakeup call if there is no SuperAgent on the same broadcast segment. Global updating utilizes the SuperAgent wakeup call to alert agents that new updates are available.
- Distributed repositories are set up and configured throughout your environment. McAfee recommends SuperAgent repositories, but they are not required — global updating functions with all types of distributed repositories.
- If using SuperAgent repositories, managed systems must be able to “see” the repository from which it updates. Although, a SuperAgent is required on each broadcast segment for systems to receive the wakeup call, SuperAgent repositories are not required on each broadcast segment, but the managed systems must “see” the SuperAgent repository from which to update.

## Pull tasks

Use pull tasks to update your master repository with DAT and engine update packages from the source repository. DAT and engine files must be updated often. McAfee releases new DAT files daily and engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.



EXTRA.DAT files must be checked into the master repository manually. They are available from the McAfee web site.

A scheduled pull task runs automatically and regularly at times and days you specify. For example, you can schedule a daily repository pull task at 5:00 AM.

You can also use the Pull now task to check updates into the master repository immediately. For example, when McAfee alerts you to a fast-spreading virus and releases a new DAT file to protect against it.

If a pull task fails you must check the packages into the master repository manually.

Once you have updated your master repository, you can distribute these updates to your systems automatically with global updating or with replication tasks.

## Considerations when scheduling a pull task

Consider the following when scheduling pull tasks:

- Bandwidth and network usage. If you are using global updating, as recommended, schedule a pull task to run when bandwidth usage by other resources is low. With global updating, the update files are distributed automatically after the pull task completes.
- Frequency of the task. DAT files are released daily, but you may not want to use your resources daily for updating.

- Replication and update tasks. Schedule replication tasks and client update tasks to ensure the update files are distributed throughout your environment.

## Replication tasks

Use replication tasks to copy the contents of the master repository to distributed repositories. Unless you have replicated master repository updates to all your distributed repositories, some systems do not receive them. Ensure all your distributed repositories are up-to-date.



If you are using global updating, replication occurs automatically — replication tasks are not necessary.

Scheduling regular replication tasks is the best way to ensure that your FTP, HTTP, and UNC distributed repositories are up-to-date. Scheduling daily replication tasks ensures that managed systems stay up-to-date.

Creating scheduled replication tasks automates replication to your distributed repositories. Occasionally, you may add files to your master repository that you want to replicate to distributed repositories immediately, rather than wait for the next scheduled replication. Run a Replicate now task to update your distributed repositories manually.



With version 3.6, you can now specify which content gets replicated from the master repository to the distributed repositories (defined by the distributed repository), and specify to which distributed repositories are replicated (defined in the task).

## Full vs. incremental replication

When creating a replication task, select incremental or full replication. Incremental replication uses less bandwidth and copies only the new updates in the master repository that are not yet in the distributed repository. Full replication copies the entire contents of the master repository.



McAfee recommends scheduling a daily incremental replication task and a weekly full replication task. This maximizes network bandwidth efficiency by updating only essential, incremental changes during the week and guarantees completeness.

## Repository selection

New distributed repositories are added to the repository list (SITELIST.XML) file containing all available distributed repositories. The agent of a managed system updates its repository list each time it communicates with the ePolicy Orchestrator server. The agent performs repository selection each time the agent (McAfee Framework Service) service starts and when the repository list changes.

Selective replication provides more control over the updating of individual repositories. When scheduling replication tasks, you can choose:

- Specific distributed repositories to which the task applies. Replicating to different distributed repositories at different times lessens the impact on bandwidth resources. These repositories can be specified when you create or edit the replication task.

- Specific files and signatures that are replicated to the distributed repositories. Selecting only those types of files that are necessary to each system that checks into the distributed repository lessens the impact on bandwidth resources. When you define or edit your distributed repositories, you can choose which packages you want to replicate to the distributed repository.



This functionality is intended for updating products that are installed on several systems only in your environment, like GroupShield and Webshield. The functionality allows you to distribute such updates only to the distributed repositories these systems check into.

## Repository selection by agents

By default, agents can attempt to update from any repository in the repository list (SITELIST.XML) file. The agent can use a network ICMP ping or a subnet address compare algorithm to find the distributed repository with the quickest response time. Usually, this is the closest distributed repository to the system on the network.

You can also tightly control which distributed repositories agents use for updating by enabling or disabling distributed repositories in the agent policy settings. McAfee does not recommend disabling repositories in the policy settings. Allowing agents to update from any distributed repository ensures they receive the updates.

## Selective updating

ePolicy Orchestrator allows you to select which updates (DAT file, engine, and product-specific updates) you want client systems to receive, so that valuable bandwidth isn't wasted transferring unnecessary files. You can use selective updating with both global updating and update tasks.

You can also use this feature to selectively update only those components that you will want updated as soon as possible once an update is released. For example, DAT files and VirusScan Enterprise updates.

Due to the challenges customers face, ePolicy Orchestrator 3.6 provides different types of update repositories and several methods for implementing them:

## About the SITELIST.XML repository list

The SITELIST.XML file is a repository list containing all of the update repositories you are managing through ePolicy Orchestrator. These include any source repositories, the master repository, and any repositories you have created. The repository list contains the location and network credential information that client systems use to select the nearest repository and retrieve updates.



When a new update repository is created, the SITELIST.XML file is updated and the locations to which agents point for updates are adjusted.

The ePolicy Orchestrator server sends the repository list to the agent during agent-to-server communication. You can also export it to a file, manually deploy it, then apply it to client systems using command-line options.

## Checking in product deployment packages manually

Check in the PKGCATALOG.Z product deployment package files to the master repository to be able to deploy them using ePolicy Orchestrator.

You must be a global administrator to check in product deployment packages.



You cannot check in packages to your master repository while pull or replication tasks are executing.

To check in a product deployment package:

- 1 Locate the PKGCATALOG.Z file you want to check in. See the product's configuration guide for details on the location.
- 2 Copy the entire contents of the folder containing the package, then save it to a temporary folder on your ePolicy Orchestrator server.



You must copy *all* the files in the PKGCATALOG.Z folder, or the package check-in fails.

- 3 In the console tree, select **Repository**.
- 4 In the details pane, under **AutoUpdate Tasks**, click **Check in package**. The **Check-in package** wizard appears.

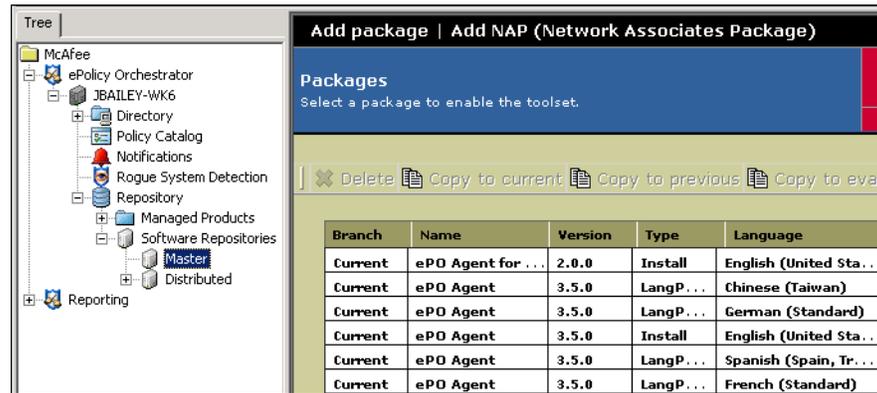
**Figure 4-3 Check-in package wizard**



- 5 Click **Next** to open the **Package Type** dialog box.
- 6 Select **Products or updates** as the package type, then click **Next**.
- 7 Browse to the PKGCATALOG.Z file that you saved in a temporary folder.
- 8 Click **Next** to view the package check-in summary information.
- 9 Click **Finish** to begin checking in the package. Wait a few minutes while the package checks into the repository.
- 10 Click **Close** when complete.

11 In the console tree, select **Repository | Software Repositories | Master**.

Figure 4-4 Packages list



12 In the details pane, scroll through the list and locate the product and version of the deployment package to verify the action was successful.

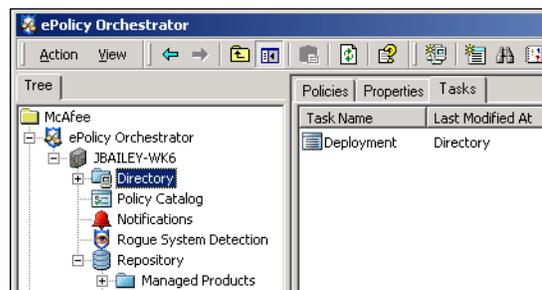
13 If you are using distributed repositories in your environment, be sure to replicate the package to them.

## Configuring the deployment task to install products on client systems

To deploy products using the product deployment task:

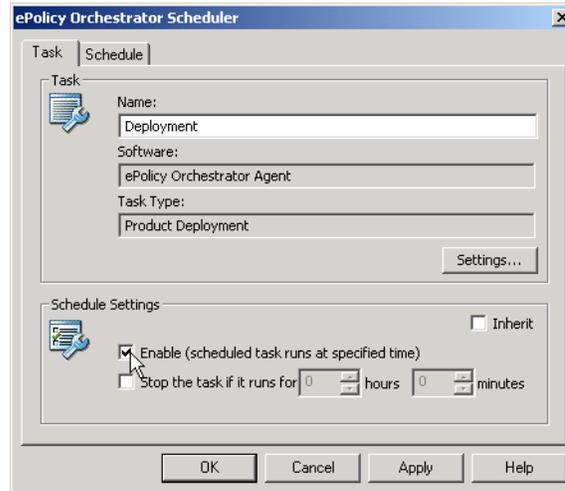
- 1 In the console tree, select the site, group, or individual system to which to deploy the product.
- 2 In the details pane, select the **Task** tab, then double-click **Deployment** in the task list. the **ePolicy Orchestrator Scheduler** dialog box appears.

Figure 4-5 Deployment task for the selected node in the Directory



- 3 Select the **Task** tab and deselect **Inherit** under **Schedule Settings**.

Figure 4-6 ePolicy Orchestrator Scheduler dialog box

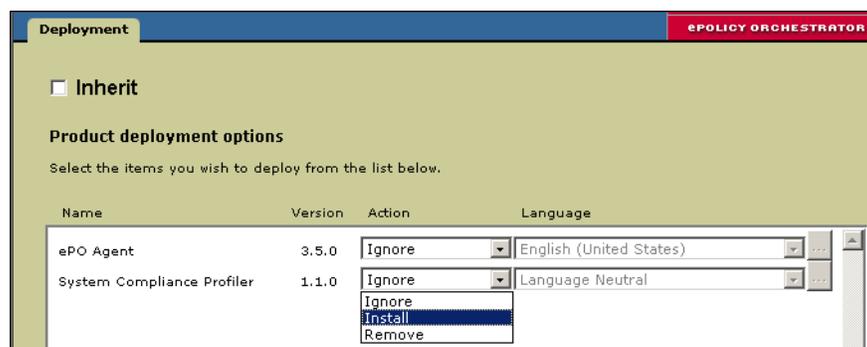


- 4 Under **Schedule Settings**, select **Enable (scheduled task runs at specified time)**. The task does not run unless you enable it here.
- 5 Click **Settings**.
- 6 On the **Deployment** tab, deselect **Inherit** to enable product deployment options.

The **Product deployment options** list shows which products are available to deploy through ePolicy Orchestrator. The products listed are those for which you have already checked in a PKGCATALOG.Z file to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product’s PKGCATALOG.Z file.

- 7 Set the **Action** to **Install** for the product you want to deploy.

Figure 4-7 Task Settings dialog box



- 8 To specify command-line install options, click **...** for each item and type the desired command-line options in the **Command line** text field. See your product documentation for information on command-line options.
- 9 Click **OK** to save the product deployment options and return to the **ePolicy Orchestrator Scheduler** dialog box.

**10** In the **ePolicy Orchestrator Scheduler** dialog box, select the **Schedule** tab.

**11** Deselect **Inherit** to enable scheduling options.

**12** Schedule as desired.

**13** Click **OK** to save your changes.

In the task list on the **Tasks** tab of the details pane, the **Enabled** status for the deployment task is set to **True**.

Once configured, the agents receive the deployment instruction when they call into the ePolicy Orchestrator server.

# 5

## Rogue System Detection

Even though you already use ePolicy Orchestrator to manage your security products, your protection is only as good as your coverage. Deploying agents to the systems you know about in your network and keeping them up-to-date is only part of a comprehensive strategy. The next step is ensuring you cover each system that connects to your network.

In any managed network, there are inevitably a small number of systems that do not have an agent on them at any given time. These can be systems that frequently log onto and off from the network, including test servers, laptop systems, or wireless devices. Unprotected systems are often the weak spot of any security strategy, creating entry points by which viruses and other potentially harmful programs can access to your network.

Rogue System Detection helps you monitor all the systems on your network — not only the ones ePolicy Orchestrator manages already, but the rogue systems as well. A rogue system is any system that is not currently managed by an ePolicy Orchestrator agent, but should be.

Rogue System Detection provides real-time detection of rogue systems by means of a sensor placed on at least one system within each network broadcast segment (typically a subnet). The sensor listens to network broadcast messages and spots when a new system has connected to the network.

When the sensor detects a new system on the network, it sends a message to the ePolicy Orchestrator server. The server then checks whether the newly-identified system has an active agent installed and managed. If the new system is unknown to the ePolicy Orchestrator server, Rogue System Detection allows you to take remediation steps including alerting network and anti-virus administrators or automatically deploying an ePolicy Orchestrator agent to the system.

### The Rogue System sensor

The sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect systems, routers, printers, and other network devices connected to your network. The sensor gathers information about the devices it detects, and forwards the information to the ePolicy Orchestrator server.

The sensor is a small Win32 native executable application. Similarly with an ePolicy Orchestrator SuperAgent, you must have at least one sensor in each broadcast segment, usually the same as a network subnet, in your network. The sensor runs on any NT-based Windows operating system, such as Windows 2000, Windows XP, or Windows 2003.

## Passive listening to layer-2 traffic

To detect systems on the network, the sensor utilizes WinPCap, an open source packet capture library. Using WinPCap, the Rogue System sensor captures layer-2 broadcast packets sent by systems connected to the same network broadcast segment. The sensor listens passively to all layer-2 traffic for Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and IP traffic. The sensor is able to listen to the broadcast traffic of all devices on its broadcast segment.

The sensor does not actively probe the network to search for which devices are connected.



The sensor does not determine whether the system is a rogue system. It detects systems connected to the network and reports these detections back to the ePolicy Orchestrator server.

## Intelligent filtering of network traffic

The sensor implements intelligent filtering of network traffic to ignore unnecessary messages and capture only what it needs: Ethernet and IP broadcast traffic. By filtering out unicast traffic, which may contain non-local IP addresses, the sensor focuses only on devices that are part of the local network. For example, if a system on the network happens to be browsing McAfee, packets appear on the local network with the IP address belonging to mcafee.com. The sensor detects systems on your local network only, so it ignores all such unicast packets because their sources cannot be guaranteed to be a local system.

To optimize performance and minimize network traffic, the sensor is designed to limit its communication to the server by only relaying new system detections, and to ignore any re-detected systems for a user-configurable time. For example, the Rogue System sensor detects itself among the list of detected systems. If the sensor sent a message every time it detected a packet from itself, the result would be a network overloaded with sensor detection messages.

The sensor further filters on systems already detected:

- The sensor always reports any system the first time it is detected on the network.
- The sensor adds the MAC address of each detected system to the packet filter, so that it is not detected again until removed from the filter.
- The sensor implements aging on the MAC filter so that after a time period, MAC addresses for systems that have already been detected are removed from the filter, causing those systems to be re-detected and reported to the server.

## Data gathering and communications to the server

Once the sensor detects a system located on the local network, it attempts to gather as much information about that system from the information contained in the network packet. The information gathered includes DNS name, operating system version, and NetBIOS information such as domain membership, system name, and the list of currently logged-in users.

All of the NetBIOS-related information gathered is subject to standard limitations of authorization and other limitations, as documented in the Microsoft management API.

The sensor packages the gathered information about the detected system into an XML message. It sends this message via secure HTTPS to the ePolicy Orchestrator server for processing. The server then queries the ePolicy Orchestrator database to determine whether the system is a rogue system.

To save bandwidth in large deployments, you can configure how often the sensors send detection messages to the server. You can configure the sensor to cache detection events for a given time period, such as one hour, and then send a single message containing all the events from that time period.

## Choosing systems to host sensors

Systems on which the sensor is installed should be likely to remain on and connected to the network all the time, such as a server. If you don't have a server running in a given broadcast segment, deploy several sensors to several workstations to ensure that at least one of them is connected to the network at any time.

### Best practices information

To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor in each broadcast segment of your network. Installing more than one sensor in a broadcast segment does not create issues around duplicate messages — the server filters any duplicate detection messages. However, additional active sensors in each subnet results in traffic sent from each sensor to the server. While maintaining as many as five or ten sensors in a broadcast segment should not cause any bandwidth issues, you should not maintain more sensors in a broadcast segment than is necessary to guarantee that the broadcast segment is covered.

## Primary and inactive sensors

When deploying multiple sensors to the same subnet, you can configure how many are actively reporting to the server at any one time (three by default). These are the primary sensors. Any additional sensors you deploy are backups that remain inactive until the ePolicy Orchestrator server makes them become active.

At regular intervals, the ePolicy Orchestrator server changes primary sensors so that it is not dependant on any one sensor for too long. Also, if the primary sensor is disabled or stops responding, the ePolicy Orchestrator server automatically assigns a different sensor on that broadcast segment the role of primary sensor.

The **Subnet List** table on the **Subnets** tab of the Rogue System Detection interface allows you to view the subnets in your network where you already have ePolicy Orchestrator agents. From here you can deploy sensors to systems.

## Configure sensor policy settings before deploying

Before you deploy sensors, you should configure the sensor policy settings to suit your needs. These needs are probably the same for all sensors in your environment. Most likely, you can configure sensor policy settings at the Directory root of the console tree and let them inherit throughout the Directory.

## Machine status and rogue type

*Machine status* and *rogue type* are classifications ePolicy Orchestrator uses to determine which systems are rogue systems. Each detected system is listed in the **Machine List** table with a status and, if classified as a rogue system, a rogue type. These classifications are very useful for grouping systems in the **Machine List** table. You can also use status and rogue type as criteria for automatic responses.

