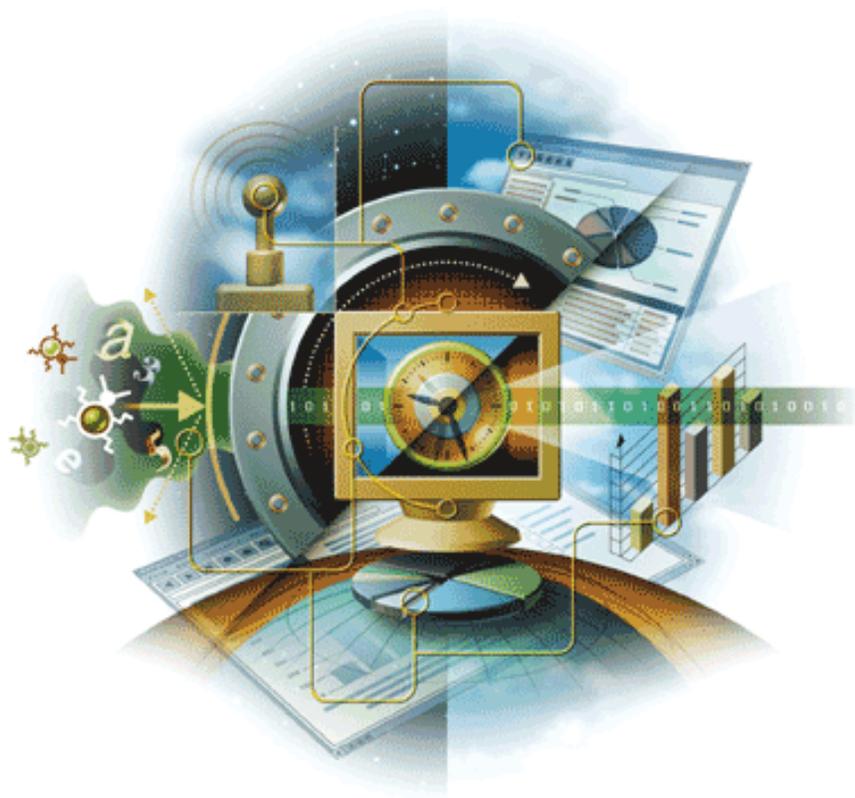


ePolicy Orchestrator

Reports and Queries

version 3.5



McAfee®
System Protection

Industry-leading intrusion prevention solutions



COPYRIGHT

Copyright © 2004 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Entercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Viruscan, Virusscan, Virusscan (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. 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.

PATENT INFORMATION

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

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.
- 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, © 1989.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems, Inc. © 2003.
- Software copyrighted by Gisle Aas. © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, © 1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martijn Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, © 2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Krempp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, © 2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Contents

1	Getting Started with Reporting	5
	About pre-defined reports in ePolicy Orchestrator	6
	How to generate a report in ePolicy Orchestrator	7
	Viewing report results in the report window	8
	Print or export reports into publishable formats	9
	Running Queries to get detail	10
	Saving filtered reports and queries as templates	10
	Writing custom reports in Crystal Reports	11
2	Reporting	12
	Reporting concepts	12
	Crystal Reports 8.5	13
	Authentication and user accounts	13
	Getting started with Reporting	14
	Specifying global reporting options	14
	Limiting report and query results by client computer	15
	Reporting	16
	Reporting options	16
	Running reports	17
	Working with reports in the report window	21
	Queries	25
	Running queries	25
	Report Repository maintenance	25
	Saving customized reports selections as report templates	26
	Adding a custom report templates	26
	Modifying report templates	27
	Deleting report templates	27
	Creating report groups	27
	Deleting report groups	27
	Adding report templates from new products to the Report Repository	28
	Query Repository maintenance	28
	Adding custom query templates	29
	Modifying query templates	30
	Deleting query templates	31
	Creating query groups	31
	Deleting query groups	31
3	ePolicy Orchestrator Databases and Reports	32
	Getting started with ePolicy Orchestrator databases	32
	User accounts and working with events	32
	Logging on to, off of, and removing ePolicy Orchestrator database servers	33
	Defining which events are stored in the database	36
	Reporting and multiple databases	37
	Merging ePolicy Orchestrator databases together	37
	Importing events into the database	42
4	Report and Query Templates	44
	Anti-Virus report templates	44
	Coverage report templates	44

Infection report templates	54
Anti-Virus Coverage and Infection subreports	67
Rogue System Detection report templates	68
Entercept report templates	69
System Compliance Profiler report templates	70
Criteria used to limit report results	72
Computer query templates	74
Events query templates	75
Installations query templates	78

1

Getting Started with Reporting

An introduction to running reports with ePolicy Orchestrator

You can produce reports and queries for a group of selected client computers. You can also limit report results by product or computer criteria; for example, product name, product version number, or operating system. You can export reports into a variety of common file formats to distribute to key people or groups in your organization.

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 part of the ePolicy Orchestrator console tree is included in the report.
- Set a Data Filter, by using logical operators, to define precise filters on the data returned by for 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.

What is and is not covered in this chapter

This chapter contains an introduction to reporting only. It does not go into great detail about how reports work in ePolicy Orchestrator, or about advanced reporting features such as defining filters and writing custom reports and queries. For additional details on running reports in ePolicy Orchestrator, see the *Reports and Queries Implementation Guide*.

The topics covered in this section are:

- [About pre-defined reports in ePolicy Orchestrator](#)
- [How to generate a report in ePolicy Orchestrator](#)
- [Viewing report results in the report window](#)
- [Print or export reports into publishable formats](#)
- [Running Queries to get detail](#)
- [Saving filtered reports and queries as templates](#)
- [Writing custom reports in Crystal Reports](#)

About pre-defined reports in ePolicy Orchestrator

The ePolicy Orchestrator agent on the client systems communicates a variety of useful information back to the server. This information is stored in the reports database. You can run reports and queries against this stored information.

There are over 40 pre-defined reports that come with ePolicy Orchestrator. The default reports fall into two main categories: Coverage reports and Infection reports. In addition to the reports that available through ePolicy Orchestrator, you may also create your own report templates with the help of Crystal Reports 8.0.

What is the report repository?

The report repository contains both the pre-defined reports and queries that come with ePolicy Orchestrator and also any custom reports and queries you create yourself.

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 to 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, the administrator can easily view anti-virus policy compliance. Coverage reports provide snapshots of the anti-virus protection that is currently active on your computers. These reports are based on the computer and product property information stored in the server's database.

Examples of coverage information include what anti-virus product has been deployed and what version of DAT and engine files are installed on which clients. Compliance reports can help illustrate graphically problems you may be having with your ePolicy Orchestrator coverage, such as with getting DAT updates to particular computers. Run these reports and review them frequently to look for areas to improve your ePolicy Orchestrator coverage.

Infection reports show which viruses have been detected

Infection reports, by contrast, alert you to actual virus detections that may have occurred in your network. These reports can list which computers have the most virus detections (most likely your e-mail servers running GroupShield or Internet gateway running WebShield). They can list which specific viruses are being detected, and what actions were taken by the anti-virus software deployed in your network.

View summary information and drill down to detail

Another benefit when using ePolicy Orchestrator is the ability to receive both summary and detailed information from the same report. In this section, we will look at different reports and drill down into the reports for detailed analysis.

Summary reports can also be very 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. Most people are stunned to learn how many viruses ePolicy Orchestrator is routinely detecting, cleaning or removing.

Control access and filter results

You can control what visibility the different ePolicy Orchestrator users, such as global administrators or site reviewers, have into report information. Site administrators and site reviewers can only report on those client computers in sites to which they have rights.

How to generate a report in ePolicy Orchestrator

There are several ways in which you can control what data 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 computers 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.)

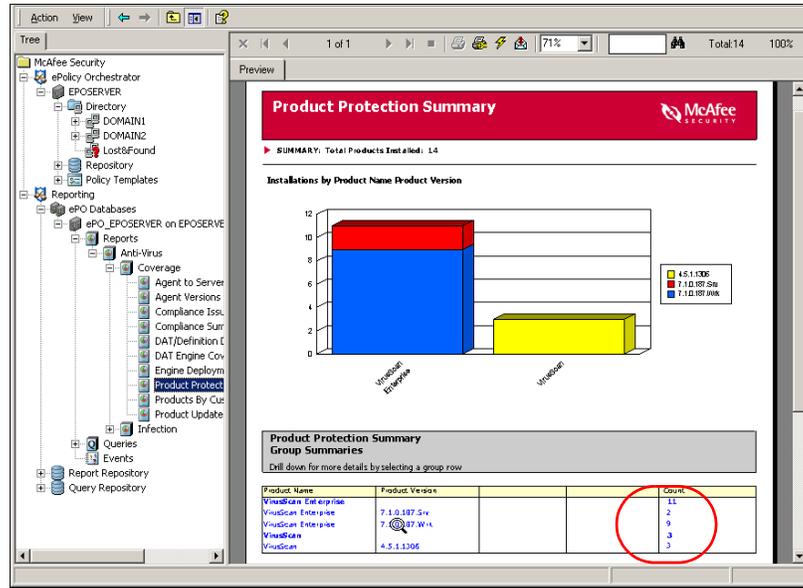
Once the results of a report appear, you can then perform a number of tasks on the data. You can view details on desired report data. (For example, to determine which client computers do not have a compliant version of VirusScan installed on them.) Some reports even provide links to other reports, called 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.

Generating a Product Protection Summary report

To run a *Product Protection Summary* report:

- 1 From the left-pane 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 in to the database, type your MSDE `sa` 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.

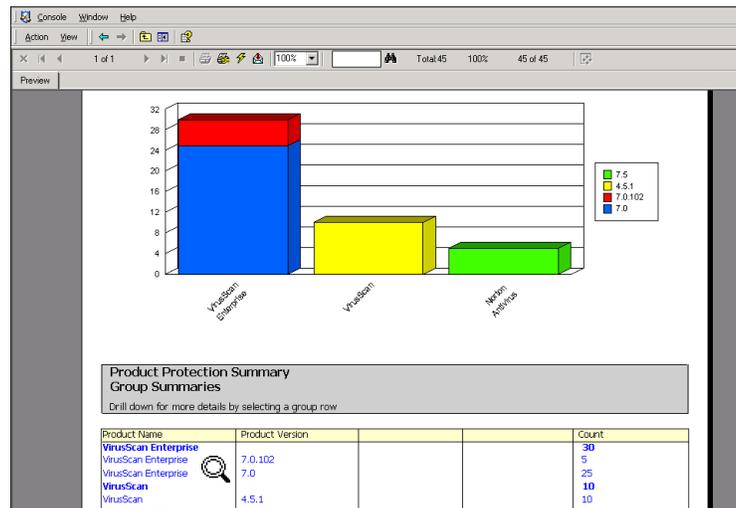
Figure 1-1 The Product Summary Report results show VirusScan Enterprise successfully installed on all servers and workstations



Viewing report results in the report window

The results of reports appear in the report window. You 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.

Figure 1-2 Highlighting report data



Select bits to drill down to.

If no additional data is listed, you've reached the details section of the report for the selected data.

Figure 1-3 Viewing details on report data

Product Protection Summary
Group Summary and Details

DRILLDOWN PATH: Product Name: VirusScan Enterprise > Product Version: 7.0.102

Product Name	Product Version		Count
VirusScan Enterprise	7.0.102		5

Page

Directory Path	ComputerName Username	Agent Version Contact Engine DAT	IPAddress DomainName OS Version Language
Directory_AVTest_WorkStations60.S1	Agents55.S1_AgentVer10.0.0.S1, AV45.S1,VirusScan2FW-10.S1,Engine45.S1,DAT8.S1		
Comp_Computer1.DAT8.S1	VirusScan Enterprise 7.0.102 SP1 HF1	3.0.123 2002-12-15 12:12:12	4.1.44 4.0.4136 Extrabab
Comp_Computer2.DAT8.S1		3.0.123 2002-12-15 12:12:12	0409

Print or export reports into publishable formats

After generating a report, you can print it to a network printer or export it to any number of standard formats such as an Adobe PDF document, Microsoft Excel spreadsheet, or HTML web page. Distributing reports or making them available for viewing is an important part of on-going ePolicy Orchestrator administration. Post a daily summary report on DAT compliance or top 10 viruses to a corporate web site. Distribute a weekly PDF report detailing virus infection and security information to key people in your organization to help remediate problems.

Some common export formats are:

- Adobe PDF
- Crystal Reports (RPT)
- Data Interchange Format (DIF)
- Microsoft Excel
- HTML and XML
- Text, Tab-delimited text
- Rich Text and Microsoft Word.

How to export a report data to other file formats

- 1 After running the report, click **Export** on the report toolbar.
- 2 In the **Export** dialog box, select the desired export **Format**.
- 3 Click **OK**. The **Choose Export File** dialog box appears.
- 4 Specify the name and location of the file, then click **Save**.

Running Queries to get detail

Queries provide a specific, single view. A query can either be a group summary or a detailed point view. They run faster than reports but do not support drilling down and some filtering.

Queries display data in a raw tabular form. They support Directory filtering and the creation of new user SQL queries. But do not support data filtering, drilling down, and the subreport features of reports.

In addition to the predefined queries that are available, you can also create your own custom queries if you have some experience writing SQL. In addition, you can refresh query data or go to specific rows in a query.

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 computers in a selected site or group, set a Directory filter.
- 3 In the console tree under **Reporting | ePO Databases | <DATABASE SERVER> | Queries | <QUERY GROUP>**, right-click **<QUERY>**, then select **Run**.
- 4 The resulting query appears in the details pane.
- 5 If you want 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**.
- 6 If you want 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.

Saving filtered reports and queries as templates

To save the selections you made in the **Current Protection Standards**, **Enter Report Inputs**, and **Report Data Filter** dialog boxes as a report template:



You can also save the selections you made in the **Enter Report Inputs** dialog box at the same time that you are making them.

- 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 location to which you want to store it temporarily, then click **Save**.
- 6 Add the Report Template file to the **Report Repository**.

Writing custom reports in Crystal Reports

ePolicy Orchestrator 3.5 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. Neither the *Product Guide* nor the *Reports and Queries Implementation Guide* go into detail about how to use Crystal Reports to write custom reports and queries. For information on how to do that, consult your Crystal Reports documentation.

2 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 then stored in the ePolicy Orchestrator database.

The ePolicy Orchestrator software includes a number of predefined report and query templates. These templates are stored in the **Report Repository** and **Query Repository** 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 44](#).

You can produce reports and queries for a group of selected client computers. You can also limit report results by product or computer 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.

- [Reporting concepts on page 12](#).
- [Getting started with Reporting on page 14](#).
- [Reporting on page 16](#).
- [Queries on page 25](#).
- [Report Repository maintenance on page 25](#).
- [Query Repository maintenance on page 28](#).

Reporting concepts

Before beginning to use ePolicy Orchestrator software's reporting functionality, there are some concepts about it that you should understand:

- [Crystal Reports 8.5 on page 13](#).
- [Authentication and user accounts on page 13](#).

Crystal Reports 8.5

ePolicy Orchestrator 3.5 software uses Business Objects Crystal Reports 8.5 to generate reports from data stored in the ePolicy Orchestrator database. We have provided a large number of report templates to use. If you want to create custom report templates for your reporting purposes, see the Crystal Reports 8.5 documentation.

For a list of the reports provided with ePolicy Orchestrator 3.5, and the data they display, please see the *Report Template Reference Guide*.

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 you begin using these functionalities, it is important that you understand how certain settings or situations affect what data is reported:

- [Database authentication on page 13](#).
- [ePolicy Orchestrator authentication and working with events on page 13](#).
- [User accounts and the data that appears in reports on page 14](#)

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 limit, remove, import, or repair events.

When using NT authentication, local administrators on the database server have all of the permissions needed to access ePolicy Orchestrator databases and limit, remove, 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 Windows NT or SQL authentication, all users can only view and change options 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 computers 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 computers in sites to which they have rights.

Getting started with Reporting

Before you begin generating reports, there are some configurations you can make to limit the data retrieved. Some reporting settings affect ePolicy Orchestrator database servers, and all reports and queries. You might find it helpful to review these settings before you run reports and queries to ensure that the desired data is displayed in them.

- [Specifying global reporting options on page 14.](#)
- [Limiting report and query results by client computer on page 15.](#)

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 also 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** if you want to add a local database server under **ePO Databases** every time you start the software.
- 3 Select **Encrypt and save passwords between sessions** if you want 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 Choose whether to 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), try increasing this value.
- 5 Choose whether to 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), try increasing this value.

- 6 Specify whether to display event information in infection reports in local time as reported on the client computer (**Local**), or in Greenwich mean time (**GMT**) under **Select Reporting Time**.
- 7 Click **OK** when done.

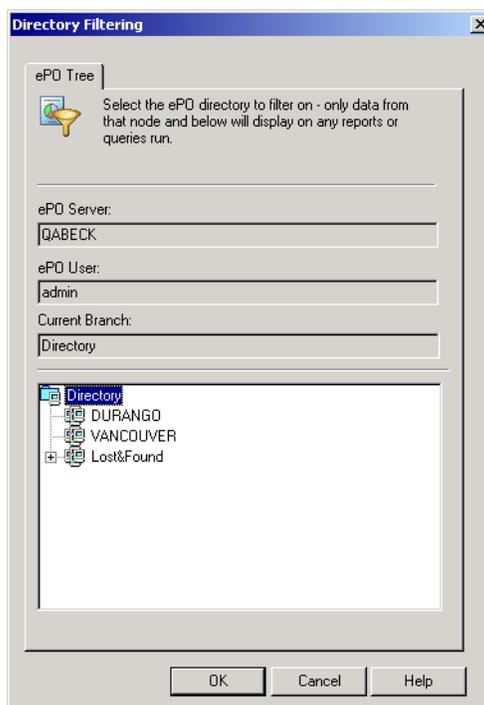
Limiting report and query results by client computer

You can limit the results of reports and queries by client computers under a selected site or group, and all groups and computers 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 computers under a selected site or group, and all groups and computers underneath it:

- 1 Log on to the desired ePolicy Orchestrator database server.
- 2 In the console tree under **Reporting | ePO Databases**, right-click the desired database server, then select **Set Directory Filter**. The **Directory Filtering** dialog box appears.

Figure 2-1 Directory Filtering dialog box



- 3 Select the desired site or group for which you want to generate reports and queries.
- 4 Verify that the desired site or group appears in **Current Branch**, then click **OK**.

Reporting

There are several ways in which you can control what data 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 computers 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 tasks on the data. You can view details on desired report data. (For example, to determine which client computers 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.

Topics in this section include:

- [Reporting options on page 16.](#)
- [Running reports on page 17.](#)
- [Working with reports in the report window on page 21.](#)

Reporting options

Depending on the report you select to run, an input dialog box with one or more tabs may appear allowing you to define the data that displays in the report. More specifically, these allow you to do the following in corresponding reports:

- [Defining compliance rules for reports on page 16.](#)
- [Specifying viewing and printing options for reports on page 16.](#)
- [Defining how to group data on reports on page 17.](#)
- [Limiting report results within a time period or data group on page 17.](#)
- [Limiting report results by selected criteria on page 17.](#)
- [Saving and reusing report input settings on page 17.](#)

Defining compliance rules for reports

You can create rules that define what compliance means in your company. 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 computers with the 2.0, 1.1, or 1.0 version of the agent appear on the report.

Specifying viewing and printing options for reports

You can select the type of chart that appears in the main section of the report. 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.

Defining how to group data on reports

You can group data in up to four different levels.

Limiting report results within a time period or data group

You can limit the results of selected reports to data recorded within the time period you specify; for example, within the last three days. Also, use this procedure to limit the results of selected reports by custom data groups; for example, within anti-virus products only.

Limiting report results by selected criteria

You can limit the data that appears on selected reports by the computer, infection, or product criteria you specify. For example, you might want to view only coverage information about VirusScan Enterprise 7.0. For information on the criteria available for each report, see [Report and Query Templates on page 44](#).

You can also save the selections you make in the **Report Data Filter** dialog box for future use. For instructions, see [Saving customized reports selections as report templates on page 26](#).

Saving and reusing report input settings

You can save the selections you made 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.

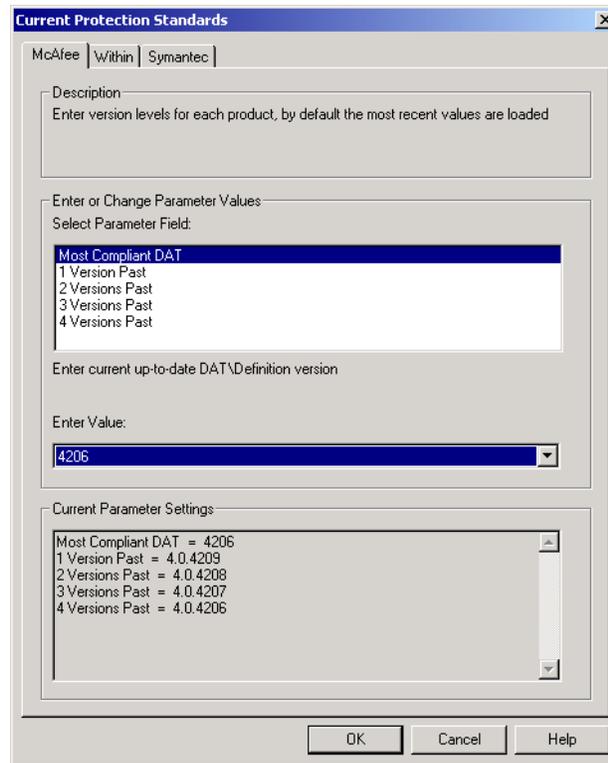
Running reports

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 [Saving and reusing report input settings on page 17](#) and [Saving customized reports selections as report templates on page 26](#), respectively.

To run a report:

- 1 Log on to the desired ePolicy Orchestrator database server.
- 2 Select the desired report under **Reporting | ePO Databases | <DATABASE SERVER> | Reports | <REPORT GROUP>** in the console tree.
- 3 If the **Current Protection Standards** dialog box appears, specify the version numbers of virus definition files or the virus scanning engine on which you want to report.

Figure 2-2 Current Protection Standards dialog box



- 4 If the **Enter Report Inputs** dialog box appears, make selections on any of the tabs that may appear: **Rules**, **Layout**, **Data Grouping**, **Within**, **Saved Settings**.



Which tabs appear depends on which report is selected.

Rules tab

Use the **Rules** tab to define compliance rules for the report:

- a In **Select Parameter Field**, select the desired item. A definition of the selected item appears under **Select Parameter Field**.
- b In **Enter Value**, select or type the cutoff value. The current settings appear under **Current Parameter Settings**.
- c Repeat [Step a](#) and [Step b](#) to define rules for each item listed in **Select Parameter Field**.



If you want to modify a setting, select the desired item in **Select Parameter Field**, then select or type a different value in **Enter Value**.

If you want to delete a settings, select the desired item in **Select Parameter Field**, then clear the value in **Enter Value**.

- d Click **OK** when you have finished making selections on the present tabs.

Layout tab

Specify viewing and printing options for the report:

- a Select **Chart Type** in **Select Parameter Field**, then select the desired chart type in **Enter Value**. The current settings appear under **Current Parameter Settings**.
- b 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**.

- c Click **OK** when you have finished making selections on the present tabs.

Data Grouping tab

Define how data is grouped on the report:

- a 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**.
- b In **Enter Value**, select the desired data value. The current settings appear under **Current Parameter Settings**.
- c Repeat [Step a](#) and [Step b](#) 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**.

- d Click **OK** when you have finished making selections on the present tabs.

Within tab

Limit the results of the report to a time period or data group:

- a 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**.

- b** 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**.

- c** Click **OK** when you have finished making selections on the present tabs.

Saved Settings tab

The **Saved Settings** tab allows you to save and reuse the selections you make in the **Enter Report Inputs** dialog box. This tab also allows you to delete such previously saved settings.

To save settings for reuse:

- a** In **Select Parameter Field**, select **Save**.
- b** Type a descriptive name in **Enter Value**, type a descriptive name for the report input settings. The current settings appear under **Current Parameter Settings**.

To reuse settings already saved:

- a** In **Select Parameter Field**, select **Open**.
- b** In **Enter Value**, select the desired report settings. The current report settings appear under **Current Parameter Settings**.
- c** Make changes as needed.
- d** Click **OK** when you have finished making selections on the present tabs.

To save settings based on another set of already saved settings:

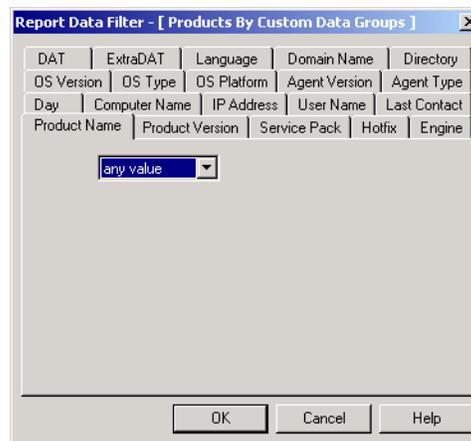
- a** In **Select Parameter Field**, select **Open**.
- b** In **Enter Value**, select the desired report settings.
- c** Make changes as needed.
- d** Click the **Saved Settings** tab.
- e** In **Select Parameter Field**, select **Save As**.
- f** In **Enter Value**, select the same report settings you selected in [Step d](#). The current report settings appear under **Current Parameter Settings**.
- g** Click **OK** when you have finished making selections on the present tabs.

To delete saved settings:

- a** In **Select Parameter Field**, select **Delete**.
 - b** In **Enter Value**, select the desired report input settings you want to delete.
 - c** Click **OK** when you have finished making selections on the present tabs.
- 5** 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:

- a Select the tab (for example, **Product Version**) that corresponds to the criteria 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 in the following ways:
 - 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 criteria.
- 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**. This statement is useful 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 2-3 Report Data Filter dialog box



- 6 View report details. For instructions, see [Viewing the details of report data on page 23](#).

Working with reports in the report window

The results of reports appear in the report window. You 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.

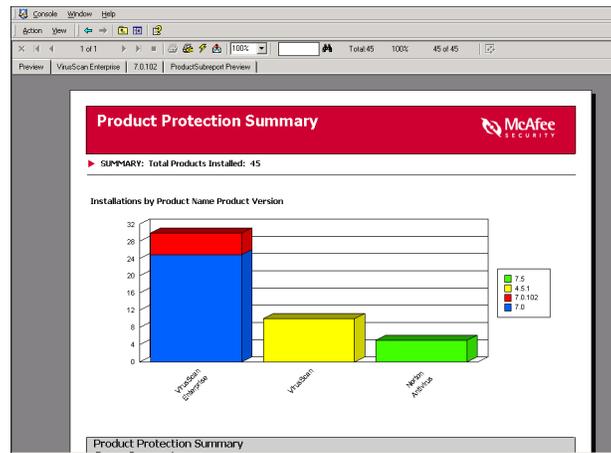
This section includes the following topics:

- [The report window components on page 22.](#)
- [The report toolbar on page 22.](#)
- [Viewing the details of report data on page 23.](#)
- [Printing reports on page 24.](#)
- [Exporting report data to other formats on page 24.](#)

The report window components

The report window provides the following components:

Figure 2-4 Report window 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 22.](#)

The report toolbar

The report toolbar is one of the main components found in the report window. Each button on this toolbar is described below.

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



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 **Preview** tab.
- 

Export the selected section of the report in a variety of file formats.
- Reduce or enlarge the display of the selected section of the report.
- 3.0.0

Specify the words or phrases that you want to find in the selected section of the report.
- 

Locate the words or phrases you specify in the 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. 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 44](#).

- 1 Run the report. For instructions, see [Running reports on page 17](#). The main section of the desired report appears in the report window.
- 2 Click any blue text to drill down for more detailed information.
- 3 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 example below, 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 2-5 Viewing group-level report data



- 4 Repeat [Step 3](#) to view more group-level report data.
If no additional data is not listed, you've reached the details section of the report for the selected data.
- 5 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.
- 6 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:

- 1 Add a printer. For instructions, see printing-related topics in the Microsoft Windows Help file.
- 2 Run the report. For instructions, see [Running reports on page 17](#).
- 3 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.
- 4 To print the selected section of the report, click the **Print** button on the report toolbar.

Exporting report data to other formats

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 17](#).
- 2 To export the selected section of the report, 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

In addition to the predefined queries that are available, if you have experience writing SQL `SELECT` statements and working with SQL databases, you can also create your own custom queries. In addition, you can refresh query data or go to specific rows in a query.

- [Running queries on page 25](#).
- [Report Repository maintenance on page 25](#).

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 computers in a selected site or group, set a query filter. For instructions, see [Limiting report and query results by client computer on page 15](#).
- 3 In the console tree under **Reporting | ePO Databases | <DATABASE SERVER> | Queries | <QUERY GROUP>**, right-click **<QUERY>**, then select **Run**.
- 4 The resulting query appears in the details pane.
- 5 If you want 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**.
- 6 If you want 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 to 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 reports selections as report templates on page 26.](#)
- [Adding a custom report templates on page 26.](#)
- [Modifying report templates on page 27.](#)
- [Deleting report templates on page 27.](#)
- [Creating report groups on page 27.](#)
- [Deleting report groups on page 27.](#)

Saving customized reports selections as report templates

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 is the only way you can save the selections you made in the **Current Protection Standards** and **Report Data Filter** dialog boxes for future use.

You can also save the selections you made in the **Enter Report Inputs** dialog box at the same time that you are making them. For instructions, see [Saving and reusing report input settings on page 17.](#)

- 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 location to which you want to store it temporarily, then click **Save**.
- 6 Add the Report Template file to the **Report Repository**. For instructions, see [Adding a custom report templates on page 26.](#)

Adding a custom report templates

To add report templates to the desired report group in the **Report Repository**.

- 1 In the console tree, right-click the desired report group under the **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 27.](#)

- 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 the >> button 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** when done. 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 Click the desired report template in the console tree under the **Report Repository**. 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 the **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 the **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 3.5, you can add report templates to the Report Repository that come bundled in the .NAP file.