### Machine status for detected systems

Each detected system has a basic status of **Managed**, **Rogue**, **Exception**, or **Inactive**. This status is displayed in the **Status** column of the **Machine List** table.

**Table 5-1 Types of machine status**

<b>Machine Status</b>	<b>Description</b>
<b>Managed</b>	A system that has an active agent installed and running. The vast majority of systems in the <b>Machine List</b> table should have this status.
<b>Rogue</b>	A system that does not have an agent on it.
<b>Exception</b>	A system you have identified as an exception. An exception is a piece of network equipment, such as a network router, switch, or printer, that you know does not require an agent.
<b>Inactive</b>	A system that is listed in the ePolicy Orchestrator database but has not been detected by a rogue system sensor in a configurable time period. These are mostly likely systems that are shut down or disconnected from the network.

### Types of rogue systems

Systems with a status of **Rogue** or **Inactive** also are assigned a rogue type. These may be systems that are not listed in the database, but are also not necessarily true rogue systems at a given point in time. Rogue types allow you to define what exactly is a rogue system in your network.

For example, a new system may have just logged onto the network. This system had an agent installed with a network login script at its initial logon. Since the initial agent call to the server may take up to ten minutes, the rogue system sensor detects the system before the agent communicates with the server and is added to the database as a managed system. The system is classified as a rogue system, even though it is not really a rogue system because it already has an agent. If you configure automatic responses or automatic e-mail alerts for rogue detections, specifying a reasonable grace period using the **Rogue (Grace Period)** rogue type can help you minimize false positive detections.

The following table lists and describes each rogue type and its description:

**Table 5-2 Types of rogue systems**

<b>Rogue Type</b>	<b>Description</b>
<b>No Agent</b>	The detected system has no agent installed. This is the most common rogue type.
<b>Grace Period</b>	<p>The detected system has no agent installed, but was detected within a user-configured time period, or grace period. This is useful if you have many systems that join and leave the network. It is also useful if you use login scripts to install the agent when new systems log onto the network. Using the grace period allows you to create a time buffer to avoid false positive rogue detections for systems that are not really rogue systems.</p> <p>The grace period is disabled by default, so all systems without agents are classified as <b>Rogue (No Agent)</b>. You might consider enabling the grace period if you are configuring automatic responses for the rogue detection event.</p>
<b>Inactive Agent</b>	The detected system has an agent installed, but it has not called into the server for some configurable period of days.
<b>Alien Agent</b>	<p>The detected system has an agent installed, but the agent does not report into your server. This can occur if your organization is large and you use multiple ePolicy Orchestrator servers to manage different parts of your network. Laptop users who may travel and log onto your network could have an alien agent. This rogue type is distinct as you probably would not want to take action on these systems as they are already managed. But since they are not managed by your server, you don't want them to be classified as managed either.</p> <p>To reduce false positive rogue detections, you can fine-tune automated responses to avoid deploying agents or sending e-mail alerts when alien agents are detected.</p>
<b>Managed</b>	For systems with a status of <b>Inactive</b> only. The system has not been detected by a sensor within a configured length of time, but when last detected it did have an agent.

## Subnet status

Each subnet listed in the **Subnet List** table on the **Subnets** tab receives a status of **Covered** if there is an active rogue system sensor is installed on a system in that subnet. A subnet has an **Uncovered** status if there are no sensors present. You can click each subnet to view a list of all systems in the subnet that have an active agent installed.

## Distributing Rogue System sensors

The sensor reports only on detections occurring within its local broadcast segment. You must install at least one sensor per broadcast segment in your network for coverage.



Depending on your network configuration, a broadcast segment may or may not be the same as a subnet.

If your organization is large, installing sensors manually on individual systems throughout your network could require more of your time than you can afford. Although you can install sensors manually on managed systems, consider using ePolicy Orchestrator to deploy sensors to appropriate systems throughout your network.

Before distributing sensors, configure the settings on the **Rogue System Sensor** policy pages.

## Deploying Rogue System sensors

You deploy (send and install) Rogue System sensors from the **Subnet List**. You can only install sensors to managed systems (systems that are running an ePolicy Orchestrator agent).



In the future, network access sensors will be deployed from the **Subnet List**.

You can allow sensor host systems to be selected automatically based on specific criteria, or you can manually select them. As part of the sensor deployment, a **Rogue System Sensor Install** client task is created for the host systems. This task allows you to uninstall the sensor or upgrade it to a newer version.

If you allow Rogue system Detection to pick systems automatically on the subnet, you can specify criteria for choosing systems. You can specify any or all of the criteria listed here when configuring automatic sensor deployment:

**Table 5-3 Automatic sensor deployment criteria**

Criteria	Description
<b>Most Recent ePO Agent Communication</b>	Most recent agent-server communications indicates a system is more likely to be connected and up-to-date at any given time.
<b>Server OS</b>	Servers are more likely than workstations to remain on and connected to the network at all times. Selecting this criterion can help ensure continuous coverage.
<b>Hostname</b>	ePolicy Orchestrator can select systems based on a text string you use in the DNS name. For example, if you add an "SRV" prefix to the names of your server systems, you could deploy a sensor to a system with "SRV" in its DNS name.  If you add <b>Hostname</b> to the <b>Selected criteria</b> list, type the text string that appears in your server DNS names in the <b>Hostname</b> text box.
<b>Most Memory</b>	Although the sensor is not a memory-intensive application, you can ensure resource efficiency by choosing the criterion.
<b>Fastest CPU</b>	Although the sensor is not a processor-intensive application, you can ensure resource efficiency by choosing the criterion.

For instructions, see the *ePolicy Orchestrator 3.6 Product Guide*.

## Installing the sensor manually

If you do not want to deploy sensors from the ePolicy Orchestrator console, you can perform the installation manually. To do so, you must be at the system you want to host the sensor. You must also be using an account that has administrative privileges on the system.

You can install the sensor either via a `SETUP.EXE` installation wizard or via the command line.

For specific instructions, see the *ePolicy Orchestrator 3.6 Product Guide*.

---

## Taking actions on detected rogue systems manually

You can perform actions on one or more systems listed in the **Machine List** table. For example, you may want to deploy an agent to a detected rogue system or mark systems for later action. In addition to these manual actions, you can configure automatic responses that can be initiated by a detection event.

The following table lists the manual actions you can take on selected systems in the **Machine List** table. Some of these are covered in greater detail in following sections.

**Table 5-4 Available manual actions**

Action	Description
<b>Add to ePO tree</b>	Adds a system node to a <b>Rogue System</b> site in the Directory. You can place the systems into an appropriate site or group manually after it is added to this site.
<b>Mark for Action</b>	Marks the detected system as a system still needing action.
<b>Mark as Exception</b>	Marks selected system as a machine that does not require an agent. For example, routers and printers.
<b>Push ePO Agent</b>	Instructs the server to deploy an agent to the selected system.
<b>Query ePO agent</b>	Queries the detected system to ascertain whether there is an agent installed on it. This query is required for systems to appear as the <b>Alien Agent</b> rogue type.  Consider creating an automatic response that uses this action if you have multiple ePolicy Orchestrator servers in your network. If travellers from other parts of your organization frequently log onto your network, they appear as rogue systems even if they have an agent from another server.
<b>Remove Host</b>	Hides the detected system in the <b>Machine List</b> table but does not delete it from the database.
<b>Unmark for Action</b>	Unmarks systems that you have already marked for action.
<b>Unmark as Exception</b>	Unmarks systems that you have already marked as exceptions.

## Configuring automatic responses for specific events

You can configure automatic responses so that ePolicy Orchestrator responds automatically to the Rogue System Detection events. There are two specific Rogue System Detection events for which you can configure automatic responses:

- **Rogue Machine Detected.** A new system is found that had not already found in the ePolicy Orchestrator database.
- **Subnet Uncovered.** A subnet in your network, that does not have a rogue system sensor installed, is discovered.

You can also configure responses for any event.

An automatic response can contain one or more of the actions described in the following table. For example, if you configure a response to deploy an ePolicy Orchestrator agent to newly-detected systems, you may also want to send an e-mail to administrators to follow up on the agent installation.

**Table 5-5 Actions available for automatic responses**

Action	Description
<b>Add to ePO tree</b>	Adds the system to a <b>Rogue System</b> site within the Directory. After the system is added to this site, you can move the system to an appropriate location manually.
<b>Mark for Action</b>	Selects the detected system as a system still needing action.
<b>Mark as Exception</b>	Marks selected system as a machine that does not require an agent. For example, routers and printers.  For example, in your organization you may reserve a range of IP addresses within each subnet for network equipment such as routers, switches, and printers. You can create an automatic response to mark such equipment as exceptions and add a condition to initiate the response only if the detected system's IP address falls within a certain range. Or, maybe you use certain vendors for network equipment that are always different from your vendors for server or workstation systems. In this case, you can use the <b>OUI Org</b> condition to initiate an automatic response to mark systems as exceptions if the system's MAC address contains a specific vendor code.
<b>Push ePO Agent</b>	Instructs the server to deploy an agent to the selected system.
<b>Query ePO agent</b>	Queries the detected system to ascertain whether there is an agent installed on it. This query is required when using the <b>Alien Agent</b> rogue type.  Consider creating an automatic response that uses this action if you have multiple servers in your network. If travellers from other parts of your organization frequently log onto your network, they appear as rogue systems even if they have an agent from another server installed.
<b>Remove Host</b>	Hides the detected system in the <b>Machine List</b> table but does not delete it from the database.
<b>Send E-mail</b>	Sends a pre-configured e-mail message to pre-configured recipients.
<b>Send ePO Server Event</b>	Forwards Rogue System Detection and Subnet Uncovered events to the server. This is required if you plan to use Notifications to automatically send e-mail alerts for Rogue System Detection events.

**Table 5-5 Actions available for automatic responses**

Action	Description
Unmark for Action	Deselects systems that you have already marked for action.
Unmark as Exception	Deselects systems that you have already marked as exceptions.

### Import and export exceptions from and to an XML file

To prevent having to identify systems as exceptions again if you need to reinstall the ePolicy Orchestrator server, you can easily save your exceptions list to an XML file. This XML exceptions list preserves your exceptions information so you can re-import it if needed.

For instructions see the *ePolicy Orchestrator 3.6 Product Guide*.

# 6

## ePolicy Orchestrator Notifications

The ePolicy Orchestrator Notifications feature can alert you to any events that occur on the managed systems in your environment or on the ePolicy Orchestrator server itself. You can configure rules in ePolicy Orchestrator to send e-mail, SMS, or text pager messages (or SNMP traps), as well as run external commands, when specific events are received and processed by the ePolicy Orchestrator server. The ability to specify the event categories that generate a notification message and the frequencies with which notifications are sent are highly configurable.

This feature notifies specified individuals when the conditions of a rule are met. These can include:

- Detection of a virus or other potentially unwanted program by your anti-virus software product. Although almost any anti-virus software product is supported, events from VirusScan Enterprise 8.0i include the IP address of the source attacker so that you can isolate the system infecting the rest of your environment.
- Outbreak situations. For example, 1000 virus detected events are received within five minutes.
- Compliance events from McAfee System Compliance Profiler. For example, systems are found that are not current with the latest Microsoft patches.
- High-level compliance of ePolicy Orchestrator server events. For example, a replication task did not complete.
- Detection of rogue systems.

This feature also allows you to configure notification rules to execute command lines and launch registered executables when the specified conditions are met.

---

### About Notifications

Before you plan the implementation of Notifications, you should understand how this feature works with ePolicy Orchestrator and its Directory.



This feature does not follow the inheritance model of policy enforcement.

When events occur on systems in your environment, they are delivered to the ePolicy Orchestrator server, and the notification rules (associated with the group or site that contains the affected systems and each parent above it) are applied to the events. If the conditions of any such rule are met, a notification message is sent, or an external command is run, per the rule's configurations.

This design allows you to configure independent rules at the different levels of the Directory. These rules can have different:

- Thresholds used to send a notification message. For example, a site administrator wants to be notified if viruses are detected on 100 systems within 10 minutes on the site, but a global administrator does not want to be notified unless viruses are detected on 1000 systems within the same amount of time within the entire environment.
- Recipients for the notification message. For example, a site administrator wants to receive a notification message only if a specified number of virus detection events occur within the site. Or, a global administrator wants each site administrator to receive a notification message if a specified number of virus detection events occur within the entire Directory.

## Throttling and aggregation

You can configure when notification messages are sent by setting thresholds based on *aggregation* and *throttling*.

### Aggregation

Use aggregation to determine the thresholds of events at which the rule sends a notification message. For example, you can configure the same rule to send a notification message when the ePolicy Orchestrator server receives 100 virus detection events from different systems within an hour *or* whenever it has received 1000 virus detection events altogether from any system.

### Throttling

Once you have configured the rule to notify you of a possible outbreak situation, you may want to use throttling to ensure you do not get too many notification messages. If you are administering a large network, then you may be receiving tens of thousands of events during an hour, creating thousands of notification messages based on such a rule. ePolicy Orchestrator Notifications allows you to throttle the number of notification messages you receive based on a single rule. For example, you can specify in this same rule that you don't want to receive more than one notification message in an hour.

When using throttling, the notification message received contains a summary of events that occurred within the throttling period that would have triggered the rule otherwise.

## Notification rules and Directory scenarios

To show how this feature functions with the Directory, two scenarios are used.

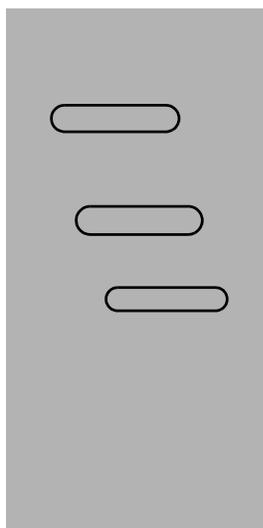
For both scenarios, we can assume that each group, site, and the Directory root of the console tree has a similar rule configured. Each rule is configured to send a notification message when 100 virus infection events have been received from any product within 60 minutes. For reference purposes, each rule is named **VirusDetected\_<node name>**, where <nodename> is the name of the node as it appears in the Directory (for example, **VirusDetected\_Group2c**).

### Scenario one

For this scenario, 100 virus infections are detected in Goup2C within 60 minutes in a single day.

Conditions of the rules **VirusDetected\_Group2C**, **VirusDetected\_Site2**, and **VirusDetected\_Directory** are met, sending notification messages (or launching registered executables) per the rules' configurations.

**Figure 6-1 Console tree**

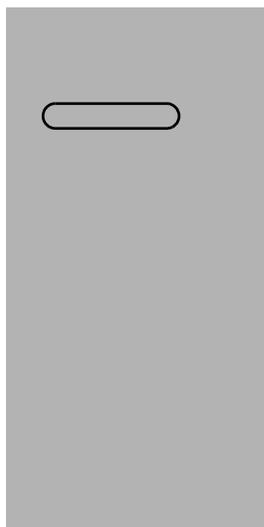


## Scenario two

For this scenario, 50 virus infections are detected in **Group2C** and 50 virus infections are detected in **Group3B** within 60 minutes in a single day.

Conditions of the **VirusDetected\_Directory** rule are met, sending notification messages (or launching registered executables) per the rules' configurations. This the only rule that can be applied to all 100 events.

Figure 6-2 Console tree



---

## Determining when events are forwarded

The ePolicy Orchestrator server receives notifications from the Common Management Agent (CMA). You must configure its policy pages to forward events either immediately to the ePolicy Orchestrator server or only at agent-to-server communication intervals.

If you choose to have events sent immediately (as set by default in ePolicy Orchestrator Agent 3.5.0 McAfee Default policy), the agent forwards all events as soon as they are received. If you want all events sent to the ePolicy Orchestrator server immediately so that they can be processed by Notifications when the events occur, configure the agent to send them immediately.

If you choose not to have events sent immediately, the agent only forwards events immediately that are designated by the issuing product as high priority. Other events are only sent at the agent-to-server communication intervals.

If the currently applied named policy is not set for immediate uploading of events, either edit the currently applied named policy or create a new named policy for the **ePO Agent 3.5.0 | Configuration** policy pages. This setting is configured on the **Events** tab of these policy pages.

---

## Determining which events are forwarded

Along with being able to determine when events are forwarded to the server, you can also select which events are forwarded.



If you choose not to select which events are forwarded, all events are forwarded. This is the default setting.

To select which events are forwarded immediately:

- 1 In the console tree, select the desired ePolicy Orchestrator database server under **Reporting** and log onto it with ePolicy Orchestrator authentication.
- 2 Select **Events** in the console tree under the database server.
- 3 Select the **Filtering** tab in the details pane.



You must be a global administrator to make any changes to the **Filtering** tab.

- 4 Select **Send only the selected events to ePO** on the **Filtering** tab.
- 5 Select the desired events in the list and click **Apply**.

---

## Planning

Before creating rules that send notifications, you can save time by planning:

- The types of events (both product and server) that could generate and send a notification message in your environment.
- Who should receive which notifications. For example, it may not be necessary to notify the site administrator of site B about a failed replication in site A, but you may want all site administrators to know that an infected file was discovered in site A.
- Which types and levels of thresholds you want to set for each rule. For example, you may not want to receive an e-mail message every time an infected file is detected during an outbreak. Instead, you can choose to have such an e-mail message sent — at most — once every five minutes, regardless of how often that server is receiving the event.
- Which command lines or registered executables you want to run when the conditions of a rule are met.

## Rules

Rules allow you to define when, how, and to whom, notifications are sent, as well as any executables you want to run when the rule is triggered. You can create or edit rules once you have made some specific configurations to the feature.

But until all of your configurations are complete and you've familiarized yourself with the abilities of ePolicy Orchestrator, you can use the default rules provided with the product.



Notification rules do not have a dependency order.

## Configuring ePolicy Orchestrator Notifications

To create and use rules, you need to configure the following in Notifications:

- E-mail server from which to send notification messages.
- E-mail contacts list from which you select recipients for notification messages.
- List of SNMP servers to use while creating rules. You can configure rules to send SNMP traps to SNMP servers when the conditions are met for a rule.
- List of external commands to run when the conditions of a rule are met.

These are all configured through the interface of Notifications. For instructions, see the *ePolicy Orchestrator 3.6 Product Guide*.

## Default rules

ePolicy Orchestrator provides six default rules that you can enable for immediate use while you learn more about the feature.



Once enabled, the default rules send notification e-mail messages to the e-mail address you provided on the **Set E-mail Address** panel of the installation wizard. This is also the **Administrator** address in both the Notifications and Rogue System Detection contact lists.

You can edit any of the default rules as necessary.

Before enabling any of the default rules:

- Specify the e-mail server from which the notification messages are sent.
- Ensure the recipient e-mail address is the one you want to receive e-mail messages.
- Send a test e-mail from the **Basic Configuration** section of the **Configuration** tab.

The default rules are described in [Table 6-1](#):

**Table 6-1 Default notification rules**

Rule name	Associated events	Configurations
Daily unknown product notification	Any events from any unknown products.	Sends a notification message at most, once a day.
Daily unknown category notification	Any event of an unknown category.	Sends a notification message at most, once a day.

Table 6-1 Default notification rules

Rule name	Associated events	Configurations
Virus detected and not removed	<b>Virus Detected and Not Removed</b> events from any product.	Sends a notification message: <ul style="list-style-type: none"> <li>■ When the number of events exceeds 1000 within an hour.</li> <li>■ At most, once every two hours.</li> <li>■ With the source system IP address, actual threat names, and actual product information, if available.</li> </ul>
Virus detected heuristics and not removed	<b>Virus Detected (Heuristics) and Not Removed</b> events from any product.	Sends a notification message: <ul style="list-style-type: none"> <li>■ When the number of events exceeds 1000 within an hour.</li> <li>■ At most, once every two hours.</li> <li>■ With the source system IP address, actual threat names, and actual product information, if available.</li> </ul>
Repository Update or Replication Failed	<b>Repository update or replication failed</b> events.	Sends a notification message when any events are received.
Non-compliant computer detected	<b>Non-compliant Computer Detected</b> events.	Sends a notification message: <ul style="list-style-type: none"> <li>■ When any events are received.</li> <li>■ Once per each rule of the Compliance Check server task. (This task sends one event per each of the four rules associated with the Compliance Check server task.)</li> </ul>

## Creating rules

Creating a rule is a four-step process:

- 1 Describe the rule — Naming the rule and defining the level of the **Directory** to which it applies.
- 2 Set filters for the rule — Specifying the products, event categories, and any threat names that apply to the rule.
- 3 Set thresholds of the rule — Defining the aggregation and throttling of the rule.
- 4 Configure the notifications for the rule — Defining the messages you want sent, their delivery type, and any executables you want to run when the rules conditions are met.

For complete instructions, see the *ePolicy Orchestrator 3.6 Product Guide*.

---

## Viewing the history of Notifications

This feature allows you to view the history of notifications sent. You can view a collective summary of all notifications sent, by product or category, or a list of all the specific notifications sent.

## Notification summary

The **Notification Summary** page allows you to view a summary of the number of notifications sent by product, category, priority, or rule name:

- 1 In the console tree, select **Notifications**.
- 2 Select the **Log** tab, then click **Summary**.
- 3 Select the **Time** by which you want to limit the **Notification Summary** data. These include:
  - **All Times**
  - **Last Hour**
  - **Last 8 Hours**
  - **Last Day**
  - **Last Week**
- 4 Select the **Site** for which you want to limit the **Notification Summary** data. You can select individual sites or **All** sites.



If the global administrator has not allowed reviewers and site administrators to view Directory notifications and rules, site administrators and site reviewers are limited to viewing only notifications and rules for their sites. Site administrators and site reviewers can never view notifications and rules specific only to other sites.

- 5 In **Group by**, select **Product**, **Category**, **Priority**, or **Rule name** from the drop-down list, and the quantity of notifications sent for the **Group by** selection.

## Notification list

The **Notification List** page allows you to view a list of all notifications sent. This list can be sorted by the data of any column by clicking the column title.

- 1 In the console tree, select **Notifications** under the desired **Directory** in the console tree.
- 2 Select the **Log** tab, then click **List**.
- 3 Click any column title (for example, **Notification Type**) to sort the list by that column.



If the global administrator has not selected to allow reviewers and site administrators to view Directory notifications and rules, site administrators and reviewers are limited to viewing only notifications and rules for their sites. Site administrators and site reviewers can never view notifications and rules specific only to other sites.

## Notification details

Click any notification from the **Notification List** page to view its details, including:

- Time notification sent
- Rule priority
- First event time
- Notification rule name
- Rule site
- Rule defined at

- Actual number of events
- Number of computers
- Affected computer IP addresses
- Affected computer names
- Source computers
- Notification status
- Notification type
- Event IDs
- Affected objects
- Actual products
- Selected products
- Actual categories
- Selected categories
- Actual threat or rule names
- Selected threat or rule names
- Message subject
- Event descriptions
- Additional information

### Using custom filters

Custom filters provide flexibility to view the notification list. By defining a filter, you can choose to have specific notification log items included or excluded from those displayed.

ePolicy Orchestrator Notifications allows you to create multiple conditions on which to filter the **Notification List**.

You can filter notification log items based on:

- Sites.
- Received products.
- Actual event categories.
- Priority of the notification message.
- Rule names.

## Product and component list

You can configure rules to generate notification messages for specific event categories for specific products and components. This is a list of products and components for which you can configure rules and a list of all possible event categories.

- Dr. Ahn
- Desktop Firewall
- Entercept
- ePO Server
- ePO Agent
- GroupShield Domino
- GroupShield Exchange
- System Compliance Profiler
- Symantec NAV
- NetShield
- NetShield for NetWare
- PortalShield
- Stinger
- ThreatScan
- Unknown product
- Virex
- VirusScan
- VirusScan PDA
- WebShield
- LinuxShield



Checking in additional NAP files can add products to this list.

Event categories for which rules can be configured:

- Access Protection rule violation detected and blocked
- Access Protection rule violation detected and NOT blocked
- Banned content or file detected and NOT removed
- Banned content or file detected and removed
- Computer placed in quarantine mode
- E-mail content filtered or blocked
- Encrypted/corrupted file detected and removed
- Firewall rule triggered
- Virus detected (heuristic) and NOT removed
- Virus detected (heuristic) and removed
- Unwanted program detected (heuristic) and NOT removed
- Unwanted program detected (heuristic) and removed
- Intrusion detected
- System Compliance Profiler rule violation
- Non-compliant computer detected
- Normal operation
- On-access scan disabled
- Policy enforcement failed
- Repository update or replication failed
- Virus detected and removed
- Scan cancelled
- Scan line item results
- Software deployment failed
- Software deployment succeeded
- Software failure or error
- Spam detected and handled
- Unknown category
- Unwanted program detected and NOT removed
- Unwanted program detected and removed
- Update/upgrade failed
- Update/upgrade succeeded
- Virus detected and NOT removed



Checking in additional NAP files can add event categories to this list.

# 7

## Outbreaks

The most effective response to viruses is to know your system, have current anti-virus software installed, detect outbreaks early, then respond quickly and efficiently. An effective strategy includes both prevention as well as response.

The ePolicy Orchestrator software can help reduce the costs of managing an outbreak. When you use ePolicy Orchestrator, you can manage all of your sites from a central location, which makes management easier, more efficient, and ensures consistently applied policies across your enterprise.

This section contains the following topics:

- [Tasks to do on a daily or weekly basis to stay prepared](#)
- [Checklist — Are you prepared for an outbreak?](#)
- [Other methods to recognize an outbreak](#)
- [Checklist — You think an outbreak is occurring](#)

---

### Tasks to do on a daily or weekly basis to stay prepared

You can use features of the software to help prepare your site or company before an outbreak occurs. Use the Are you prepared for an outbreak? checklist to determine your level of preparedness.

### Server and client tasks you should schedule to run regularly

Create and schedule these server tasks and client tasks to run scans and keep client software up to date with the latest updates. It takes some time to configure and schedule these tasks initially, but after that they should run regularly and automatically.

You can also re-configure any of these scheduled tasks to **Run Immediately** should you need to run a particular task manually.

**Table 7-1 Suggested server tasks**

Server task	Description
Daily DAT & engine pull task	Performs a repository pull for updated weekly DATs or engine files from the default source repository on the McAfee FTP site. The task is scheduled as <b>Hourly</b> , every <b>6</b> hours.
Daily incremental repository replication	Replicates only changes to the master repository to all distributed repositories. The task is scheduled as <b>Hourly</b> , every <b>6</b> hours.
Weekly full repository replication	A weekly task runs once each Sunday to perform a full replication to all distributed repositories. This extra layer of redundancy is a good way to ensure that all distributed repositories are fully up-to-date at least once a week.
Daily inactive agent task	Daily task scans the <b>Directory</b> for systems with agents that have not communicated with the server and places them in an "Inactive Agents" group.

To keep anti-virus and security software on client systems up-to-date, make sure you have the right client tasks created and scheduled for the appropriate parts of your Directory. The following describes a sample of what your client task configuration might look like in a typical deployment.

**Table 7-2 Suggested client tasks**

Client task	Task type	Description
Daily DAT-only client update task	agent Update	Update DATs every day for products using the CMA common updater, such as VirusScan Enterprise.  The task is scheduled to run 4 times every day, starting at 3 am, one hour after your replication server task. <b>Repeat task</b> is selected to repeat the task every 6 hours, so it occurs 4 times a day.  In the <b>Task Settings</b> , select only <b>DAT</b> and <b>EXTRA.DAT</b> . These are updated the most often.
Weekly engine-only client update task	agent Update	Update anti-virus engines once a week. McAfee releases new engines only about once every 2-3 months, so save network bandwidth by updating them less frequently than DATs.  In the <b>Task Settings</b> , select only <b>Engine</b> .
Weekly agent patch and service pack update	agent Update	Update the agent and security products like VirusScan Enterprise or Desktop Firewall with patches and service packs. Run the task once per week.  In the <b>Task Settings</b> , select all the <b>Service Pack</b> and <b>Patch</b> types. These are updated the most often.
Daily VirusScan 4.5.1 update	VirusScan 4.5.1 for Windows AutoUpdate	Update DATs daily for Windows 9X client systems using VSC 451. Schedule it to run several times a day, similar to the DAT update task for CMA products.
Daily VirusScan 4.5.1 On-Demand Scan	VirusScan 4.5.1 for Windows ODS	Daily ODS scan for VirusScan 4.5.1.
Daily update task for Novell NetWare servers	NetShield for NetWare 4.6 On-Demand Scan	Daily update for NetShield for NetWare on Novell NetWare servers.

---

## Checklist — Are you prepared for an outbreak?

- Know your network and specifically what creates traffic, and how much, on it.
- The ePolicy Orchestrator software has been fully installed and implemented.
- An anti-virus software product has been installed and configured on your systems. For example, McAfee VirusScan Enterprise 8.0i.
- Your anti-virus software is up-to-date with the latest virus definition (DAT) files. You are performing regular, scheduled updates of the virus scanning engine and virus definition (DAT) files for each of the anti-virus products that you manage through ePolicy Orchestrator. You can also use reports to determine coverage. For more information and instructions, see the reporting guide.
- Turn off all network appliances and services you are not using.
- Examine which services need inbound and outbound traffic, and which ports they use. (Specifically, which of the first 1024 ports are used. On your gateway firewall, disallow traffic on ports not used by your appliances and services.
- Examine what types of e-mail attachments are acceptable in your environment, and disallow others.
- Your Microsoft products running on managed systems are up-to-date with the latest patches and Service Packs. (Generally, Microsoft releases these on a monthly basis.) You can use McAfee System Compliance Profiler to ensure all of your systems are compliant to the latest Microsoft patches and Service Packs.
- You have configured Notifications to send a message to you or others when specified events (like a virus detection) are received and processed by the server.
- The Rogue System Detection feature is implemented to recognize and deploy agents to rogue systems and devices coming on to your network.
- You are performing regular, scheduled updates of products through ePolicy Orchestrator to ensure your security products are running the latest patch or Service Pack.
- You have enabled the agent wakeup call and tested the agent's communication with the systems on your network.

---

## Other methods to recognize an outbreak

There are several key indicators that you can use to determine if your network is experiencing an outbreak. The following key indicators are covered in this section:

- Network utilization key indicators.
- E-mail utilization key indicators.
- Virus detection events.

### Network utilization key indicators

The following are indicators that network utilization may be affected by an outbreak:

- Users complain of slowness. Users are often the first to notice when a full-scale outbreak is taking place. Systems slow down, network systems stop responding, and applications start displaying messages.

- Monitoring tools (for example, tools from Sniffer Technologies) detect a change in the network utilization levels.

## E-mail utilization key indicators

The following are indicators that e-mail utilization may be affected by an outbreak:

- Users complain of slowness. Users are often the first to notice when a full-scale outbreak is taking place. E-mail slows down or does not work at all.
- CPU utilization of Microsoft Exchange servers goes up significantly.
- Monitoring tools (for example, tools from Sniffer Technologies) detect a change in the e-mail utilization levels.
- Microsoft Exchange Performance Monitor counters register a change in the e-mail utilization levels.
- McAfee Outbreak Manager notifies you via e-mail that a potential outbreak may be indicated. McAfee Outbreak Manager analyzes incoming e-mail messages and identifies behaviors that are indicative of an outbreak.
- The McAfee WebShield e500 appliance collects data that can help identify if an outbreak is occurring.

## Virus detection events

The following events are indicators that a virus has been detected:

- A notification message is received from the ePolicy Orchestrator server, indicating a virus has been detected.
- An ePolicy Orchestrator report identifies that a virus has been detected.
- McAfee Outbreak Manager notifies you via e-mail that a potential outbreak may be indicated.
- McAfee Alert Manager notifies you that a virus has been detected.

When an outbreak occurs, you can respond in many ways. Use the You think an outbreak is occurring checklist to respond to an outbreak.

---

## Checklist — You think an outbreak is occurring

If you think an outbreak might be occurring, perform the following in your environment:

- Visit the AVERT home page to get the latest virus information.
- Submit samples of potentially infected files to WebImmune for testing.
- Modify the firewall and network security settings to block viral activity. To help you determine what to block and how the virus behaves, visit the Virus Information Library on the AVERT web site.
- Increase detection settings for all anti-virus products to meet the threat. Visit the Virus Information Library for an analysis of the threat.

- Regularly enforce agents with an agent wakeup call, and run coverage reports to determine that protection is in place.



To ensure full coverage, you must have the ePolicy Orchestrator agent installed on each system.

- Search for traffic on unexpected ports, then disallow the traffic.
- Use the global updating feature to perform the following:
  - Download supplemental (EXTRA.DAT) and full virus definition (DAT) files.
  - Update the virus scanning engine.
- Perform an on-demand scan of infected systems.
- Run anti-virus coverage reports to ensure that anti-virus coverage on infected systems is complete.

If you do not have a McAfee anti-virus product installed or do not have the ePolicy Orchestrator agent deployed to each system, you must manually scan the system or system using the command-line scanner, or use another anti-virus product.



## SECTION 2

# Lab Evaluation

This section provides instructions for setting up a simple ePolicy Orchestrator implementation in a lab environment.

---

*[Installing and setting up](#)*

*[Advanced Feature Evaluations](#)*

# 8

## Installing and setting up

This section describes how to install and deploy ePolicy Orchestrator in a test environment. It provides easy steps to get ePolicy Orchestrator 3.6 up and running quickly, and presents important features of the product.

The steps, divided into two sections, are:

### **Installation and Setup**

- 1 *Install the ePolicy Orchestrator server and console.*
- 2 *Create your Directory of managed systems.*
- 3 *Deploy agents to the systems in your Directory.*
- 4 *Set up master and distributed repositories.*
- 5 *Set VirusScan Enterprise 8.0i policies before deploying.*

### **Maintaining and Monitoring your Environment**

- 6 *Deploy VirusScan Enterprise to client systems.*
- 7 *Run a report to confirm your coverage.*
- 8 *Update DAT files with a client update task.*
- 9 *Schedule automatic repository synchronization.*
- 10 *Test global updating with SuperAgents.*

### What is covered and what is not covered

This section of the guide does not cover everything that ePolicy Orchestrator can do, for example, many advanced features and installation scenarios typical in real-world deployments. For your live deployment, you can follow many of these basic steps, but you may need more information. For complete information on all aspects of the product, refer to the *ePolicy Orchestrator 3.6 Product Guide*.

What is covered	What is not covered	Comments
Setting up a single ePolicy Orchestrator server and console.	Setting up multiple ePolicy Orchestrator servers and remote consoles.	In a small test environment, one server is enough.
Running MSDE database on the same server as ePolicy Orchestrator.	Running SQL Server databases or remote database servers.	Using the MSDE database packaged with ePolicy Orchestrator is simpler for testing in a small lab network.
Using ePolicy Orchestrator to deploy agents and VirusScan Enterprise.	Using login scripts or third-party tools to deploy agents and VirusScan Enterprise.	Manually installing the agent is also covered.
Setting up a simple network environment with NT domains and Active Directory.	Setting up UNIX, Linux, or NetWare environments	These examples use NT domains and Active Directory to illustrate key product features.

## Setting up a lab environment

Before you install and test ePolicy Orchestrator, you must first create a safe test network. Planning and testing a live deployment is an involved process, especially in a large organization. However, you can create a small test environment in a matter of hours, and if you identify existing systems in your network for testing, the process takes even less time.

A test environment should contain:

- One server system to host the ePolicy Orchestrator server.
- One or more client systems (servers or workstations) to which you deploy agents and VirusScan Enterprise 8.0i.



See the *ePolicy Orchestrator 3.6 Installation Guide* and *VirusScan Enterprise 8.0i Installation Guide* for complete software and hardware requirements for the ePolicy Orchestrator server, the agent, and VirusScan Enterprise 8.0i.

## Configure your network?

Before setting up your test environment, ensure your network is correctly configured for ePolicy Orchestrator:

### 1 Create trusted domain connections to any remote NT domains.

To deploy the agent to systems outside the local NT domain (where the ePolicy Orchestrator server resides), you must create a trusted connection between the domains. This connection is required for the server to deploy agents and install software on remote systems. See your Microsoft Windows documentation for instructions. You must also have a user account with administrator rights in the remote domain.

## 2 Test network connectivity.

From the system where you plan to install the ePolicy Orchestrator server, ping client systems where you plan to deploy agents.