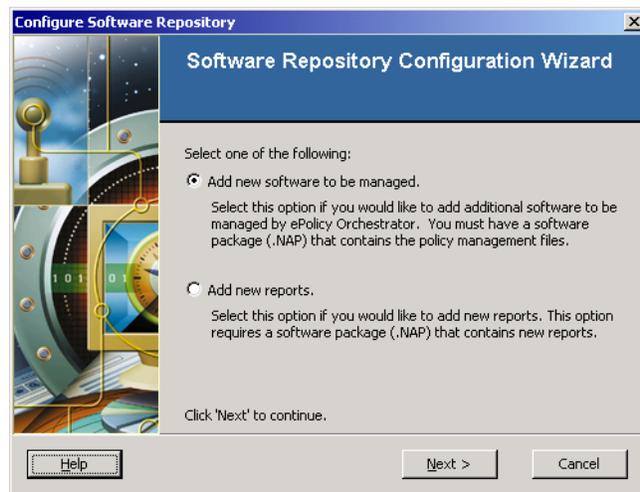
To add report templates from a .nap file to the **Report Repository**:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 In the console tree under **ePolicy Orchestrator | <SERVER>**, right-click **Repository**, then select **Configure Repository**. The **Software Repository Configuration Wizard** appears.



Although you right-click the software **Repository** to initiate this task, the report template is added to the **Report Repository** and not the software **Repository**.

Figure 2-6 Software Repository Configuration Wizard



- 3 Select **Add new reports**, then click **Next**. The **Select a Software Package** dialog box appears.
- 4 Select the desired language version .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.
- 5 Log back into the ePolicy Orchestrator database using ePolicy Orchestrator authentication to download the reports into the Report Repository.



You must use ePolicy Orchestrator authentication to download the reports.

Query Repository maintenance

You can organize the **Query Repository** to suit your needs, or add your own custom query templates.

- [Adding custom query templates on page 29.](#)
- [Modifying query templates on page 30.](#)
- [Deleting query templates on page 31.](#)
- [Creating query groups on page 31.](#)
- [Deleting query groups on page 31.](#)

Adding custom query templates

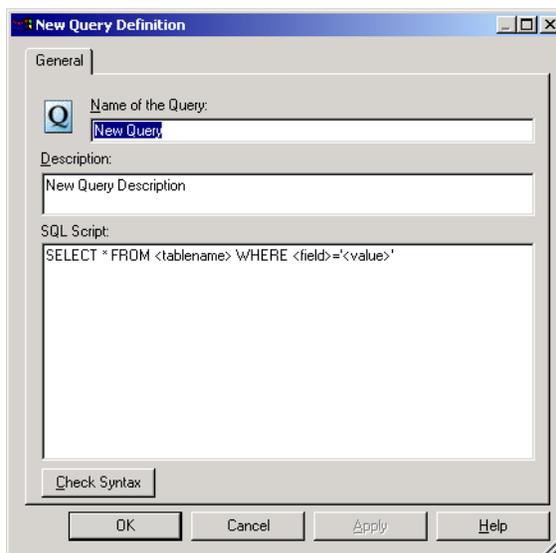
To add custom query templates to the desired query group in the **Query Repository**:

- 1 Right-click the desired query group under the **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 31](#).

Figure 2-7 New Query Definition dialog box



- 2 Type the **Name of the Query** as you want it to appear in the console tree.
- 3 Type a literal **Description** of the query.
- 4 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.

- 5 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.

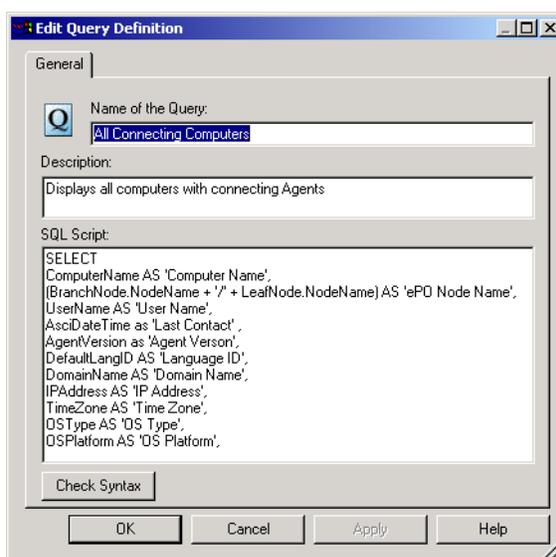
- b** Select the desired database server, then click **OK**.
- 6** Click **OK** when done. The query template appears in the **Query Repository**.

Modifying query templates

To modify existing query templates:

- 1** Click desired query template in the **Query Repository**. The **Query Definition** dialog box appears in the details pane.
- 2** Click **Edit** to open the **Edit Query Definition** dialog box.

Figure 2-8 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 **Query Repository**, then select **Remove**.

Creating query groups

You can create query groups to better organize the **Query Repository**. To add query groups to the **Query Repository**:

- 1 Right-click the **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.

Figure 2-9 New Query Group dialog box



- 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**.

3

ePolicy Orchestrator Databases and Reports

You can either use Microsoft Data Engine or Microsoft SQL Server as your ePolicy Orchestrator database server. Regardless of which one you use, your ePolicy Orchestrator databases require some management. Database servers can reside on the same computer as the ePolicy Orchestrator server or on a separate computer. You can work with multiple databases within the same console session.

You can use a combination of tools to maintain ePolicy Orchestrator databases. You will use a slightly different set of tools depending on whether you are using a Microsoft Data Engine (MSDE) 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.

Topics in this section include:

- [Getting started with ePolicy Orchestrator databases on page 32.](#)
- [Reporting and multiple databases on page 37.](#)

Getting started with ePolicy Orchestrator databases

Once your ePolicy Orchestrator databases are installed, you need to be able to understand and perform some basic tasks, configure which events are going to be stored for efficient reporting.

- [User accounts and working with events on page 32.](#)
- [Logging on to, off of, and removing ePolicy Orchestrator database servers on page 33.](#)
- [Defining which events are stored in the database on page 36.](#)

User accounts and working with events

The ePolicy Orchestrator administrator account that you use to log on to ePolicy Orchestrator database servers affects 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 on to, off of, and removing 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 on to ePolicy Orchestrator database servers on page 33.](#)
- [Logging off of ePolicy Orchestrator database servers on page 35.](#)
- [Removing ePolicy Orchestrator database servers on page 36.](#)

Logging on to ePolicy Orchestrator database servers

Typically, you must log on to database servers every time you start the software. 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, so that you do not need to manually log on to them.

You can also save logon information for all database servers. For instructions, see [Specifying global reporting options on page 14.](#)

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 computer as the ePolicy Orchestrator server, the database server appears automatically in the console tree. For instructions on changing this setting, see [Specifying global reporting options on page 14.](#)

ePolicy Orchestrator database server names are displayed in two parts in the console tree:

```
DATABASE_NAME(AUTHENTICATED_SERVER_NAME)
```

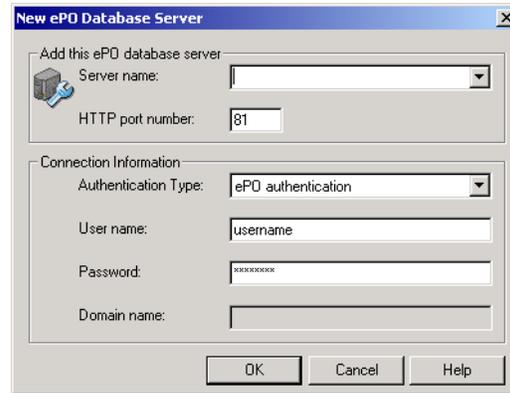
The name contained within the parentheses is the name of the server to which you authenticate, which is not necessarily the server on which the database is housed.

- [Logging on to database servers that appears in the console tree on page 33.](#)

Logging on to database servers that appears in the console tree

To log on to 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.

Figure 3-1 ePO Database Login dialog box

- 2 If **Connection Information** items do not appear in this dialog box, click **Options** to display them. These items allow you to select the authentication mode.
- 3 Under **Connection Information**, select the **Authentication Type** that you want to use 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 **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**.



If you select **Save connection information and do not prompt again**, be sure to password-protect the corresponding database server. Otherwise, other 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.

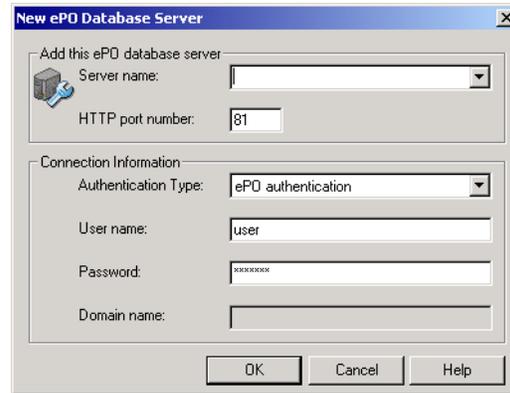
Logging on to ePolicy Orchestrator database servers that do not appear in the console tree

You can add multiple database servers to the console tree. This enables you to work with more than one database server in the same session.

To add and log on to an ePolicy Orchestrator database server to the console tree:

- 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 3-2 New ePO Database Server dialog box



- 2 Select the **Authentication Type** that you want to use 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 choose 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**.



If you select **Save connection information and do not prompt again**, be sure to password-protect the corresponding database server. Otherwise, other 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 of 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 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 If you want to clear the saved logon information:
 - a Exit the software.
 - b Log on to the desired database server. Be sure to deselect **Save connection information and do not prompt again**.



Once you clear the logon information, you will need to log on to the database server every time you start the software.

Defining which events are stored in the database

ePolicy Orchestrator databases store events from computers and appliances that it manages. ePolicy Orchestrator allows you to define, by filtering, which events you want stored in the ePolicy Orchestrator database for reporting purposes.

These events are then stored in the ePolicy Orchestrator database for reporting purposes. Events that are already in the database are not affected by your choices.

Because service events (for example, starting or stopping software) are numerous, they are not collected by default. We recommend that you accept these 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 begin at the next agent-to-server communication).

Reporting and multiple databases

Although you can log on to 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 together. This is useful when the databases were created using version 3.0 or later. For instructions see, [Merging ePolicy Orchestrator databases together on page 37](#).
- 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 42](#).

Merging ePolicy Orchestrator databases together

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 on page 37](#).
- [Merging databases using a Merge Settings \(.TXT\) file on page 41](#).

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 (.TXT) file so that you can run the program later using the database merge settings you define here. You might find this helpful if you merge the same ePolicy Orchestrator databases together on a routine basis.

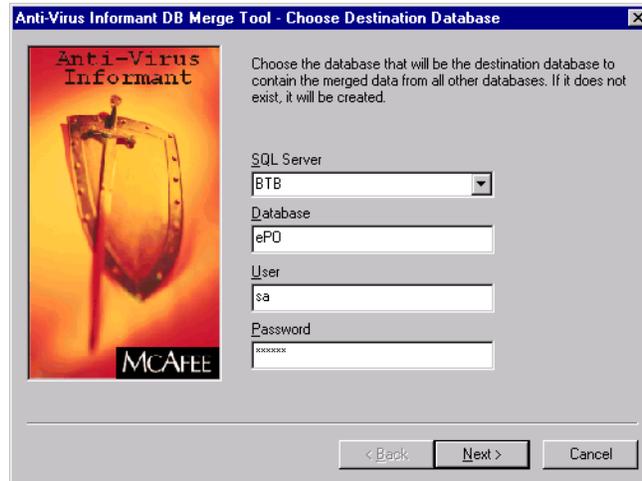
To merge multiple ePolicy Orchestrator databases into a new or existing database:

- 1 Start the DB Merge Tool (AVIDB_MERGE_TOOL.EXE). The default location is:

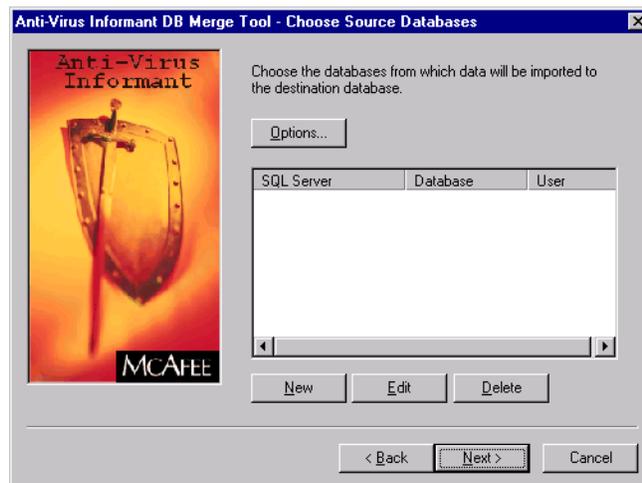
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\AVI

If you upgraded the software from version 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFFEE\EPO\3.5.0\AVI

Figure 3-3 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 3-4 Choose Source Databases dialog box

- 4 Click **New** to open the **Source Database** dialog box to specify the databases that you want to merge together.

Figure 3-5 Source Database dialog box

- 5 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.
- 6 Click **OK** to save the current entries and return to the **Choose Source Databases** dialog box. Then repeat [Step 4](#) through [Step 6](#) for each desired database.
- 7 Click **Options** to open the **Merge Tool - Options** dialog box to specify merge settings for all of the databases that are being merged together:



If you are merging databases into an existing database, these settings do not affect that database.

Figure 3-6 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\MCAFFEE\EPO3.5.0\AVI

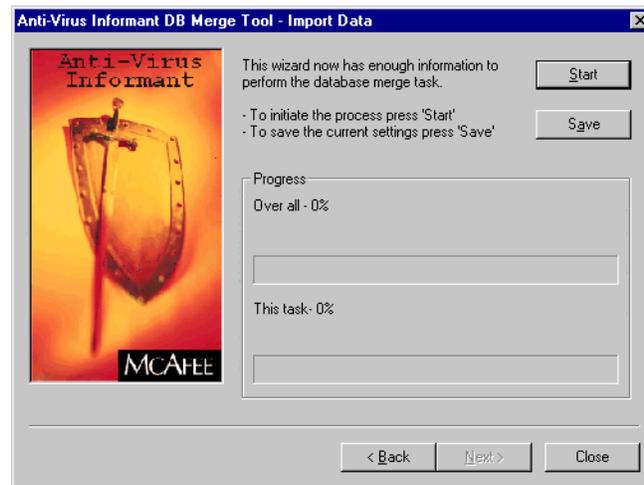
- d Under **Event Import**, specify whether to include events in the destination database.



We recommend 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 computer 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 3-7 Import Data dialog box



- 8 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 (.TXT) file (for example, C:\PROGRAM FILES\MCAFFEE\EPO3.5.0\AVI\SETTINGS.TXT).
 - c Click **Save** to return to the **Import Data** dialog box.
- 9 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**.

- 10 Click **Close** when done.



If the merge process could not connect to a server, the merge database is not created.

Merging databases using a Merge Settings (.TXT) file

You can merge ePolicy Orchestrator databases together using predefined database merge settings. After you create a Merge Settings (.TXT) 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 on page 41.](#)
- [Merging databases with the Merge Settings file from the command line on page 41.](#)
- [Merging databases in the background using the Merge Settings file on page 42.](#)

Merging databases with a Merge Settings file using the drag-and-drop operation

To drag the Merge Settings (.TXT) file that contains predefined database merge settings to the application window:

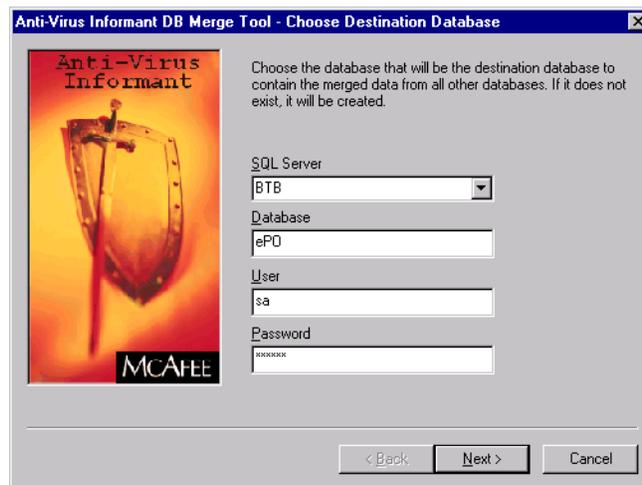
- 1 Start the DB Merge Tool (AVIDB_MERGE_TOOL.EXE). The default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\AVI

If you upgraded the software from version 2.0, 2.5, or 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFFEE\EPO\3.5.0\AVI

Figure 3-8 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** when done.

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 (.TXT) file.

For example, if the program and Merge Settings file are in the default location, type the following:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3\AVI\AVIDB_MERGE_TOOL.EXE  
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\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** when done.