- On the server, open a command window (**Start | Run**) and type `cmd` at the prompt.
- Type `ping` commands to test the system name and IP address:

```
ping MyComputer
```

```
ping 192.168.14.52
```

## 3 Confirm that client NT Admin\$ share folders are accessible from the server.

From the system on which you plan to install the ePolicy Orchestrator server, test access to the default `Admin$` share folder on each client system. This access is required for the ePolicy Orchestrator server to install agents and other software, and testing confirms your administrator credentials.

- On the ePolicy Orchestrator server, open a command window (**Start | Run**).
- Type the path to the client `Admin$` share (use system name or IP address):

```
\\MyComputer\Admin$
```

```
\\192.168.14.52\Admin$
```

If systems are properly connected over the network, your credentials have sufficient rights, the `Admin$` share folder is present, and you see a Windows Explorer dialog box.

## 4 Install Microsoft updates on Windows 95, Windows 98, or Windows Me client systems.

If your test systems are running Windows 95, Windows 98, or Windows Me, download and install VCREDIST.EXE and DCOM 1.3 updates from the Microsoft web site, as required. ePolicy Orchestrator agents will not run on these systems without the update. See the *ePolicy Orchestrator 3.6 Installation Guide* or the following links for information:

[support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q259403&](http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q259403&)

[www.microsoft.com/com/dcom/dcom95/dcom1\\_3.asp](http://www.microsoft.com/com/dcom/dcom95/dcom1_3.asp)

## 5 Enable File and Print Sharing on Windows 95, Windows 98, or Windows Me client systems.

To deploy the agent to systems running Windows 95, Windows 98, or Windows Me, you must first enable **File and Print Sharing**. After the agent is deployed, you can disable **File and Print Sharing** and still be able to manage agent policies on those systems.



If you install the agent manually or through another method such as login scripts, this step is not required.

### About the sample lab environment

The lab environment used in these examples consists of one NT domain and one Active Directory container, each with several servers and several workstations.

Having multiple NT domains or Active Directory containers in your lab environment is not required to test ePolicy Orchestrator.

**Table 8-1 Systems in Domain1 (IP addresses 192.168.14.1-255)**

System	Details
ePO Server	Windows 2000 Server SP 4 running SQL Server 2000 SP 3. This system hosts the ePolicy Orchestrator server, console, database, and master software repository.
4 clients	Running Windows 2000 Professional.

**Table 8-2 Systems in Domain2 (IP addresses 192.168.15.1-255)**

System	Details
2 servers	Windows 2000 Server SP 4.
3 clients	Running Windows 2000 Professional.

### Get installation files from McAfee

Before you start installing, get the installation files for ePolicy Orchestrator and VirusScan Enterprise from the McAfee web site or your product CD, if you have one. If you want to use the 30-day evaluation versions for your tests, download them from the McAfee web site. The files you need are:

- **EPO360EML.ZIP.** The installation files necessary for installing the ePolicy Orchestrator 3.1 server, console, and database.
- **VSE800EEN.ZIP.** The VirusScan Enterprise 8.0i installation files, including the PkgCatalog.z package file required to deploy VirusScan Enterprise through ePolicy Orchestrator.
- **VSC451Lens1.ZIP.** The VirusScan 4.5.1 installation files and PkgCatalog.z file. You only need VirusScan 4.5.1 if you have client systems running Windows 95, Windows 98, or Windows ME, because VirusScan Enterprise 8.0i does not run on these operating systems.

To download the files from the McAfee web site:

- 1 From the system on which you plan to install the ePolicy Orchestrator server and console, open a web browser and go to:

<http://www.mcafeesecurity.com/us/downloads/evals/>

- 2 Select **ePolicy Orchestrator Enterprise Edition 3.6** from the list and click the **TRY** link.
- 3 Fill out the form and follow directions to download the EPO360EML.ZIP file.
- 4 Extract the contents of the EPO360EML.ZIP to a temporary folder, such as C:\ePOTemp.
- 5 Repeat these steps to download the VSE80iEVAL.ZIP evaluation version of VirusScan Enterprise 8.0i and the VSC451Lens1.ZIP of VirusScan 4.5.1.
- 6 Extract the contents of the downloaded .ZIP files into a temporary folder on the system you plan to use as your test ePolicy Orchestrator server.

You need to access files in these folders at various times during the deployment process covered in this guide.

## STEP

## 1

## Install the ePolicy Orchestrator server and console

Install the ePolicy Orchestrator server, console, and database on the system you plan to use as your ePolicy Orchestrator server. In the examples used in this guide, we install the ePolicy Orchestrator server to the system called *ePOServer* that is running the Windows 2000 Server operating system.

To install the ePolicy Orchestrator console and server:

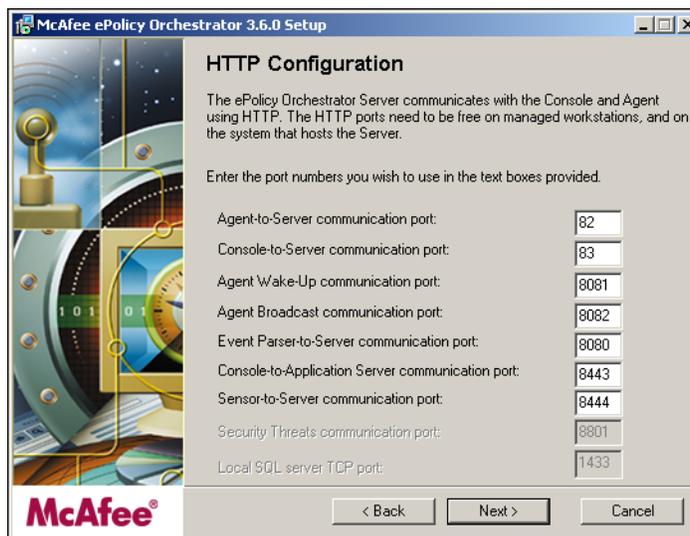
- 1 Locate and start the SETUP.EXE file located in the root of the folder where you extracted the EPO360EML.ZIP.
- 2 Click **Next** at the initial page of the **ePolicy Orchestrator 3.6.0 Setup** wizard.
- 3 If you are installing an evaluation version, click **OK** at the **Evaluation** page.
- 4 Read the license agreement. If you agree to the terms select **I accept the terms in the license agreement**, then click **OK**. (If you don't agree, then click **Cancel** and quit the product evaluation.)
- 5 On **Installation Options**, select **Install Server and Console** and click **Next**. You can also change the installation folder if desired.
- 6 If you see a message box stating that your server does not have a static IP address, ignore it by clicking **OK**.

While McAfee recommends installing ePolicy Orchestrator on a system with a static IP address in your production environment, a DHCP-assigned IP address can be used for testing purposes.

- 7 On the **Set Administrator Password** dialog box, enter the password you would like to use for the ePolicy Orchestrator server. You cannot leave this blank.
- 8 On the **Select Database Server** dialog box, select **Install a server on this computer and use it**. This option installs the free MSDE database included with ePolicy Orchestrator.
- 9 Click **Next**.
- 10 On the **Database Server Account** dialog box, deselect **Use the same account as the Server service**, then select **This is a SQL Server account**. Type in and verify a secure password. This is the *sa* account that your ePolicy Orchestrator server service uses to access the MSDE database.
- 11 Click **Next** to save the database account information.

- 12 On the **HTTP Configuration** dialog box, change the **Agent-to-Server communication port** to **82** and the **Console-to-Server communication port** to **83**.

**Figure 8-1 HTTP Configuration dialog box**



Some HTTP ports (ports 80 and 81 in particular), are commonly used by many HTTP applications and services. Because of this, port 80 may already be in use and not available. McAfee recommends changing the port number to avoid any conflicts.

- 13 Click **Next** to save the port information.

If you do see a warning message saying that one or more HTTP ports are in use, click **OK** and repeat [Step 12](#), this time specifying unused HTTP ports.

- 14 On the **Set E-mail Address** dialog box, type the e-mail address to which the default notification rules send messages once they are enabled.

This e-mail address is used by the ePolicy Orchestrator Notifications feature. This feature is covered in this guide, so enter an e-mail address that receives messages you can view.

- 15 On the **Ready to Install** dialog box, click **Install** to begin the installation.

The installation takes approximately 20 minutes to complete and may prompt you to reboot the system during the installation.

- 16 Click **OK** when prompted to reboot and be sure to log back in when the system reboots to allow the installation to continue.

- 17 When the installation is finished, click **Finish**.

Once the installation is complete, you can open the ePolicy Orchestrator console to begin deploying agents and anti-virus products to the client systems in your network.

### Start the ePolicy Orchestrator console for the first time

Now your server is installed and running. Open the ePolicy Orchestrator console to begin using ePolicy Orchestrator to manage policies on your network.

To open the console from your ePolicy Orchestrator server:

- 1 Click the **Start** button, then select **Programs | McAfee | ePolicy Orchestrator 3.6.0 Console**.
- 2 On the **Start Page**, click **Log on to server**.
- 3 When the **Log on to Server** dialog box appears, make sure the **Server name** displays the name of your ePolicy Orchestrator server and that the **User name** is `admin`, type the **Password** you set during the installation wizard, then click **OK**.
- 4 If you have installed an evaluation version, click **OK** at the **Evaluation** splash screen.

Wait a few moments while the ePolicy Orchestrator server initializes. You are now ready to use the ePolicy Orchestrator console.

## STEP

# 2

## Create your Directory of managed systems

The Directory is in the console tree of the ePolicy Orchestrator console. The Directory lists all the systems in your network that are managed by ePolicy Orchestrator — all systems that are running active ePolicy Orchestrator agents that are reporting to this server.

Before you start managing anti-virus policies for client systems on your network, you must add those systems to your ePolicy Orchestrator Directory. After installing the server, you initially have one system in the Directory — the ePolicy Orchestrator server itself.

To organize your systems, you can group them into logical collections called *sites* and *groups*. You can create a hierarchy of sites and groups, much like you would create a hierarchy of folders in Windows Explorer. Grouping is useful for assigning policies and tasks. You can group systems according to any criteria that makes sense for your organization.

This guide uses three common types of grouping:

- **NT Domain.** Using your existing NT network domains as sites makes creating your Directory fast and easy. Having your Directory structure mirror your network structure can also mean you only have to remember one hierarchy, not two.
- **Active Directory containers.** Using your existing Active Directory network containers as sites makes creating your Directory fast and easy. Having your Directory structure mirror your network structure also means you only have to remember one hierarchy.
- **Servers and workstations.** You may want to configure separate policies for products like VirusScan Enterprise 8.0i, depending on whether the software is running on a server or a workstation. Dividing your Directory into groups is not required, especially for testing in a small lab environment. However, you can use groups to experiment with setting policies for groups of systems or for how you might want to organize your Directory.

Other typical methods of grouping include, but are not limited to:

- **Geographical divisions.** If you have locations in various portions of the world, or in multiple time zones, you may want to divide your ePolicy Orchestrator Directory according to those divisions. Some of your policy or task coordination is much easier across multiple time zones if you place these systems in such sites.
- **Security divisions.** If users have various levels of security access in your environment, creating your Directory structure to mirror those levels may make enforcing policy much easier.

## 1 Add systems to your Directory

The first step in creating your Directory is to add systems from your network. Try one of these three methods:

- *Option A: Automatically add entire existing NT domains to your Directory.* Very easy and fast. Useful if you plan to deploy agents to every system in that domain. Use this method if you organized your test client systems into domains in your lab network, as in the examples in this guide.
- *Option B: Automatically add entire Active Directory containers to your Directory.* Very easy and fast. Useful if all or part of your environment is controlled by Active Directory and if you want portions of your ePolicy Orchestrator Directory to mirror portions of your Active Directory.
- *Option C: Manually add individual systems to your Directory.* While this may be too slow when deploying ePolicy Orchestrator in a live network, it is fast enough for adding a handful of systems in your test network.

### Option A: Automatically add entire existing NT domains to your Directory

ePolicy Orchestrator allows you to import all systems in an NT domain into your **Directory** with just a few clicks. Use this feature if you organized your test client systems into domains in your lab network.

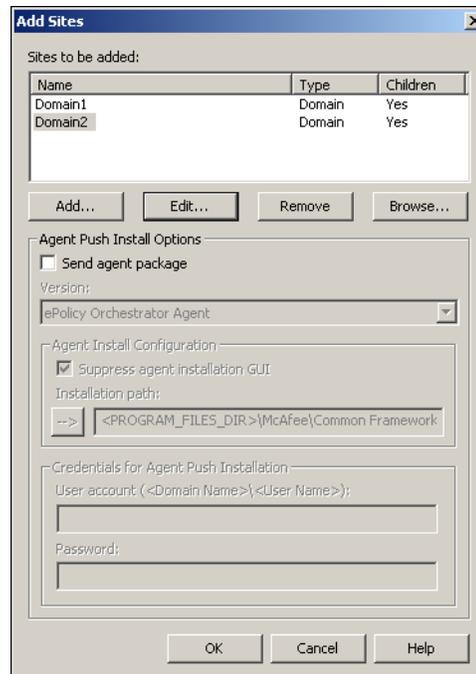
The examples in this guide use this method to create **Directory** sites from an NT domain on the test network, **Domain1**.

To add entire NT domains to your **Directory**:

- 1 Right-click the **Directory** and select **New | Site**.
- 2 In the **Add Sites** dialog box, click **Add**.
- 3 In the **New Site** dialog box, type a name for the site. Make sure the name you type matches exactly the name of your NT domain.
- 4 Under **Type**, select **Domain** and **Include computers as child nodes**.
- 5 Click **Add** under **IP Management** to specify an IP address range for the site.
- 6 In the **IP Management** dialog box, type an IP subnet mask or IP range to specify the IP address ranges of systems that belong to this site.
- 7 Click **OK** to save the IP settings.
- 8 Click **OK** to save the new site and close the **New Site** dialog box.

- 9 In the **Add Sites** dialog box, make sure that **Send agent package** is NOT selected and click **OK** to create and populate the sites in the Directory. Although you can deploy agents at this point, you will do that in a later step once we have modified the agent policy settings.

**Figure 8-2 Add Sites dialog box**



After a few moments, the systems are added to your Directory. When completed, you can see that ePolicy Orchestrator first created a site in the Directory with the name of your network test domain and added all the systems in that domain as children of that domain.

### Option B: Automatically add entire Active Directory containers to your Directory

ePolicy Orchestrator allows you to import all systems in an Active Directory container, and its sub-containers, into your Directory with just a few clicks. Use this feature if you organized your test client systems into Active Directory containers in your lab environment.

The examples in this guide use this method to create Directory sites from an Active Directory container, with two sub-containers.



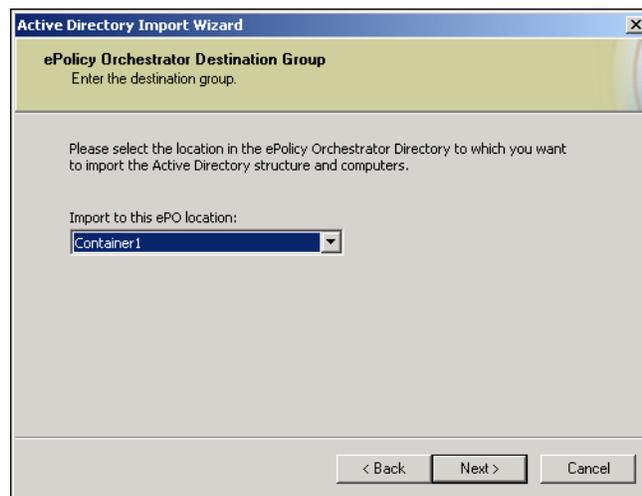
To use ePolicy Orchestrator software's Active Directory tools, it is important that both the ePolicy Orchestrator server and the system running the console (if different) can reach the Active Directory server.

The **Active Directory Import** wizard is a tool to import Active Directory systems for the first time, while you create the entire Directory, or only a specific site of the Directory. Use the **Active Directory Discovery** task to poll these Active Directory containers regularly for any new systems.

To add Active Directory containers and sub-containers to your Directory:

- 1 Right-click **Directory**, and select **New | Site**.
- 2 In the **Add Sites** dialog box, click **Add**.
- 3 In the **New Site** dialog box, type a name for the site, for example **Container1**, then click **OK**.
- 4 Make sure that **Send agent package** is NOT selected, then click **OK**.
- 5 Right-click **Directory**, and select **All Tasks | Import Active Directory Computers**.
- 6 Click **Next** when the **Active Directory Import** wizard appears.

**Figure 8-3 Active Directory Import wizard**



- 7 On the **ePolicy Orchestrator Destination Group** panel of the wizard you can select the root or a site of the Directory to import the Active Directory systems.

For the purposes of this guide, select the site you just created from the **Import to this ePO location** drop-down list, then click **Next**.



If you want to import your entire Active Directory structure, minus exceptions, to use as your ePolicy Orchestrator **Directory**, select **Root** from this list. This results in the Active Directory structure, minus exceptions, being imported into the Lost&Found of the **Directory** root.

- 8 On the **Active Directory Authentication** panel, type Active Directory user credentials with administrative rights for the Active Directory server.
- 9 In the **Active Directory Source Container** dialog box, click **Browse** to select the desired source container in the **Active Directory Browser** dialog box, then click **OK**.
- 10 If you wish to exclude a specific sub-container of the selected container, click **Add** under **Exclude the following sub-containers**, then select the desired sub-container to exclude and click **OK**.
- 11 Click **Next**, and view the active log for any new systems that have been imported. Verify in the console tree that these systems were imported.

**12** Click **Finish**.

The Active Directory systems have been imported into the Lost&Found group of the site to which you imported them. If your Active Directory container included sub-containers, the Lost&Found group retains the Active Directory hierarchy.

**13** Click and drag the top of this structure from the Lost&Found group, to the site above it. (The site you selected in the wizard. For example **Container1**.)

Congratulations. You have imported your Active Directory systems into a site in the ePolicy Orchestrator **Directory**.

In a production environment, once Active Directory containers have been imported, you should create an **Active Directory Discovery** task. This task regularly polls administrator-specified Active Directory containers for any new systems, and for systems that have been removed. See the *ePolicy Orchestrator 3.6 Product Guide* for instructions. This task is beyond the scope of this guide.

### Option C: Manually add individual systems to your Directory

When you deploy ePolicy Orchestrator in your production network, consider populating the Directory automatically by importing your NT domains or Active Directory containers as shown in the previous sections. However, for testing purposes in a small lab environment, you can also add sites, groups to your Directory manually, then add systems to them manually.

**To create a new site manually:**

- 1 Right-click **Directory** node in the console tree and select **New | Site**.
- 2 In the **Add Sites** dialog box, click **Add**.
- 3 Type a name for the site, such as *Domain1* in our example, into the **Name** field of the **New Site** dialog box.
- 4 Specify an IP mask or address range for the site if needed. See the previous section for details.
- 5 Click **OK**. The *Domain1* site is added to the **Sites to be added** list on the **Add Sites** dialog box.
- 6 Repeat the previous steps to create additional sites, if desired.
- 7 Click **OK**. ePolicy Orchestrator adds the new, empty sites to the Directory.

**To add new systems to your site:**

- 1 In the console tree, right-click the site you added and select **New | Computer**.
- 2 In the **Add Computers** dialog box, add new systems either by clicking **Browse** to locate them in your NT Network Neighborhood, or by clicking **Add** and typing the system's NetBIOS name.
- 3 Click **OK** once you have added the names of all the systems.

ePolicy Orchestrator adds the new systems to the Directory beneath the site.

## 2 Organize systems into groups for servers and workstations

Depending on how you've created your sites, and populated the Directory, you may need to create additional groups and to further levels of organization in your Directory. For example, by operating system.

The example in this guide creates groups in each site for servers and workstations. Use these groups later when setting different VirusScan Enterprise policies for servers and workstations.



The VirusScan Enterprise 8.0i policy pages for ePolicy Orchestrator 3.6.0 allow you to set separate policy settings for servers and workstations without creating these groups. However, grouping systems by operating system is a conceptually simple way to illustrate how using Directory groups can make managing policies easier. If needed, create other kinds of groups that better fit your test network or policy management needs.

### To add groups to sites in your Directory and add systems to them:

- 1 Right-click a site that you added to the **Directory** and select **New | Group**.
- 2 In the **Add Groups** dialog box, click **Add**.
- 3 On the **New Group** dialog box, type the name `workstations` into the **Name** text box.
- 4 If your network is designed to allow you to assign specific IP addresses to servers and workstations, create an IP range for the group. For example, in the test network shown in this guide, servers in Domain1 have IP addresses between 192.168.14.200 - 255; workstations in Domain1 have addresses 192.168.14.1 - 199.



You must also set an IP mask at the parent site. The IP mask or IP range that you set for the group must be consistent with the IP range specified at the site level. In the examples used in this guide, the workstations and servers in Domain1 all fit within the 192.168.14.0/24 subnet.

Also note that IP management is not necessary for Active Directory systems.

### To set an IP range for a group:

- a Under **IP Management** on the **New Group** dialog box, click **Add**.
  - b In the **IP Management** dialog box, type an IP subnet mask or IP range to specify the IP address ranges of systems that belong to this site.
  - c Click **OK** to save the IP settings and close the **IP Management** dialog box.
- 5 Click **OK** to close the **New Group** dialog box. The group is added to the **Groups to be added** list.
  - 6 Click **OK** on the **Add Groups** dialog box to add the group to your **Directory**.

### To add systems to the new groups you created:

Once the new groups appear in the Directory, drag systems from that site into the appropriate group as you would drag files in Windows Explorer. You must drag systems in the Directory one at a time; you cannot select multiple systems. Alternatively, you can use the Directory search feature (right-click **Directory** and select **Search**) to move multiple systems at one time.

While dragging systems into groups, ignore the **IP Integrity warning** message if you see it by clicking **OK**.

**To create additional groups and subgroups as needed:**

Repeat all these steps to create a server group for your site, as well as additional server and workstation groups for other sites, if you have them. You can also make groups within groups. For example, the test network shown in this guide has systems running both Windows 2000 and Windows 98. Due to limitations with older versions of Windows, we need to set different policies for systems running Windows 98. Creating *Win98* and *Win2K* subgroups within our Workstation group makes setting these different policies easier.

Now your test Directory is finished. You have created sites and added systems, either manually or by importing existing NT domains on your network. And you have separated the systems in each site into separate groups for servers and different types of workstation operating systems. You're ready for the next step—deploying agents.

STEP

3

## Deploy agents to the systems in your Directory

Before you can manage the client systems in your Directory, you must install an ePolicy Orchestrator agent on each client system. The agent is a small application that resides on the client system and periodically checks in with the ePolicy Orchestrator server for updates and new instructions.

Deploying the agent from the ePolicy Orchestrator server requires the following:

- **A network account with administrator privileges.** You must specify administrator credentials when you deploy agents.
- **Domain trusts to other NT domains, if necessary.** To deploy agents outside the local NT domain that hosts your ePolicy Orchestrator server, you must have a domain trust relationship configured between the local and target domains.
- **For Windows 95 and Windows 98 systems, install extra Microsoft updates.** Windows 95 and Windows 98 first edition require that you install additional Microsoft updates to be able to run the ePolicy Orchestrator agent. See the *ePolicy Orchestrator 3.6 Installation Guide* for information on finding and installing these updates. You must install these updates to run the agent on these systems at all, even if you do not use ePolicy Orchestrator to deploy it.
- **For Windows 95 and Windows 98 systems, turn on file and print sharing.** Enable file and print sharing on each client to which you plan to deploy the agent. Note that this is only a requirement to deploy the agent from the ePolicy Orchestrator server, not to manage policies. Once you have deployed the agent to a Windows 95 or Windows 98 system, you can disable file and print sharing.
- **For Windows 95 and Windows 98 systems, agent installation completes at next logon.** After deploying the agent installation package to systems running these operating systems, the installation does not complete until the next time the system logs on to the network.

From the Directory in the console tree, you can install the agent on each system in a site at once. To do this, send an agent install command to the site. Because of inheritance, you can specify an agent installation at the parent site (or group) level and all child nodes inherit the command.

Initiate separate agent installations to separate sites of your Directory. These two agent installation commands install the agent to all systems in these sites.

To deploy agents to a site:

- 1 [Configure the agent policy settings before deployment.](#)
- 2 [Deploy agents.](#)

Alternatively, if you do not plan to use ePolicy Orchestrator to deploy the agent, you can install the agent manually from the client system. See [Installing agent manually on client systems on page 94](#).

## 1 Configure the agent policy settings before deployment

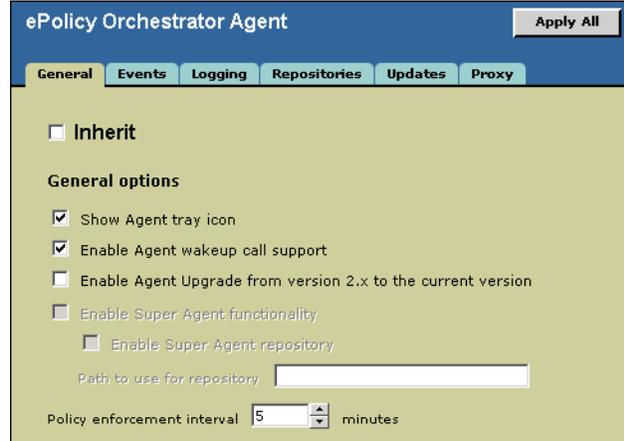
You can deploy agents with the default policy settings. However, for testing purposes, modify the policy settings to allow the agent tray icon to display in the Windows system tray on the client system. Not only will this expose you to setting agent policies, it also makes it easier to see when the agent has installed on your client systems. When you make this policy change at the site level, it applies to all test systems within this site. This allows you to configure the policy settings once then deploy it to all your systems within a site.

**To change the agent policy settings so that the agent icon appears in the system tray after installation:**

- 1 In the console tree, select the desired site.
- 2 In the details pane, select the **Policies** tab, then open **ePO Agent 3.5.0** from the list of products.
- 3 Click **Edit** at the right end of the **Configuration** row.
- 4 Select **New Policy** from the **Policy Name** drop-down list. The **Create new policy** dialog box appears.
- 5 Provide a **New policy name** for the policy (for example, `New Agent Policy`), then click **OK**. The **Policy Settings** dialog box appears.

- On the **General** tab, select **Show Agent tray icon**.

**Figure 8-4 General tab**



- Click **Apply All**, then click **Close**. The new policy is created and added to the **Policy Catalog** page.
- Click **Apply** at the end of the **Configuration** row on the **Assign Policies** page to assign the new policy to the site selected in the console tree.

**To assign the new policy to another Directory node:**

- In the console tree, select the desired Directory node to which you want to assign the new policy.
- In the details pane, select the **Policies** tab, then open **ePO Agent 3.5.0** from the list of products.
- Click **Edit** at the right end of the **Configuration** row.
- Select the name of the new policy (for example, `New Agent Policy`) from the **Policy Name** drop-down list.
- Click **Apply**.

Now your policies are set and your agents are ready to deploy. The next step is to begin an agent install.

## 2 Deploy agents

Use the **Send Agent Install** feature to deploy agents to your client systems. Deploy agents to all your test systems in a site at once by initiating the agent installation at your site level in the Directory.

To initiate an agent installation for all systems in a site:

- In the console tree, right-click the desired site, then select **Send Agent Install**.
- Provide credentials with administrator rights on the target systems for the agent installation.
- Click **OK** on the **Install Agent** dialog box to accept all default settings and begin the agent installation.

- 4 Repeat these steps for other sites.

The agent installations begin immediately.

## Deploying agents to systems running Windows 95, Windows 98, or Windows Me

When deploying agents to systems running Windows 95, Windows 98, or Windows Me remember that the installation does not complete until the next time the system logs back onto the network. If, after logging off and back into the Windows 95, Windows 98, or Windows ME client systems, the agent still does not appear, wait 10 minutes, then try deploying it again. If that still does not work, you can install the agent manually at the client system (see [Installing agent manually on client systems on page 94](#)).

## Deploying to systems outside the local NT domain

If the other site(s) contain systems residing in a different NT domain than your ePolicy Orchestrator server, you may need to specify other domain administrator credentials for the target domain.

Before deploying the agent, deselect **Use ePO server credentials** on the **Install Agent** dialog box, and type an appropriate user name and password with domain administrator rights in the target domain.

## Monitoring the agent installations

It may take up to 20 minutes for all the agents to be installed on all systems in your test sites, and for the console tree to update with the new covered status. In the meantime, you can check the ePolicy Orchestrator server for events, which can alert you of failed agent installations. To view server events:

- 1 In the console tree of the ePolicy Orchestrator console, right-click your server and select **Server Events**.
- 2 Skim the **Server Event Viewer** for events. Successful agent installations are not displayed here, but failed installs are.

When agent deployment is complete and the agents have called back to the server for the first time, the systems in your Directory are marked with green checks.

If the agents have installed and the Directory does not reflect this, manually refresh the Directory by right-clicking Directory and selecting **Refresh**. Note that the Directory does not show the systems as managed until they call back to the server, usually within 10 minutes. This is true even though the agent is installed and running on the client systems.

You can also watch the installation from any of your client systems. The default policy suppresses the installation interface (which we did not change when we set agent policies in this example). So you cannot see the installation interface. However, you can open the Task Manager on the client system and watch the CPU usage spike briefly as the installation begins. Once the agent is installed and running, two new services appear in the **Processes** window: `UPDATERUI.EXE` and `FRAMEWORKSERVICE.EXE`. Also, because of how we modified the agent policies before deploying, the agent icon appears in the system tray after installing and reporting back to the server.

---

## Installing agent manually on client systems

Rather than use ePolicy Orchestrator to deploy the agent, you may want to install it manually at the client system. Some administrators may want to install software on client systems manually and use ePolicy Orchestrator to manage policies only. Or, maybe you have many Windows 95 or Windows 98 client systems and do not want to enable print and file sharing on them. In these cases, you can install the agent at the client instead.

Use the FRAMEPKG.EXE file located on your ePolicy Orchestrator server to install the agent. The FRAMEPKG.EXE file is automatically created when you install the ePolicy Orchestrator server. It contains address information for your ePolicy Orchestrator server to allow the new agent to communicate with the server immediately.

By default, FRAMEPKG.EXE is located in the following folder on your ePolicy Orchestrator server:

```
C:\Program Files\Mcafee\ePO\3.6.0\DB\Software\Current\  
EPOAGENT3000\Install\0409
```

### To install the agent manually:

- 1 Copy the FRAMEPKG.EXE file to the local client or network folder accessible from the client.
- 2 Run FRAMEPKG.EXE by double-clicking it. Wait a few moments while the agent installs.

At some random interval within ten minutes, the agent reports back to the ePolicy Orchestrator server for the first time. At this point, the system is added to the Directory as a managed system. If you specified IP address filtering for your Directory sites and groups, the client is added to the appropriate site or group for its IP address. Otherwise, the system is added to the Lost&Found group. Once the system is added to the Directory, you can manage its policies through the ePolicy Orchestrator console.

You can bypass the ten-minute callback interval and force the new agent to call back to the server immediately. You do this from any system on which an agent has just been installed.

To manually force the initial agent callback:

- 1 From the client system where you just installed the agent, open a DOS command window by selecting **Start | Run**, type `command`, and press **Enter**.
- 2 In the command window, navigate to the agent installation folder containing the CMDAGENT.EXE file.
- 3 Type the following command (note the spaces between command line options):

```
CMDAGENT /p /e /c
```

- 4 Press ENTER. The agent calls into the ePolicy Orchestrator server immediately.
- 5 From the ePolicy Orchestrator console on your server, refresh the Directory by pressing F5. The new client system on which you installed the agent should now appear in your Directory.

## STEP

## 4

## Set up master and distributed repositories

Now you have agents installed on your client systems, but what can they do? The purpose of an agent is to allow you to manage client security software policies centrally through ePolicy Orchestrator. But until you have security software installed on the client systems, your agents have nothing to do. The next step is to use ePolicy Orchestrator to deploy VirusScan Enterprise 8.0i anti-virus software to your client systems.

Software deployed with ePolicy Orchestrator is stored in software repositories. There are many ways to set up your repositories. This guide demonstrates a typical example that you can use in your test environment.

### About using master and distributed repositories in your test network

ePolicy Orchestrator uses repositories to store the software that it deploys. This section illustrates using both master and distributed repositories for deploying software and updating. Repositories store the software, such as the agent or VirusScan installation files, and updates, such as new virus definition (DAT) files, that you plan to deploy to client systems. The master repository is located on the ePolicy Orchestrator server, and is the primary storehouse for your software and updates. Distributed repositories are copies of the master that reside in other parts of your network. Systems in those other parts of your network can update more quickly from local servers than across a WAN to your ePolicy Orchestrator server.

Domains and Active Directory containers can be geographically separated and connected via a WAN. In this case, create a distributed repository, which is simply a copy of the master repository, on a system in the remote location. Systems in that location, **Container1** in our example, can update from the distributed repository instead of having to copy updates across the WAN.

Systems in the **Domain1** site receive updates and product deployments directly from the master repository, located on the ePolicy Orchestrator server. Systems located in the **Container1** site, however, receive them from a distributed repository.

Use the following procedure for using and setting up repositories in your test environment:

- 1 [Add VirusScan Enterprise to the master repository.](#)
- 2 [Pull updates from McAfee source repository.](#)
- 3 [Create a distributed repository.](#)

## 1 Add VirusScan Enterprise to the master repository

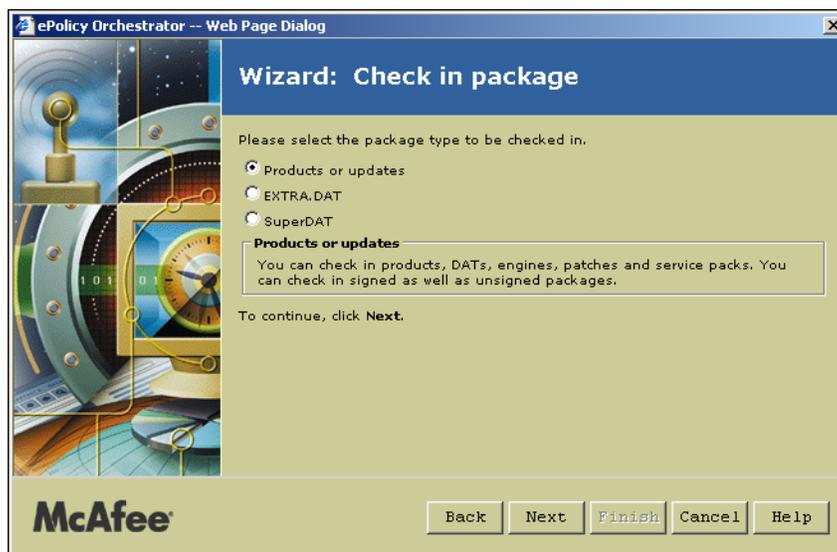
The VirusScan Enterprise 8.0i NAP file, allows you to manage VirusScan Enterprise 8.0i policies once it has been installed on client systems in your network. However, to be able to first use ePolicy Orchestrator to deploy VirusScan Enterprise 8.0i to those client systems, you must also check in the VirusScan Enterprise deployment, or installation, package to the master software repository. The deployment package file is called PKGCATALOG.Z and is contained in the VSE80IEVAL.ZIP you downloaded from McAfee (see [Get installation files from McAfee on page 81](#)).

### To check in the VirusScan Enterprise 8.0i package to your master repository:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Check in Package**. The **Check in package** wizard appears.

- 3 Click **Next**.
- 4 On the second page of the wizard, select **Products or updates**, then click **Next**.

**Figure 8-5 Check in Package wizard**



- 5 Browse to your temporary folder containing your VirusScan Enterprise 8.0i installation files.
- 6 Locate and select the PKGCATALOG.Z package file, then click **Next**.
- 7 At the final wizard page, click **Finish** to begin the package check-in.

Wait a few moments while ePolicy Orchestrator uploads the package to the repository.

**To check in the VirusScan 4.5.1 package (for Windows 95, Windows 98, or Windows ME client systems):**

VirusScan Enterprise 8.0i does not run on Windows 95, Windows 98, or Windows ME. If you have client systems in your test network running these versions of Windows, deploy VirusScan 4.5.1 to these systems. To do this, repeat the same procedure above to check in the VirusScan 4.5.1 deployment package to the software repository. The 4.5.1 package is also called `PkgCatalog.z` and is located in your temporary folder to which you have extracted the VirusScan 4.5.1 installation files.