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 together 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\NETWORK ASSOCIATES\EPO\3.5.0\AVI\AVIDB_MERGE_TOOL.EXE  
/SILENT C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\AVI\SETTINGS.TXT
```

- 2 A **Anti-Virus Informant DB Merge Tool - Choose Destination Database** taskbar button appears on the taskbar to indicate that the merge process is running.

Importing events into the database

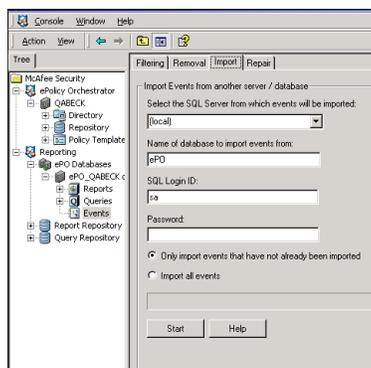
You can import events from another ePolicy Orchestrator database into the current one, so that the selected events are available for reporting purposes.



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 on to 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 3-9 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.

4

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** 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. For instructions on working with database servers, reports, and queries, see [Reporting on page 12](#).

The data that each report and query template provides and samples of each report is provided here. 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 *Configuration Guide* for that product.

- [Anti-Virus report templates on page 44](#).
- [Anti-Virus Coverage and Infection subreports on page 67](#).
- [Rogue System Detection report templates on page 68](#).
- [Intercept report templates on page 69](#).
- [System Compliance Profiler report templates on page 70](#)
- [Criteria used to limit report results on page 72](#).
- [Computer query templates on page 74](#).
- [Events query templates on page 75](#).
- [Installations query templates on page 78](#).

Anti-Virus report templates

Anti-virus report templates are divided between two categories:

- [Coverage report templates on page 44](#).
- [Infection report templates on page 54](#).

Coverage report templates

These are the predefined report templates available under **Reporting | Anti-Virus | Coverage**:

- [Agent to Server Connection Info report template on page 45](#).

- [Agent Versions report template on page 46.](#)
- [Compliance Issues report template on page 46.](#)
- [Compliance Summary report template on page 48.](#)
- [DAT/Definition Deployment Summary report template on page 48.](#)
- [DAT Engine Coverage report template on page 50.](#)
- [Engine Deployment Summary report template on page 51.](#)
- [Product Protection Summary report template on page 52.](#)
- [Products By Custom Data Groups report template on page 52.](#)
- [Product Updates By Custom Event Groups report template on page 54.](#)

Agent to Server Connection Info report template

Specify the time period that defines an inactive agent, then view report data for computers with active agents (**Current**), inactive agents (**Late**), and **No Agent**, in a pie chart format.

You can also view historical data for computers using the Tasks, Policies, Update, and Infection subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 67.](#)

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:

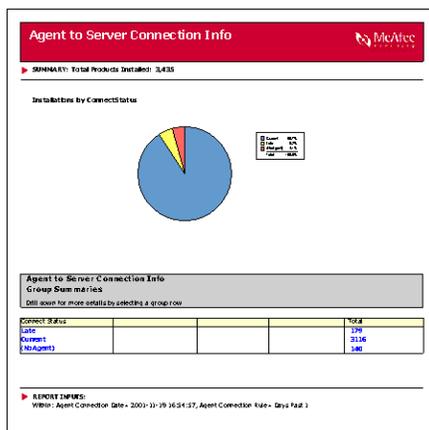
- **Agent Connection Date** — Specifies a cutoff date and time that defines an inactive agent. Agents that have not communicated with the server since the date you specify are reported as inactive (late).
- **Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) that 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 72.](#)

Sample report

Figure 4-1 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 computers, in a bar chart format. Use this report for an overall view of how up-to-date the agents are on client computers.



Legacy agents are not fully functional in ePolicy Orchestrator 3.5. For full agent functionality, you must upgrade to agent version 3.5.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Compliance Issues report template

View all compliance issues on computers that violate the compliance rules you specify. You can also view computers with unresolved detections. In addition, you can view historical data for computers using the Tasks, Policies, Update, Infection, and Compliance History subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 67](#).

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** and **Engine\DAT** tabs 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 computers 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):

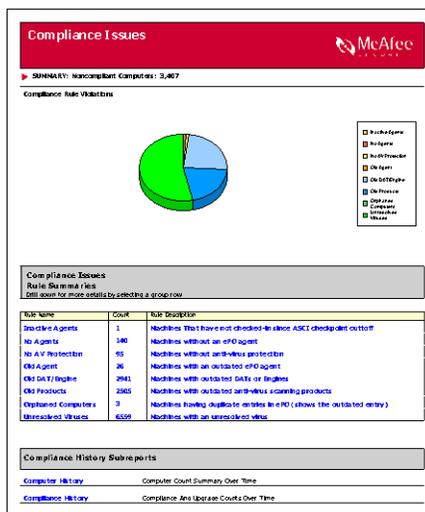
- **Late Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for computers with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Late Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) for agent communication. Data for computers 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 72](#).

Sample report

Figure 4-2 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 72](#).

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 computers, 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 computers, and to determine which client computers need to be updated with the most current virus definition files. In addition, you can view historical data for computers using the Tasks, Policies, Update, Infection, and Compliance History subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 67](#).

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 52](#).

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 and Symantec tabs (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. Computers with older versions of virus definition files 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):

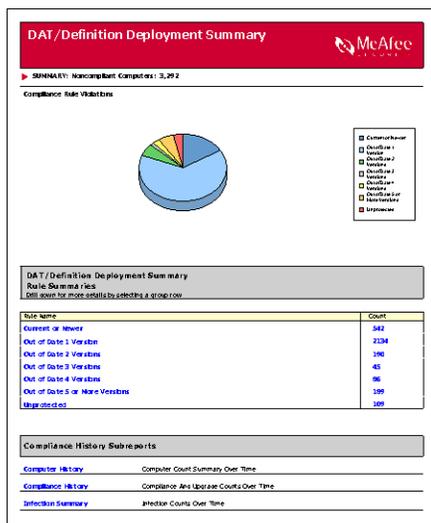
- **Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for computers with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Agent Connection Rule** — Specifies a relative time period (for example, Current Week) for agent communication. Data for computers 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 72](#).

Sample report

Figure 4-3 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 computers, 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 computers, and to determine which client computers need to be updated with the most current virus definition files or engine. In addition, you can view historical data for computers using the Tasks, Policies, Update, Infection, and other subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 67](#).

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 52](#).

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** and **Symantec** tabs (**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. Computers with older versions of virus definition files or 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):

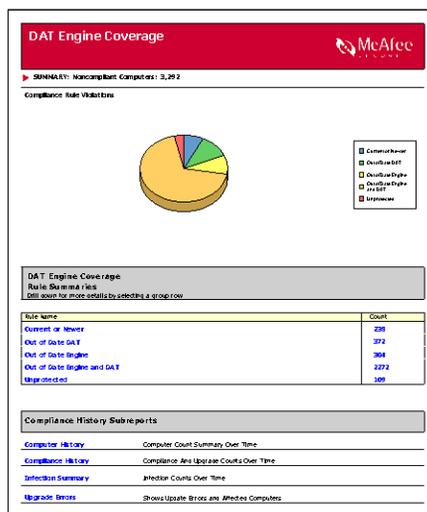
- **Agent Connection Date** — Specifies a cutoff date and time for agent communication. Data for computers with agents that have not communicated with the ePolicy Orchestrator server since this date and time appear on the report.
- **Agent Connection Rule** — Specifies a relative time period (for example, **Current Week**) for agent communication. Data for computers 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 72](#).

Sample report

Figure 4-4 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 computers, 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 computers, and to determine which client computers need to be updated with the most current engine. In addition, you can view historical data for computers using the Tasks, Policies, Update, Infection, and other subreports. For more information on subreports, see [Anti-Virus Coverage and Infection subreports on page 67](#).

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 52](#).

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 and Symantec tabs (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. Computers 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 computers 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 computers 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 72](#).

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 computers without any anti-virus protection software and computers without an agent, in a stacked column chart format. In addition to computers without any anti-virus protection software, client computers 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 point 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 52](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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. Computers 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. Computers 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 then next time the report runs.
- **Connection Type** — Specifies whether to include data for all computers, current computers only, or late computers 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 then 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.

A number of predefined settings are provided for you:

- **Agent Version** — Provides the same data as the Agent Version report, but also groups data by connection status.
- **Domain to Group** — Organizes sites and groups by the domains to which they belong. Use this report to match the **Directory** structure to the domain layout.
- **Engine DAT** — Provides the same data as the DAT/Definition Deployment Summary, DAT Engine Coverage, and Engine Deployment Summary reports, but groups data by version number instead of by out-of-date versions. Use this report to view summary data at the virus definition file and virus scanning engine level.
- **Group to Domain** — Groups domains by the site or group to which they belong. Use this report to match the **Directory** structure to the domain layout.
- **Language** — This report replaces the Language Summary report from previous versions of the software. Use this report to view the language versions of supported anti-virus and security products installed on client computers.
- **Last Contact** — Provides the same data as the Agent To Server Connection Info report, but allows you to change the format of the chart that appears on the main page of the report.
- **OS Product** — Lists supported anti-virus and security product versions installed on client computers by operating system version.
- **Product Protection** — Provides the same data as the Product Protection Summary report. It is provided here as a base for you to customize as desired.
- **Connections by OS Platform** — Lists the last connection of client computer by operating system platform. Use this report to identify laptop computers, or connection issues on critical computers; for example, servers.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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.

A number of predefined settings are provided for you:

- **Initiator summary** — Summarizes product updates by the updating method: global updating, the **Update** client task based updating, or client-based pull updating.
- **Server activity** — Provides the distribution of update activity across distributed software repositories servers and the types of product or product update packages (for example, patch releases, service pack releases, virus definition (DAT) files, etc.) being replicated to repositories.
- **Update Errors** — Lists updating messages grouped by message ID number.
- **Weekly updates** — Provides the updates that occurred each week by product or product update type and version number.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Infection report templates

The anti-virus infection report templates are divided among three categories: Action Summaries, Detections, Top Tens, and WebShield. However, they are all listed individually here.

- [Action Summary By Top 10 Files Resolved report on page 56](#).
- [Action Summary By Top 10 Files Unresolved report on page 56](#).
- [Action Summary By Top 10 Viruses report on page 56](#).

- [Action Summary report template on page 56.](#)
- [Infection History report template on page 57.](#)
- [Infections By Custom Data Groups report template on page 57.](#)
- [Number Of Infections Detected By Product For Current Quarter \(3D Bars\) report template on page 59.](#)
- [Number Of Infections Detected Monthly Showing Viruses report template on page 59.](#)
- [Number Of Infections For the Past 24 Hours report template on page 60.](#)
- [Outbreaks - Weekly History report template on page 60.](#)
- [Outbreaks - Current report template on page 60.](#)
- [Product Events By Severity report template on page 60.](#)
- [Number Of Infections From Removable Media report template on page 61.](#)
- [Security Summary report template on page 61](#)
- [Virus Type report template on page 61.](#)
- [Viruses Detected report template on page 61.](#)
- [Top 10 Detected Viruses report template on page 62.](#)
- [Top 10 Infected Files report template on page 62.](#)
- [Top 10 Infected Machines report template on page 62.](#)
- [Top 10 Infected Users report template on page 63.](#)
- [Content Filter Report By Rule template on page 63.](#)
- [Content Filter Report By Rule And Time template on page 63.](#)
- [Content Filter Report Rules Triggered template on page 63.](#)
- [Content Scanning Detections By Appliance report template on page 64.](#)
- [Infection History report template \(WebShield\) on page 64.](#)
- [Spam Detections By Appliance report template on page 64.](#)
- [Top Ten Spammers report template on page 65.](#)
- [URLs Blocked report template on page 65.](#)
- [Virus Detections By Appliance report template on page 65.](#)
- [Virus Detections Timing report template on page 66.](#)
- [Virus Type report template \(WebShield\) on page 66.](#)
- [Viruses Detected report template \(WebShield\) on page 66.](#)

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.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Action Summary By Top 10 Files Unresolved report

Use this report to view the ten most frequently infected files that have been unsuccessfully resolved by the scanning engine. Data is grouped by file name, action taken, and infection 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 72](#).

Action Summary By Top 10 Viruses report

Use this report to view the actions performed on the ten most detected viruses, in a stacked bar chart format. It provides a good 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 57](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Action Summary report template

Use this report to view the actions performed when viruses were detected by supported anti-virus protection products, in a bar 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 57](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Infection History report template

Use this report to view 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 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).

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 go to 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 57](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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 8.0i only.
- **Potentially unwanted programs** — For VirusScan 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 past four weeks. Use this report to view all actions performed over the past 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 floppy disks) 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 72](#).

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 computers 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 Version 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 72](#).

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, and 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 Name, 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 57](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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 name 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 57](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Outbreaks - Weekly History report template

Use this report to view historical data on detected infections within an outbreak for each week within a quarter, in a three-dimensional bar chart format.

The report allows the user to enter an outbreak definition. A historic outbreak is defined as occurring over at least a minimum number of distinct computer or distinct files infected within the time frame of a week.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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. Its 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 at least a minimum number of distinct computer (x) or distinct files (y) infected within a time frame specified in hours (z). In others words, an outbreak is said to have occurred if x distinct computers or y distinct files have been infected by the same virus within z hours.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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 72](#).

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.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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 bar chart format.

You can view report details by virus type, virus subtype, virus name, and product name.

For definitions of virus types (for example, trojan horse), see the Virus Glossary on the AVERT web site:

<http://www.mcafeeb2b.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 72](#).

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 go to 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 57](#).

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

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 Name, followed 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 72](#).

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.

Limit report results

You can limit the results of this report using the criteria listed in [Criteria used to limit report results on page 72](#).

Top 10 Infected Machines report template

Use this report to view the ten most infected client computers, in pie chart format. It allows you to identify the most common computers within your organization that are attempting to access infected files. You may want to investigate how the computers 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, product name, and product version number, then the detailed list of occurrences for that system, 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 72](#).

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 that are attempting to access infected files. You may want to investigate how they are using their computers and the external information sources that they are accessing (possible sources for the infections).

Drill down within users to view counts by virus name, product name, and product version number, then the detailed list of occurrences for that user, 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 72](#).

Content Filter Report By Rule template

Use this report to view the number of times each content rule was triggered 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 72](#).

Content Filter Report By Rule And Time template

Use this report to view the number of times each content rule was triggered 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 72](#).

Content Filter Report Rules Triggered template

Use this report to view the number of times individual users triggered a content rule by month, in a stacked bar chart format.

You can view report details by computer 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 72](#).

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 72](#).

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 triggering 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 go to 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 72](#).

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 72](#).

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 72](#).

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 triggered the event (Offending IP), action taken, and the URL that triggered 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 72](#).

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 triggered 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 the AVERT link next to each virus name to go to 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 72](#).

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 each virus name to go to 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 72](#).

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 72](#).

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 the AVERT link next to each virus name to go to 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 72](#).

Anti-Virus Coverage and Infection subreports

Most coverage reports and several infection reports include links to subreports that provide historical data on computers, compliance, upgrades, and infections and detailed data on policies, tasks, updates, and infections.

- [Compliance Summary subreport on page 67](#).
- [Computer Summary subreport on page 67](#).
- [Infection History subreport on page 67](#).
- [Infection Summary subreport on page 67](#).
- [Policy subreport on page 67](#).
- [Task subreport on page 67](#).
- [Update Errors subreport on page 67](#).
- [Upgrade History subreport on page 68](#).

Computer Summary subreport

Use this subreport to compare compliant versus non-compliant computers over time.

Compliance Summary subreport

Use this subreport to view the percentage of compliant computers over time.

Infection History subreport

Use this subreport to view the infection history on client computers.

Infection Summary subreport

Use this subreport to compare detected and unresolved infections and to view the number of infected computers over time.

Policy subreport

Use this subreport to view the policy settings on client computers.

Task subreport

Use this subreport to view the tasks scheduled on client computers.

Update Errors subreport

Use this subreport to view client computer messages related to updating.

Upgrade History subreport

Use this subreport to view the product upgrade history of client computers.

Rogue System Detection report templates

The Rogue System Detection report templates are:

- [Rogues Detected by Time](#) on page 68.
- [Missing Sensor](#) on page 68.
- [Rogues Detected by Domain](#) on page 68.

Rogues Detected by Time

Use this report to view the number of rogue systems detected over a period of time.

Missing Sensor

Use this report to view known monitored subnets and known unmonitored subnets.



This report does not show any information regarding any subnets about which the ePolicy Orchestrator does not know.

Rogues Detected by Domain

Use this report to view the number of rogue systems detected per domain.

Entercept report templates

The Entercept report templates are:

- [Entercept Agent Details](#)
- [Entercept Agent State](#)
- [Entercept Agent Type](#)
- [Entercept IPS Events Details](#)
- [Entercept Firewall Event Details](#)
- [Top 10 Attacked Machines — IPS](#)
- [Top 10 Attacked Machines — Firewall](#)

Entercept Agent Details

Use this report to view the current details (in a column chart format) of the Entercept agents in your environment. Details include:

- Agent machine name
- Version
- Type
- Host IPS state-mode
- Network IPS state-mode
- Firewall state-mode

Entercept Agent State

Use this report to view the details of the state of the Entercept agents in your environment. The details are represented in two pie charts. Details include:

- Agent IPS status/operating mode
- Firewall status/operating mode

Entercept Agent Type

Use this report to view the distribution of types of Entercept agents across your environment. The distribution details are represented in a pie chart.

Entercept IPS Events Details

Use this report to view historical details of Entercept 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

The System Compliance Profiler report templates are:

- [Historical Summary by Severity](#).

- [Compliance & Non-Compliance Summary.](#)
- [Non-compliance by Computer Name.](#)
- [Non-Compliance Summary by Group.](#)
- [Non-Compliance Summary by Severity.](#)



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 computers violated it, and when.

Compliance & Non-Compliance Summary

Use this report to view the number of scanned computers 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 computers that contributed to the percentage of non-compliant computers.
- Computer details — Provides information on a specific computer, 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 computer violates. The table lists each scanned computer's host name and IP address.

You can drill down and view more specific data on:

- **Computer summary** — Provides system information for a specific computer, 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 computers that violated a specific rule.
- **Violation time details** — Provides system information for a specific computer, 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 computers violated each rule.
- **Rule details** — Provides detailed information on a specific rule, indicating which computers violated it, and their general system information.

Criteria used to limit report results

You can limit the results of reports in the **Report Data Filter** dialog box using these criteria. The criteria vary depending on the report. Criteria for all predefined reports are described below:

- **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 computer 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 computers in the selected site or group under the **Directory**. Data for groups and computers 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 computers.
- **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 computer.

- **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.

Computer query templates

The computer queries provide information on the computers in your organization:

- [All Connecting Computers query template on page 74.](#)
- [Hourly ASCII Count query template on page 74.](#)
- [Computers With No Protection query template on page 74.](#)
- [Computers By Language query template on page 75.](#)
- [Computers By OS Type query template on page 75.](#)
- [Computers By Timezone query template on page 75.](#)
- [Computers By ePONode query template on page 75.](#)
- [Count Of All Connecting Computers query template on page 75.](#)
- [OS Summary query template on page 75.](#)
- [Policy Changes \(Computers\) query template on page 75.](#)
- [Policy Changes \(Groups\) query template on page 75.](#)

All Connecting Computers query template

Use this query to view the computer properties of all client computers with agents that have connected to the ePolicy Orchestrator server, sorted by computer 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 computers without any supported anti-virus protection software, sorted by each computer's location in the **Directory (ePONodeName)**. In addition to computers without any supported anti-virus protection software, client computers 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 computers, sorted by locale ID and each computer's location in the **Directory** (ePONodeName). Because this query provides the locale settings of client computers, 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 computers, sorted by operating system platform, version and each computer's location in the **Directory** (ePONodeName). Because this query provides operating system information of client computers, 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 computers, sorted by time zone and each computer's location in the **Directory** (ePONodeName). Because this query identifies the time zone in which client computers 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 computers sorted by their location in the **Directory** (ePONodeName).

Count Of All Connecting Computers query template

Use this query to view the total number of computers 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 computers. Use with the **Computers by OS Type** query to view outdated software and upgrade requirements.

Policy Changes (Computers) query template

Use this query to view policy changes by computer.

Policy Changes (Groups) query template

Use this query to view policy changes by group.

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 76.](#)
- [All Scanning Events By ePONode query template on page 76.](#)
- [All Non-Compliance Events on page 76.](#)
- [All Product Update Events query template on page 76.](#)
- [All Replication Failures on page 76.](#)
- [All ePO Server Events on page 77.](#)
- [Count Of All Scanning Events query template on page 77.](#)
- [Count Of All Product Update Events query template on page 77.](#)
- [Count of All Infections query template on page 77.](#)
- [Scanning Event Summary query template on page 77.](#)
- [First Virus Occurrence query template on page 77.](#)
- [Summary of Past Outbreak Events query template on page 77.](#)
- [Upgrade Summary query template on page 77.](#)
- [Upgrade Summary by Date query template on page 77.](#)
- [Server Task Log query template on page 77.](#)
- [All Infections query template on page 77.](#)
- [All Infections By Virus Name query template on page 77.](#)

All Scanning Events query template

Use this query to view all events generated when files are scanned on client computers, 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 computer, 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 computer, 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 computers.

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 computer.

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 computers 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 computers. These queries are based on the computer and product properties stored in the ePolicy Orchestrator database.

- [All AV Installations by Last Contact query template on page 78.](#)
- [All Installations query template on page 78.](#)
- [All Installations By ePONode query template on page 78.](#)
- [Compliance Comparison query template on page 78.](#)
- [Count Of All AV Installations query template on page 78.](#)
- [Count Of All Installations query template on page 78.](#)

All AV Installations by Last Contact query template

Use this query to view all anti-virus product installations and computer 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 computer'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 computer's location in the **Directory** (ePONodeName) and product.

Compliance Comparison query template

Use this query to view computers 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, 56
- adding
 - custom report templates, 26
 - your own queries, 29
- Agent versions report, 46
- agent-to-server communication interval(See ASCII)
- ASCII
 - connection interval report, 45

C

- compliance reports
 - Product Protection Summary, 52
- configuring
 - report filter, 15
- creating
 - SQL queries, 25
 - your own SQL query tables, 29
- Crystal Reports, 11

D

- DAT file
 - deployment summary report, 48
 - engine coverage report, 50

E

- Engine deployment summary report, 51
- exporting
 - report data to other formats, 9, 24

F

- filter, for reports, 15

G

- generating
 - SQL queries, 25
 - your own custom query tables, 29

N

- number of infections detected
 - monthly showing viruses report, 59 to 60

P

- printing your report, 24
- Product Protection Summary report, 52

Q

- queries, 10 to 25
 - saving as template, 10
 - SQL, 25
 - templates, 74 to 78
- query results, copy and paste, 25

R

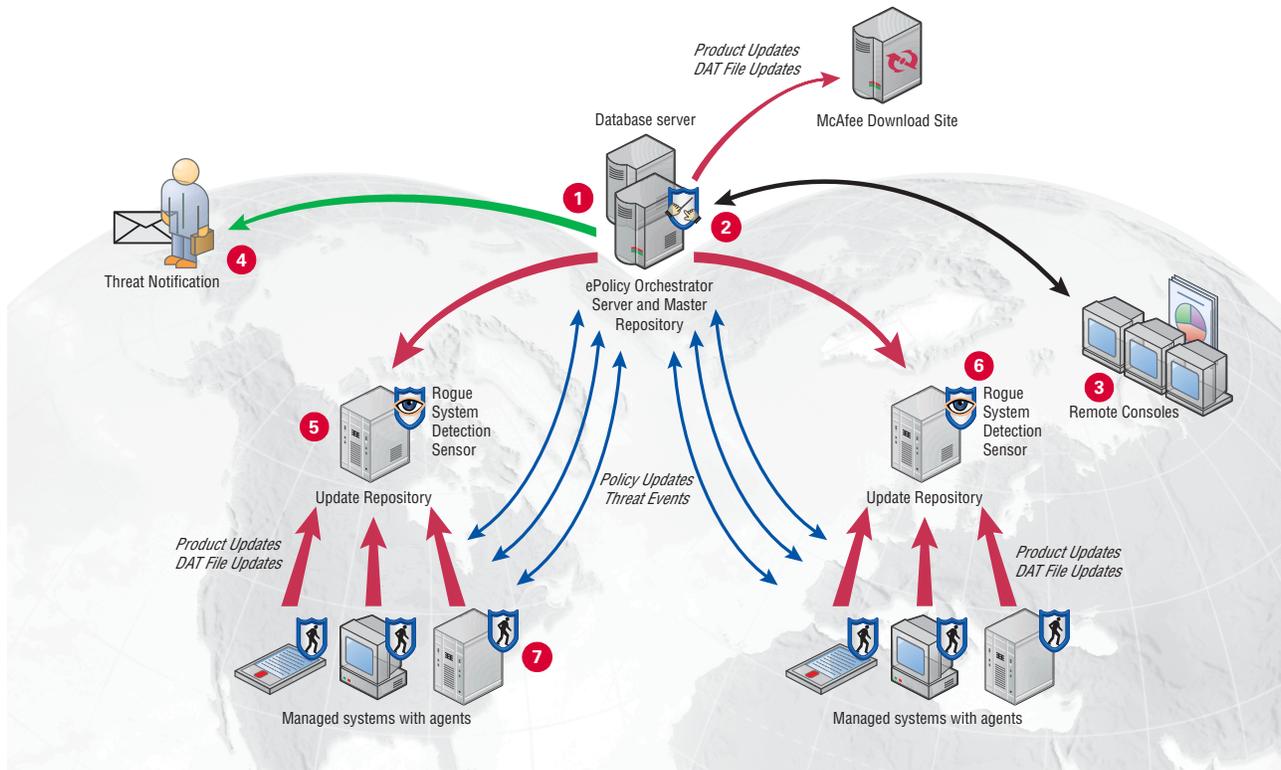
- release features
 - Product Protection Summary report, 52
- report filter, 15
 - setting, 15
- reporting
 - exporting reports, 9
 - generating, 7
 - introduction, 5
 - queries, 10
 - results, 8
 - saving reports and queries as template, 10
- reports
 - about, 6
 - Action Summary By Top 10 Files Resolved, 56
 - exporting data to other formats, 9, 24
 - Product Protection Summary, 52
 - regenerating, 24
 - specifying options, 14
 - templates, 56 to 78

S

- setting
 - report filter, 15
- specifying
 - reporting options, 14
- SQL
 - queries, generating, 25

T

- templates
 - report and query, 44 to 78
- Top 10 reports
 - detected viruses report, 62
 - infected files bar report, 62
 - infected machines bar report, 62
 - infected users bar report, 63



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 updates and signatures. Update repositories provide user-specified updates and signatures to the managed systems from the master repository.
- 3 Remote consoles** — Used to access 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** — ePolicy Orchestrator can alert you immediately to threat and compliance events in your environment via standard e-mail, text pager, SMS, or SNMP trap. See *Alerting you to specific events in your environment*.
- 5 Update repository** — 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 set up, 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. For more details, see *Keeping your systems up-to-date*.
- 6 Rogue System Detection (RSD) sensor** — The sensor resides on one system per subnet and notifies you when a rogue system enters the environment and can then initiate an automatic response to take on that system, such as deploying an agent. See *Detecting rogue systems on your network automatically*.
- 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 of the managed systems.

Detecting rogue systems on your network automatically

Knowledge of all systems connected to the network is critical to enforcing policy compliance successfully and reducing risk for the enterprise. Rogue System Detection enables ePolicy Orchestrator administrators to see previously unknown and unmanaged systems that connect to their LAN.

Rogue System Detection identifies unmanaged systems by passively listening on each subnet, enabling administrators to improve system security compliance significantly and reduce these potential threat propagation sources or infection targets. Through distributed sensors, ePolicy Orchestrator is constantly monitoring, in real time, new system connections to the LAN and establishing a **Rogue** or **Managed** status. ePolicy Orchestrator then provides several manual or automatic responses.

Checking the status of your systems and machines

- 1 Click **Rogue System Detection** in the console pane.
- 2 Select the **Machines** tab in the details pane.
- 3 Click **Summary** for an overview of all systems or all subnets and their status.
- 4 Click **List** to view a list of all systems and their status.

Machines		
Rogue Machines	133	99%
Inactive Machines	0	0%
Managed Machines	1	0%
Exception Machines	0	0%
Total Machines	134	99%

Subnets		
Uncovered Subnets	0	0%
Covered Subnets	1	100%
Total Subnets	1	100%

Detecting rogue systems automatically

The new Rogue System Detection feature allows you to configure automated responses to detected rogue systems:

- Identify and provide notification of unmanaged systems when they come on to the network.
- Deploy an agent to the system and enforce policies.
- Place the now managed system in a site in the **Directory**.
- Notify the desired individuals when this occurs.
- Execute a specified command line.

Automatic responses when a system is detected

An automatic response is defined by setting conditions that, when met, launch a specified action.

Conditions include but are not limited to:

- **Address** — MAC or IP address.
- **Name** — NetBIOS or DNS name.
- **Operating system information** — Operating system platform, family or version.
- **Detect time** — First or last detection.
- **Rogue type** — Examples: managed, without an agent, with an inactive agent, with an alien agent.
- **Status** — Examples: exception, inactive, rogue, managed.
- **Friendly name** — The name of a system (DNS, NetBIOS, IP, or MAC). Using this condition allows you to single out a specific system for a specific action. For example, you want to push an agent and enforce policy onto any system that comes into your environment, except a system that is managed by a different ePolicy Orchestrator server.

Actions include but are not limited to:

- **Send e-mail** — Sends an e-mail to desired recipients that the event occurred.
- **Add to ePO tree** — Adds the system to the ePolicy Orchestrator **Directory**.
- **Push ePO Agent** — Pushes the agent to the system.
- **Mark for Action** — Identifies the system as one requiring the administrator to take action on it manually.
- **Mark as Exception** — Identifies the system as one that does not require any action.

Property	Comparison	Value	Delete
Friendly Name	contains	DSK_FINANCE	<input checked="" type="checkbox"/>

Method	Parameters	Delete
Mark For Action	(none)	<input checked="" type="checkbox"/>

Available Actions:

- Mark For Action
- Add to ePO tree
- Mark as Exception
- Push ePO Agent
- Query ePO agent
- Remove Host
- Send E-mail
- Send ePO Server Event

Ensuring systems on your network are compliant

First released in February 2004 as a standalone product, the System Compliance Profiler is an integral component of ePolicy Orchestrator 3.5, enabling administrators to quickly assess the presence of Microsoft security patches and specified files or applications. Profiling is based on rules (customized by the administrator or downloaded templates from McAfee) that search for a file, service, registry key or specific Microsoft patch number. Patch fingerprinting (utilizing MD5 hash codes) is also available to ensure absolute integrity of Microsoft security patches and prevent patch spoofing. Severity of compliance is set by the administrator and easily monitored in the form of detailed, graphical compliance reports.

The release of ePolicy Orchestrator 3.5 marks the first time that System Compliance Profiler is packaged and shipped with ePolicy Orchestrator and includes a number of administrative efficiency and usability enhancements, including:

- Improved accuracy through reboot state awareness.
- Improved user interface performance for large sets of rules.
- Customized grouping and sorting of templates.

System Compliance Profiler rules

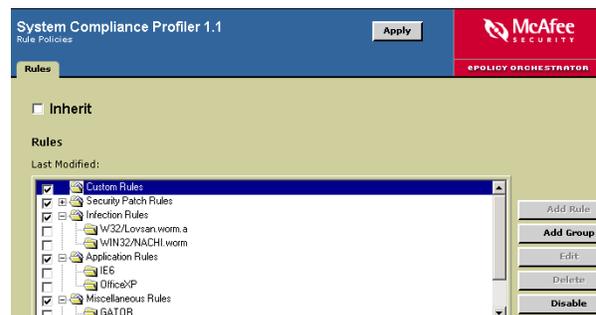
System Compliance Profiler uses rules to determine the compliance of the systems in your environment. Although you can add rules and customize them and their organization, several are shipped with ePolicy Orchestrator by default. Rules can be readily enabled or disabled.

Default rule groups include:

- **Security Patch Rules** — Check for compliance of Microsoft patches on your systems.
- **Infection Rules** — Search for the presence of malware on your systems.
- **Application Rules** — Identify which systems are not installed with specific applications, such as Microsoft Internet Explorer 6, or Office XP.
- **Miscellaneous Rules** — Search for systems that have specific instant messaging or peer-to-peer file sharing programs.

You can view and enable or disable these rules (as well as create your own) by clicking the **Directory** in the console tree, then selecting **System Compliance Profiler | Rules** on the **Policies** tab of the upper details pane.

System Compliance Profiler rule selection



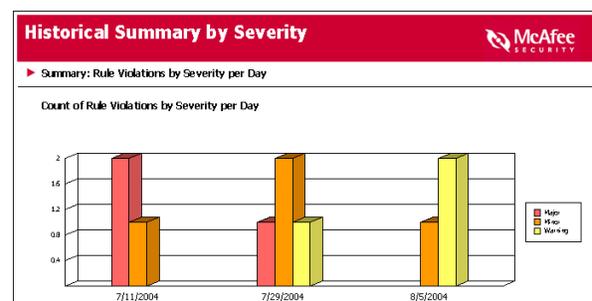
Viewing System Compliance Profiler results

Results of System Compliance Profiler scans are viewable with the reporting functionality of ePolicy Orchestrator. ePolicy Orchestrator 3.5 ships with five report templates specific to System Compliance Profiler:

- Historical Summary Distributed by Severity
- Compliance/Non-Compliance Summary
- Non-Compliance by Computer Name
- Non-Compliance Summary by Group
- Non-Compliance Summary by Severity

You can create a rule in ePolicy Orchestrator Notifications to send an e-mail message when non-compliance is found by the System Compliance Profiler.

System Compliance Profiler Report



Alerting you to specific events in your environment

Instant, proactive information is critical for a security professional especially when monitoring compliance and threat activity. ePolicy Orchestrator 3.5 delivers integrated alerting and notification on compliance, threat activity and rogue systems within the environment. Thresholds, defined by the administrator, enable critical alerts to be sent to specified individuals via e-mail, SMS, text pager or SNMP trap. Notifications cover threat activity, anti-virus compliance levels and rogue system connections. Administrators can also enable proactive execution of specific commands (for example, RUN.EXE) when a rule's conditions are met.

These rules not only allow you to associate specific events, but they also allow you to define the number and frequency of events to be received for the rule to be triggered. For example, you can define these rules to send administrators messages when 1000 virus detection events have occurred within an hour, or whenever a replication or pull task failed.

Creating a rule to alert you of events

Although ePolicy Orchestrator comes with several default rules, you can create rules once you configure Notifications. Click **Notifications** in the console tree, then select the **Rules** tab and click **Add Rule** to begin the **Create or Edit Notification Rule** wizard.

This wizard allows you to create the rules that, when triggered, send notification messages to alert you to events you have specified. The wizard contains five steps:

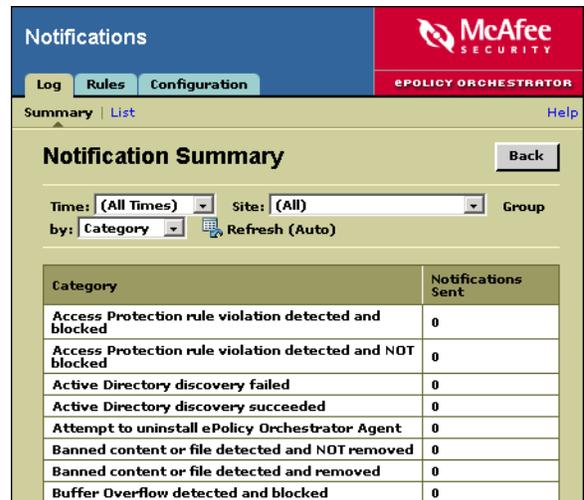
- **Describe Rule** — This page allows you to name and describe the rule, define the site or group to which the rule applies and select the **Rule Priority** so that e-mail messages are flagged appropriately.
- **Set Filters** — This page allows you to select the event categories that trigger the rule. These can be, but not necessarily, specified by product. Here you can also choose whether the rule applies to workstation or server operating systems, or both.
- **Set Thresholds** — This page allows you to specify **Aggregation** and **Throttling** for the rule. Aggregation options allow you to specify when the rule is triggered. For example, you can specify that a notification message is sent when the number of systems affected reaches a specific number, or when a specified number of these events are received within a specified time frame. Throttling allows you to define an amount of time within which you don't want to receive more than one message for the type of event specified in the rule. Using throttling and aggregation allows you to save bandwidth and prevent your inboxes from getting cluttered with unnecessary messages. For example, you can set a virus detection rule to send a notification message when the number of affected systems is at least 500 or when the number of events is at least 1000, either within one hour. Then you can also specify that you want this rule to send no more than one message every 5 hours.
- **Create Notifications** — This page allows you to specify the messages that are sent, their types, and their recipients. Here you can also specify any external commands you want to run when the rule is triggered.
- **View Summary** — This page displays a summary of the rule's configuration and allows you to choose whether to enable the rule.

Viewing a summary or list of all notifications

ePolicy Orchestrator Notification keeps a log of the notification messages it generates. You can view these in either a summary view or a list view. Both views are configurable so that you can choose to arrange the information, any moment, by different pieces of information. For example, in the summary view, you can choose to sort the information by product, category, priority, or rule name. And in the list view, you can filter the information by criteria, such as systems, Domain Controllers, and many others.

To view the Notification log:

- 1 Select **Notifications** in the console tree.
- 2 Select the **Log** tab in the details pane.
- 3 Click **Summary** or **List**, as desired.
- 4 Select a **Time**, **Site**, or **Category** to provide a more specific view of the desired notifications in the log.



The screenshot shows the McAfee ePolicy Orchestrator interface. The top navigation bar includes 'Log', 'Rules', and 'Configuration' tabs. Below this, there are 'Summary' and 'List' buttons. The main content area is titled 'Notification Summary' and includes a 'Back' button. There are filters for 'Time' (set to 'All Times'), 'Site' (set to 'All'), and 'Group'. A 'Refresh (Auto)' button is also present. Below the filters is a table with two columns: 'Category' and 'Notifications Sent'.

Category	Notifications Sent
Access Protection rule violation detected and blocked	0
Access Protection rule violation detected and NOT blocked	0
Active Directory discovery failed	0
Active Directory discovery succeeded	0
Attempt to uninstall ePolicy Orchestrator Agent	0
Banned content or file detected and NOT removed	0
Banned content or file detected and removed	0
Buffer Overflow detected and blocked	0

Integrating Active Directory into your Directory management

System discovery and administrative efficiency are a key focus of ePolicy Orchestrator 3.5. This is especially true for enterprises that have made a significant investment in Microsoft Active Directory. ePolicy Orchestrator 3.5 provides administrators with simplified change control within Active Directory environments with two tools: The **Active Directory Import** wizard and the **Active Directory Computer Discovery** task.

The combination of these tools allows you to both create and maintain your ePolicy Orchestrator **Directory** directly from Microsoft Active Directory. Customers upgrading from a previous version of ePolicy Orchestrator will notice time savings.

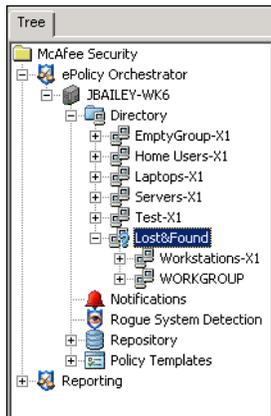
For both the **Active Directory Import** wizard and the **Active Directory Computer Discovery** task, you can define any Active Directory subcontainers as exceptions—if there's a group (or groups) of computers that are organized in their own subcontainers that you do not want managed by ePolicy Orchestrator, you can exclude those subcontainers.

Active Directory Import

Use the **Active Directory Import** wizard for the first-time creation of the ePolicy Orchestrator **Directory**, or whenever you are creating complete sites from scratch. This tool imports systems from Active Directory directly into the ePolicy Orchestrator **Directory** root or a site of the **Directory**, creating the same structure as the one you are pulling in from Active Directory.

To begin the wizard, simply right-click **Directory** in the console tree and select **All Tasks | Active Directory Import**. When the wizard appears, click **Next** to begin.

New sites brought into Lost&Found

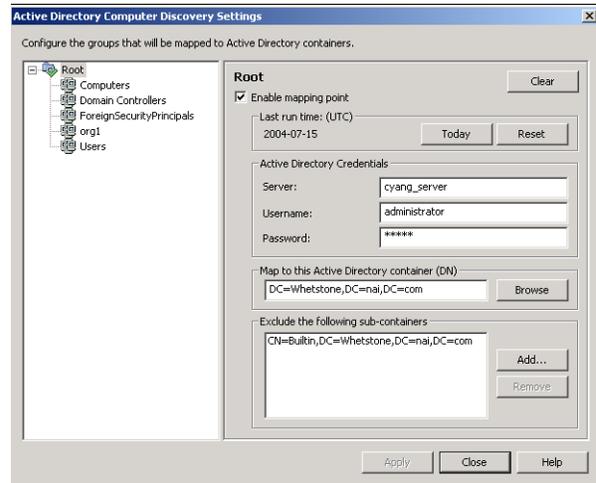


When the computers have been imported into the **Lost&Found** of the ePolicy Orchestrator **Directory**, you can easily deploy agents to them, and then move the structure from the **Lost&Found** to the root of the tree to create your managed ePolicy Orchestrator **Directory**.

Active Directory Computer Discovery

If you've already created your ePolicy Orchestrator **Directory**, then use the **Active Directory Computer Discovery** task to bring any new systems into it—whether they were created by the **Active Directory Import** wizard or created in a previous version of ePolicy Orchestrator.

Configuring the Active Directory Computer Discovery task



After mapping Active Directory containers to sites within the ePolicy Orchestrator **Directory**, this task regularly polls Active Directory containers at an interval set by the administrator to discover any new systems that have been added to the network. It then imports those systems into the **Lost&Found** group of the site corresponding to the Active Directory container within which the system was found. When they are placed in **Lost&Found**, they are nested into a copy of the **Directory** structure, indicating which site or group where they should be placed once you've determined they have functioning agents.

The combination of the wizard and the discovery task enables you to fully integrate the power of Microsoft Active Directory into your ePolicy Orchestrator **Directory** management.

Keeping your systems up-to-date

One of the most difficult aspects of proactively managing a security policy is keeping all systems updated with the latest protection. ePolicy Orchestrator 3.5 allows you to easily keep the security software on the systems of your network up-to-date. The software provides the ability to configure different updating infrastructures for different environments, or for different parts of a single environment. Regardless of the method you choose, you can automate the updating process or initiate it manually.

ePolicy Orchestrator can manage the updating of:

- Signatures and engines — For example, IDS signatures, virus definition (DAT) files, and System Compliance Profiler rules.
- Patches and service packs — For managed McAfee products, and even Norton Antivirus.

You can set up SuperAgent repositories or distributed repositories for your updating needs. Regardless of which type you choose, you can select which types of updates (DAT files, engine, products, or patches) you want to deploy, and which types you don't want to deploy.

SuperAgent repositories and global updating

Using SuperAgent repositories and the global updating capability of ePolicy Orchestrator allows you to update your security products automatically as soon as a new DAT or update of a specified product is checked into the master repository. This method is also faster, updating as many as 50,000 client systems within an hour. This method utilizes your SuperAgents as repositories, therefore it is unnecessary for you to create, configure, and organize additional distributed repositories. To implement global updating:

- Enable an agent on each subnet as a SuperAgent repository.
- Enable global updating.

For each system you want to host a SuperAgent repository:

- 1 Select the system in the **Directory**.
- 2 On the **Policies** tab of the upper-details pane, select **ePolicy Orchestrator Agent | Configuration**.
- 3 On the **General** tab in the lower-details pane, deselect **Inherit**, then:
 - a Select **Enable SuperAgent functionality**.
 - b Select **Enable SuperAgent repository**.
 - c Type a path to use for the repository.
 - d Click **Apply All**.

To enable global updating:

- 1 Select the ePolicy Orchestrator server in the console tree.