## 2 Pull updates from McAfee source repository

Use the McAfee HTTP or FTP site as your source repository, from which you can update your master repository with the latest DAT and engine files. Initiate a pull from the source repository to your master repository to:

- Test that your ePolicy Orchestrator server can connect over the Internet to the source repository.
- Update your master repository with the latest DAT files.

DAT files are updated often, and the DAT files included in your VirusScan Enterprise installation files are not the latest. Pull the latest DAT files from the source repository before deploying VirusScan Enterprise to your network.

**To configure proxy settings:**

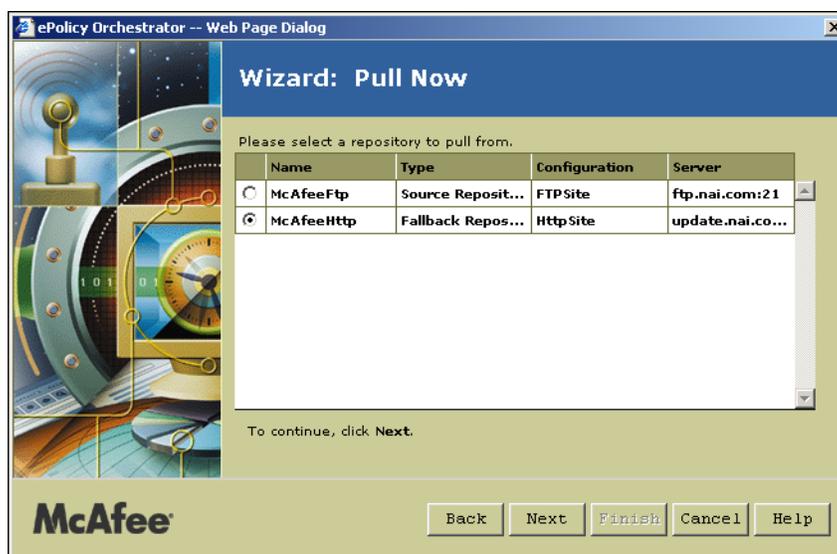
Your ePolicy Orchestrator server must be able to access the Internet to pull updates from the McAfee source repository.

ePolicy Orchestrator by default uses your Internet Explorer proxy settings. If you have not yet done so, configure your LAN connection for Internet Explorer. Be sure to select the **Use proxy for all protocols (both FTP and HTTP)** and select **Bypass proxy for local addresses** options.

Alternatively, you can manually specify proxy server information using the **Configure proxy settings** option. Refer to the *ePolicy Orchestrator 3.6 Product Guide* for information on how to do this.

**To initiate manual pull from the McAfee source repository:**

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Pull now**. The **Pull Now** wizard appears.
- 3 Click **Next**.
- 4 Select **McAfeeFtp**, then click **Next**.

**Figure 8-6 Pull Now wizard**

- 5 If you are managing older products, such as VirusScan 4.5.1 for Windows 95 or 98 systems, be sure to select **Support legacy product update**.
- 6 Click **Finish** to accept all defaults on this page and begin the pull task. The Server Task Log appears.
- 7 Monitor the task status until it completes.

Now you have checked in VirusScan Enterprise to your master repository and also updated the master repository with the latest DAT and engine files from the McAfee source repository. The systems located in the same domain as your ePolicy Orchestrator server, those systems in your **Domain1** site in the Directory in this example, get VirusScan Enterprise from the master repository.

But where do other systems get their software and updates? If these systems are located in different subnets or a WAN-connected location, it may be more efficient to create a distributed repository that is more easily accessible to these systems.

### 3 Create a distributed repository

Now we need to create a distributed repository for **Container1** so that those systems can update from there. Your test network, with only a few client systems and one ePolicy Orchestrator server, is small enough to not require a distributed repository structure. However, you can use the distributed repository examples in this guide to simulate a probable real-world scenario. Such a scenario could include systems in remote domains that cannot update efficiently over a WAN-connected master repository on the ePolicy Orchestrator server.

You can use FTP, HTTP, or UNC to replicate data from the master repository to your distributed repositories. This guide describes creating a UNC share distributed repository on one of the systems in the **Container1** site.

To do this:

- 1 *Create a shared folder on the system to use as a repository.*
- 2 *Add the distributed repository to the ePolicy Orchestrator server.*
- 3 *Replicate master repository data to distributed repository.*
- 4 *Configure remote sites to use the distributed repository.*

#### 1 Create a shared folder on the system to use as a repository

Before you add the UNC distributed repository to ePolicy Orchestrator, you must first create the folder to use. In addition, you must set the folder to enable sharing across the network so that your ePolicy Orchestrator server can copy files to it.

To create a shared folder for a UNC distributed repository:

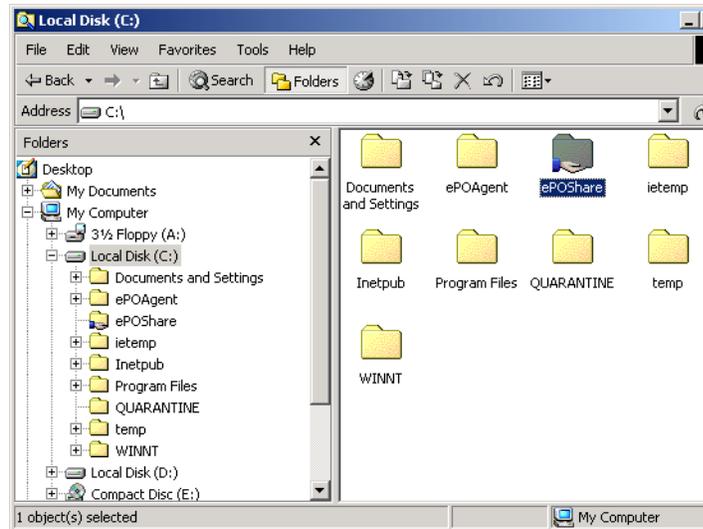
- 1 From the system on which you plan to host the repository, create a new folder using Windows Explorer.
- 2 Right-click the folder and select **Sharing**.
- 3 On the **Sharing** tab, select **Share this folder**.

- 4 Click **OK** to accept all other defaults and enable sharing for this folder.



Creating a UNC share in this way could be a potential security problem in a production environment, because it allows everyone on your network access to the share. If creating a UNC folder in a production environment, or if you are not sure that your network test environment is secure, be sure to take extra security precautions as necessary to control access to the shared folder. Client systems only require read access to retrieve updates from the UNC repository, but administrator accounts, including the account used by ePolicy Orchestrator to replicate data, require write access. See your Microsoft Windows documentation on how to configure security settings for shared folders.

**Figure 8-7 Microsoft Explorer**



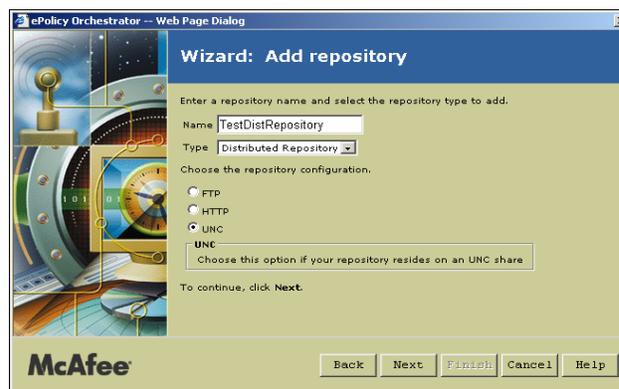
## 2 Add the distributed repository to the ePolicy Orchestrator server

Once you have created the folder to use as the UNC share, add a distributed repository to the ePolicy Orchestrator repository and point it at the folder you created.

To add the distributed repository:

- 1 From the console tree, click **Repository**.
- 2 Select **Add distributed repository** from in the details pane **Repository** pane.
- 3 Click **Next** at the first page of the wizard.

- 4 Type a **Name**. Note this is the name that appears in the repository list in the ePolicy Orchestrator console. It does not need to be the same as the name of the shared folder that actually hosts the repository.

**Figure 8-8 Add repository wizard**

- 5 Select **Distributed Repository** from the **Type** drop-down list.
- 6 Select **UNC** for the repository configuration and click **Next**.
- 7 Type the path of the shared folder you created. Be sure to type a valid UNC path.
- 8 Click **Next**.
- 9 On the download credentials page, deselect **Use Logged On Account**.
- 10 Type appropriate domain, user name, and password credentials that client systems should use when downloading updates from this distributed repository.
- 11 Click **Verify** to test the credentials. After a few seconds, you should see a confirmation dialog box confirming that the share is accessible to client systems.  
  
If your site is not verified, check that you typed the UNC path correctly on the previous wizard page and that you configured sharing correctly for the folder.
- 12 Click **Next**.
- 13 Enter replication credentials by typing a domain, user name and password in the appropriate text boxes.  
  
The ePolicy Orchestrator server uses these credentials when it copies, or replicates, files from the master repository to the distributed repository. These credentials must have administrator rights in the domain where the distributed repository is located. In our examples, these can be the same credentials used to deploy the agent. See [Deploy agents on page 92](#).
- 14 Click **Verify** to test that your ePolicy Orchestrator server can write to the shared folder on the remote system. After a few seconds, you should see a confirmation dialog box confirming that the server can do this.
- 15 Click **Finish** to add the repository. Wait a few moments while ePolicy Orchestrator adds the new distributed repository to its database.
- 16 Click **Close**.

### 3 Replicate master repository data to distributed repository

Now you have created a UNC share on a system to host a distributed repository, and added the repository location to your ePolicy Orchestrator database. Now, all that is missing in the new repository is data. If you browse to your share folder you created, you can see that it is still empty.

Use the **Replicate now** feature to manually update your distributed repositories with the latest contents from your master repository. Later, we'll schedule a replication task so this happens automatically.

To initiate replication manually:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, click **Replicate now**. The **Replicate Now** wizard appears.
- 3 Click **Next**.
- 4 From the list of available distributed repositories, select the distributed repository you have created, then click **Next**.
- 5 Select **Incremental replication**.

Because this is a new distributed repository, and this is the first time you are replicating to it, you could also select **Full replication**. However, for future replications, it is recommended to use incremental replication to save time and bandwidth.

- 6 Click **Finish** to begin replication. The Server Task Log appears.
- 7 Monitor the status of the task until it completes.

If you browse to your `ePOShare` folder now, you can see that it now contains subfolders for agents and software.

### 4 Configure remote sites to use the distributed repository

Since you have created a distributed repository, why not make sure it gets used? Your test network is too small to really require distributed repositories. But for the sake of simulating how they work, we can configure your updating to force systems in one site to update only from the distributed repository instead of the master.

To simulate this in your test, let's configure the agent policies for one of the sites to use only the new distributed repository. In our example network used in this guide, this is the **Container1** site, which is where the system hosting your newly-created distributed repository resides.

To configure the ePolicy Orchestrator agent policy for the **Container1** site to use the distributed repository for updating:

- 1 In the console tree, select the site whose systems that you want to use the distributed repository.
- 2 In the details pane, select the **Policies** tab, then open **ePO Agent 3.5.0** from the list of products.
- 3 Click **Edit** at the right end of the **Configuration** row.
- 4 Select **New Policy** from the **Policy Name** drop-down list. The **Create new policy** dialog box appears.

- 5 Select **Duplicate the following policy**, then select the policy you created earlier (to display the agent system tray icon) from the drop-down list.
- 6 Provide a **New policy name** for the policy (for example, `New Agent Policy--custom repository`), then click **OK**. The **Policy Settings** dialog box appears.
- 7 Select the **Repositories** tab, then deselect **Inherit**.
- 8 Under **Repository selection**, select **User defined list**.
- 9 In the **Repository list**, deselect all repositories until only your distributed repository is selected.
- 10 Click **Apply All**, then click **Close**.
- 11 Click **Apply** at the end of the **Configuration** row on the **Assign Policies** page to assign the new policy to the site selected in the console tree.

Now, when the systems in this site require updates, they retrieve them from the distributed repository.

Again, forcing updates from certain repositories is shown here only for the purposes of simulating distributed repositories in a lab network. This is not something you would do in a production environment, where you would want to have some repository redundancy available for fail-over. Due to faster local network connections, client systems would likely update from a local distributed repository, rather than over a WAN to the master repository, even if not specifically configured to do this. On the other hand, if the distributed repository were unavailable for any reason, the client could still update from other repositories on the network if necessary.

## STEP

# 5

## Set VirusScan Enterprise 8.0i policies before deploying

Now that you have created your repositories and added the VirusScan Enterprise deployment package to them, you are almost ready to deploy VirusScan Enterprise to your client systems. Before deploying VirusScan Enterprise, however, let's modify the policies slightly. Remember the NAP file you checked in? We can use it to configure how VirusScan Enterprise functions once it is installed on the client system. To demonstrate, we'll use a simple example: changing the policies for workstations to install VirusScan Enterprise 8.0i with minimal user interface. Servers keep the default policy, which is to display the full interface.

This could be a potentially useful implementation in your real network, where you may want to hide the system tray interface on your workstations to prevent end-users from easily changing policies or disabling features.

To set these policies, we'll use the **Workstations** groups created when you made your Directory. You can change the policy once for each workstation group (within **Domain1** and **Container1**) to have it inherit to all systems within those groups. For servers, we can leave the default policy, which installs VirusScan Enterprise with the full menu options available in the system tray.

To change the VirusScan Enterprise policies for workstations:

- 1 In the console tree, select your workstations group.
- 2 In the details pane, select the **Policies** tab.
- 3 Select **VirusScan Enterprise 8.0.0**, then click **Edit** at the end of the **User Interface Policies** row.
- 4 Select **New Policy** from the **Policy Name** drop-down list. The **Create new policy** dialog box appears.
- 5 Provide a **New policy name** for the policy (for example, `Workstation UI`), then click **OK**. The **Policy Settings** dialog box appears.
- 6 Select **Workstation** from the **Settings for** drop-down list at the top of the page.



The **Settings for** drop-down list allows you to set separate policies for servers and workstations without using Directory groups. ePolicy Orchestrator detects the operating system on the client system and applies the right policy. However, for testing purposes, it can be useful to create server and workstation groups.

- 7 Deselect **Inherit** to enable user interface policy options.
- 8 Select **Show the system tray icon with minimal menu options**.
- 9 Click **Apply**, then click **Close**.
- 10 Click **Apply** at the end of the **Configuration** row on the **Assign Policies** page to assign the new policy to the site selected in the console tree.
- 11 Repeat these steps for any other workstation groups in your Directory.

## STEP

# 6

## Deploy VirusScan Enterprise to client systems

You have created master and distributed repositories, added the VirusScan Enterprise 8.0i PKGCATALOG.Z file to your master repository, and replicated this to a new distributed repository. Your systems are added to your Directory and they all have ePolicy Orchestrator agents installed on them. You've defined your VirusScan Enterprise policies for servers and workstations. You are now ready to have ePolicy Orchestrator deploy VirusScan Enterprise on all the client systems in your test network.

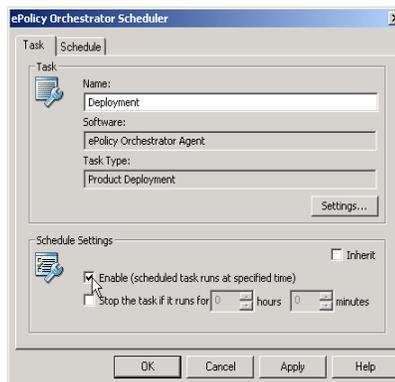
Unlike deploying agents, which must be done at the site, group, or system level, you can deploy VirusScan Enterprise from the Directory level of the console tree to install it on all the systems in your Directory at once. Note that whatever policies you have set for specific sites or groups within your Directory, such as the **Servers** and **Workstations** groups in this example, still apply when VirusScan Enterprise is installed to client systems within those groups. Alternatively, you can deploy VirusScan Enterprise to sites, groups, or individual systems — the procedure is the same.

### To deploy VirusScan Enterprise 8.0i to all systems in the Directory:

- 1 In the console tree, select Directory.
- 2 In the details pane, select the **Task** tab, then double-click the Deployment task in the task list. The **ePolicy Orchestrator Scheduler** appears.

- 3 Click the **Task** tab and deselect **Inherit** under **Schedule Settings**.

**Figure 8-9 ePolicy Orchestrator Scheduler dialog box**



- 4 Under **Schedule Settings**, select **Enable (scheduled task runs at specified time)**.
- 5 Click the **Settings** button.
- 6 On the **Deployment** page, deselect **Inherit** to enable product deployment options.
- 7 Set the **Action** for the **VirusScan Enterprise 8.0i** deployment task to **Install**.
- 8 Click **OK** to save the product deployment options and return to the **ePolicy Orchestrator Scheduler** dialog box.
- 9 On the **ePolicy Orchestrator Scheduler** dialog box, click the **Schedule** tab.
- 10 Deselect **Inherit** to enable scheduling options.
- 11 From the **Schedule Task** drop-down list, select **Run Immediately**.
- 12 Click **OK** to save your changes.

In the task list on the **Tasks** tab of the details pane, the **Enabled** status for the deployment task is set to **True**.

You have now configured your default deployment task to install VirusScan Enterprise on all client systems in your test site. The deployment occurs the next time the agents call back to the ePolicy Orchestrator server for updated instructions. You can also initiate an agent wakeup call to have the deployment occur immediately. See [Send an agent wakeup call to force agents to call back immediately on page 105](#).

#### **To deploy VirusScan 4.5.1 to Windows 95, Windows 98, or Windows ME systems:**

If you have any Windows 95, 98, or ME systems in your test network, you can repeat the steps in this section to deploy VirusScan 4.5.1 to these systems only. Make sure you have already checked the VirusScan 4.5.1 deployment package into the repository. Deploying VirusScan 4.5.1 to several systems is easiest if you have organized your Windows 95, Windows 98, or Windows ME systems into a group in your Directory, but you can also run the deployment task for individual systems too.

- 1 In the console tree, select the desired group or system.
- 2 In the details pane, select the **Task** tab, then double-click the Deployment task in the task list. The **ePolicy Orchestrator Scheduler** appears.

- 3 Click the **Task** tab and deselect **Inherit** under **Schedule Settings**.
- 4 Under **Schedule Settings**, select **Enable (scheduled task runs at specified time)**.
- 5 Click the **Settings** button.
- 6 On the **Deployment** page, set VirusScan 4.5.1 to **Install**.
- 7 Complete the steps to configure the deployment. ePolicy Orchestrator deploys VirusScan 4.5.1 the next time the agents on these systems call back to the server.

## Send an agent wakeup call to force agents to call back immediately

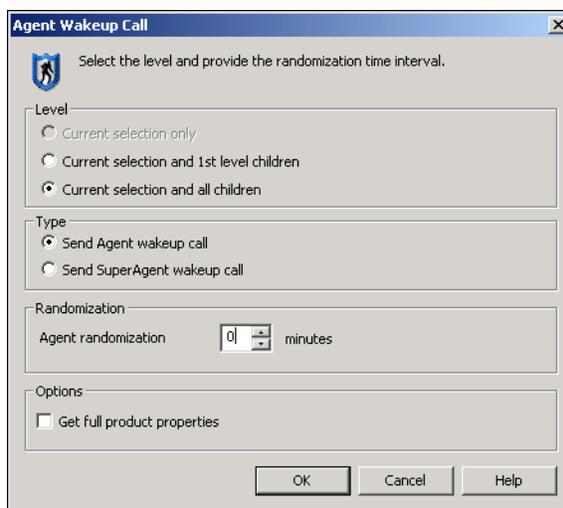
If you want, you can send the agents an immediate agent wakeup call. This forces the agents to check in immediately with the ePolicy Orchestrator server, rather than wait for the next regularly scheduled agent callback, which by default could be as long as 60 minutes. When the agents call back, they see that the VirusScan Enterprise deployment is set to install rather than ignore. The agents then pull the VirusScan Enterprise `PkgCatalog.z` file from the repository and install VirusScan Enterprise. Note that each agent pulls the `PkgCatalog.z` file from whichever repository it is configured to. In our example test network, the systems in the **Domain1** site pull from the master repository and systems from **Container1** pull from the distributed repository we created.

You can send an agent wakeup call to any site, group, or individual system in your Directory. Since we want to wake up all systems in the Directory, we'll initiate one wakeup call for each site, which inherit down to groups and systems within that site.

### To send an agent wake-up call to begin VirusScan Enterprise deployment immediately:

- 1 Right-click the target site in the console tree and select **Agent Wakeup Call**.
- 2 Set the **Agent randomization** to 0 minutes.

Figure 8-10 Agent Wakeup Call dialog box



- 3 Click **OK** to accept all other defaults and send the wakeup call.
- 4 Repeat these steps for other sites in your Directory.

The agents call back immediately, retrieve the new deployment policy changes, and begin installing VirusScan Enterprise. Wait a few minutes while VirusScan Enterprise 8.0i is deployed and installed.

**To verify that the software has successfully installed on client systems check one of the following:**

- Run a *Product Protection Summary* report.
- The MCSHIELD.EXE process is running and visible in the **Processes** tab of your **Windows Task Manager**.
- A VirusScan folder is added to your `Program Files/McAfee` folder.
- As long as you did not change the policy to hide it, the VShield icon appears in the system tray next to the agent icon. You may need to reboot to display the system tray icon. Note that VirusScan is active and running even if the VShield icon has not yet displayed in the system tray.

**STEP****7**

## Run a report to confirm your coverage

Run a *Product Protection Summary* report to confirm that your VirusScan Enterprise deployment was successful. Note that you may need to wait an hour before the database has been updated with the new status.

To run a *Product Protection Summary* report:

- 1 In the console tree, select **Reporting | ePO Databases | ePO\_ePOServer**. ePOServer is the name of the ePolicy Orchestrator database used in this example.
- 2 If you are prompted to log into the database, type your MSDE user name and password that you created when installing the console and database.
- 3 Select **Reports | Anti-Virus | Coverage | Product Protection Summary**.
- 4 Select **No** when prompted to set a data filter. Wait a moment while ePolicy Orchestrator generates the report.

Once the report has generated, the results should show the number of servers and workstations on which VirusScan 4.5.1 and VirusScan Enterprise 8.0i are currently installed. If you later deploy other products, such as McAfee Desktop Firewall, they show up in this report as well.

**STEP****8**

## Update DAT files with a client update task

One of the most common things you will want to do with ePolicy Orchestrator is update DAT files. VirusScan Enterprise by default performs an update task immediately after installing. So, if you followed the steps in this section to configure your repositories and pulled the latest DAT files to your master repository before deploying, VirusScan Enterprise is up-to-date shortly after being deployed.

Once VirusScan Enterprise is installed, however, update DAT files frequently. Your anti-virus software is only as good as its latest DAT files, so it is essential to keep them up-to-date. In a later section in this guide, you will see how to schedule a regular automatic client update task to occur regularly, such as daily or weekly. For now, let's assume you want to initiate an immediate DAT file update. You will likely be required to do this at some point; for example, if McAfee releases updated DAT files in response to a newly-discovered virus and you want your client systems to update without waiting for their regularly scheduled task.

To do this, create and run a client update task from your ePolicy Orchestrator console. This forces all your client anti-virus software to perform an update task.

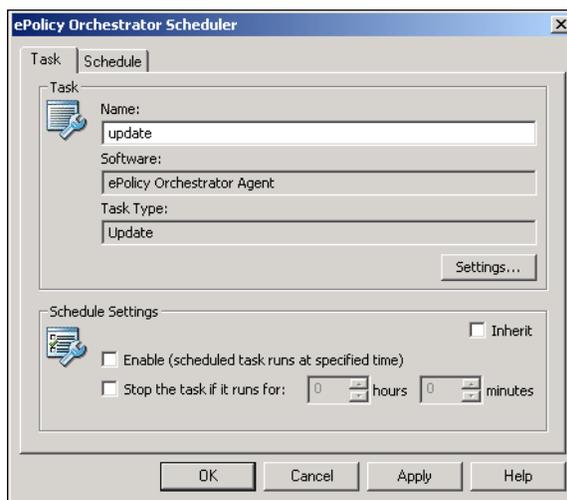


Before you run a client update task, make sure you have first pulled any updated DAT or engine files into your master and distributed repositories, if you have them. See [Set up master and distributed repositories on page 95](#).

To create and run a client update task:

- 1 In the console tree, right-click **Directory | All Tasks | Schedule task**.
  - 2 In the **Schedule Task** dialog box, type a name into the **New Task Name** field, such as **Update client DATs**.
  - 3 In the software list, select **ePolicy Orchestrator Agent | Update** for the task type.
  - 4 Click **OK**.
  - 5 Go to the **Tasks** tab in the details pane, then press **F5** to refresh the console and make the new task appear in the list on the **Task** tab.
- Note that it is scheduled to run daily at the current day and time. Also note that the **Enabled** flag is set to **False**—we now need to set this to **True** and run it immediately.
- 6 Right-click the new task in the task list and select **Edit Task**.
  - 7 Deselect **Inherit** under the **Schedule Settings** section of the **ePolicy Orchestrator Scheduler** dialog box.

**Figure 8-11 ePolicy Orchestrator Scheduler dialog box**



- 8 Select **Enable**.
- 9 Click **Settings**, then deselect **Inherit** on the **Update** tab.
- 10 Ensure that **This task updates only the following components** is selected. This selection allows you to specify which components you want to update. Specifying these allows you to save network resources by limiting which updates are distributed in your environment.
- 11 Leave the default selections under **Signatures and Engines**.
- 12 Under **Patches and Service Packs**, select **VirusScan Enterprise 8.0**, then click **OK**.
- 13 Click the **Schedule** tab and deselect **Inherit**.
- 14 Set the **Schedule Task** option to **Run Immediately** and click **OK**.
- 15 Initiate agent wakeup calls to all sites in your Directory so your agents call in immediately to pick up the agent update task. See [Send an agent wakeup call to force agents to call back immediately](#) on page 105.

#### How can I tell that VirusScan Enterprise has actually updated to the latest DATs?

First, check the DAT version that is currently checked into your master repository. These are the DATs that should now be on your client systems after they updated. To do this:

- 1 From the console tree, select the ePolicy Orchestrator server, then select the **General** tab.
- 2 Under **MyAVERT Security Threats**, check which DAT file version is **Current in Repository**. This should be a 6-digit number like **4.0.4576**.

Next, check the DAT versions used by client software, such as VirusScan Enterprise, from the ePolicy Orchestrator console. Note that the console does not show the updated status until the next time the agent calls into the server as part of its regular agent-to-server communication. To do this:

- 1 In the console tree, select any system that has recently been updated.
- 2 In the details pane, select the **Properties** tab, then select **VirusScan Enterprise 8.0i | General** to expand the list of general properties.
- 3 Check the **DAT Version** number. It should match the latest DAT version in your master software repository.

## STEP

# 9

## Schedule automatic repository synchronization

In just a few hours, you now have a fully-functional installation of ePolicy Orchestrator deployed in your test network. You have agents deployed to client systems, and these agents are active and calling back to the server for updated instructions regularly. You've also used ePolicy Orchestrator to deploy VirusScan Enterprise to your client systems, and have created a small software repository that you can use to deploy updates and additional software to your client systems.

The next step is to schedule regular pull and replication tasks to synchronize your source, master, and distributed repositories so that all your repositories are up-to-date. Then create a scheduled client update tasks to make sure client software such as VirusScan Enterprise checks regularly for updated DAT and engine files.

To do this:

- 1 [Schedule a pull task to update master repository daily.](#)
- 2 [Schedule a replication task to update your distributed repository.](#)
- 3 [Schedule a client update task to update DATs daily.](#)

## 1 Schedule a pull task to update master repository daily

Pull tasks update your master software repository with the latest DAT and engine updates from the source repository. By default, your source repository is the McAfee web site. Let's create a scheduled pull task to pull the latest updates from the McAfee web site once per day.

To schedule a pull task:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Schedule pull tasks** to open the **Configure Server Tasks** page.
- 3 Select **Create task** to open the **Configure New Task** page.

Figure 8-12 Configure New Task page

- 4 Type a name into the **Name** field, such as `Daily Repository Pull task`.
- 5 Select **Repository Pull** from the **Task type** drop-down menu.
- 6 Make sure **Enable task** is set to **Yes**.
- 7 Select **Daily** from the **Schedule Type** drop-down list.
- 8 Schedule the day and time for the task to run.

- 9 Click **Next** at the top of the page.
- 10 Select **NAIHttp** in the **Source repository** drop-down list.
- 11 Leave the destination branch set to **Current**.
- 12 If you have older versions of McAfee products, such as VirusScan 4.5.1, in your test network, select **Support Legacy product update**.
- 13 Click **Finish**. Wait a moment while the task is created.

The new pull task is added to the **Configure Server Tasks** page.

## 2 Schedule a replication task to update your distributed repository

Using your new pull task, your ePolicy Orchestrator server is configured to automatically update the master repository with the latest updates from the source repository on the McAfee web site. The task runs once a day and keeps your master repository current.

But an up-to-date master repository won't be of any use to those client systems on your network that get their updates from a distributed repository, such as the systems in the **Container1** site in our sample test network. The next step, therefore, is to make sure the updates added to your master repository are also automatically replicated to your distributed repository. To do this, create a replication task and schedule it to occur every day after the scheduled pull task you already created.

To schedule a replication task:

- 1 In the console tree, select **Repository**.
- 2 In the details pane, select **Schedule pull tasks** to open the **Configure Server Tasks** page.
- 3 Select **Create task** to open the **Configure New Task** page. This is the same page that you used to schedule your automatic pull task.
- 4 Type a **Name**, such as `Daily Distributed Repository Replication task`.
- 5 Select **Repository Replication** from the **Task type** drop-down menu.
- 6 Make sure **Enable task** is set to **Yes**.
- 7 Select **Daily** from the **Schedule Type** drop-down list.
- 8 Schedule the day and time for the task to run. Make sure you set the time for the task to at least five minutes after the pull task is scheduled.
- 9 Click **Next** at the top of the page.
- 10 Select **Incremental replication** and click **Finish**. Wait a moment while the task is created.

The new replication task appears in the **Configure Server Tasks** table along with your scheduled pull task.

## 3 Schedule a client update task to update DATs daily

After all your repositories have been updated, schedule a client update task to make sure that VirusScan Enterprise gets the latest DAT and engine updates as soon as they are in your repositories.

You can use the client update task you created earlier after you deployed VirusScan Enterprise (see [Update DAT files with a client update task on page 106](#)). Simply modify the schedule of this task from **Run Immediately** to **Daily** and set the start time to run about an hour after your replication task begins.

## STEP

## 10

## Test global updating with SuperAgents

Global updating can automatically update all your client systems every time you check new updates into your master repository. Every time you change your master repository, ePolicy Orchestrator automatically replicates the contents to any distributed repositories you have. Then it alerts all agents deployed in your network that have managed products, such as VirusScan Enterprise 8.0i, to perform an immediate update task.

The global updating feature is useful in a virus outbreak situation. Assume that McAfee's AVERT team has posted updated DAT files in response to a newly-discovered virus. With global updating enabled, you simply initiate a pull task from your ePolicy Orchestrator console to update your master software repository with the new DAT files. ePolicy Orchestrator's global updating feature does the rest—updating the DAT files for all systems running active, communicating agents on your network within an hour.

---

## Use SuperAgents to wake up all agents on the network

ePolicy Orchestrator uses something called a SuperAgent to initiate the global update. SuperAgents are ePolicy Orchestrator agents that can also wake up other agents located in the same network subnet. When you have a SuperAgent installed in each network subnet, you send a SuperAgent wakeup call to your SuperAgents, and then the SuperAgents send wakeup calls to the ePolicy Orchestrator agents in the same subnet. The regular agents can then call back to the ePolicy Orchestrator server for policy instructions and update client software.



SuperAgents can also act as distributed repositories. These SuperAgent repositories use a proprietary McAfee replication protocol called SPIPE, and can either replace or augment other HTTP, FTP, or UNC distributed repositories you have created. This guide does not cover SuperAgent repositories, however. Refer to the *ePolicy Orchestrator 3.6 Product Guide* for information on SuperAgent repositories.

To enable global updating:

- 1 [Convert an agent on each subnet into a SuperAgent.](#)
- 2 [Enable global updating on ePolicy Orchestrator server.](#)

## 1 Convert an agent on each subnet into a SuperAgent

You can turn any regular ePolicy Orchestrator agent into a SuperAgent. Use the ePolicy Orchestrator Agent policy pages to do this. Since you only need one SuperAgent per network subnet, be sure to configure SuperAgents for individual systems in your Directory, and not for whole groups or sites as you did when deploying agents or VirusScan Enterprise.

For example, in the sample test network used in this guide, we would convert one agent into a SuperAgent in the **Domain1** site.

To do this:

- 1 In the console tree, select a desired system to host the SuperAgent. In a production environment, you would want to select a system that is likely to be up and running all the time.
- 2 In the details pane, open **ePO Agent 3.5.0**.
- 3 Click **Edit** at the right end of the **Configuration** row.
- 4 Select **New Policy** from the **Policy Name** drop-down list. The **Create new policy** dialog box appears.
- 5 Select **Duplicate the following policy**, then select the policy you created earlier (to display the agent system tray icon) from the drop-down list.
- 6 Provide a **New policy name** for the policy (for example, *SuperAgent Policy*), then click **OK**. The **Policy Settings** dialog box appears.
- 7 On the **General** tab, select **Enable SuperAgent functionality**.
- 8 Click **Apply All**, then click **Close**.
- 9 Click **Apply** at the end of the **Configuration** row on the **Assign Policies** page to assign the new policy to the site selected in the console tree.

You can also create a SuperAgent repository on the system, but they are not required for global updating and are not covered in this guide. See the *ePolicy Orchestrator 3.6 Product Guide* for information on SuperAgent repositories.

- 10 Click **Apply All** to save the policy changes.
- 11 Right-click the system in the **Directory** and select **Agent Wakeup Call**.
- 12 Set **Agent Randomization** to **0** and click **OK**.
- 13 Repeat these steps if you have systems in other network subnets.

Wait a few moments while the SuperAgent is created.

You can use these SuperAgents to wake up other agents in the local subnet. This can save bandwidth, especially in a large network with many remote, WAN-connected sites. Send out wakeup calls to a few SuperAgents and let them wake up the other agents in the local LAN.

## 2 Enable global updating on ePolicy Orchestrator server

Global updating is a feature that you can turn on or off from the ePolicy Orchestrator console. When turned on, selected changes to your master repository trigger an automatic replication to distributed repositories, if any, followed by a SuperAgent wakeup call to your entire Directory. The SuperAgents in turn wake up agents in their local subnets.

To enable on global updating:

- 1 In the console tree, select your ePolicy Orchestrator server.
- 2 In the details pane, select the **Settings** tab.
- 3 At the bottom of the **Server Settings** page, set **Enable global updating** to **Yes**.
- 4 For the purposes of this evaluation change the **Global updating randomization interval** to 1 minute.
- 5 Leave the default selections under **Signatures and Engines**.
- 6 Under **Patches and Service Packs**, select **VirusScan Enterprise 8.0**.
- 7 Click **Apply Settings** to save the change.

Now that you have SuperAgents deployed to subnets your network and global updating enabled, any time you change the DAT files, engine files, or VirusScan Enterprise 8.0i files in your master repository, the changes automatically replicate to your repositories. Once that replication is completed, the ePolicy Orchestrator server sends a SuperAgent wakeup call to the SuperAgents. The SuperAgents in turn send out a wakeup call to all agents in the local subnet. Those agents check in with the server and download policy changes. From checking in the changes to your master repository to your last client system receiving its update, this process should take no longer than one hour.

### STEP

## 11

### Where to go from here?

By now you have had a chance to explore most of the major features of ePolicy Orchestrator 3.6.0. But there is also much more you can do with ePolicy Orchestrator and VirusScan Enterprise. Please refer to the *ePolicy Orchestrator 3.6 Product Guide*, the *VirusScan Enterprise 8.0i Product Guide*, and the *VirusScan Enterprise 8.0i Configuration Guide* for complete information on advanced product features. These and other helpful resources are available for download from the McAfee web site.

# 9

## Advanced Feature Evaluations

This section of the *guide* demonstrates how you can configure and use two of the advanced features not covered in the previous section:

- [ePolicy Orchestrator Notification](#).
- [Rogue System Detection](#) on page 118.