- 2 Select the **Settings** tab in the details pane.
- 3 Click **Yes** next to **Enable global updating**.
- 4 Select the desired signatures, engines, and the desired products you wish to update via global updating

Distributed repositories

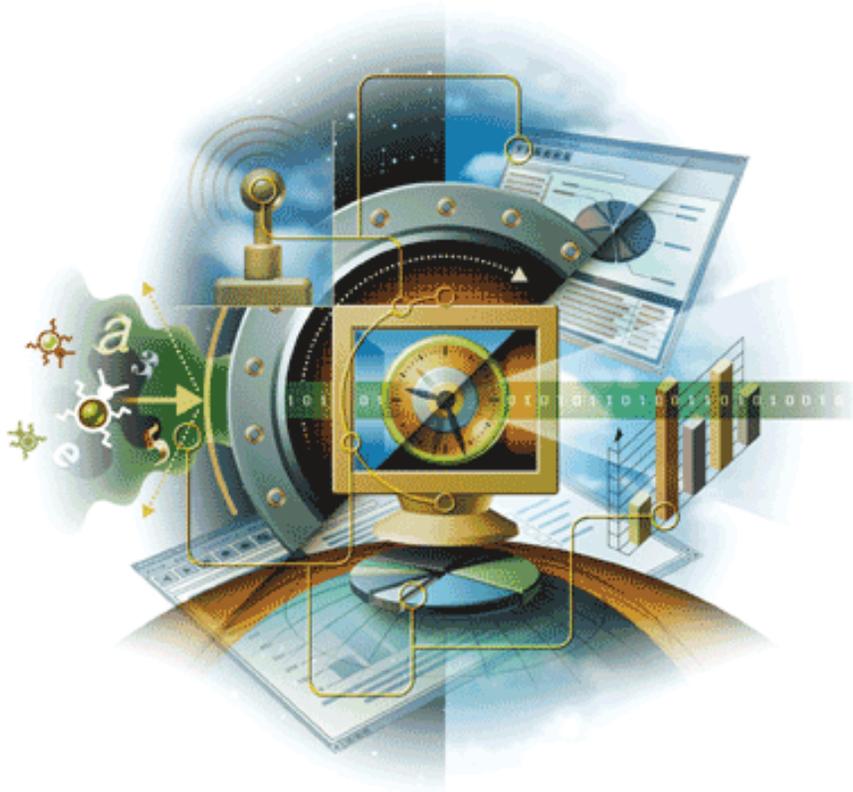
Distributed repositories can be HTTP, FTP, or on a UNC share. Using distributed repositories allows you to spread updating throughout your network if your subnets are not organized in a way that would spread the updating load efficiently. Distributed repositories receive the update packages from the master repository when a replication task is executed. Then, when a pull task is executed, the client systems pull the updates from the distributed repositories. To implement updating with distributed repositories:

- 1 Determine which systems you want to host distributed repositories.
- 2 Create the repository on the specified system. For example, a UNC share.
- 3 Add the repository to the ePolicy Orchestrator server with the **Add repository** wizard.
- 4 Configure and schedule the pull and replication tasks or initiate the pull and replication tasks manually.

ePolicy Orchestrator®

Deploy and manage anti-virus and security products
for your entire enterprise

version 3.5



McAfee® System Protection

Industry-leading intrusion prevention solutions

COPYRIGHT

Copyright © 2004 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Entercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Coliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Viruscan, Virusscan, Virusscan (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. 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.

PATENT INFORMATION

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

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 provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. • Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. • Software written by Douglas W. Sauder. • Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. • Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. • FEAD™ Optimizer™ technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In™ Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In™ HTML Export, © 2001 Stellent Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1989. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems®, Inc. © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, © 1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, © 2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors. • Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>). • Software copyrighted by Kevin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. • Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, © 2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. • Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Contents

Getting Started

1	Introducing ePolicy Orchestrator	7
	About ePolicy Orchestrator	8
	What's new in this release?	10
	Using this guide.	14
	Resources	16
2	Getting Started with ePolicy Orchestrator Servers	21
	Logging onto ePolicy Orchestrator servers	21
	Install the security certificate for Notification and Rogue System Detection	23
	Managing accounts for ePolicy Orchestrator administrators.	25
	About server settings, tasks, and events	29
	Viewing server events from the console.	33
	Viewing the ePolicy Orchestrator server version number	34
	The Getting Started wizard	35
3	Creating a Directory of Managed Computers	39
	About creating the Directory	40
	Things to consider when planning Directory organization.	46
	Methods for creating the Directory.	48
	Adding WebShield appliances	56
4	Deploying Agents, SuperAgents, and Sensors	57
	About deploying the ePolicy Orchestrator agent	57
	Using ePolicy Orchestrator to deploy the agent	60
	Installing the agent with logon scripts.	64
	Installing the agent manually.	66
	Other ways to deploy the agent	67
	Upgrading agents from a previous version	69
	Deploying the agent to Novell NetWare servers and WebShield appliances	72
	Uninstalling the agent	72
	Agent installation command-line options	73
	Deploying SuperAgents to distribute agent wakeup calls	75
	Deploying Rogue System Detection sensors	78
5	Deploying Anti-Virus and Security Software	88
	About deploying products with ePolicy Orchestrator	89
	Check in product deployment packages to the master repository	89
	Check in NAP files to manage new products	93
	Use the deployment task to install products on clients	94

Creating an Update Infrastructure

6	Keeping DATs and Engines Up-to-Date	99
	About master, source, and fallback repositories	100
	Define a source repository to update DATs and engines	103

	Use Pull tasks to update the master repository from a source repository	107
	Manually check in engine, DAT and EXTRA.DAT updates	112
	Distributing DAT and engine updates to clients.	115
	Evaluate new DATs and engines before deploying to your whole organization. . .	123
	Moving or deleting DAT and engine packages.	127
7	Update Large Networks with Distributed Repositories	130
	About distributed repositories.	130
	Create distributed repositories	132
	Replicating the master repository contents to distributed repositories	139
	Configure agent policies to use appropriate distributed repository.	141
	Using local distributed repositories that are not managed through ePolicy Orchestrator	143
	Managing the SITELIST.XML repository list	145

Managing Policies for Agents and Products

8	Managing Deployed Agents	148
	About the agent-to-server communication interval (ASCI)	148
	Sending manual agent wakeup calls	150
	Using the agent policy pages to set policies.	153
	Viewing properties of the agent and products from the console	158
	Checking agent logs	159
	Working with the agent from the client computer	161
9	Managing Product Policies and Running Client Tasks	163
	About policies and ePolicy Orchestrator	163
	Using policy pages to manage product settings	164
	Remove policy pages for unused products from the Repository	168
	Copying, exporting, and importing policies	169
	Reset the default policy settings	173
	Configure client on-demand scans and update tasks	174
10	Determining Compliance	180
	System Compliance Profiler	180
	Compliance Check server task	181
	ePolicy Orchestrator Notification	183

Dealing Proactively with Events

11	Rogue System Detection	185
	About Rogue System Detection	185
	Monitor detected systems and deployed sensors	192
	Configure Rogue System Detection sensor policies.	197
	Take manual actions on detected rogues	201
	Configure automatic responses for specific events	207
	Configure third party command line executables to use in automatic responses	212
	View status of actions taken and view event history	214
	Customize the Rogue System Detection server and interface	217
	Configuring Rogue System Detection for ePolicy Orchestrator Notification	221
	Frequently Asked Questions	223
12	ePolicy Orchestrator Notification	224
	Understanding how it works	225
	Determining when events are forwarded	229
	Determining which events are forwarded	230
	Planning.	231
	Configuring ePolicy Orchestrator Notification	231

Viewing the history of Notifications	240
Frequently asked questions	245

Stay Prepared with Periodic Maintenance

13	Getting Started with Reporting	247
	About pre-defined reports in ePolicy Orchestrator	248
	How to generate a report in ePolicy Orchestrator	249
	Viewing report results in the report window	250
	Print or export reports into publishable formats	251
	Running Queries to get detail	252
	Saving filtered reports and queries as templates	252
14	Maintaining the Directory	254
	Using Active Directory discovery	254
	Keeping imported NT domains synchronized with sites in the Directory	257
	Maintaining IP filters for sites and groups	260
	Scheduling a daily server task to find inactive agents in your Directory	265
	Use Directory Search to find computers in the Directory	267
	Manually moving nodes in the Directory	268
15	Preparing for and Managing Virus Outbreaks	270
	Things to do on a daily or weekly basis to stay prepared	270
	Checklist — Are you prepared for an outbreak?	272
	Other methods to recognize an outbreak	273
	Checklist — You think an outbreak is occurring	274
16	Maintaining ePolicy Orchestrator Databases	276
	Perform daily or weekly database maintenance	276
	Back up your ePolicy Orchestrator database regularly	279
	Repairing events and computer names in the database	281
	Deleting old events from the database periodically	282
	Changing SQL Server user account information	283
	Restoring ePolicy Orchestrator databases in the event of software or hardware failure	285

Appendices, Glossary, and Index

Minimum Escalation Requirements Tool	288
Audit log	288
Internet scenarios	290
Remote access via VPN and RAS	290
Corporate intranet	291
Connecting through an ISP and a firewall	291
Configuring the firewall for ePolicy Orchestrator	292
Agent-to-server communications packet size	292
How to read operating system data	293
Action taken numbers	294
Locale IDs	294
Product IDs	295
Variables	296
Glossary	297
Index	308

SECTION 1

Getting Started

Provides an overview of ePolicy Orchestrator and covers tasks for getting up and running with your initial deployment after you have installed the ePolicy Orchestrator server. These include creating your **Directory** and ePolicy Orchestrator agents and security products such as VirusScan Enterprise to computers in your network.

Some of the tasks and features covered here, such as creating your **Directory** by importing NT domains or Active Directory containers, are one-time things you must do as part of your initial deployment. Others you may need to perform regularly as part of your daily and weekly server maintenance.

[Chapter 1, Introducing ePolicy Orchestrator](#)

[Chapter 2, Getting Started with ePolicy Orchestrator Servers](#)

[Chapter 3, Creating a Directory of Managed Computers](#)

[Chapter 4, Deploying Agents, SuperAgents, and Sensors](#)

[Chapter 5, Deploying Anti-Virus and Security Software](#)

1

Introducing ePolicy Orchestrator

An overview of the components and new features of version 3.5

ePolicy Orchestrator provides a scalable tool for centralized anti-virus and security policy management and enforcement. It also provides comprehensive graphical reporting and product deployment capabilities. Using ePolicy Orchestrator, you can manage policies for anti-virus and network security products and deploy McAfee products and product updates through a single point of control.

What is in this guide

<i>Getting Started</i>	<i>Chapter 1, Introducing ePolicy Orchestrator</i> <i>Chapter 2, Getting Started with ePolicy Orchestrator Servers</i> <i>Chapter 3, Creating a Directory of Managed Computers</i> <i>Chapter 4, Deploying Agents, SuperAgents, and Sensors</i> <i>Chapter 5, Deploying Anti-Virus and Security Software</i>
<i>Creating an Update Infrastructure</i>	<i>Chapter 6, Keeping DATs and Engines Up-to-Date</i> <i>Chapter 7, Update Large Networks with Distributed Repositories</i>
<i>Managing Policies for Agents and Products</i>	<i>Chapter 8, Managing Deployed Agents</i> <i>Chapter 9, Managing Product Policies and Running Client Tasks</i>
<i>Dealing Proactively with Events</i>	<i>Chapter 11, Rogue System Detection</i> <i>Chapter 12, ePolicy Orchestrator Notification</i>
<i>Stay Prepared with Periodic Maintenance</i>	<i>Chapter 14, Maintaining the Directory</i> <i>Chapter 16, Maintaining ePolicy Orchestrator Databases</i> <i>Chapter 15, Preparing for and Managing Virus Outbreaks</i>

What is in this chapter

This chapter contains the following topics:

- About ePolicy Orchestrator
- What's new in this release?

About ePolicy Orchestrator

The ePolicy Orchestrator software is comprised of the following components:

- The ePolicy Orchestrator server — A repository for all data collected from distributed ePolicy Orchestrator agents.
- The ePolicy Orchestrator console — A clear, understandable view of all virus activity and status, with the ability to manage and deploy agents and products.
- The ePolicy Orchestrator agent — An intelligent link between the ePolicy Orchestrator server and the anti-virus and security products that enforces policies and tasks on client computers.

The ePolicy Orchestrator server

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

- A robust database that accrues data about product operation on the client computers in your network.
- A report-generating engine that lets you monitor the virus protection performance in your company.
- A software repository that stores the products and product updates (for example, Service Pack releases) 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 computers.

The ePolicy Orchestrator agent

The ePolicy Orchestrator agent is installed on target client computers and servers where it gathers and reports data, installs products, enforces policies and tasks, and sends events back to the ePolicy Orchestrator server. The agent runs in the background on client computers. It retrieves incremental changes to policies and tasks from the ePolicy Orchestrator server, then executes the policies, installs any downloaded products on the client computer, and performs all scheduled tasks.

When activity relating to products occurs on the client computer, the agent notifies the server. For example, if a virus appeared on the client computer, the information is sent back to the ePolicy Orchestrator console. This activity is invisible to the user of the client computer.

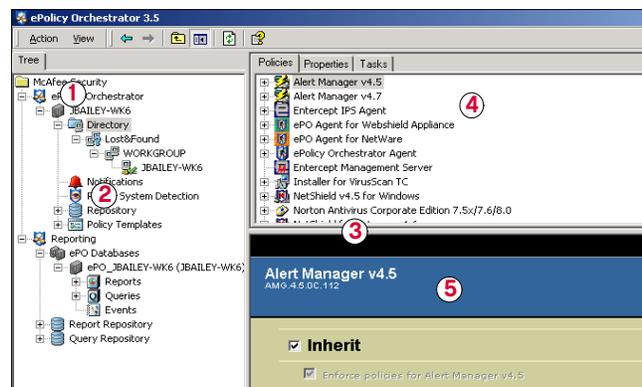
The ePolicy Orchestrator console provides great flexibility in deploying the agent. While it is designed for pushing the agent to your client computers, you can also copy the agent installation package onto a floppy disk, into a network share, or onto some other medium for manual installation on your client computers.

The ePolicy Orchestrator console

The ePolicy Orchestrator console allows you to manage your entire company's anti-virus and security protection and view client computer properties easily. Housed within the Microsoft Management console (MMC) user interface, the ePolicy Orchestrator console provides the ability to set and enforce anti-virus and security policies to all agents on client computers, or to selected computers. It also provides a task scheduling feature that lets you target specific computers or groups with scheduled tasks and policies. Finally, the console allows you to view and customize reports to monitor your deployment, virus outbreaks, and current protection levels.

When you start the ePolicy Orchestrator software, the ePolicy Orchestrator console appears. The console uses standard components of the Microsoft Management Console (MMC). The main components of the ePolicy Orchestrator console are described below. For more information on using the ePolicy Orchestrator console, see the MMC Help file.

Figure 1-1 Components of the console



- ① **Console tree** — Appears in the left pane of the console, and contains all of the console tree items.
- ② **Console tree items** — Include the **Directory**, **Repository**, and **Reporting**.
- ③ **Details pane** — Appears in the right pane of the console, and shows details of the currently selected console tree item. Depending on the console tree item you select, the details pane can be divided into upper and lower panes.
- ④ **Upper details pane** — Contains the **Policies**, **Properties**, and **Tasks** tabs.
- ⑤ **Lower details pane** — Contains the configuration settings for the products listed on the **Policies** tab in the upper details pane.

What's new in this release?

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

- [Rogue System Detection](#).
- [McAfee System Compliance Profiler integration](#).
- [ePolicy Orchestrator Notification](#).
- [Active Directory integration](#).
- [ePolicy Orchestrator Administrator auditing](#).
- [Support for variable MAC address](#).
- [Support for variable MAC address](#).
- [McAfee Enterccept integration](#).
- [Selective updating](#).

Rogue System Detection

Current release Rogue System Detection allows you to detect unmanaged computers that come on to your network, so that you can deploy an agent to the computer and enforce policies on it.

Benefits The risks associated with unmanaged and unprotected computers entering and infecting other computers in your network environment is diminished greatly.

Where to find In the console tree under the ePolicy Orchestrator server, click **Rogue System Detection**. The Rogue System Detection configuration tabs appear in the details pane.

For more information

- [Deploying Rogue System Detection sensors on page 78](#)
- [Chapter 11, Rogue System Detection](#)

McAfee System Compliance Profiler integration

- Current release** McAfee System Compliance Profiler 1.1 is shipped with ePolicy Orchestrator 3.5 and can be configured and managed like other products. This application allows you to determine when managed computers are non-compliant with Microsoft patches and Service Packs.
- Benefits** Lower risk of computers with out of date patches and service packs on your network becoming gateways for virus or hacker attack. Identify these computers to limit their exposure to security vulnerabilities.
- Where to find** The System Compliance Profiler deployment package and NAP files are installed on the ePolicy Orchestrator server. Deploy System Compliance Profiler and manage policies as you would any security product.
- For more information**
- [Chapter 10, Determining Compliance.](#)
 - The McAfee System Compliance Profiler 1.0 Configuration Guide.

ePolicy Orchestrator Notification

- Current release** The ePolicy Orchestrator Notification feature allows you to define rules that filter events from the managed products and the ePolicy Orchestrator server. When events from specified products, components, and of a specified category are received and processed a notification message is sent to specified individuals in your organization. These messages are configurable and can be sent via standard e-mail, SMS, text pager, or SNMP trap. This feature also provides the ability to execute specific external commands when the conditions of a rule are met.
- Benefits** Now you and other network security administrators can be alerted almost immediately when anti-virus and security events occur in your network.
- Where to find** In the console tree under the ePolicy Orchestrator server, click **Notification**. The Notification configuration tabs appear in the details pane.
- For more information** [Chapter 12, ePolicy Orchestrator Notification.](#)

Active Directory integration

Previous release	In previous releases, you had to import Active Directory computers manually from your network environment.
Current release	<p>The ePolicy Orchestrator Active Directory integration feature is comprised of two tools.</p> <p>The Active Directory Getting Started wizard is designed to import the Active Directory tree, and the computers contained in the tree, into the ePolicy Orchestrator Directory. This wizard allows you to create your ePolicy Orchestrator Directory, or portions of it, based on the Active Directory structure. This tool is only recommended when you are creating your ePolicy Orchestrator Directory, and if you want your ePolicy Orchestrator Directory, or portions of it, to be the same as your Active Directory structure.</p> <p>The Active Directory Computer Discovery task allows you to regularly poll Active Directory containers to discover new computers that have entered the network. When this task discovers unmanaged computers in Active Directory, they are placed in the Lost&Found group of the specified site, so you can easily deploy an agent to them and place them in the necessary site or group of the ePolicy Orchestrator Directory.</p>
Benefits	This feature allows you to more easily populate and manage the portions of your ePolicy Orchestrator Directory that contain computers from Active Directory, as well as assist you in enforcing compliance on new computers discovered on the network.
Where to find	In the console tree, right-click the Directory then select either Active Directory Import or Active Directory Discovery Settings , depending on your needs.
For more information	<ul style="list-style-type: none">■ Creating the Directory tree by importing from Active Directory on page 49■ Using Active Directory discovery on page 254

ePolicy Orchestrator Administrator auditing

Current release	<p>The audit log tracks many actions performed by ePolicy Orchestrator administrators and reviewers. These actions include:</p> <ul style="list-style-type: none">■ Logins■ Role changes■ Password changes■ Uninstallation of an agent by deletion■ Policy changes■ Addition or deletion of a site, group, computer, or user accounts.■ Renaming of sites, groups, or computers.
Benefits	<p>The ability to track ePolicy Orchestrator administrator and reviewer actions provides you greater efficiency when you need to research changes that have happened in your ePolicy Orchestrator environment.</p>
Where to find	<p>Once the feature is installed on the computer running the ePolicy Orchestrator database server, a log is created prior to midnight on each day and is stored in:</p> <pre>c:\epoaudit\</pre>
For more information	<p>Audit log on page 288.</p>

Support for variable MAC address

Current release	<p>The ePolicy Orchestrator 3.5 software supports variable MAC addresses. If you have laptops in your environment that connect to the network in multiple methods, they appear as the same computer regardless of which method it uses to connect to the network. For example, by network interface card (NIC) or docking station.</p>
Benefits	<p>If users in your environment use multiple methods to connect their computers to the network, being able to always identify that computer as a single computer provides greater efficiency in managing them.</p>
Where to find	<p>This is not a feature that has controls in the user interface.</p>

McAfee Enterscept integration

Previous release	This functionality did not exist in any previous release.
Current release	McAfee Enterscept is supported in this release. This application allows you to recognize and prevent intrusions into your environment. The ePolicy Orchestrator Notification rules can be configured to receive and process Enterscept events, and the ePolicy Orchestrator Report Repository includes several predefined Enterscept reports to consolidate and view Enterscept data.
Benefits	Enterscept integration in ePolicy Orchestrator allows you to proactively prevent intrusions in your environment, from the same central place you enforce policies and determine compliance, providing greater efficient use of your time.
For more information	See your McAfee Enterscept Configuration Guide.

Selective updating

Current release	The ePolicy Orchestrator 3.5 software allows you to tune updating to maximize protection and minimize network traffic. Configure separate update tasks to update clients with any combination of anti-virus signatures, engines, and product update packages in the repositories. Define what kinds of package check-ins to the master repository trigger a global update.
Benefits	By choosing exactly which update packages are going to be delivered over your network, you can utilize your available bandwidth more efficiently.
Where to find	<p>For global updating, select the ePolicy Orchestrator server in the console tree, then select the Settings tab. If you choose to Enable global updating, you can then specify which signatures, engines and products to update.</p> <p>For the desired site, group, or computer create an update task. On the Update tab of the Task Settings dialog box for the task, you can select which signature, engines and products to update.</p>
For more information	<ul style="list-style-type: none">■ Use global updating to automatically distribute updates to all clients immediately on page 115■ Create and schedule a daily DAT and engine client update task on page 118

Using this guide

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

Audience

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

Conventions

This guide uses the following conventions:

Bold Condensed	All words from the user interface, including options, menus, buttons, and dialog box names. Example: Type the User name and Password of the desired account.
<i>Courier</i>	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). Examples: The default location for the program is: <code>C:\Program Files\McAfee\EPO\3.5.0</code> Visit the McAfee web site at: <code>http://www.mcafee.com</code> Run this command on the client computer: <code>C:\SETUP.EXE</code>
<i>Italic</i>	For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material. Example: Refer to the <i>VirusScan Enterprise Product Guide</i> for more information.
<TERM>	Angle brackets enclose a generic term. Example: In the console tree under ePolicy Orchestrator , right-click <SERVER>.
	Note: Supplemental information; for example, an alternate method of executing the same command.
	Tip: Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.
	Caution: Important advice to protect your computer system, enterprise, software installation, or data.
	Warning: Important advice to protect a user from bodily harm when interacting with a hardware product.
	New: New or redesigned feature or option of this release of the product.

Resources

McAfee® products denote years of experience, and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects — all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

Refer to these sections for additional resources:

- Getting product information
- Links from within the product
- Product services
- 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.

Installation Guide — System requirements and instructions for installing and starting the ePolicy Orchestrator server.

Product Guide — Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.

Reports and Queries Implementation Guide — Detailed reference of reporting features and report and query templates.

Evaluation Guide — A quick introduction to the product focused on getting you up and running quickly in a limited test environment.

Help — High-level and detailed information accessed from the software application: Help menu and/or Help button for page-level help; right-click option for *What's This?* help.

Configuration Guide — *For use with ePolicy Orchestrator®.* Procedures for deploying and managing supported products through the ePolicy Orchestrator management software.

Quick Reference Card* — A handy card with information on basic product features, routine tasks that you perform often, and critical tasks that you perform occasionally.

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

Contacts^ — Contact information for McAfee services and resources: technical support, customer service, Security Headquarters (AVERT Anti-Virus & Vulnerability Emergency Response Team), beta program, and training. This file also includes phone numbers, street addresses, web addresses, and fax numbers for company offices in the United States and around the world.

License — The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement sets forth general terms and conditions for the use of the licensed product.

* A printed manual that accompanies the product CD. Note: Some language manuals may be available only as a .PDF file.

^ Text files included with the software application and on the product CD.

Links from within the product

The **Help** menu in the product provides links to some useful resources:

- Online Help
- Virus Information Library
- Submit a Sample
- Technical Support

Online Help

Use this link to access the online Help topics for the product.



If the product's built-in help system (accessed from within the software by clicking the **Help** menu) displays incorrectly on your system, your version of Microsoft® Internet Explorer may not be using ActiveX controls properly. These controls are required to display the help file. Make sure that you install the latest version of Internet Explorer.

Virus Information Library

Use the **Virus Information** link to access the McAfee Anti-Virus & Vulnerability Emergency Response Team (AVERT) Virus Information Library. This web site has detailed information on where viruses come from, how they infect your system, and how to remove them.

In addition to genuine viruses, the Virus Information Library contains useful information on virus hoaxes, such as those virus warning that you receive via e-mail. A *Virtual Card For You* and *SULFNBK* are two of the best-known hoaxes, but there are many others. Next time you receive a well-meaning virus warning, view our hoax page before you pass the message on to your friends.

To access the Virus Information Library:

- 1 Open the product interface.
- 2 Select **Virus Information** from the **Help** menu.

Submit a Sample

Use the **Submit a Sample** link to access the McAfee AVERT WebImmune web site. If you have a suspicious file that you believe contains a virus, or experience a system condition that might result from an infection, McAfee recommends that you send a sample to its anti-virus research team for analysis. Submission not only initiates an analysis, but a real-time fix, if warranted.

This option is available from the client security software interface, such as from the VirusScan Enterprise console. It is not available through the ePolicy Orchestrator console.

To submit a sample virus to AVERT:

- 1 Open the product interface.
- 2 From the **Help** menu, select **Submit a Sample**.
- 3 Follow the directions on the web site.

Technical Support

Use the **Technical Support** link to access the McAfee PrimeSupport KnowledgeCenter Service Portal web site. Browse this site to view frequently asked questions (FAQs), documentation, and perform a guided knowledge search.

To submit a sample virus to AVERT:

- 1 Open the product interface.
- 2 From the **Help** menu, select **Technical Support**.
- 3 Follow the directions on the web site.

Product services

The following services are available to help you get the most from your McAfee products:

- Beta program
- Patches
- Product “end-of-life” support

Beta program

The McAfee beta program enables you to try our products before full release to the public — you can learn about and test new features for existing products, as well as try out entirely new products. This program can help you test and implement updated and new features earlier, and in a safe environment. You get the chance to suggest new product features, as well as deal directly with McAfee engineering staff.

To find out more, visit:

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

Patches

Patches are released with updated files, drivers, and executables between the major releases of a product. To access the latest patches, visit:

<http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp>

Product “end-of-life” support

Your anti-virus software must be kept up-to-date to remain effective against viruses and other potentially harmful software. It is important to update the virus definition (DAT) files regularly. To enable the software to counter the continuing threat, we often make architectural changes to the way that the DAT files and virus-scanning engine work together. It is therefore important that you update your engine when a new version is released. An older engine will not catch many of the new emerging threats.

When we release a new engine, we announce the date after which the existing engine will no longer be supported. For information on our product “end-of-life” policy and for a full list of supported engines and products, visit:

http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

Contact information

Technical Support

Home Page	http://www.mcafeesecurity.com/us/support/
KnowledgeBase Search	https://knowledgemap.mcafeesecurity.com/phpclient/homepage.aspx
PrimeSupport Service Portal *	https://mysupport.mcafeesecurity.com

McAfee Beta Program

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

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

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

Download Site

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

Training

On-Site Training	http://www.mcafeesecurity.com/us/services/security/home.htm
McAfee University	http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm

Customer Service

E-mail	https://secure.mcafeesecurity.com/us/forms/support/request_form.asp
Web	http://www.mcafeesecurity.com/us/index.asp http://www.mcafeesecurity.com/us/support/default.asp

US, Canada, and Latin America
toll-free:

+1-888-VIRUS NO or **+1-888-847-8766**

Monday – Friday, 8 a.m. – 8 p.m., Central Time

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

Getting Started with ePolicy Orchestrator Servers

An introduction to the server, console, and user accounts

The ePolicy Orchestrator server is the “brain” of your managed security service. Using the server, you can manage all aspects of policy management, reporting, product deployment, and every thing else that ePolicy Orchestrator can do.

Before you begin using ePolicy Orchestrator to create your **Directory**, deploying agents and security products, and manage other aspects of your network’s anti-virus and security policies, there are a few things you should understand about the ePolicy Orchestrator server and the console.

This chapter covers the following topics:

- [Logging onto ePolicy Orchestrator servers](#)
- [Install the security certificate for Notification and Rogue System Detection](#)
- [Managing accounts for ePolicy Orchestrator administrators](#)
- [About server settings, tasks, and events](#)
- [Viewing server events from the console](#)
- [Viewing the ePolicy Orchestrator server version number](#)
- [The Getting Started wizard](#)

Logging onto ePolicy Orchestrator servers

When you open an ePolicy Orchestrator console, you must log into an ePolicy Orchestrator server to be able to manage it through the console.

Adding and removing servers in the console doesn’t start and stop the server

The ePolicy Orchestrator server runs as an NT service on the server computer. 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.

How to log on to ePolicy Orchestrator servers

You can use the ePolicy Orchestrator console to log into any ePolicy Orchestrator server. If you are at the computer where the ePolicy Orchestrator server is installed, you can log into the local server. If the server is located on a different computer from the console, as would be the case if you installed a remote console, you can use the remote console to log into an ePolicy Orchestrator server on another computer.

To add an ePolicy Orchestrator server to the console tree and log into it:

- 1 Launch ePolicy Orchestrator by choosing **Start | Programs | Network Associates | ePolicy Orchestrator**.
- 2 In the console tree, select **ePolicy Orchestrator**.
- 3 In the details pane under **Global Task List**, click **Log on to Server**. The ePolicy Orchestrator Login dialog box appears.

Figure 2-1 ePolicy Orchestrator Login dialog box



- 4 If you are at the ePolicy Orchestrator server, accept the default **Server name** that appears. If you are on a remote console and want to log into a server running on a different computer, type the name of that computer in **Server name**.
- 5 Type the **User name** and **Password** of the account you will use to log in. This account must be a valid ePolicy Orchestrator account that already exists on the server you're logging into.
- 6 Type the **HTTP Port** number used by the ePolicy Orchestrator server for console-to-server communication. If you are logging into a server running on the local computer, the HTTP Port field is automatically populated with the correct port number. If you are at a remote console, type the port number.
- 7 Click **OK** to add the server and to connect to it.

Removing ePolicy Orchestrator servers from the console

To remove an ePolicy Orchestrator server from the console tree, right-click <SERVER> in the console tree under **ePolicy Orchestrator**, then select **Remove Server**.

Logging off ePolicy Orchestrator servers without removing them

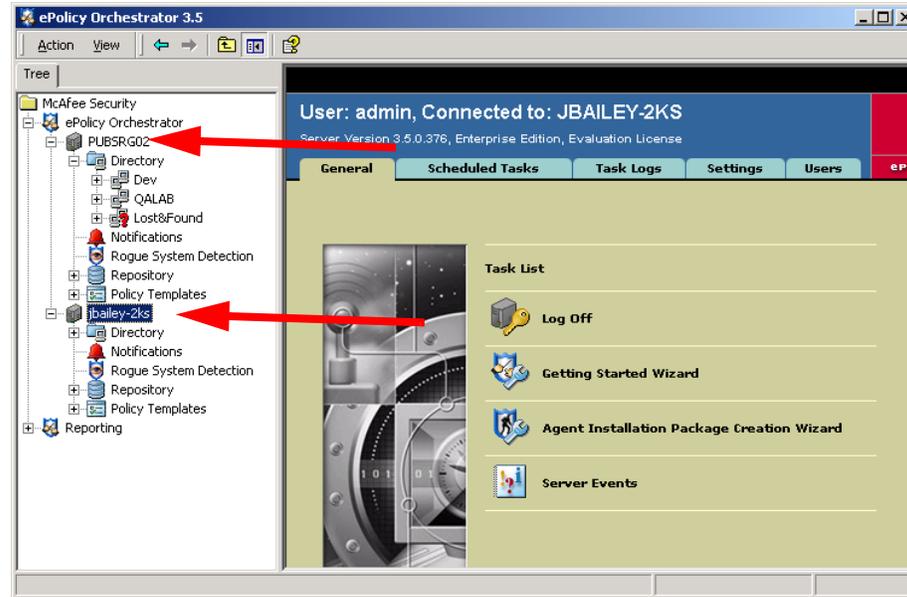
You can log off an ePolicy Orchestrator server without removing it. To do this, right-click the server in the console tree under **ePolicy Orchestrator**, then select **Log off**.

Adding additional ePolicy Orchestrator servers to a console session

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

If your organization is very large, or especially if it is divided into multiple large sites, you might consider installing a separate ePolicy Orchestrator server at each site. This can help reduce network traffic by managing agents, sending updates, replicating to distributed repositories all within a local LAN, rather than communicating across WAN, VPN, or other slower network connections typically found between remote sites.

Figure 2-2 You can manage more than one server in the same console session.



Having multiple ePolicy Orchestrator servers allows you to manage each server in the same console session.

Install the security certificate for Notification and Rogue System Detection

ePolicy Orchestrator 3.5 uses Secure Socket Layer (SSL) to improve security for communication between the ePolicy Orchestrator console and the Tomcat web server used with the new Notification and Rogue System Detection features.

When you log onto the console and access either Rogue System Detection or Notifications, you will be prompted to accept a security certificate to be able 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 into the ePolicy Orchestrator console.

To do this:

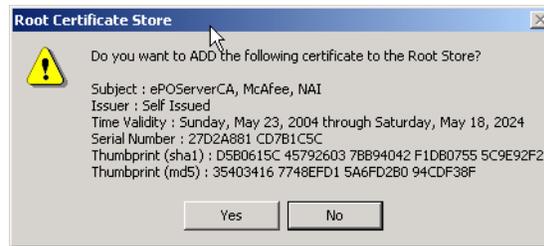
- 1 Log into your ePolicy Orchestrator server.
- 2 Click the **Notification** or **Rogue System Detection** node in the console tree.

Figure 2-3 The SSL security certificate alert

- 3 Click **View Certificate** when the **Security Alert** dialog box appears.
- 4 In the **Certificate** dialog box, select **Certification Path** tab.
- 5 Select **ePOServerCA** to enable certificate import.

Figure 2-4 View the certificate to install

- 6 Click **View Certificate** to open the second **Certificate** dialog box.
- 7 Click **Install Certificate** to open the **Certificate Import Wizard**.
- 8 Click **Next**, then **Next** again, then **Finish** to accept all wizard defaults and import the certificate.
- 9 Click **Yes** on the **Root Certificate Store** dialog box.

Figure 2-5 Accept the Root Store Certificate prompt

10 Click **OK** twice to close the two **Certificate** dialog boxes.

11 Click **Yes** on the final **Security Alert** dialog box.

Now that you have installed the security certificate, whenever you start the ePolicy Orchestrator console and access **Notifications** or **Rogue System Detection**, you will no longer be prompted to accept the certificate.

Managing accounts for ePolicy Orchestrator administrators

If you plan to have multiple people administer ePolicy Orchestrator, or administer policies for different parts of your network, you can create additional user accounts in the ePolicy Orchestrator console. Fellow administrators can use these accounts to log into the console. The different types of user accounts you can create are:

- Global Administrator
- Global Reviewer
- Site Administrator
- Site Reviewer

What's covered in this section

- [About global administrator accounts](#)
- [About site-restricted accounts and remote consoles](#)
- [About Global reviewers and site reviewers](#)
- [Adding, editing, or deleting user accounts](#)

About global administrator accounts

Global administrators have read, write, and delete permissions and rights to all operations. When you install the ePolicy Orchestrator server and console, a global administrator account with user name `admin` is created. You cannot delete this primary global user account.

In addition, you can create additional global administrator user accounts for other people who need global administrative rights to all aspects of the ePolicy Orchestrator console.

Global administrators can use the ePolicy Orchestrator console to deploy agents and security products, change agent or product policies, create and run client tasks for updating DATs or performing on-demand scans for any node in any site in the **Directory**. In addition, global administrators are the only user accounts that can perform a variety of server-based functions. These are:

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 ePolicy Orchestrator 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.

Manage ePolicy Orchestrator server settings and tasks

- 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.
- Use the **Getting Started** wizard.
- 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.

Global-level Directory functions

- Create, rename, or delete sites.
- Move computers from the global **Lost&Found**.

About site-restricted accounts and remote consoles

Site administrators have read, write, and delete permissions and rights to all operations (except those restricted to global administrator user accounts) for a particular **site** in the **Directory**. Sites are first-level groups in the **Directory** that may contain groups or computers. See [Chapter 3, Creating a Directory of Managed Computers](#) for more information on **Directory** sites and how to create them.

Site administrators can use the ePolicy Orchestrator console to deploy agents and security products, change agent or product policies, create and run client tasks for all groups or computers within their site in the **Directory**. Site administrators and reviewers can also run reports, but the reports only show data on computers located in their site. The site administrator can't view or work in any other sites in the **Directory**.

When you might need site administrators

You will probably need to create site administrator accounts if you have a very decentralized network with no single global administrator account and 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 locale IT or network administrators with rights to install and manage software on computers in that part of the network. Maybe the ePolicy Orchestrator server account does not have domain administrative privileges in these remote offices.

You can create site administrator accounts for these local administrators so they can log into the server from their remote locations via a Remote Console. The site administrator user will have full read, write, and delete rights to all child nodes within the site. The site administrator will be able to see, but not change, other sites in the **Directory**.

Creating site administrator user accounts

Follow the instructions in this section below for creating ePolicy Orchestrator user accounts. Select **Site Administrator** from the **Role** drop-down list, then select a site to which to bind this user account from the **Site** drop-down list. The drop-down list displays the sites that currently exist in the **Directory** tree, so you must create the site in the **Directory** before creating site administrator (or site reviewer) user accounts for it. See [Methods for creating the Directory on page 48](#) for details on creating sites.

About Global reviewers and site reviewers

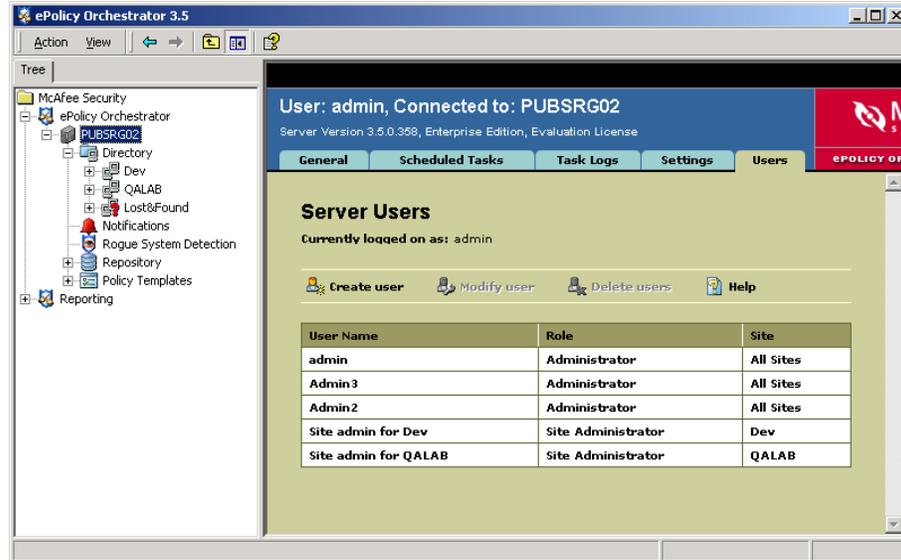
Global reviewers can view, but not edit, all settings in the console, including property settings, policy, and task settings for all nodes in the **Directory**. Site reviewers can only view settings for a single site in the **Directory**.

Adding, editing, or deleting user accounts

You must be a global administrator to add, edit, or delete user accounts in the ePolicy Orchestrator console. To see what user accounts are currently created for a particular ePolicy Orchestrator server:

- 1 Select the ePolicy Orchestrator server in the console tree.
- 2 In the details pane, click the **Users** tab.

Figure 2-6 Click the Users tab to view all current user accounts



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

To add a user account to the ePolicy Orchestrator server:

- 1 From the **Server Users** page of the ePolicy Orchestrator console, select **Create user**.
- 2 In the **Add New User** dialog box, type a descriptive name for the user in the **Name** field.
- 3 Select the type of user account from the **Role** drop-down list.
- 4 If you selected site administrator or site reviewer in the previous step, select a site from the **Site** drop-down list that shows the sites currently created in the **Directory** tree.
- 5 Type a **Password** (a minimum of one character), then **Confirm password**.
- 6 Click **Save** to save the current entries and return to the **Users** tab.

Deleting user accounts

You must be a global administrator to delete user accounts. Also, you cannot delete the default global administrator user account (`admin`), even if you are logged in with a global administrator account.

To delete an existing user account:

- 1 From the **Server Users** page of the ePolicy Orchestrator console, select one or more users from the list of created user accounts.
- 2 Click **Delete users** and click **OK** in the confirmation dialog box.

Changing roles or passwords on user accounts

You can change the user account privileges or the passwords for existing user accounts. Global administrators can change passwords on any user account. Other users can only change passwords on their own accounts.

- 1 From the **Server Users** page of the ePolicy Orchestrator console, select a user account from the list of created user accounts.
- 2 Click **Modify user** to open the user account in the **Modify User** page.
- 3 Change the **Role** and **Site** settings as needed.
- 4 To change the password, select change password to clear the current password, then type a new one and confirm it in the **Password** and **Confirm password** fields.
- 5 Click **Save** at the top of the page to save the changes.

About server settings, tasks, and events

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

This section contains the following topics:

- [Changing ePolicy Orchestrator server settings](#)
- [How to change server settings](#)
- [About server tasks](#)

Changing ePolicy Orchestrator server settings

The Server Settings page shows all the current configuration for server functionality like agent-to-server communication settings. A global administrator can change the server settings on a selected ePolicy Orchestrator server. Make sure you understand the impact of a specific setting before modifying it.

Client-to-server connection settings

You can configure many settings around how agents, SuperAgents, and rogue system sensors communicate with the ePolicy Orchestrator server.

Server setting	Description
Maximum connections	The maximum number of simultaneous connections between the ePolicy Orchestrator server and client computers. The default is 1000 . You can set this to a maximum of 10,000 . If the load of connections is straining server memory, you can reduce the maximum number of connections.
Concurrent legacy Agent auto-upgrade download limit	The maximum number of legacy agents can auto-upgrade concurrently. The default is 25. You can set this to a maximum of 10,000. This option effects only agents 2.5.1 or earlier.
Event log size	The maximum size of the event log file. The default is 2,048kb . You can set this to a maximum of 100,000kb .
Agent-to-Server port	The HTTP port that the agent uses to communicate to the server. This port is set during the installation wizard. The default is 82. Note: If you change this port number, wakeup calls are disabled until the next agent-to-server communication.

Server setting	Description
Console-to-server port	The HTTP port that consoles use to communicate to the ePolicy Orchestrator server. The default is 81. Changes take effect within one minute. Note: If you change the port number used for console-to-server communication, be sure to make the change on all consoles and use the new port number when logging on to the server.
Agent wakeup port	The HTTP port the server uses to send agent-wakeup calls. The default is 8081. Note: If you change this port number, wakeup calls are disabled until the next agent-to-server communication.
SuperAgent wakeup port	The HTTP port the server uses to send SuperAgent wakeup calls. The default is 8082.
Rogue System Detection port	The HTTP port used for Rogue System Detection server-to-console communication. The default port is 8080.
Rogue System Detection Secure port	The secure HTTP port used for secure Rogue System Detection server-to-console communication. The default port is 8443.

Global updating server settings

Global updating was a new feature introduced in ePolicy Orchestrator 3.0. Global updating has been improved in ePolicy Orchestrator 3.5 to include selective updating, which allows you to select exactly which kinds of updates to the master repository trigger a global update. See [Use global updating to automatically distribute updates to all clients immediately on page 115](#) for more information on enabling global updating.

The global updating settings you can configure are:

Table 2-1 Global updating server settings

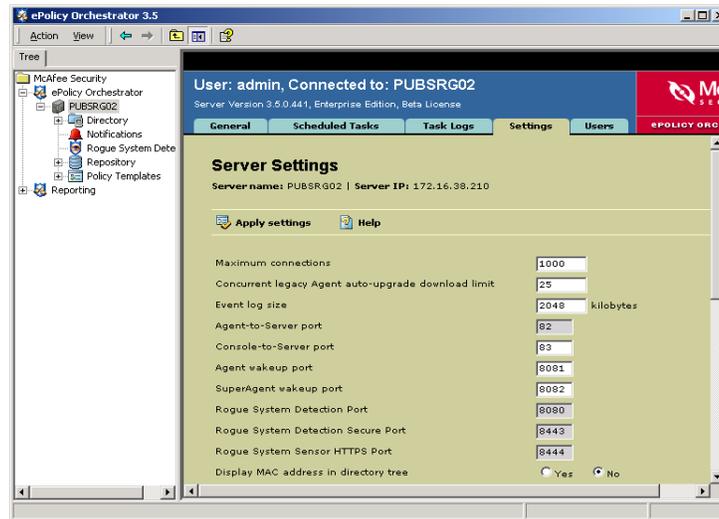
Server setting	Description
Enable global updating	Enables or disables global updating. When this is selected, checking in changes to the components selected trigger a global update, which includes a repository replication, SuperAgent wakeup call and client update.
Global updating randomization interval	Sets the global updating randomization interval, in minutes. Each client update occurs at some randomly selected time within the randomization window, which can help distribute network load by reducing the number of clients that update at a given time. For example, if you update 1000 clients using the default randomization interval of 20 minutes, roughly 50 clients update each minute, thus lowering the load on your network and on your ePolicy Orchestrator server at any point in time. Without the randomization, all 1000 clients would update simultaneously. Especially when updating very large networks (thousands of clients), randomization intervals can greatly ease the network and server load of the global update.
Only the following component check-ins trigger a global update	Select exactly which updates trigger a global update. When packages of the specified types are checked into the master repository, a global update is triggered. When other package types are checked in, no global update is triggered. To reduce network traffic, you would probably only select anti-virus signatures (DATs) and possibly scan engines to trigger a global update.

How to change server settings

To change ePolicy Orchestrator server settings:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 In the console tree under **ePolicy Orchestrator**, select <SERVER>, then click the **Settings** tab in the details pane. A list of the server settings the global administrator can define appears.

Figure 2-7 Settings tab



- 3 Make the desired changes to the server settings, then click **Apply settings**. For information about the specifics of these settings, see [About server settings, tasks, and events on page 29](#).



You cannot change the HTTP port on which the server listens for communications from deployed agents. If you do this, deployed agents would not be able to communicate with the server, and there is no 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 ePolicy Orchestrator server. Re-install the server and assign the new port number when you re-install the server.

About server tasks

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

What server tasks are there

- **Inactive Agent Maintenance** — Moves computers with inactive agents to a specified group or deletes them from the **Directory**. This task does not uninstall the agent. This task can also be performed manually. For instructions, see [Scheduling a daily server task to find inactive agents in your Directory on page 265](#).
- **Synchronize Domains** — Synchronizes selected Windows NT domains that you have imported into the **Directory** with their counterparts on the network. This task can also be performed manually. For instructions, see [Keeping imported NT domains synchronized with sites in the Directory on page 257](#).

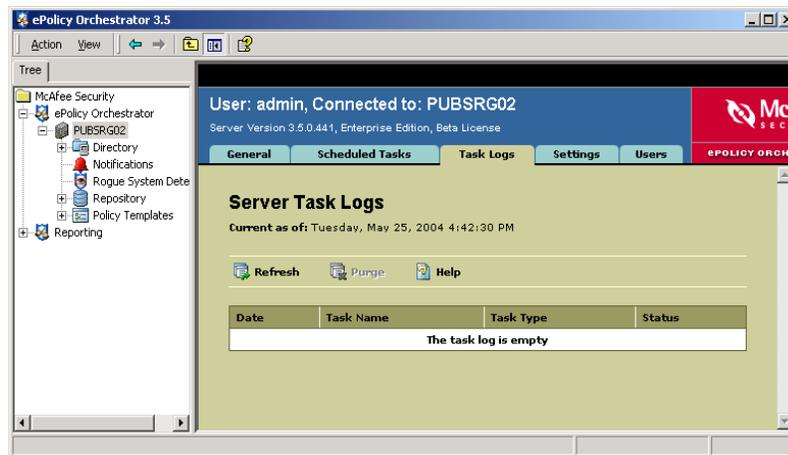
- **Repository Replication** — Updates distributed repositories from the master repository. See [Replicating the master repository contents to distributed repositories on page 139](#).
- **Repository Pull** — Retrieves packages from the source repository, then places them in the master repository. See [Use Pull tasks to update the master repository from a source repository on page 107](#).
- **Active Directory Computer Discovery** — Imports any new computers in Active Directory to the appropriate **Lost&Found** site in the ePolicy Orchestrator **Directory**. See [Using Active Directory discovery on page 254](#).
- **Compliance Check** — Run one or more compliance rules that check your managed computers for compliance with specified DAT, engine, agent or VirusScan versions. See [Compliance Check server task on page 181](#).

Reviewing the status of server tasks

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

- 1 Select your ePolicy Orchestrator server in the **Directory** tree of the console.
- 2 In the details pane, click the **Task Logs** tab to see the server task logs.

Figure 2-8 View task logs to check status of server tasks



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 Successfully** — Task completed successfully.
- **Executing** — Task was started.
- **Scheduled** — This message appears when you create or change server tasks.
- **Ran With Errors** — Task was started, but was not completed successfully.

If you want to delete the contents of the server task log, click **Purge**.

Viewing server events from the console

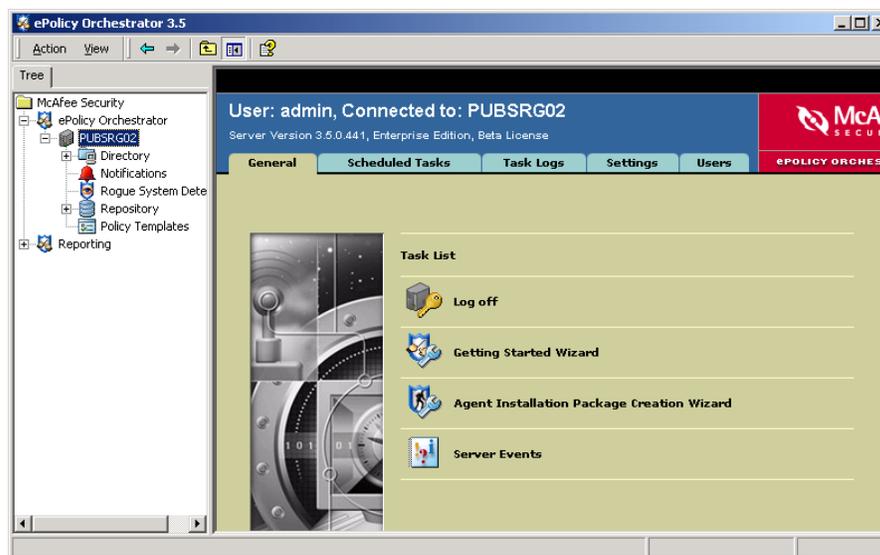
In the ePolicy Orchestrator console, you can view, save, and print all information, warning, and error events for each ePolicy Orchestrator server. Checking the server event window is a useful way to confirm the success or failure of actions initiated from the server, such as an agent push or pulling updated DATs from a source repository.

In addition, you can also manage what events are saved in the ePolicy Orchestrator database. See [Chapter 16, Maintaining ePolicy Orchestrator Databases](#) for more information about managing events in the database.

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

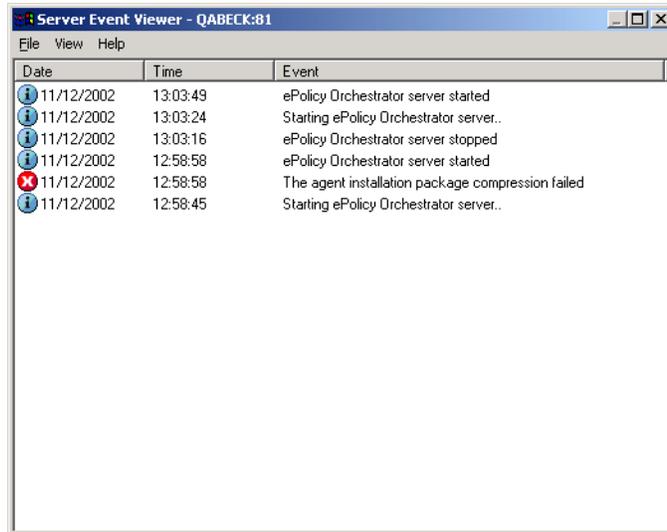
- 1 Log on to the desired ePolicy Orchestrator server.
- 2 In the console tree under **ePolicy Orchestrator**, select the server node, then click the **General** tab in the details pane.

Figure 2-9 General tab of the ePolicy Orchestrator server



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

Figure 2-10 Server Event Viewer dialog box



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

View 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.

Save 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**.

Print server events

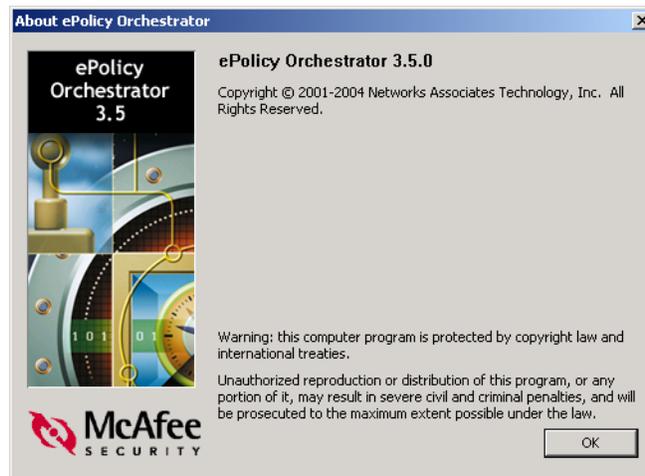
To print all server events to the default printer, click **Print** on the **File** menu. To print only selected server events to the default printer, select the desired events, then select **File | Print**.

Viewing the ePolicy Orchestrator 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 on to the desired ePolicy Orchestrator server. This information appears below the title (for example, **Server Version: 3.5.0.494, Enterprise Edition, Licensed**) in the details pane.

Figure 2-11 Version number of the software

You can also right-click **ePolicy Orchestrator** in the console tree, then select **About ePolicy Orchestrator**. The version number appears at the top of the **About ePolicy Orchestrator** dialog box.

Figure 2-12 About ePolicy Orchestrator dialog box

The Getting Started wizard

The **Getting Started** wizard allows you to get up and running quickly with ePolicy Orchestrator, and is designed for simpler deployments in a small business environment. Use the **Getting Started** wizard if you have less than 1000 client computers in your network and plan to manage them from a single ePolicy Orchestrator server.

You may want to briefly review later chapters in this guide that deal with deploying agents, creating Directories, deploying agents, managing policies, and deploying VirusScan Enterprise before using the **Getting Started** wizard.



The **Getting Started** wizard allows you to deploy VirusScan Enterprise to client computers after you deploy the agent to them. The agent deploys VirusScan Enterprise 7.0 to computers using Windows NT or above and VirusScan 4.5.1 to older computers using Windows 95, Windows 98 or Windows ME.

If you chose to use the **Getting Started** wizard to deploy VirusScan, you must first check the deployment packages for VirusScan Enterprise and, if you have older Windows 95 and Windows 98 computers, VirusScan 4.5.1 into the master repository on the ePolicy Orchestrator server. Do this before you run the **Getting Started** wizard. See [Check in product deployment packages to the master repository on page 89](#) for details on how to check in deployment packages.

The wizard allows you to:

- Deploy the ePolicy Orchestrator agent to all computers in a Windows NT domain in your network.
- Download the agent installation package (FRAMEPKG.EXE) for manual deployment to computers.
- Enable VirusScan deployment upon installation of the agent.
- Apply small business policies.

Predefined small business policies and client tasks

ePolicy Orchestrator allows lots of flexibility in setting agent and product policies and what kinds of client tasks, such as update and scan tasks, you can configure for clients. To help simplify this complexity and help you get started quickly, the **Getting Started** wizard can deploy a set of predefined policies and scan tasks to your agents that are ideally suited for a small business deployment.

You can change any of these policies or tasks later if you want. See [Managing Policies for Agents and Products on page 147](#) for more detailed information on changing policies and client tasks.

The policies and tasks included with the **Getting Started** wizard are:

- The agent's agent-to-server communication interval (ASCI) is set to 1 hour. This means the agent checks in with the server every hour to send updated properties and events to the server and check for any new or updated policies and tasks.
- Agents forward high-priority events to the server immediately, rather than wait for the next agent-to-server communication interval. This allows you to always have the most current critical data in reports.
- Client computers check the McAfee web site for new virus definition (DAT) files every fifteen minutes.
- VirusScan runs a scheduled on-demand scan to scan computers for virus infections every day at 12:00 PM local time.
- The agent enforces policies on the client computer every five minutes.
- Performs regular domain synchronization tasks. This task re-imports the computers in the NT domain into the console **Directory** tree. This ensures that your **Directory** accurately reflects what computers are currently connected to the network.

How to launch the Getting Started wizard

- 1 Log on to the desired ePolicy Orchestrator server using a global administrator user account.
- 2 In the console tree under **ePolicy Orchestrator**, select <SERVER>, then click the **General** tab in the details pane.
- 3 Under **Task List**, click **Getting Started Wizard** to launch the wizard.
- 4 Click **Next** to open the **Agent Deployment — Configure Automated Deployment** dialog box.
- 5 If you want to deploy the agent to all computers in your NT domains:
 - a Select **I want to automatically deploy the agent to the Windows NT domains I specify**, then click **Next**.
 - b On the **Select Domains** page, select domains to deploy agents to from the list of available domains the ePolicy Orchestrator server can reach.
 - c Click **Next**.
 - d On the **Provide Domain Administrator User Accounts** page, select each domain and enter credentials for a domain administrator account. ePolicy Orchestrator cannot deploy agents unless the account specified has administrative rights in the target domain.
 - e Click **Next**.

If you don't have domains (for example, if you use NetWare), or you don't want to change the current settings with the wizard, do the following from the **Agent Deployment — Configure Automated Deployment**:

- a Select **I want to skip this step**, then **Next**.

From the **Agent Deployment — Manual Deployment** dialog box you can download the agent installation package (FRAMEPKG.EXE) to deploy manually to computers running Windows 95, Windows 98, or Windows Me (that do not have remote administrator enabled). This is also useful to deploy the agent to computers that do not belong to a Windows NT domain.
- b Click **Download** and select the location to which you want to save the agent installation package. You can then
- c Create an e-mail message with installation instructions, attach the agent installation package, then send the e-mail message when desired.
- d Click **Next**.

If you do not want to deploy the agent installation program manually, click **Next**.

- 6 On the **Agent Policies and Tasks — Enable VirusScan Deployment Task** dialog box, choose whether the agents deploy VirusScan when they are installed, then click **Next**. Remember that you must first check the appropriate VirusScan deployment packages into the master repository.
- 7 On the **Part 2: Agent Policies and Tasks — Enable Policies** dialog box, choose whether to enable the small business policies, then click **Next**.
- 8 On the **Ready to Start** dialog box, review the tasks that the wizard will perform, then click **Next**.

- 9 Click **Finish** to begin the agent and policy deployment.

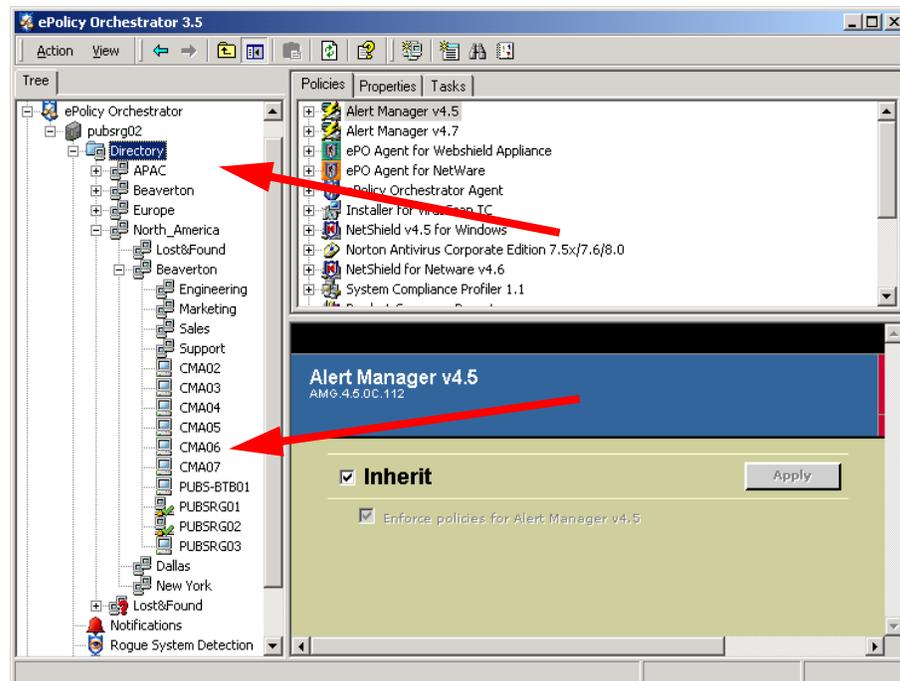
3

Creating a Directory of Managed Computers

Create sites and groups and add computers to them

The **Directory** contains all of the computers that you want to manage via ePolicy Orchestrator and is the link to the primary interfaces for managing these computers. You can organize computers under the **Directory** into logical groupings (for example, functional department or geographic location) or sort them by IP address using console tree items called *sites* and *groups*. You can set policies (product configuration settings) and schedule tasks (for example, updating virus definition files) for computers at any level under the **Directory** and at the **Directory** level itself.

Figure 3-1 The Directory contains the computers managed by ePolicy Orchestrator



Before configuring the ePolicy Orchestrator software to deploy and/or manage the anti-virus and security software in your environment, you will need to conduct some preliminary planning. This planning includes deciding the best groupings to create for management of software and the designation of administrative rights.



Many factors can influence how you should create and organize your **Directory**, especially how you plan to deploy and manage agents and McAfee products, and also how you plan to keep these agents and products updated. It is therefore recommended that you take some time to review the other sections of your guide before you begin creating your **Directory**.

What's in this chapter

- [About creating the Directory](#)
- [Things to consider when planning Directory organization](#)
- [Methods for creating the Directory](#)
 - [Creating the Directory tree by importing from Active Directory](#)
 - [Creating sites or groups by importing NT domains](#)
 - [Creating sites and groups manually](#)
 - [Import computers and groups from a text file](#)
- [Adding WebShield appliances](#)

About creating the Directory

The **Directory** keeps managed computers organized for an ePolicy Orchestrator server in units so that you can best monitor, set policies, and schedule tasks for those computers. Before creating your **Directory**, it is important to understand:

- [Sites, groups, and inheritance.](#)
- [About IP address filters and sorting.](#)
- [Deploying the agent when adding a site, group, or computer to the Directory.](#)

Sites, groups, and inheritance

As part of the planning process, you should consider the best way to divide computers into sites and groups prior to beginning the configuration of ePolicy Orchestrator.

Organize computers into sites and groups

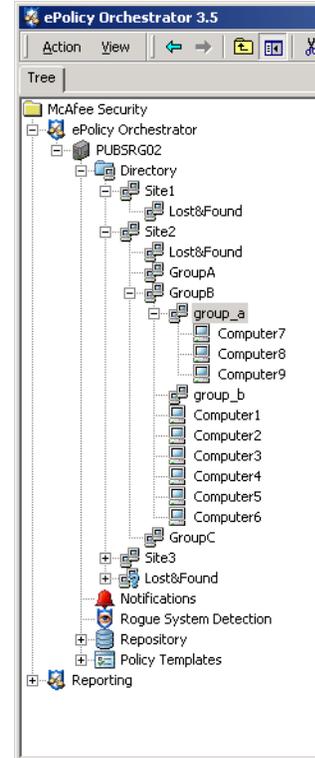
The **Directory** tree contains all the computers in your network that you are managing with ePolicy Orchestrator. If you choose, it is possible to add all the computers to be managed by ePolicy Orchestrator into one site in the **Directory**. However, this flat, unorganized list makes setting different policies for different computers very difficult, especially for very large networks. It also makes the **Directory** very difficult to navigate visually.

The **Directory** allows you to group these computers into groupings called sites and groups. Clumping computers with similar properties or requirements into sites and groups allows you to manage policies in one place, at the site or group level, rather than having to set policies for each individual computer. It can also make visually browsing your **Directory** much easier.

Figure 3-2 Directory organized into sites and groups

A **site** is a first-level group directly under the **Directory** root on the console tree. A **group** is a secondary grouping beneath a site. In many respects sites and groups are very similar. Both can contain sublevels of groups and also individual computers. You can create both sites or groups manually, or create them automatically by importing lists of computers directly from your NT Network Neighborhood or Active Directory.

In some respects, though, sites are different. First, you can use sites to define administrative roles by creating site administrator and site reviewer user accounts in ePolicy Orchestrator that are specific to a site. Site administrators can only work within that site and do not have access to other parts of the **Directory**. Sites also contain **Lost&Found** groups. These are temporary containers for computers that ePolicy Orchestrator cannot place automatically in other sites or groups in your **Directory**. For example, if you are using IP filters to automatically sort computers into sites and groups based on network IP address. Finally, only ePolicy Orchestrator global administrators can create sites. Site administrators can make groups within the site over which they have administrator rights.



You can manually drag and drop groups and individual computers to different locations in the **Directory** tree. You cannot, however, “promote” a group to a site in this way.

Inheritance: set policies once for many computers

Inheritance is a very important property of the ePolicy Orchestrator **Directory** tree that makes policy administration simpler. Inheritance means that lower-level nodes in the **Directory** hierarchy inherit policies that have been set at higher levels. Policies set at the **Directory** root level inherit to sites, site policies inherit to groups or individual computers within that site. Group policies inherit to sub-groups or individual computers within that group. Inheritance is enabled by default for all sites, groups and individual computers you add to your **Directory**. This allows you to set policies and schedule client scan tasks in fewer places. For example, at the higher levels of your **Directory**.

To set custom policies for a site, group, or individual computer, you can break Inheritance and set the policies. Those changed policies will inherit to groups or computers below.

A parent node is a container object, such as a site or group, which has other sub-nodes or branches under it. A child is a node that is in a container object, or is subordinate to a form of grouping. A child node can be a computer or another group. Thus, a child node may be both a child to another node (for example, a group inside a site), and it can be a parent (for example, a group) with child nodes under it. At the lowest level of the tree, a child has no nodes under it. For example, computer nodes in this structure can be only child nodes, because they cannot have any sub-nodes or branches under them.



Let inheritance do the work for you! While you can set anti-virus and security policies and schedule client on-demand scan or DAT update tasks at any node of the **Directory**, consider setting policies at the highest node possible. If you can set policies at the site or group level only, you'll have fewer changes to keep track of. Avoid setting policies at the individual computer level if at all possible.

Lost&Found groups

The server uses IP management settings, computer names, Active Directory, and domain, site or group names to determine where to place computers. **Lost&Found** groups store computers whose locations could not be determined. The administrator must move the computers in **Lost&Found** groups to the appropriate place in the **Directory** to manage them.

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

Lost&Found groups appear under the **Directory** and under every site in the console tree.

About IP address filters and sorting

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. These organizational groupings can be useful ways to group computers for setting policies through ePolicy Orchestrator. For this reason, ePolicy Orchestrator allows you to set IP address filters to sites and groups in the **Directory**. ePolicy Orchestrator provides tools, such as IP sorting and IP integrity check tasks that can automatically place computers in the right site or group according to IP address. This can be a very powerful tool for automatically populating your **Directory** and making sure computers stay where they're supposed to.

This feature is especially useful if you do not use ePolicy Orchestrator to deploy agents to clients on your network. If you use another network software tool, such as Microsoft SMS, or if you deploy the agent using NT login scripts, the agent is installed on the client before the computer 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 computer is added to the appropriate location. Otherwise, it is added to the **Lost&Found** group and you will have to move it manually to the appropriate group. Especially in a large network, using IP filters to get the computer in the right location can save time manually moving new computers into 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.



Automatic IP address sorting does not apply to computers that you add to the **Directory** using the new **Active Directory Computer Discovery** task in ePolicy Orchestrator 3.5.

Apply IP filters at each level of the Directory

If you use IP filtering, you should set the IP filtering properties at each level of the **Directory** properly. To set an IP filter for a group, you must also set IP filters in parent groups or sites. Furthermore, the IP ranges specified in lower level groups must be a subset of the IP range of the parent, for example, the IP range of the child group must “fit” completely inside the IP range of the parent. Finally, 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 which 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 to make sure your IP filter hierarchy is valid. The check alerts you if there are any conflicts or overlaps between IP filters for different sites or groups. See [Check integrity of IP filters on page 262](#) for details.

How ePolicy Orchestrator uses IP filtering

These guidelines apply only the first time that the agent communicates with the ePolicy Orchestrator server. After the initial contact, the agent updates whatever location to which it has been assigned. When an agent contacts the server for the first time, the server searches for the appropriate site whose IP mask or range matches the agent’s IP address.

Automatically placing computers in the **Directory** is the result of a complex algorithm that uses both IP filters you create and domain information for the NT domain to which the new computer 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 computer to go to the appropriate IP group, you should either create the IP group under the domain site or group or not create the domain group under the site.

The ePolicy Orchestrator server uses the following search algorithm to place computers in the **Directory**:

- 1 Site IP filter** — If a site with a matching IP filter is found, the computer is placed in that site. ePolicy Orchestrator tries the following, in order, to place the computer within the site:
 - a** In a group named the same as the NT domain to which the computer belongs.
 - b** In a group with a matching IP filter.
 - c** If no group match for IP address or domain name is found, the computer is placed in the site Lost&Found group.
- 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 computer belongs. If such a site is found, the server searches for a group with a matching IP filter and places the computer in it. If no group is found, the computer is placed in the site Lost&Found.
- 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 computer to the global Lost&Found.

Adding IP filters when creating sites and groups

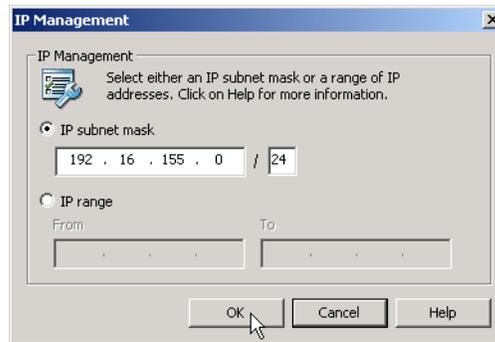
You can specify IP filters for a site or group as you create them. Or, you can create them later at any time. See [Maintaining IP filters for sites and groups on page 260](#) for more information on changing IP filters for existing sites and groups.

When creating a new site or group, specify the IP filter information in the **New Site** or **New Group** dialog box. See [Creating sites or groups by importing NT domains on page 51](#) or [Creating sites and groups manually on page 53](#). The procedure for creating IP filters is basically the same for both new sites and new groups. The example in this procedure shows creating an IP filter for a new site.

To assign an IP filter to a new site:

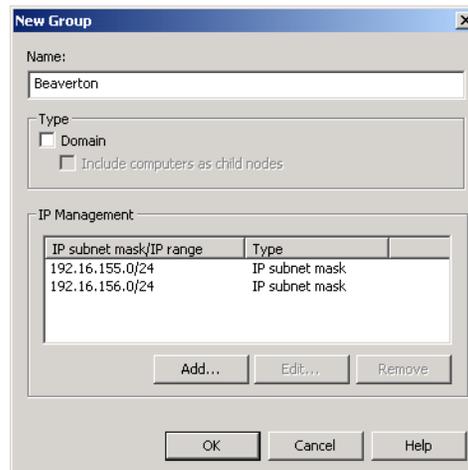
- 1 In the **Add Sites** dialog box, select the site from **Sites to be added**, then click **Edit** to open the **New Site** dialog box.
- 2 In the **IP Management** section, click **Add**. The **IP Management** dialog box appears.

Figure 3-3 IP Management dialog box



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

Figure 3-4 IP Management lists what IP filters you have configured for the new site



- 5 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.
- 6 When you have created all the IP filters required for your site, click **OK** on the **New Site** dialog box to save them.

Deploying the agent when adding a site, group, or computer to the Directory

If you chose, you can use ePolicy Orchestrator to push the agent to new computers that you import into the **Directory** using the NT domain or Active Directory import feature.

Before you deploy agents to your network at all, be sure to first review the information in this guide that deal with agent deployment and management. See [Chapter 4, Deploying Agents, SuperAgents, and Sensors](#) for more information on deploying the agent.



McAfee does not recommend pushing the agent during a **Directory** import if the imported domain or Active Directory container is very large. Pushing the 1.5 MB agent deployment package to many computers at once may flood your network with network traffic. Instead, import the domain or Active Directory group, and then later push the agent to groups of computers at a time rather than all at once.

You can push agents to all computers in a site listed in the **Sites to be added** dialog box. See [Creating sites or groups by importing NT domains on page 51](#) or [Creating sites and groups manually on page 53](#) for information on how these dialog boxes appear in the context of adding sites to the **Directory**.

To push the agent while importing computers to the **Directory**:

- 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 client computer where the agent is installed. (Click  to insert variables into the **Installation path**. See [Variables on page 296](#).)
- 4 If you installed the ePolicy Orchestrator server with a domain administrator account credentials, you can select **Use ePO server credentials**. Otherwise, specify a user name and password for a user account with domain administrator rights to install software on the clients in that domain.

After adding the computers and deploying the agent, check the ePolicy Orchestrator server events page to see if the agent install was successful. If the events page shows a failed agent install, the push failed. If it doesn't show anything regarding agent installation, the installation did not fail (the events page does not indicate if the agent install was successful).

Things to consider when planning Directory organization

An efficient and well-organized **Directory** can make maintaining ePolicy Orchestrator much easier. Many administrative options can affect how your **Directory** is structured, and you should think ahead about these before you begin creating your **Directory**. Especially for a very large network containing thousands or tens of thousands of client computers, you only want to create the **Directory** once.

ePolicy Orchestrator offers flexibility in creating and populating the **Directory** with computers and deploying agents. If your NT domain or Active Directory structure is organized in a way that makes sense for managing anti-virus and security policies, you can quickly import entire domains or Active Directory containers into your **Directory** as sites. If you want to, you can create the site and group structure by hand, and add each computer manually. You can have a flat directory structure where each site contains hundreds or even thousands of computers in a flat list, or you can create a very deep and detailed group structure where each group contains much fewer computers.

There is no one way to organize a **Directory**, and since every network is different, your **Directory** organization will be as unique as your network layout. However, this section contains some suggestions to consider while planning how to create and organize your **Directory**.

You won't use all the Directory creation methods...

Having so many options for creating and organizing your **Directory** may make you think you need to use them all. You won't. For example, if you use Active Directory in your network, you would probably import your Active Directory containers rather than your NT domains. If you don't use Active Directory and your NT domain organization does not make sense for ePolicy Orchestrator policy management, then you prefer to generate your **Directory** layout outside of ePolicy Orchestrator in a text file and import it into your **Directory**. If you have a smaller network, you may create your **Directory** by hand and import each computer manually; if your **Directory** is large, you would never do this.

...but you will probably use more than one

While you won't use all of the **Directory** creation methods available, you also probably won't use just one. In many cases, the combination of methods you use balance two things: the ease of creating your **Directory** quickly through one of the import features, and the need for additional structure, through groups, to make policy management more efficient.

For example, you might create the **Directory** in two phases. First, you can create 90% of the general directory structure by importing whole NT domains or Active Directory containers into sites. Then, you can manually create groups within each site to classify computers together that may have similar anti-virus or security policy requirements. For example, if one NT domain is very large or spans several geographic areas, you can create groups under the site and point the computers in each at a separate distributed repository to make updating more efficient. Or, you can create smaller functional groupings, such as for different operating system types or business functions, as you may set different policies for these types of groupings. Having this extra layer of organization can make managing policies for thousands of computers in large networks much easier over time.

Geographic location of sites or offices

If your company is large and has multiple locations in different cities or locations, consider using geography as the primary grouping mechanism. Create a site for each geographic location. This can be either a single office location, such as a site called “New York.” This could also be a general geographic region, such as “Europe,” which could in turn contain separate groups for individual office locations within that site (London, Paris, Prague). Or, maybe your organization isn’t spread out around the world, but rather concentrated in several large buildings on one campus. Create a site for each building (or floor within a building, or whatever makes sense).

Grouping computers first by geography has several advantages for setting policies. First, you can set the update policies for the site or group to have all the client computers in them update from one or more distributed software repositories located nearby. Second, if sites are located in other countries, you can deploy language-specific versions of the ePolicy Orchestrator agent or client software like VirusScan Enterprise to these clients. Having all the computers grouped together in one site or group means you set the update and product deployment policies once for the whole site or group.

Use of IP filters to automate Directory organization

You should consider using IP filters if at all possible 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**. Computers automatically populate the right locations.

In many cases, geographic site locations will use specific subnets or IP ranges, so you can create a site for a geographic location *and* set an IP filter or 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 mechanism.

Use NT domains or Active Directory to create the Directory quickly

Importing entire NT domains or Active Directory containers into a **Directory**, sites, or groups is a fast and easy way to create your ePolicy Orchestrator **Directory** automatically. Then you can manually create groups within the imported site to organize computers as needed for policy management. If you have different network domains for each geographic part of your network, you can import each domain as a geographic site. Or, if your domains span multiple geographic sites, you can import the domain to your **Directory** as a site, and then create geographic groups within that site with IP filters.

Network infrastructure and bandwidth limitations

Managing anti-virus and network security is a constant balance between protection and performance. So you will need to organize your **Directory** to make the best use of ultimately limited network bandwidth. Consider in particular how the ePolicy Orchestrator server connects to all the parts of your network, especially remote locations which are often connected by slower WAN or VPN connections instead of faster LAN links. 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 links.

Who will administer which part of the Directory

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 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 ePolicy Orchestrator account. Instead, you may need to organize the **Directory** into sites and create site administrator accounts to allow other site administrators to set policies for these computers.

Functional groupings and what software is running where

One of the most important factors determining how you organize the **Directory** involves how you can set policies for the most number of computers in the fewest places possible. Geographic-specific boundaries can affect your updating and repository policies, such as pointing all the clients in the same location to a local distributed update repository. At a lower level, you may want to create groups of computers for specific functional areas.

On the business organization side, you may need to set different policies for different functional groups within your organization, such as Sales, HR, or Distribution. Different business groups may run different kinds of software that require special anti-virus or security settings. For example, you may want to group your e-mail exchange servers or SQL database servers into a group and set specific folder and file exclusions for VirusScan Enterprise on-access scanning.

Also, you may want to group computers with similar operating systems together in groups to manage operating system-specific policies more easily. For example, you may have some older client computers running Windows 9X, while most of your computers run Windows 2000, XP or 2003. You can group the Windows 9X clients into one or more groups to deploy and manage VirusScan 4.5.x to these computers. Or, you may group Novell NetWare file servers into a group to define NetShield for NetWare policies.

Don't overdo it: keep the Directory as flat as possible

If you choose, you can create a very detailed **Directory** with lots of groups and sub groups. McAfee recommends, however, that you only create as much structure as is useful for setting policies. In large networks it would not be uncommon to have hundreds or even thousands of computers together in the same container, either a site or group. Being able to set policies in fewer places may be easier than having to maintain an elaborate **Directory** structure.

Even if you do create groups just to make finding things in the **Directory** easier, try to break inheritance and set customized policies only at the higher levels. Many people deploy ePolicy Orchestrator with few customized policy or software settings at all (only use the defaults).

Methods for creating the Directory

The following section contains information on the different methods available in ePolicy Orchestrator for creating your **Directory**.

- [Creating the Directory if you deploy the agent outside of ePolicy Orchestrator](#)
- [Creating the Directory tree by importing from Active Directory](#)

- [Creating sites or groups by importing NT domains](#)
- [Creating sites and groups manually](#)
- [Import computers and groups from a text file](#)

Creating the Directory if you deploy the agent outside of ePolicy Orchestrator

You can use ePolicy Orchestrator to install the agent to client computers by “pushing” it from the ePolicy Orchestrator server. However, many people either cannot or prefer not to do this, and deploy the agent through another means, and then use ePolicy Orchestrator to deploy other anti-virus products such as VirusScan Enterprise or just to manage security policies, run reports, etc. One example of another deployment method is to write a network login script that installs the agent every time a client logs onto the network. Another is to use a third-party network management tool such as Tivoli or Microsoft SMS. Finally, you can manually run the agent installer on the client computer to install the agent manually. For more information on these ways to deploy the ePolicy Orchestrator agent, see [Chapter 4, Deploying Agents, SuperAgents, and Sensors](#).

When you use any of these methods to deploy the agent, ePolicy Orchestrator adds the computer to the **Directory** the first time that the agent on that computer calls into the server. If you have created no sites or groups in your **Directory**, ePolicy Orchestrator adds all the computers to the global Lost&Found folder under the **Directory** root. In a large deployment you will have hundreds or thousands of computers listed together in the Lost&Found group, which makes policy management difficult.

Create “shell” sites and groups for NT domains or IP ranges

To provide more structure to your **Directory** and make policy management easier, consider manually creating sites and groups. If possible, create sites and groups around one of the two following criteria listed below. When the agent calls into the ePolicy Orchestrator server for the first time, the server will try to automatically place the computer into the correct site or group.

See [About IP address filters and sorting on page 42](#) for details on how ePolicy Orchestrator uses IP address and domain information to automatically place computers in sites and groups. Also, you can run regular IP integrity sort tasks to move new computers into sites or groups whose IP filters match IP addresses. See [Schedule a regular domain synchronization server task on page 258](#) and [Periodically sort computers by IP address on page 262](#) for more information on these.

While you can create these sites and groups at any time, consider manually creating them and assigning appropriate IP filters, if possible, *before* you deploy agents to computers using a non-ePolicy Orchestrator deployment method. That way, ePolicy Orchestrator can place the computer into the appropriate site or group immediately.

Creating the Directory tree by importing from Active Directory

The Active Directory integration feature of ePolicy Orchestrator 3.5 allows you to import computers from your network’s Active Directory directly into your ePolicy Orchestrator **Directory**. You can map Active Directory source containers to import computers to the root or sites of your ePolicy Orchestrator **Directory** tree.

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

Recommendation for new vs existing installations

For new installations, we recommend you perform two tasks to use this feature optimally. We suggest that you first run the **Active Directory Import Wizard** to populate your ePolicy Orchestrator **Directory**. Then use the Active Directory computer discovery feature to help maintain the ePolicy Orchestrator **Directory** by creating a scheduled polling interval to import any new computers on the network to the appropriate ePolicy Orchestrator site. See [Using Active Directory discovery on page 254](#) for more information on maintaining Active Directory integration over time.

If you have been using a previous version of ePolicy Orchestrator and already have a fully-populated **Directory**, you can still take advantages of the new Active Directory integration features of ePolicy Orchestrator 3.5. Use the **Active Directory Computer 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 ePolicy Orchestrator **Directory** sites, allowing you to import any new computers found in Active Directory to the appropriate site of the ePolicy Orchestrator **Directory**.

Using the Active Directory Import Wizard

The **Active Directory Import** wizard allows you to import computers from Active Directory into your ePolicy Orchestrator **Directory**. When you select a source container in Active Directory, everything within the source container are searched unless you choose to exclude certain sub-containers of the source container. McAfee recommends using this wizard to create your ePolicy Orchestrator **Directory** from scratch by importing your Active Directory information.

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

To import computers from Active Directory into the ePolicy Orchestrator **Directory** tree:

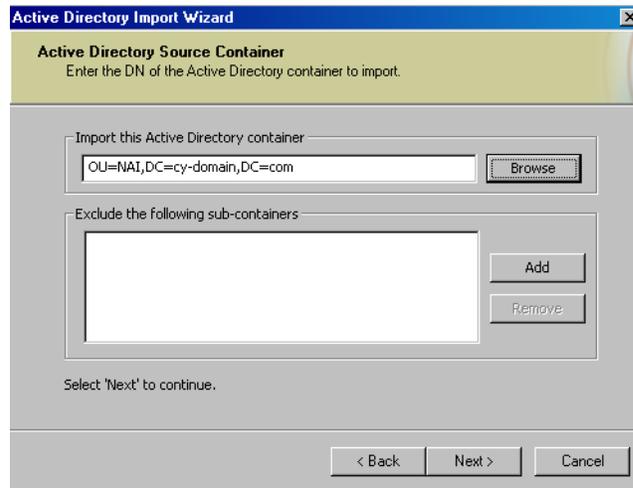
- 1 Right-click **Directory** in the ePolicy Orchestrator tree and select **All Tasks | Active Directory Import**.
- 2 Click **Next** when the **Active Directory Import** wizard appears.
- 3 On the **ePolicy Orchestrator Destination** dialog box, click **Browse** and select the ePolicy Orchestrator site to which you want to import new computers from Active Directory, then click **Next**.



You can only import to the root or sites of the ePolicy Orchestrator **Directory**.

- 4 Provide the Active Directory user credentials in the provided fields, 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 3-5 Active Directory Import Wizard



- 6 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**.
- 7 Click **Next**, and view the active log for any new computers that have been imported. Verify in the ePolicy Orchestrator tree that these computers were imported.
- 8 Click **Finish**.

After importing computers from Active Directory

Once the computers are imported, deploy agents to these computers. See [Chapter 4, Deploying Agents, SuperAgents, and Sensors](#) for more information on deploying agents. Also, plan on running periodic **Active Directory Computer Discovery** tasks to keep the parts of your **Directory** you imported up-to-date with any new computers in your Active Directory containers. See [Using Active Directory discovery on page 254](#) for information on maintaining your imported Active Directory containers.

Creating sites or groups by importing NT domains

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

If your domain is very large, you may want to also create subgroups to help with policy management or help you organize the computers in your **Directory** more easily. 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 computers into them.

The procedure for creating **Directory** containers by importing NT domains is essentially the same for both sites and groups. The steps below use the example of a site.

To create sites of the same name, and containing all the computers, of a Windows NT domain:

- 1 In the ePolicy Orchestrator console tree, right-click the **Directory**, then select **New | Site**. (If you are creating a group beneath an existing site, right-click the site and select **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 ePolicy Orchestrator can reach on the network, 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**. See [Adding IP filters when creating sites and groups on page 44](#) for more details.
- 5 You can deploy the ePolicy Orchestrator agent to all computers in the sites that appear in **Sites to be added** as you create the site. See [Deploying the agent when adding a site, group, or computer to the Directory on page 45](#) for more details.
- 6 Click **OK**.

Importing computers from a network domain to an existing site or group

In addition to creating a site or group from an NT domain and importing all the computers in that domain at the same time, you can also import all computers belonging to the selected Windows NT domain to an existing site or group. Typically, you use this procedure to import computers from your network to sites or groups you have created manually.

However, you can also import computers into a site or group you have created by importing a network domain. This could be useful if you have several smaller domains on your network that would all use the same ePolicy Orchestrator policies and tasks. To be able to define them all in one place, you could import these computers into the same site or group and manage their policies from that group level.



Import each NT domain into a separate site or group if possible. This will help you keep track of which computers belong to which domain. Also, having sites and groups named after real NT domains helps with automatically placing computers in the right site or group using IP and domain filters (see [About IP address filters and sorting on page 42](#)).

If you want to manage the same policies across several domains, manually create a site and then import each domain as a group within the site.

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

- 1 In the ePolicy Orchestrator **Directory**, 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 computers.
- 3 Click **OK** to save the selected computers and return to the **Add Computers** dialog box.
- 4 You can deploy the ePolicy Orchestrator agent to all computers in the sites that appear in **Sites to be added** as you create the site. See [Deploying the agent when adding a site, group, or computer to the Directory on page 45](#) for more details.
- 5 Click **OK**.

The computers you selected will be added to the selected site or group.

Creating sites and groups manually

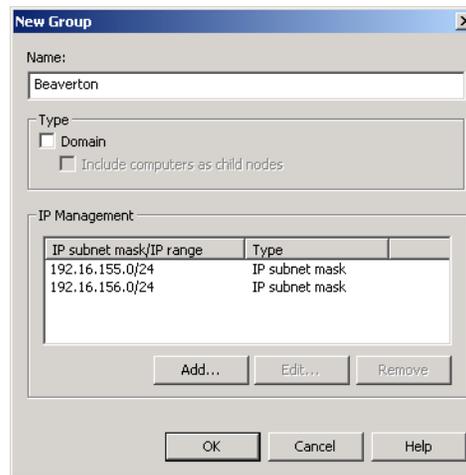
If you don't want to create sites or groups by importing Active Directory containers or NT domains, you can create them manually. You can then populate these sites and groups with computers, either by typing NetBIOS names for individual computers or by importing selected computers directly from your Network Neighborhood.

In addition, you may want to manually create groups for logical groupings of certain computers after importing an entire NT domain or Active Directory container into the ePolicy Orchestrator **Directory**. For example, you may want to create a "Servers" or "Exchange" group to set policies for special server applications.

The procedure for creating a site or group manually is the same. The instructions in this section use the example of creating a site. To create sites manually:

- 1 In the ePolicy Orchestrator console tree, right-click **Directory**, then select **New | Site**. The **Add Sites** dialog box appears. (To create a group, right-click an existing site or group beneath which you want to add a new group and select **New | Group**.)
- 2 Click **Add** to open the **New Site** dialog box and define the site that you want to add to the **Directory**.

Figure 3-6 New Site dialog box



- 3 Type a **Name** for the new site.
- 4 To add one or more IP filters, select the site from the sites to be added list and click **Edit**. See [Adding IP filters when creating sites and groups on page 44](#) for more details.
- 5 You can deploy the ePolicy Orchestrator agent to all computers in the sites that appear in **Sites to be added** as you create the site. See [Deploying the agent when adding a site, group, or computer to the Directory on page 45](#) for more details.
- 6 Click **OK**.

You can then populate these sites and groups with computers, either by typing NetBIOS names for individual computers or by importing selected computers directly from your Network Neighborhood.

Manually add specific computers to an existing site or group

In addition to creating a site or group from an NT domain and importing all the computers in that domain at the same time, you can also import all computers belonging to the selected Windows NT domain to an existing site or group. Typically, you use this procedure to import computers from your Network Neighborhood to sites or groups you have created manually. However, you can also import computers into a site or group you have created by importing a network domain.

You can also add computers under an existing site or group in the **Directory** manually.

To manually add a computer to a site or group:

- 1 In the ePolicy Orchestrator **Directory**, right-click the desired site or group, then select **New | Computer**.
- 2 Click **Add** in the **Add Computers** dialog box.
- 3 In the **New Computers** dialog box, type the NetBIOS name for the computer in the **Name** text field. Alternatively, you can click **Browse** to find the computer on your network and select it.
- 4 Click **OK** to save the computer to be added and return to the **Add Computers** dialog box.
- 5 You can deploy the ePolicy Orchestrator agent to the computers as you add them to the **Directory**. To do this, check **Send agent package**. See [Deploying the agent when adding a site, group, or computer to the Directory on page 45](#) for more details.
- 6 Click **OK**.

Import computers and groups from a text file

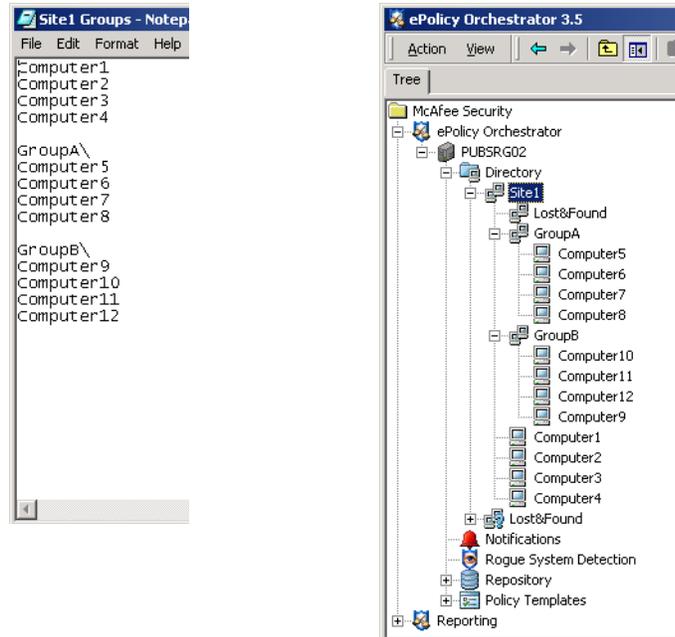
You can define the groups and computers that belong in a particular site by typing the group and computer names in a text file, and then importing that information into ePolicy Orchestrator. You may find working in a text file easier than working in the ePolicy Orchestrator console. Also, you may have network utilities, such as NETDOM.EXE utility available with the Windows Resource Kit, to generate complete text files containing complete list of the computers on your network. Then you can edit the text file to manually create groups of machines, and import the entire structure into the ePolicy Orchestrator **Directory**.

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

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

Create a text file of groups and computers to import

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

Figure 3-7 Import groups and computers 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 your ePolicy Orchestrator **Directory**. List each computer separately on its own line. If you want to organize computers into groups, type the group name and then list the computers belonging to that group beneath it, each on a separate line.