---

### ePolicy Orchestrator Notification

Real-time information about threat and compliance activity on your network is essential to your success.

You can configure rules in ePolicy Orchestrator to notify you when user-specified threat and compliance events are received and processed by the ePolicy Orchestrator server. The ability to set aggregation and throttling controls on a per rule basis allows you to define when, and when not, notification messages are sent.

Although you can create any number of rules to notify you of almost any threat or compliance event sent by your security programs, the focus in this guide on this feature is more narrow, centering on an e-mail notification message in response to a virus detected event.

In this section of the guide, you will:

- 1 [Configure Notifications](#).
- 2 [Create a rule for any VirusScan Enterprise event](#).
- 3 [Providing a sample virus detection](#).

STEP

1

### Configure Notifications

Before setting up any rules, you must define who is going to receive the notification message, in which format, and what the message communicates:

- 1 Click **Notifications** in the console tree, then select the **Configuration | Basic Configuration** tab in the details pane.

**Figure 9-1 Basic Configuration**

**Basic Configuration**

Note: Not all events are immediately forwarded by the ePO agent. You can use the Events tab Agent policy page to control the balance between immediate notification of events and network information, see the [online help](#).

**UI Related**

Number of items to view per page:	<input type="text" value="10"/>
Auto Refresh delay:	<input checked="" type="checkbox"/> 30 <input type="text"/> Seconds <input type="button" value="v"/>
Site administrators/reviewers can view Directory rules/notifications:	<input checked="" type="checkbox"/>
Site administrators can edit E-mail Contacts, SNMP Servers, and External Commands:	<input checked="" type="checkbox"/>

**E-mail Server**

Mail server:	<input type="text" value="localhost"/>
From:	<input type="text" value="alerting@example.com"/>
<input type="button" value="Send a Test E-mail"/>	

- 2 Under **E-mail Server**, type the name of a mail server to which the ePolicy Orchestrator server can route, and the desired e-mail address that you want to appear in the **From** line of the message.



When you decide which e-mail address to place here you should consider the number of administrators who may receive notification messages, and whether you want these administrators to be able to send reply messages.

- 3 Click **Apply**, then click **E-mail Contacts** at the top of the tab. This page allows you to specify all of the addresses to include in the address book from which you will select recipients during rule creation.

There should be one contact in the list already, **Administrator**. The e-mail address provided for **Administrator** is the e-mail address you entered in the **Set E-mail Address** panel of the installation wizard. If you did not change the default address in the wizard, the address is **Administrator@example.com**. If the address for **Administrator** is one that you are not able to view the mail sent to it, then click the address and change it to one at which you can receive and view e-mail messages.



From the **Configuration** tab you can also define SNMP servers at which you'd like to receive SNMP traps and external commands that you want to run when certain events are received. These tasks are beyond the scope of this guide. For more information, see the *ePolicy Orchestrator 3.6 Product Guide*.

Now that you've specified an e-mail server to be used to send the message, and an address to receive the message, you are ready to create a rule to trigger on a VirusScan Enterprise event.

STEP

2

## Create a rule for any VirusScan Enterprise event

You can create a variety of rules to handle nearly any category of events that are received from your managed security products. For more information, see the *ePolicy Orchestrator 3.6 Product Guide*.

- 1 Click the **Rules** tab, then click **Add Rule** to begin the **Add or Edit Notification Rule** wizard.
- 2 On the **Describe Rule** page, leave the default (**Directory**) for the **Defined At** text box. You can define rules for the **Directory** or any site within the **Directory**.
- 3 Provide a name for the rule in the **Rule Name** text box. For example, **Virus Detected**.
- 4 Provide a description of the rule in the **Description** text box. For example, **Viruses detected by VirusScan Enterprise**, then click **Next**.
- 5 On the **Set Filters** page:
  - a Leave all **Operating systems** checkboxes selected.
  - b Under **Products**, select **VirusScan**.
  - c Under **Categories**, select **Any category** above the list, then click **Next**.

So far the configurations you've made specify the rule to apply to any VirusScan event occurring on any managed system within the **Directory**.

Figure 9-2 Set Filters page



- 6 Although for this task you will leave the defaults on this page selected, the **Set Thresholds** page allows you to limit the number of notification messages you receive for the rule. For example, you can define any rule to send you messages only when the number of events or the number of affected systems have reached a specified number within a specified time frame (**Aggregation**). You can further limit the number of messages that are sent by specifying an amount of time to take place before receiving another message (**Throttling**). Throttling is almost always recommended by McAfee to prevent a flood of messages during an outbreak situation.

Figure 9-3 Set Thresholds page

**Add or Edit Notification Rule**

1. Describe Rule | 2. Set Filters | 3. Set Thresholds | 4. Create Notifications | 5. View Summary

For notification rule: **Daily unknown category notification**

You can use aggregation and throttling to limit the number of notifications you receive. Each sends a single notification that summarizes multiple events.

**Aggregation:**  Send a notification for every event

Send a notification for multiple events within: 5 Minutes

When the number of affected computers is at least: [input]

or

When the number of events is at least: [input]

**Throttling:**  At most, send notification every: 1 Days

Leave **Send a notification for every event** selected, and click **Next**.

- 7 On the **Create Notifications** page, click **Add E-mail Message**.
- 8 Click **Administrator** in the box on the left of the page, then click **To** so that **Administrator** moves to the **Notification Recipient(s)** box.
- This specifies that the e-mail address you configured (for the **Administrator** contact) is sent the notification message you are about to configure.
- 9 Type a **Subject** for the e-mail that will be sent to **Administrator** when this rule is triggered. For example, **Threat detected by VirusScan**.
- 10 Type a **Body** for the e-mail message that will be sent when this rule is triggered. For example, **VirusScan detected a threat**.

- 11 By inserting multiple variables into the body of the message, you can have meaningful information from the event files inserted into your notification message.

For the purpose of this section of the guide, select **Affected computer names** and click **Body**. This will place the name of the affected system, if available from the event file, in the body of the e-mail message. Click **Save**.

You can create multiple messages in multiple formats to send to multiple recipients, as well as choosing external commands to run, from the **Create Notifications** page. These are beyond the scope of this document. See the *ePolicy Orchestrator 3.6 Product Guide* for more information.

- 12 Click **Next** and verify the configurations you made to the rule you created on the **View Summary** page, then click **Finish**.

## STEP

## 3

## Providing a sample virus detection

Now that you have configured the feature and created a rule to trigger on event files from VirusScan Enterprise, you are ready to provide an event file that triggers the rule.

- 1 Download EICAR.COM to one of the workstation test systems. Each time you download this file, you are creating a sample detection, At press time, this file was available on the EICAR.ORG web site:

[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)



This file is *not* a virus.

- 2 The on-access scanner detects and quarantines the EICAR test virus at the same time that EICAR.COM is downloaded, and an event file capturing this information is sent to the ePolicy Orchestrator server.
- 3 Within minutes a notification message is created and sent to the inbox of the e-mail message recipient you provided earlier.

Congratulations! You successfully configured the product to send messages to a specific individual, created a rule to send a notification message based on events from VirusScan Enterprise, and tested the rule to ensure that it works.

---

## Rogue System Detection

In any managed network, at any given time, there are inevitably a small number of systems that do not have an ePolicy Orchestrator agent on them. These can be systems that frequently log on and off the network, such as test servers, laptop systems, or wireless devices. End users also uninstall or disable agents on their workstations. These unprotected systems are the Achilles heel of any anti-virus and security strategy and are the entry points by which viruses and other potentially harmful programs can gain access to your network.

The Rogue System Detection system helps you monitor *all* the systems on your network—not only the ones ePolicy Orchestrator manages already, but the rogue systems as well. A *rogue system* is any system that is not currently managed by an ePolicy Orchestrator agent but should be. Rogue System Detection integrates with your ePolicy Orchestrator server to provide real-time detection of rogue systems by means of a sensor placed on each network broadcast segment. The sensor listens to network broadcast messages and spots when a new system has connected to the network.

When the sensor detects a new system on the network, it sends a message to the Rogue System Detection server. The Rogue System Detection server then checks with the ePolicy Orchestrator server to determine whether the newly-identified system has an active agent installed and is managed by ePolicy Orchestrator. If the new system is unknown to ePolicy Orchestrator, Rogue System Detection allows you to take any number of remediation steps, including alerting network and anti-virus administrators or automatically deploying an ePolicy Orchestrator agent to the system.

In this section, you will:

- 1 [Configure Rogue System Detection sensor policy.](#)
- 2 [Deploy the Rogue System Detection sensor](#)
- 3 [Configure an automatic response.](#)
- 4 [Rogue detection and remediation.](#)

**STEP****4**

## Configure Rogue System Detection sensor policy

Before deploying the Rogue System Detection sensor, you should first configure the sensor policy.



These specific configurations to the sensor policy are only for the purpose of the evaluation. These are not recommended configurations for a production environment deployment of the sensor.

Once the sensor is deployed to a system in your environment, it requires one agent-to-server communication and one policy enforcement interval before it is functioning in the environment. The agent-to-server communication installs the sensor on the system in a disabled state. Then the policy enforcement retrieves policy, including security certificates. These certificates are needed by the sensor to communicate to the server directly.

The following configuration changes to the sensor policy speed up this process for this purpose of this guide.

- 1 In the console tree, select **Directory**.
- 2 In the details pane, select the **Policy** tab, then select **Rogue System Sensor 1.0.0**.
- 3 Click **Edit** at the right end of the **Configuration** row.
- 4 Select **New Policy** from the **Policy Name** drop-down list. The **Create new policy** dialog box appears.
- 5 Provide a **New policy name** for the policy (for example, `sensor1`), then click **OK**. The **Policy Settings** dialog box appears.
- 6 On the **General** tab, deselect **Inherit**, then under **Communication Intervals** make the following changes:
  - a Set **Minimum reporting interval for each detected host** to **120** seconds.
  - b Set **Minimum sensor-to-server communication interval for primary sensors** to **5** seconds.
- 7 Click **Apply All**, then click **Close**. The new policy is created.
- 8 Click **Apply** at the end of the **Configuration** row on the **Assign Policies** page to assign the new policy to the site selected in the console tree.

## STEP

## 5

## Deploy the Rogue System Detection sensor

The sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect the systems, routers, printers, and other network devices connected to your network. The sensor gathers information about the devices it detects, and forwards the information on to the Rogue System Detection server.

The sensor is a small Win32 native executable application. Similar to an ePolicy Orchestrator SuperAgent, you must deploy at least one sensor to each broadcast segment, usually the same as a network subnet, in your network. The sensor runs on any NT-based Windows operating system, such as Windows 2000, Windows XP, or Windows 2003.

For more information about the sensor and how it functions, see *Chapter 11: Rogue System Detection* in the *ePolicy Orchestrator 3.6 Product Guide*.

Depending on how you have your test environment set up, you may have more than one subnet represented in it. But you do have at least one.

To deploy the sensor:

- 1 In the console tree, select **Rogue System Detection**.
- 2 In the details pane, select the **Subnets** tab to display the **Subnet List**.
- 3 Select the subnets to which you want to deploy sensors by clicking once in the checkbox for that subnet, then click **Deploy Sensors**.

Figure 9-4 Subnet List page

<input type="checkbox"/>	Status	Address/Mask	Network Name	Sensors	Last Sensor Comm.
<input checked="" type="checkbox"/>	Uncovered	123.45.11.0/16	NetworkTest-X1	1	8/9/04 8:07:02 PM
<input type="checkbox"/>	Uncovered	123.45.5.0/16	NetworkServers-X1	1	8/9/04 8:07:03 PM
<input type="checkbox"/>	Uncovered	123.45.6.0/16	NetworkWorkstations-X1	1	8/9/04 8:07:03 PM
<input type="checkbox"/>	Uncovered	123.45.8.0/16	NetworkLaptops-X1	1	8/9/04 8:07:03 PM
<input type="checkbox"/>	Uncovered	123.45.9.0/16	NetworkHome Users-X1	1	8/9/04 8:07:04 PM
<input type="checkbox"/>	Uncovered	172.16.39.0/24	JBAILEY-WK6	0	

Checked subnets:

- 4 When the **Sensor Deployment: Set Preferences** page appears, ensure **Let me select machines manually** is selected.
- 5 Although we are not setting criteria for ePolicy Orchestrator to use to deploy sensors automatically, the availability of this criteria allows you to save time when trying to decide on which systems to install the sensors. This way, ePolicy Orchestrator finds the best systems on each subnet to install the sensors.

- 6 Click **Next**, then select the checkbox next to the desired system to which you want to deploy a sensor, click **Mark for Deployment**, then click **Next**. The **Sensor Deployment: Review and Approve** page appears.
- 7 Click **Finish**. The **Action Progress** page of the **Events** tab displays, indicating the progress of each sensor deployment.
- 8 Remember that you must wait until after one agent-to-server communication and one policy enforcement interval before the sensor calls into the server and is functioning. This can be expedited by sending agent wakeup calls:
  - a In the console tree, right-click the system on which you installed the sensor, then select **Agent Wakeup Call**.
  - b Set **Agent randomization** to **0**, then click **OK**.
  - c Wait two minutes, then repeat.
- 9 Once the **Action Status** is **Completed Successfully**, the sensor has called back to the server and is functioning.
- 10 Select the **Machines** tab and select **Summary** to view a summary of detected systems.

Now that the sensor is deployed and installed you are ready to configure a response for the feature to take on a rogue when one is detected.

## STEP

# 6

## Configure an automatic response

You can configure automatic responses for ePolicy Orchestrator to execute on rogue systems that are detected. There is a considerable amount of flexibility within this feature regarding the level of granularity available when defining the actions to take, and the conditions you can add to them. For complete information, see the *ePolicy Orchestrator 3.6 Product Guide*.

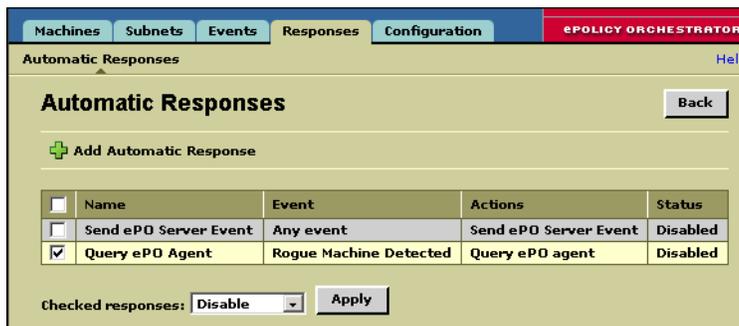
There are many situations where you may not want an automatic response to be taken. You can also set conditions around types of rogues where no actions are taken, or where the detected systems are simply marked for action.

For the purposes of this guide, you will configure a response that deploys an agent onto the rogue system once it has been discovered.

- 1 Select **Rogue System Detection** in the console tree, then select the **Responses** tab in the details pane.
- 2 Select the checkbox next to the default **Query ePO Agent** response, select **Disable** from the **Checked responses** drop-down list, then click **Apply**.

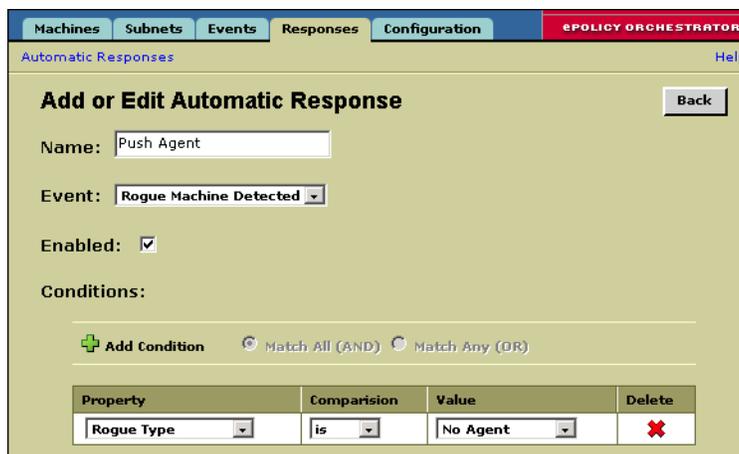
This response checks the detected system for an agent of another ePolicy Orchestrator server.

**Figure 9-5 Automatic Responses page**



- 3 Click **Add Automatic Response** to display the **Add or Edit Automatic Response** page.
- 4 Type a name for the response. For example, **Push Agent**.
- 5 Under **Conditions**, click **Add Condition**, then select **Rogue Type** from the **Property** list.

**Figure 9-6 Add or Edit Automatic Response page**



- 6 Select **is** for the **Comparison**, and **No Agent** for the **Value**.
- 7 Under **Actions**, change the default **Send E-mail** action to **Push ePO Agent** as the **Method**, and accept the default **Parameters**.
- 8 Click **OK**.
- 9 Select the checkbox next to the **Push Agent** automatic response when the **Automatic Responses** page reappears. Select **Enable** from the **Checked responses** drop-down list, then click **Apply**.

Now that the sensor is deployed, and a response has been created and enabled to handle rogues with no agent, you are ready to introduce such a rogue.

## STEP

## 7

## Rogue detection and remediation

Now you need to introduce a system into the test environment that does not have an agent. You can do this by several methods, such as joining a laptop to the test network, or by moving a system from an outside domain to the test domain you created earlier.

- 1 Add a system that does not have an ePolicy Orchestrator agent to the test network.
- 2 Go to the **Machine** tab, then click **List**. Once the sensor has detected a rogue system, it reports back to the server and places the system in the **Machine List**.
- 3 Once it appears in this list, take a five minute break to provide time for the agent installation.
- 4 Once the agent installation completes, the system has a **Rogue Type** of **Managed**.

You are not finished yet. You still must place the now managed system into its appropriate home in the **Directory**.

- 5 Once the system's **Rogue Type** changes to **Managed**, it is placed in **Directory | Lost&Found | Rogue Systems** of the console tree.

The **Lost&Found** group is a holding place for systems ePolicy Orchestrator has discovered, but doesn't know where to place within the **Directory**.

- 6 Click and drag the system to the desired site or group in your ePolicy Orchestrator **Directory**.

Congratulations! You successfully configured the sensor, deployed the sensor, configured an automatic response which you saw taken on the rogue you introduced, and placed the newly managed system into its appropriate spot in the **Directory**.