```
GroupA\
Computer1
Computer2
Computer3
Computer4
```

Be sure to manually verify the names of groups and computers and text file syntax before you use it to import computers. When you are done, save the text file to a temporary folder on your ePolicy Orchestrator server.

Import the groups and computers from the text file to the Directory

Once you have created a text file of computers to import, you can import the file into the **Directory**.

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

- 1 In the console tree, right-click the site or group into which you want to import the computers and/or groups from the text file, 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 for the text file you created containing your groups and computers.
- 4 When you locate the text file, select it and click **OK**.

ePolicy Orchestrator imports the computers to your selected site or group in the **Directory**. If your text file organized the computers into subgroups, it creates the groups and imports appropriate computers into them.

Adding WebShield appliances

You may have McAfee WebShield gateway appliances installed on your network and want to manage them with ePolicy Orchestrator. Once the WebShield appliance is installed on your network, you can add it to the **Directory**. You can add the appliance to any existing site or group.

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

- 1** In the **Directory**, 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**.

4

Deploying Agents, SuperAgents, and Sensors

Place computers on your network under management

The agent is the distributed component of ePolicy Orchestrator that is installed on each client computer in your network. The agent collects and sends information between the ePolicy Orchestrator server, repositories, and managed client computers and products. How you configure the agent and its policy settings determines how it functions and facilitates communication and updating in your environment.

This chapter covers deploying the agent to every computer in your network you wish to manage with ePolicy Orchestrator. Before you actually begin the deployment, however, it is recommended that you also review [Chapter 8, Managing Deployed Agents](#). Agent policies and other factors can influence how you deploy agents, so you should be familiar with this information.

The methods for deploying the agent are different if you are upgrading from a previous version of the agent compared to deploying it for the first time.

What's in this chapter

This chapter is divided among the following topics:

- [About deploying the ePolicy Orchestrator agent](#)
- [Using ePolicy Orchestrator to deploy the agent](#)
- [Installing the agent with logon scripts](#)
- [Installing the agent manually](#)
- [Other ways to deploy the agent](#)
- [Upgrading agents from a previous version](#)
- [Deploying the agent to Novell NetWare servers and WebShield appliances](#)
- [Uninstalling the agent](#)
- [Agent installation command-line options](#)
- [Deploying SuperAgents to distribute agent wakeup calls](#)
- [Deploying Rogue System Detection sensors](#)

About deploying the ePolicy Orchestrator agent

Consider the following details around the agent before deploying agents.

Install Microsoft updates on any Windows 9X client computers

If you have client computers in your network running Windows 95, 98, or ME, you must make sure they are able to be managed by ePolicy Orchestrator. By default, Windows 9X does not allow ePolicy Orchestrator administration. To enable this on Windows 9X clients, download VCREDIST.EXE and DCOM 1.3 updates from the Microsoft web site and install them on each client as required. See the following links for information:

support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q259403&

www.microsoft.com/com/dcom/dcom95/dcom1_3.asp

In addition, if you plan to use ePolicy Orchestrator to deploy the agent to client computers running Windows 9X, you must also enable File and Print Sharing on the Windows 9X clients. See [About pushing the agent from the ePolicy Orchestrator console on page 61](#).

Agent installation directory

The location of the agent installation directory is different depending on whether the agent is located on client computers or the ePolicy Orchestrator server.

- If the agent was installed as part of another product installation or pushed from the ePolicy Orchestrator console to client computers, it is installed by default into the <SYSTEM_DRIVE>\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK folder. See [Enabling the agent on unmanaged McAfee products on page 68](#) for more details about working with agents installed with other products.
- If you are upgrading the agent from version 2.5.1, the new agent is also installed by default to the <SYSTEM_DRIVE>\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK folder, but only after the existing agent is uninstalled.
- The agent that is installed on the ePolicy Orchestrator server during the installation is located in the COMMON FRAMEWORK folder in the ePolicy Orchestrator software installation directory.



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 client computers, you must check the desired agent language packages into the master repository, then replicate them to distributed repositories in the same manner as other product update packages.

For more information on checking deployment packages, including agent language packages, into the master repository, see [Check in product deployment packages to the master repository on page 89](#).

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 agent-to-server communication, the agent:

- 1 Retrieves language packages from repositories based on the locale being used on client computers during the **Update** client task or a global update.

- 2 If the in-use locale corresponds to an available language package, the agent retrieves the new package and applies it. In this way, the agent retrieves only language packages for the locales being used on each client computer.

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 client computers at the same time to allow end 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

Create a custom deployment package if deploying without ePolicy Orchestrator

If you are using another deployment method, such as login scripts or third-party deployment software, you may need to embed administrator user credentials in a custom agent deployment package. Because users might not have local administrator permissions, you can embed the appropriate set of credentials as part of the FRAMEPKG.EXE agent installation package by creating a custom installation package. The user account you embed is used to install the agent.

You can also create a custom deployment package with embedded user credentials if you deploy the agent via ePolicy Orchestrator. However, with this method you can also specify appropriate credentials in the **Agent Install** dialog box when you send the agent. See [Using ePolicy Orchestrator to deploy the agent on page 60](#).

To create a custom agent installation package:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 Select the desired server in the console tree, select the **General** tab in the details pane, 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** appears, showing the progress of the creation.
- 7 Click **Next**, then **Finish**.

You can distribute the custom deployment package file as needed to see that it is installed on clients in your network.

If you plan to deploy the custom package with ePolicy Orchestrator, check it into your master repository.

Using ePolicy Orchestrator to deploy the agent

You can use ePolicy Orchestrator to push agents to your client computers. This method uses Windows NT push technology.

Add computers to the Directory before deploying agents

If you chose to use ePolicy Orchestrator to deploy agents, you must first add the computers you plan to manage to the **Directory**. See [Chapter 3, Creating a Directory of Managed Computers](#) for detailed information on creating your **Directory**.

What's in this section

This section contains the following topics:

- [About pushing the agent from the ePolicy Orchestrator console.](#)
- [Push the agent to computers from the Directory.](#)
- [Deploying the agent while creating the Directory.](#)

About pushing the agent from the ePolicy Orchestrator console

Before you use ePolicy Orchestrator to push agents, there are several things you should consider. This section covers these in detail.

Do you have domain administrator credentials to push the agent?

If you specified a user name with domain administrator rights when you installed the ePolicy Orchestrator server, you can use the ePolicy Orchestrator server account. Otherwise, you'll need to specify a user account with domain administrator rights in the target domain for ePolicy Orchestrator to be able to push the agent.

Ping client computers from the server to test network communication

The ePolicy Orchestrator server must be able to "see" the client computers on the network to be able to push the agent to them. Before beginning a large agent push deployment, try pinging a few computers in different parts of your network to make sure the server can communicate with computers in those network segments. From your the ePolicy Orchestrator server, open a command window by selecting **Start | Run** and typing `cmd` at the run prompt. Then type ping commands, using the syntax below. Test ping by both computer name and IP address:

```
ping MyComputer
```

```
ping 192.168.14.52
```

If the targeted computers respond to the ping, then that means ePolicy Orchestrator can communicate with them.



Being able to ping client computers from the ePolicy Orchestrator server is not required for the agent to communicate with the server after the agent is installed. It is only a useful test for determining if you can push agents from the server to install them on clients.

Confirm that client NT Admin\$ share folders are accessible from the server

From the computer on which you plan to install your ePolicy Orchestrator server, test access the default `Admin$` shared folder on each client computer. The ePolicy Orchestrator server service will require access to this shared folder to install agents and other software, such as VirusScan Enterprise 7.1. This test will also confirm your administrator credentials, as you cannot access remote `Admin$` shares without administrator rights. To access client `Admin$` shares from the ePolicy Orchestrator server, do the following:

- 1 Select **Start | Run**.
- 2 In the run prompt type the path to the client `Admin$` share by specifying either computer name or IP address, like so:

```
\\MyComputer\Admin$
```

```
\\192.168.14.52\Admin$
```

If the computers 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.

Enable File and Print Sharing on Windows 9X clients

If you plan to deploy the agent to Windows 9X clients, you must first enable **File and Print Sharing** on those clients. Note that this is only required if you plan to *push* agents to these clients, and is not required for ePolicy Orchestrator to manage these computers after the agent is installed. If you install the agent manually or through some other method, such as a logon script, enabling **File and Print Sharing** is not required.

Furthermore, once you have pushed the agent to these Windows 9X clients, you can disable **File and Print Sharing** again and still manage agent policies on those clients with ePolicy Orchestrator.

Enabling network access on Windows XP Home computers

If you want to deploy the agent from the ePolicy Orchestrator console or install a custom agent installation package to computers using Windows XP Home, you must enable network access.

To enable network access on computers running Windows XP Home:

- 1 Click the **Start** button, then select **Control Panel**.
- 2 Click **Performance and Maintenance**.
- 3 Click **Administrative Tools**.
- 4 Select **Local Security Policy**. The **Local Security Settings** application window appears.
- 5 In the console tree under **Security Settings | Local Policies**, select **Security Options**. The available policies appear in the details pane.
- 6 Select **Network access: Sharing and security model for local accounts** to open the **Network access** dialog box.
- 7 Select **Classic - local user authenticate as themselves**, then click **OK**. Local users will be able to authenticate and access resources on the computer from the network.

Push the agent to computers from the Directory

To deploy the agent installation package (FRAMEPKG.EXE) from the ePolicy Orchestrator console to selected computers in the **Directory**:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 In the console tree under the **Directory**, right-click the desired site, group, or computer, then select **Send Agent Install**. The **Install Agent** dialog box appears.

Figure 4-2 Configure agent installation options for Send Agent Install



- 3 Choose whether to **Only install on computers that do not have an agent**.
- 4 Under **Level**, specify the computers to which you want to deploy the agent.
- 5 Choose whether **Suppress agent installation GUI** on the client computers.
- 6 Select **Force install over existing version** if you need to downgrade the agent version.



New Feature in 3.5! The **Force install over existing version** option allows you to use the ePolicy Orchestrator **Agent Install** feature to downgrade the agent. This might be necessary if you experience problems 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 ePolicy Orchestrator software repository, even if a newer version of the agent is already installed on the client computer.

- 7 Accept the default **Installation path** (<SYSTEM_DRIVE>\EPOAGENT) or type a different path install the agent on selected computers. 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 296](#).
- 8 Choose whether to use the ePolicy Orchestrator credentials to deploy the agent. If your ePolicy Orchestrator server credentials do not have rights to all computers to which you are deploying the agent, you must enter user credentials that do.



If you selected **Use Local System Account** in the **Server Service Account** dialog box when you installed the ePolicy Orchestrator server, you cannot use the ePolicy Orchestrator server credentials to deploy the agent.

To embed user credentials in the agent installation package, deselect **Use ePO server credentials**, then type the **User account** and **Password**.

- 9 Click **OK** to send the agent installation package to the selected computers.

Deploying the agent while creating the Directory

If you have not yet created the **Directory**, you can send the agent installation package to computers at the same time that you are adding sites, groups, and computers to the **Directory**. For instructions, see [Deploying the agent when adding a site, group, or computer to the Directory on page 45](#).

However, McAfee does not recommend doing this if you are creating your **Directory** by importing large NT domains or Active Directory containers. This can generate too much network traffic.

Installing the agent with logon scripts

Using network login scripts is a very reliable and popular way to make sure that every computer logging onto your network is running an ePolicy Orchestrator agent. You can write a login script to call a batch file that tests that the agent is installed on client computers attempting to log on to the network. If no agent is present, the batch file can install the agent before allowing the computer to log on. Within ten minutes of being installed, the agent will call into the ePolicy Orchestrator server for updated policies, and the computer will be added to the **Directory**.

You can also use network login scripts to test the agent version and, if the agent is older 3.0 or 2.X version, install the new 3.5 agent.



If you deploy the agent with login scripts, it is recommended that you first manually create some sites and groups in your **Directory** that use either network domain names or use IP filters. When agents call into the server for the first time, they can populate these sites and groups automatically. If you don't do this, they will all be added to the Lost&Found and you will have to manually move them later. Especially if you are deploying agents to a very large network, creating a **Directory** that uses some automated sorting method *before* deploying agents via login script can save you lots of time later. See [Creating sites and groups manually on page 53](#).

How you write the login script to install the agent may vary greatly, depending on what exactly you want the script to do. Consult your operating system documentation for more details on how to write login scripts. This section covers a basic example. To set up agent deployment via network login scripts:

- 1 [Copy the agent installation package to a central folder to which all users have permissions.](#)
- 2 [Create a batch file that tests new computers for an agent.](#)
- 3 [Save the batch file to your Primary Domain Controller \(PDC\).](#)
- 4 [Update your network login scripts to call the batch file.](#)

Copy the agent installation package to a central folder to which all users have permissions

Copy the FRAMEPKG.EXE agent installation package on your ePolicy Orchestrator server to a shared folder on a network server to which all computers have permissions. Computers logging onto the network will be directed to this folder to run the agent installation package and install the agent when they log in.

The FRAMEPKG.EXE file is created when you install the ePolicy Orchestrator server. It is a customized installation package for agents that will report to your server, and it contains all the network port, server name and IP address, and other information necessary for being able to communicate with the server. By default, the agent installation package is located in the following folder on your ePolicy Orchestrator server:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\DB\SOFTWARE\CURRENT\
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

Create a custom agent installation package if necessary

When installing the agent via a login script, you might need to create a custom agent installation package with embed administrator user credentials in it. These administrator credentials will be required for the script to be able to install the agent on the client. See [Create a custom deployment package if deploying without ePolicy Orchestrator on page 59](#) for more information.

Create a batch file that tests new computers for an agent

Create a batch file, such as EPO.BAT, that contains the lines you want to execute on client computers when they log in. The contents of this batch file will differ depending on what you need to do, but basically you want it to test whether the agent exists in the expected installation folder and install it if it's not there.

Below is a sample batch file that tests whether the agent is installed and, if it is not, runs the FRAMEPKG.EXE to install the agent. This example first tests the default install location of the older 2.5.1 agent and upgrades it to the 3.5 agent. Then it tests for the 3.5 agent in a different installation folder and, if it doesn't find it, installs the new agent.

```
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 in your deployment may be different than in this example, depending on where you have configured ePolicy Orchestrator to install the agent by default.

Save the batch file to your Primary Domain Controller (PDC)

Save the ePO.BAT batch file to the NETLOGON\$ folder of your Primary Domain Controller server. The batch file will run from the PDC every time a computer logs into the network.

Update your network login scripts to call the batch file

Add a line to your login script that calls the batch file on your PDC server. This line might look something like this:

```
CALL \\PDC\NETLOGON\EPO.BAT
```

Each computer logging into the network will run the script and install the agent at login time.

Installing the agent manually

A simple way to install the agent is to run the installer from the client computer. Some organizations may want to install software on clients manually and use ePolicy Orchestrator only to manage policies. Or, maybe you have many Windows 95 or Windows 98 clients and do not want to enable print and file sharing on them. In these cases, you can install the agent from the client instead.

You can install the agent at client computers, or distribute the FRAMEPKG.EXE installer to end-users in your organization and have them run the installer themselves. After the agent installs, it calls back to the server and ePolicy Orchestrator adds the new computer to the **Directory**.

About the FRAMEPKG.EXE agent installation package

The FRAMEPKG.EXE file is created when you install the ePolicy Orchestrator server. It is a customized installation package for agents that will report to your server, and it contains the server name, IP address, ASCII port number, and other information that will allow the agent to communicate with the server. By default, the agent installation package is located in the following folder on your ePolicy Orchestrator server:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\SOFTWARE\CURRENT\  
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

This is the same installation package that the ePolicy Orchestrator server uses to install the agent if you were to push the agent through the console. However, you can run the installation package from the client computer, just as you install any client software.

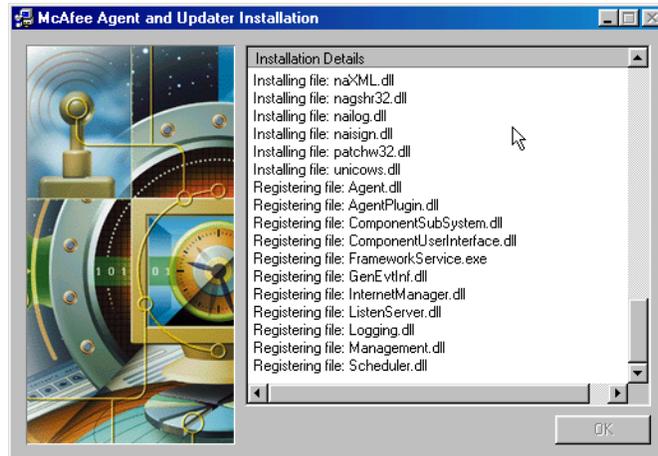
The default agent installation package contains no embedded user credentials in it. When it is executed on the client, it uses the user account of the currently logged-on user.

Distribute the FRAMEPKG.EXE installer

To have users on your network install the agent on their own client computers, distribute the agent installation package file to them. You can attach it to an e-mail, copy it to a CD-RW or floppy disk, or save it to a shared network folder accessible to all users on your network.

Installing the agent manually from a client computer

From the client computer, run FRAMEPKG.EXE by double-clicking it. Wait a few moments while the agent installs.

Figure 4-3 Wait while the agent installs

At some random interval within ten minutes, the agent will report back to the ePolicy Orchestrator server for the first time. You can bypass the ten-minute callback interval and force the new agent to call back to the server immediately. You can do this from any computer on which an agent has just been installed, not just on computers where you have manually installed the agent.

To manually force the initial agent callback:

- 1 From the client computer 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 will call back to the ePolicy Orchestrator server immediately.
- 5 From the ePolicy Orchestrator console on your server, refresh the **Directory** by clicking **F5**. The new client computer on which you have just installed the agent should now appear in your **Directory**.

What happens after the agent installs and calls into the server

When the agent calls back to the server for the first time, the computer will be added to the **Directory** tree as a managed computer. If you configured IP address filtering for your **Directory** sites and groups, the computer will be added to the appropriate site or group for its IP address. Otherwise, the computer is added to the **Lost&Found** folder. Once the computer is added to the **Directory**, you can manage its policies through the ePolicy Orchestrator console.

Other ways to deploy the agent

This section contains information on additional methods you can use to deploy the ePolicy Orchestrator agent.

Distributing the agent using third-party deployment tools

You may already use other network deployment tools 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 the ePolicy Orchestrator agent. Configure your deployment tool of choice to distribute the FRAMEPKG.EXE agent installation package located on your ePolicy Orchestrator server.

Use the default agent installation package or embed credentials in a custom one

The FRAMEPKG.EXE file is created when you install the ePolicy Orchestrator server. It is a customized installation package for agents that will report to your server, and it contains the server name, IP address, ASCII port number, and other information that will allow the agent to communicate with the server. By default, the agent installation package is located in the following folder on your ePolicy Orchestrator server:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\DB\SOFTWARE\CURRENT\  
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

If you need to, you can embed administrator credentials in a custom agent deployment package. For instructions, see [Create a custom deployment package if deploying without ePolicy Orchestrator on page 59](#).

Including the agent on a standard workstation or server install image

If your organization uses standard installation images for new workstations and servers, you can include the ePolicy Orchestrator agent on your images. You can install the ePolicy Orchestrator agent on computers used to create common images for your environment. The first time the user logs on to a computer built using a common image that includes the agent, the computer is assigned a unique ID called a global unique identifier.



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.

Enabling the agent on unmanaged McAfee products

Before you decided to buy ePolicy Orchestrator, you may have already been using McAfee products in your network. Some of the more recent McAfee products that use the AutoUpdate 7.X Common Management Agent (CMA), such as VirusScan Enterprise, install with the ePolicy Orchestrator agent in a disabled state. When you decide you want to start managing these products with ePolicy Orchestrator, you don't need to install the agent on them. Instead, you can simply "switch on" the CMA agent that is already on the client computer.

Enabling the agent in this way, rather than re-deploying the 1.5 MB agent installation package to each client computer, can save network bandwidth. This is especially true if you have many computers like this and plan to bring them all under ePolicy Orchestrator management. Note, however, that 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 some other method.

You must copy the `SITELIST.XML` repository list file from the ePolicy Orchestrator server to the client computer. The repository list contains network address information for the ePolicy Orchestrator server that the client agent needs to be able to call into the server for the first time after installing.

To enable the agent on products that already have a disabled agent installed:

- 1 Export the repository list (SITELIST.XML) from the ePolicy Orchestrator server and copy it to a temporary folder on the client computer, such as `C:\TEMP`. For instructions, see [Managing the SITELIST.XML repository list on page 145](#).
- 2 To enable the agent, run this command line on the client computer:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

Reference the `SITELIST.XML` file in the temporary folder from step 1. By default, `FRMINST.EXE` is located in the following folder on the client computer:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK
```

And where `/SITEINFO` equals the location of the repository list (`SITELIST.XML`) you exported.



Products that you may enable management for in this way most likely use an older version of the CMA agent. When you enable these older agents using the procedure in this section, they are *not* automatically upgraded to the latest agent version that is on the ePolicy Orchestrator server. To do this, you should also enable and run the default Deployment task to install the new agent on the client computer. For instructions, see [Using ePolicy Orchestrator to upgrade the 3.x agent on page 70](#).

Upgrading agents from a previous version

If you have already been using an older version of ePolicy Orchestrator and have earlier versions of the agent deployed on your network, you can upgrade those agents after you've installed your ePolicy Orchestrator 3.5 server. The procedure for upgrading the agent depends on which older agent version is running on your client computers already.



Legacy agents are not fully functional in ePolicy Orchestrator 3.5. For full agent functionality, you must upgrade to agent version 3.5.

Upgrade the 3.x agent using login scripts or manual installation

If you don't use ePolicy Orchestrator to deploy agents or products to client computers, you can use your preferred agent deployment method to upgrade existing 3.x agents to 3.5. Upgrading agents without using ePolicy Orchestrator, such as upgrading manually or using network login scripts, is the same as deploying agents for the first time. To do this, distribute the 3.5 agent `FramePkg.EXE` installation file launch it on the client using the method you prefer, such as installing manually or via a network login script.

See [Installing the agent with logon scripts on page 64](#) or [Installing the agent manually on page 66](#) for more information.

Upgrading the agent using ePolicy Orchestrator

If you use ePolicy Orchestrator to deploy agents in your network, the procedure differs slightly depending on which older version of the agent you are upgrading from. See the following sections for more detail:

- Using ePolicy Orchestrator to upgrade the 2.5.1 agent

- Using ePolicy Orchestrator to upgrade the 3.x agent



If you are upgrading your ePolicy Orchestrator deployment from a previous version, and your network is very large, don't upgrade too many agents at once. Consider using a phased upgrade procedure to upgrade one site or group in your **Directory** at a time. Upgrading fewer clients reduces network traffic by limiting the number of 1.5 MB agent deployment packages sent over the network at a given time. It also makes tracking upgrade progress and troubleshooting individual problems easier.

If you upgrade the 2.5.1 agent, set the policy changes for one site or group at a time, allow the upgrade to complete, and then set 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 deployment task to run at different times for different sites or groups in the **Directory**.

Using ePolicy Orchestrator to upgrade the 2.5.1 agent

To upgrade from the 2.5.1 agent using the agent policies:

- 1 Select a site, group, or individual computer in the **Directory** whose agent(s) you want to upgrade to 3.5.
- 2 On the **Policies** tab in the upper details pane, select **ePolicy Orchestrator agent | Configuration** to open the agent policy pages.
- 3 On the **General** tab, deselect **Inherit** to enable configuration options.
- 4 Select **Enable agent upgrade from 2.x agent to the 3.5 agent**.
- 5 Click **Apply All** to save the change.

The next time the agents in the site or group call into the server, it will pull the 3.5 agent deployment package and upgrade to the new agent version.

To upgrade the agent using login scripts, you must update your network login scripts to deploy the new 3.5 agent. See [Installing the agent with logon scripts on page 64](#) for details on how to do this.

Using ePolicy Orchestrator to upgrade the 3.x agent

Newer ePolicy Orchestrator agents version 3.0 or later that use the Common Management Agent (CMA) updating architecture. To give you more control over when and how you upgrade these agents to version 3.5, you need to run the default **Deployment** task in the ePolicy Orchestrator console. This is the same deployment task that can be used to deploy products such as VirusScan Enterprise or Desktop Firewall to clients that are already running ePolicy Orchestrator agents. See [Chapter 5, Deploying Anti-Virus and Security Software](#) for more details on using the Deployment task to deploy security products.

Retrieve agent FRAMEPKG.EXE package to deploy new agents in the future

You can use the procedures to upgrade to new agents released in the future. McAfee releases newer versions of the agent periodically, either to improve the agent itself, but more often to add compatibility for new products. You can deploy and manage these newer versions of the agent with your ePolicy Orchestrator 3.5 server. Before deploying these newer post-3.5 agents, first download the agent deployment package from the McAfee web site and check it into the Master Repository.



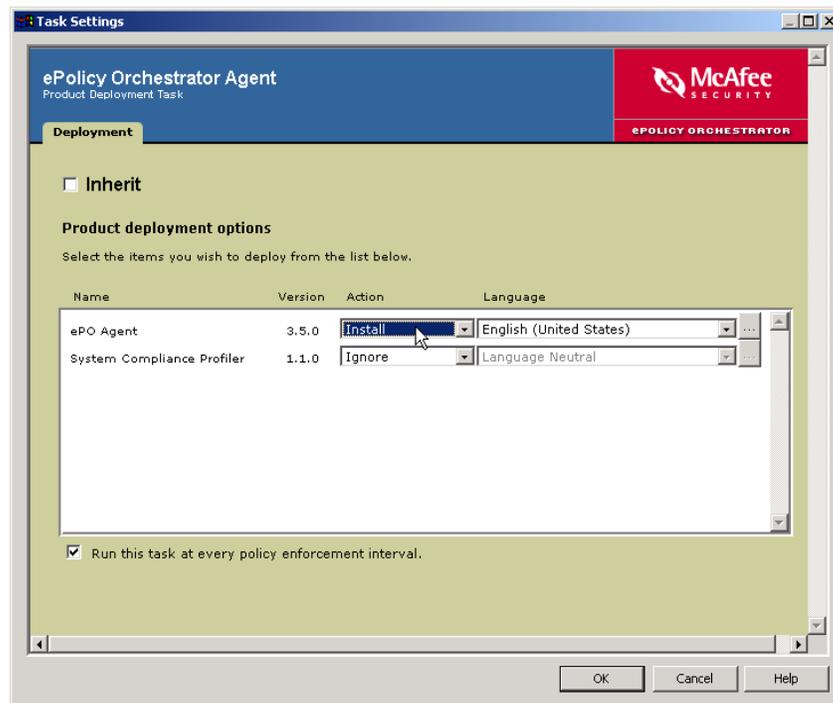
Don't confuse *upgrading* the agent using the **Deployment** task in ePolicy Orchestrator with *updating* an existing agent using the **ePolicy Orchestrator Agent Update** task. Upgrading the agent using the Deployment task is for installing a new major version of the agent over an older one, such as installing the 3.5 agent over the 3.0.x agent. The update task is used to update an existing version of the agent with additional updates such as DATs and engines, patches, service packs, or language packs, such as updating the 3.0.1 agent to version 3.02.

How to upgrade the 3.x agent with the deployment task

To upgrade the agent version 3.x or later to the 3.5 agent, configure and run the default **Deployment** task from the ePolicy Orchestrator console:

- 1 Make sure that the most recent agent deployment package is checked into the master software repository. See [Check in product deployment packages to the master repository on page 89](#) for information on checking in deployment packages to the master repository. Note that this section covers checking in *product* deployment packages, but the procedure is the same for checking in *agent* deployment packages.
- 2 In the ePolicy Orchestrator console **Directory** tree, select the site or group for which you want to upgrade the agent.
- 3 In the upper right details pane, click the **Tasks** tab.
- 4 Double-click the **Deployment** task 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 4-4 Configure Task Settings to “Install” to upgrade the agent



- 8 Click **OK** to save the setting change.
- 9 To schedule the task to run at a specific time, click the **Schedule** tab and schedule the task appropriately.
- 10 Click **OK** when done to close the **ePolicy Orchestrator Scheduler** dialog box.

The deployment task's **Enabled** status shows **True**. Agents on client computers will pick up the task information the next time the agents call back into the server. The agents will run the task at the scheduled time.

Deploying the agent to Novell NetWare servers and WebShield appliances

Installing agents on your Novell NetWare servers and WebShield appliances is very important as both of these are particularly exposed to virus and security threats that come across the network. Indeed, since it is located at the network gateway to the Internet, your WebShield appliances will likely take the biggest pounding. Having active agents deployed to these systems and keeping them up-to-date is critical.

You cannot use ePolicy Orchestrator to push the agent to Novel NetWare servers or WebShield appliances. Instead, use another deployment method, such as login script or manual install. The details of deploying to these different types of systems may vary, so consult your product documentation for details. The basic procedure is as follows:

- 1 Download the agent packages for the agent for NetWare and/or the agent for WebShield appliances. These agent installation packages are not installed on the ePolicy Orchestrator server by default.
- 2 Copy the agent installation packages to the appropriate systems and install them.
- 3 Add the systems to the ePolicy Orchestrator console **Directory**.

Uninstalling the agent

You can uninstall the ePolicy Orchestrator agent from a client computer using one of several methods.



You cannot remove the agent using the **Deployment** task, which you use to remove other products, such as VirusScan Enterprise, from client computers.

Run 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. The syntax looks something like this:

```
FRMINST.EXE /REMOVE=AGENT
```

See [Agent installation command-line options on page 73](#) for more details on the FRMINST.EXE command line options.

Uninstalling the agent by removing computers from the Directory

To remove the agent from one or more computers using the ePolicy Orchestrator console, delete the computer from the **Directory** and remove the agent when you do so. You can either delete individual computers, or delete a whole site or group.



Know that when you delete a group or site, it also deletes all child groups and computers. If you select the uninstall agent option when deleting from the **Directory**, ePolicy Orchestrator uninstalls agents from all child computers. **Make absolutely sure you want to uninstall the agent from all child computers before you delete sites or groups from the Directory.**

To remove the agent from computers in the **Directory**:

- 1 In the ePolicy Orchestrator **Directory**, right-click the desired site, group, or computer to remove from the **Directory**, then select **Delete**.
- 2 Select **Uninstall agent from all connected computers**.
- 3 Click **Yes**.

Uninstalling the agent when removing computers after a Directory search

You can also remove the agent from desired computers as you remove the computer from the **Directory** after finding them using one of the **Directory** search queries. These search queries are available in the ePolicy Orchestrator console, for example the **Inactive ePolicy Orchestrator agents** search. See [Use Directory Search to find computers in the Directory on page 267](#) for details on running **Directory** searches.

To remove an agent from a client computer that is returned after a **Directory** search has run:

- 1 Right-click the desired computer name in the list of **Search Results** at the bottom of the **Directory Search** dialog box and select **Delete**.
- 2 In the confirmation dialog box, select **Uninstall agent from all connected computers**.
- 3 Click **Yes**.

Agent installation command-line options

Depending on whether the agent is already installed, you can use these command-line options when you run the agent installation package (FRAMEPKG.EXE) or the agent framework installation (FRMINST.EXE) program.

You can also use any of these command lines when using the agent **Deployment** task to upgrade a new version of the agent over an older version. To do this from the **Task Settings** page of the **Deployment** task, click the  button to enter command line options. See [Upgrading agents from a previous version on page 69](#).

These options are *not* case-sensitive, but their values are.

Table 4-1 FRAMEPKG.EXE command line options

Command	Description
/DATADIR	Specify the folder on the client computer to use for agent data files. The default location is: <Documents and Settings>\All Users\Application Data\Network Associates\Common Framework If the operating system doesn't use a documents and settings folder, the default location is a data subfolder in the agent installation folder Sample FRAMEPKG /INSTALL=AGENT /DATADIR=<AGENT DATA PATH>
/DOMAIN /USERNAME /PASSWORD	Specify an NT domain, user name and password to use for installing the agent. The account must have at least the rights to create and start services on the computer. If not specified, the credentials of the currently logged-in user are used. If you want to use an account that is local to the current computer, use the computer's name as the domain. Sample FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=rgibson /PASSWORD=password
/INSTALL=AGENT	INSTALL=AGENT installs the agent if necessary, and enables the agent. Sample FRAMEPKG /INSTALL=AGENT
/INSTALL=UPDATER	INSTALL=UPDATER enables the Common Management Agent (CMA) if it has already been installed, and does NOT change whether the agent is enabled. This command line is used to upgrade the agent. Sample FRAMEPKG/INSTALL=UPDATER
/INSTDIR	Specify the installation folder for CMA on the client computer. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default install folder is: <DRIVE>:\program files\network associates\common framework Sample FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent
/REMOVE=AGENT	Disables the agent, and removes CMA if it is not in use. Sample FRMINST /REMOVE=AGENT
/SILENT or /S	Installs the agent in silent mode, which hides the installation interface from the end-user. Sample FRAMEPKG /INSTALL=AGENT /SILENT

Table 4-1 FRAMEPKG.EXE command line options

Command	Description
/SITEINFO	Specify the folder path to a specific SITELIST.XML repository list. See Managing the SITELIST.XML repository list on page 145 . Sample FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\MYSITELIST.XML
/USELANGUAGE	Specify 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 of CMA, the locale you select in Regional Settings determines the language version in which CMA appears. Sample FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404 For more information see Locale IDs on page 294 for a list of locale IDs.

Deploying SuperAgents to distribute agent wakeup calls

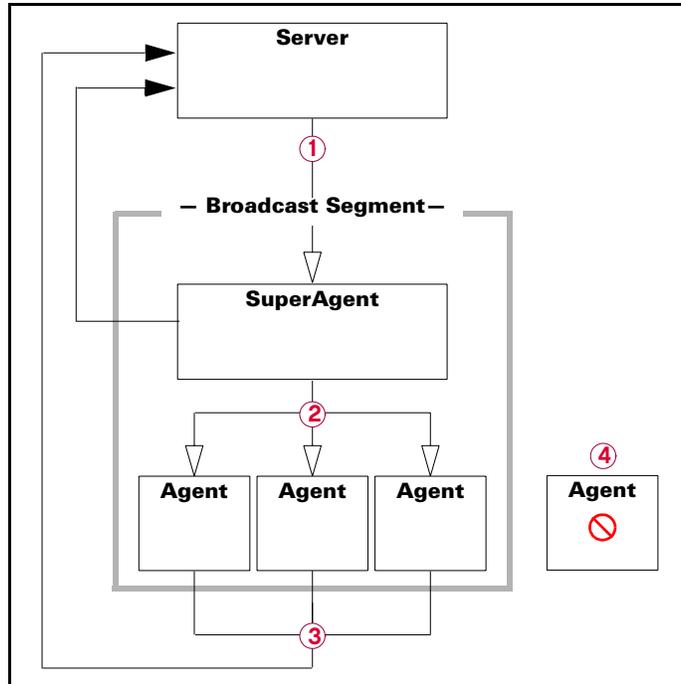
If you plan to use regular agent wakeup calls in your network, consider deploying SuperAgents to distribute the agent wakeup call and minimize network traffic. Depending on your network environment, you might find SuperAgent wakeup calls to be a more efficient way to prompt wakeup agents.

If you plan to use the global updating feature to aggressively update DATs, and possibly anti-virus scan engines too, you must deploy SuperAgents.

About SuperAgent broadcast wakeup calls

A SuperAgent is an agent that can send broadcast wakeup calls to other ePolicy Orchestrator agents located on the same network broadcast segment. Instead of having the ePolicy Orchestrator server send agent wakeup calls to every agent, it can send them only to a few SuperAgents. This helps reduce network traffic by sending fewer agent wakeups from the ePolicy Orchestrator server. This can be especially beneficial in large networks where ePolicy Orchestrator may manage agents in remote sites across by lower-speed WAN or VPN connections. Send out wakeup calls to a few SuperAgents and let them wake up the other agents in the local LAN.

Figure 4-5 The server wakes up SuperAgents, which wake up regular agents



- 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 will not be prompted to communicate with the server.

When you send a SuperAgent wakeup call to a selected node (probably a site or group) in your **Directory**, the server sends a wakeup call to all SuperAgents deployed in those groups. Then each SuperAgent sends an agent wakeup call to all agents in the same broadcast segment as the SuperAgent. The agents then call into the ePolicy Orchestrator server for updates.



You must know how physical broadcast segments and logical subnets are organized in your network to be able to deploy the right number of SuperAgents to the right locations. Any agents that do not have a SuperAgent in the local broadcast segment will not receive the broadcast wakeup call.

Usually a broadcast segment is the same as a network subnet, since most network routers block ICMP traffic between subnets by default. However, you may have configured your routers to allow ICMP traffic between certain subnets. In this case you only need to deploy one SuperAgent for all these ICMP-connected subnets. Conversely, you may have one subnet separated into several broadcast segments. In this case, you need to install a SuperAgent in each broadcast segment within the subnet.

SuperAgent wakeup call uses ICMP ping

Similar to the regular agent wakeup call, the SuperAgent wakeup call is an ICMP PING command sent from the ePolicy Orchestrator server. Many network routers block ICMP traffic between subnets by default. If your network is configured this way, using SuperAgent wakeup calls will not be able to wake up any computers located outside the local subnet where the ePolicy Orchestrator server is installed. If your network is configured in this way, do not use agent or SuperAgent wakeup calls. Use the regular agent ASCII, which uses the SPIPE protocol for all agent-to-server communication.

SuperAgent broadcast wakeup call is required if you use global updating

If you have global updating enabled, you must deploy SuperAgents. The global updating feature uses the SuperAgent broadcast wakeup call to have agents call in for update changes. See [Use global updating to automatically distribute updates to all clients immediately](#) on page 115.

SuperAgent repositories not the same as SuperAgents

SuperAgents can also be configured to function as a distributed repository for updates. This is separate SuperAgent functionality and is not related to the SuperAgent broadcast wakeup call. See [Creating SuperAgent distributed repositories](#) on page 132.

How to “deploy” a SuperAgent to a computer in the Directory

The only way to deploy a SuperAgent is to use the ePolicy Orchestrator Agent policy page in the console to enable SuperAgent functionality in an already-installed agent. You cannot deploy a SuperAgent installation package the same way you deploy the regular agent. This is partly because you do not deploy SuperAgents to every or even many computers in your network; you only deploy one to each network broadcast segment, which is usually a network subnet.

To turn a regular agent into a SuperAgent:

- 1 In the ePolicy Orchestrator **Directory**, select an individual computer that you want to turn into a SuperAgent. You can only enable the SuperAgent functionality at the computer level, and not at the site or group level.
- 2 In the upper details pane, click the **Policies** tab and select **ePolicy Orchestrator Agent | Configuration**.
- 3 In the lower details pane, deselect **Inherit** on the **General** tab.
- 4 Select **Enable SuperAgent functionality** and click **Apply All** to save the change.

The SuperAgent functionality is enabled the next time the agent calls into the ePolicy Orchestrator server for the policy change. If you have configured the agent policy to show the agent icon in the system tray of the client computer, the SuperAgent icon will look a little different from the regular agent icon.

Figure 4-6 The SuperAgent system tray icon looks a little different than a regular agent



Now the computer is ready to receive a SuperAgent wakeup call from the ePolicy Orchestrator server and then wakeup other agents in the same part of the network. See [Sending manual agent wakeup calls on page 150](#) for details on how to use SuperAgent wakeup calls.

Deploying Rogue System Detection sensors

The Rogue System Detection component is a new feature in ePolicy Orchestrator 3.5 that allows you to use the ePolicy Orchestrator console to detect computers on your network that don't have an agent installed on them. To do this, ePolicy Orchestrator uses a small Win32 application called a sensor that is distributed throughout your network. The sensor "listens" on the network for layer 2 broadcast traffic, and reports back to the ePolicy Orchestrator server. Any computer that the sensor detects on the network that does not have an ePolicy Orchestrator agent on it is classified a rogue system.

Understand how Rogue System Detection works before deploying sensors

This section only covers how to deploy Rogue System Detection sensors, and does not go into detail on the rest of Rogue System Detection. You can follow the steps in this section to deploy sensors to your network using mostly default settings. However, some sensor configuration options may affect how and where you deploy your sensors. We strongly recommend familiarizing yourself with how the Rogue System Detection feature works before you begin deploying sensors. See [Chapter 11, Rogue System Detection](#) for more details.

What's covered in this section

The rest of this section covers the following specific topics around sensor deployment:

- [About deploying Rogue System Detection sensors in your network.](#)
- [Deploying sensors from the Rogue System Detection Subnet List.](#)
- [Manually installing the sensor.](#)
- [Uninstalling the sensor.](#)

About deploying Rogue System Detection sensors in your network

Because of the way the sensor is designed, you must install one sensor per broadcast segment in your network. Note that, depending on how your network is configured, this might not be the same thing as the physical broadcast segment.

By default, the sensor is configured to report only on detections occurring within its local logical subnet. If you use this default configuration, which McAfee recommends, then you must deploy at least one sensor to each logical subnet in your network.

Where should I install Rogue System Detection sensors?

The computer on which the sensor is installed should be a computer that is likely to remain on and connected to the network all the time, such as a server if possible. If you don't have a server running in a given subnet, deploy several sensors to several workstations to maximize the chance that any one of them will be turned on and connected to the network at a given time.

To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor in each network broadcast segment in your network. Typically, a network broadcast segment is the same as a network subnet. You can install more than one sensor in a subnet—the Rogue System Detection server filters duplicate detection messages. Note, however, that having multiple active sensors in each subnet *will* result in duplicate messages sent from each sensor to the server. While maintaining as many as five or ten sensors in a subnet should not cause problems, McAfee recommends to not maintain more sensors in a subnet than is necessary to guarantee that the subnet is covered. The more sensors you have, the more network traffic Rogue System Detection generates.

About 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 (by default there are 3). These are the **Primary Sensors**. Any additional sensors you deploy are backups that sleep until told by the Rogue System Detection server to become active. These are the **Inactive Sensors**. At regular intervals, the Rogue System Detection 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 will automatically make a different sensor on that subnet the primary sensor.

The **Subnet List** on the **Subnets** tab of the Rogue System Detection interface allows you to quickly see the subnets in your network on which you already have ePolicy Orchestrator agents. From here you can deploy sensors to computers.

Consider sensor policies before deploying

Before you deploy sensors, you should configure the sensor-to-server parameters to suit your network needs. These will probably be the same for all sensors that communicate to your Rogue System Detection server. Because of this, you can configure sensor policies at the highest levels of the **Directory** and let them inherit to lower levels.

See [Configure Rogue System Detection sensor policies on page 197](#) for details about setting sensor policies.

The Rogue System Detection sensor installation requirements

The Rogue System Detection sensor is a small Win32 application that runs unobtrusively on any server or workstation computer. The sensor installs and runs on any computer running a Windows NT-based operating system, such as Windows NT, Windows 2000, Windows XP, Windows 2003. The sensor does not run on older versions of Windows, such as Windows 95, 98, ME, or on non-Windows operating systems like Novell NetWare or Linux.

Additional installation recommendations are as follows:

- File system - NTFS recommended.
- Memory - 128 MB RAM.

- Processor - 166 MHz processor or higher.
- An Ethernet interface that supports 802.3, Ethernet II, or 802.11 protocols.

What happens when the computer where the sensor is installed changes subnets?

Occasionally, you may need to move the computer where a sensor is installed from one subnet to another. For example, this can happen when the computer on which the sensor is deployed is a laptop that may connect to different subnets on the network at different times.

The sensor is designed to correctly recognize when its subnet location has changed and report this change to the Rogue System Detection server. If the computer running the sensor changes subnets, this will be reflected immediately in the Subnets list in the Rogue System Detection server Web interface. See [Monitor your sensors deployed to network subnets on page 195](#) for details.

If you deploy a sensor to a computer that may change subnets, such as a laptop, make sure you deploy another sensor to cover that subnet. For example, assume your subnet A is covered by sensor 1. If sensor 1 moves to subnet B for whatever reason, that means subnet A will be without a sensor and therefore rogue systems on that subnet will remain undetected.

Deploying sensors from the Rogue System Detection Subnet List

Especially if your organization is large, installing sensors one by one throughout your network can be a very difficult and time-consuming task. This can be particularly true if you are rolling out Rogue System Detection for the first time and need to deploy many sensors to all the subnets in your organization at once. Use the Rogue System Detection server to centrally deploy sensors to your network from within the ePolicy Orchestrator console.

Deploy these sensors from the **Subnet List**, located on the **Subnets** tab of the Rogue System Detection interface. When deploying sensors from Rogue System Detection, you have two options. You can either manually pick specific computers to host the sensors, or you can let the Rogue System Detection server automatically pick computers from the available computers on the subnet.



Rogue System Detection uses the ePolicy Orchestrator product deployment architecture to deploy the Rogue System Detection sensor. Therefore, you can only deploy sensors from the Rogue System Detection server to computers that have active ePolicy Orchestrator agents installed on them.

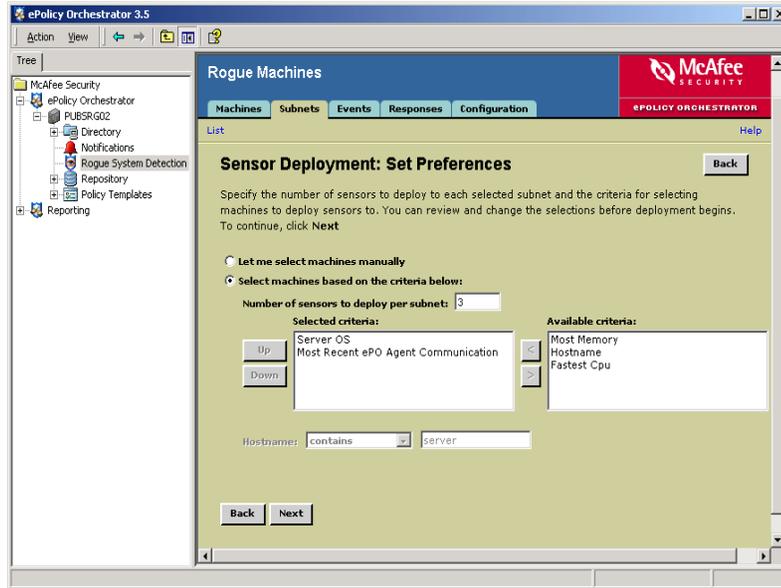
To deploy Rogue System Detection sensors to your network from the **Subnet List**:

- 1 In the ePolicy Orchestrator console, select **Rogue System Detection** from the console Tree.
- 2 In the Rogue System Detection details pane, click 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 in the **Subnet List** table. If you are deploying sensors to all your subnets at once, such as you may do when deploying sensors for the first time, you can select all subnets in the list by clicking **Check All**.

As you are mostly likely deploying sensors to subnets that currently do not have any sensors in them, these subnets will have the *Uncovered* status.

- 4 Select Deploy Sensors.
- 5 On the Set Preferences page, make sure the Select machines based on the criteria below is selected.

Figure 4-7 Specify whether you want to manually select sensor hosts or let Rogue System Detection do it



Change any of the automatic sensor selection criteria if needed. Rogue System Detection uses these criteria when selecting computers on the subnet to deploy sensors to. For example, you can choose to deploy 3 sensors and specify the **Server OS** and **Most Memory** criteria. Rogue System Detection selects the three computers with server operating systems that have the most memory and deploys a sensor to each.

Use the left and right arrow buttons to move a criteria from **Available criteria** to **Selected criteria**. To prioritize Selected criteria, click once on the criteria in the **Selected criteria** list and click **Up** or **Down** to prioritize that criteria accordingly. The higher a specific criteria is listed in Selected criteria, the higher the priority.

You can specify any or all of the criteria listed in [Table 4-2](#) when configuring automatic sensor deployment:

Table 4-2 Automatic sensor deployment criteria

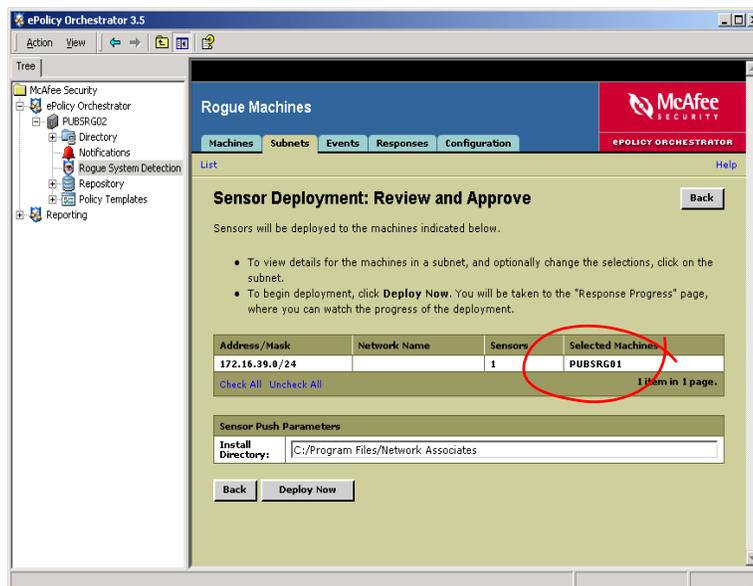
Criteria	Description
Most Recent ePO Agent Communication	More recent agent communications mean a computer is more likely to be constantly connected to the network and currently active.
Server OS	Servers are more likely than workstations to remain on and connected to the network at all times. The sensor can only detect if the computer on which it is installed is on and connected to the network.

Table 4-2 Automatic sensor deployment criteria

Criteria	Description
Hostname	If you use naming conventions when creating the DNS names for computers, you can have Rogue System Detection select sensor hosts by a text string you use in the DNS name. For example, if you add a “SRV” prefix to all your server computers, you could have Rogue System Detection deploy to a computer with “SRV” in its DNS name. If you add Hostname to the Selected criteria list, type the text string that appears in your server DNS names in the Hostname text box.
Most Memory	The more the better, although the Rogue System Detection sensor is not a memory-intensive application.
Fastest CPU	The faster the better.

- 6 Click **Next** to save your automatic sensor deployment criteria.
- 7 On the **Review and Approve** page, review and confirm the selected computers and installation folder to which the sensors are to be deployed.

Figure 4-8 Review auto-selected sensor hosts and begin sensor deployment



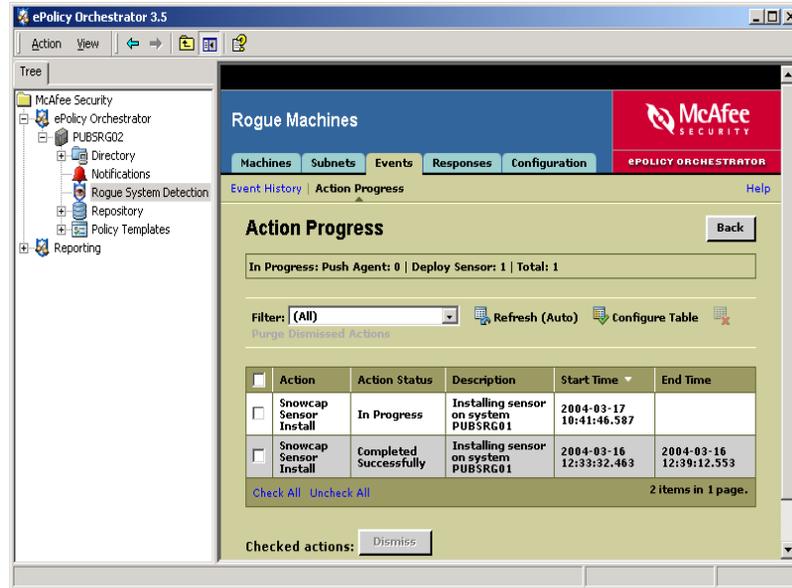
The computers that Rogue System Detection has automatically selected for automatic sensor deployment are listed in the **Selected Machines** field for each subnet.

You can manually change any of the selected computers at this point. To change the computers to which sensors will be deployed, click that row in the table to open the **Review Selected Machines** page for that subnet and make any changes. Click **Close** to save the changes made on the **Review Selected Machines** page and return to the **Review and Approve** page.

- 8 Click **Deploy Now** to initiate the sensor deployment.

After clicking **Deploy Now** to initiate a sensor deployment, you arrive automatically at the **Response Progress** page of the **Responses** tab. The sensor deployment you have just initiated appears in the table and the end time field is not yet populated to indicate that the deployment is still in progress.

Figure 4-9 Response progress after initiating a sensor deployment



ePolicy Orchestrator deploys the sensors the next time that the agent installed on that computer contacts the ePolicy Orchestrator server. To force the sensor deployment to occur immediately, manually initiate an immediate agent wakeup call.

To initiate an immediate agent wakeup call:

- 1 Right-click the ePolicy Orchestrator server listed in the **Directory** tree and select **Agent Wakeup Call**.
- 2 On the **Agent Wakeup Call** dialog box, set the **Agent randomization** to 0 minutes and click **OK**.

Wait a few moments for the agent wakeup call to begin. Once the sensor installation is complete, the **End Time** field of the **Response Progress** table is updated to show the date and time that the sensor installation is complete.

You can also click the **Machine** tab to watch as the **Machine List** table begins populating with computers that the new sensors have detected on their subnets. The sensor should begin detecting computers immediately after installing. Click **Refresh** periodically to refresh the **Machine List**.

It may take several minutes for the sensor to detect all the active computers on the network.

Manually installing the sensor

If you do not wish to deploy your rogue system sensors from the ePolicy Orchestrator console, you can perform the installation manually. To manually install the sensor, you must be at the computer where the sensor is to be installed and have administrative privileges on that computer.

You can install the sensor either via a `SETUP.EXE` installation wizard or via the command line.

Where can I find the sensor installer?

The Rogue System sensor `SETUP.EXE` and other installation files are located in the following subfolder under your ePolicy Orchestrator installation folder:

```
<Install Folder>/3.5.0/DB/Software/Current/Rogue System  
Detection_1000/Install/0409
```

Installing the sensor manually using SETUP.EXE

Copy the entire contents of this folder to a CD or shared network folder that you can access while you install the sensor to the computers in your network.

To manually install the Rogue System Detection sensor:

- 1 Double-click the Rogue System Detection sensor `SETUP.EXE` file.
- 2 Click **Next** at the **Welcome to the McAfee Rogue System Detection Sensor 1.0.0 Installation Wizard**.

- 3 On the **Destination Folder** screen, specify an installation folder and click **Next**.

The default is `C:\Program Files\Network Associates\Rogue System Detection Sensor`.

- 4 On the **Rogue System Detection Server Information** screen, type the DNS name or IP address of the computer hosting the Rogue System Detection server into the **Server Host Name or IP address** text box.
- 5 In the **Server Port Number** text box, type the port number used by the Rogue System Detection server for secure HTTPS communication. By default this is 8443.



Be sure to specify the correct port number, especially if you configured the Rogue System Detection server to use a port other than 8443. Also, be sure to specify the port used for HTTPS secure communication and not regular HTTP.

- 6 Click **Next** to go to the **Ready to Install** screen.
- 7 Click **Next** to begin the installation.
- 8 After the sensor has been installed, click **Finish** to close the setup wizard.
- 9 Repeat the sensor installation steps for computers in each subnet in your network.

The sensor automatically installs and registers as an NT service on the client, so it is not necessary to manually start the sensor after installation. The sensor begins detecting after the next time the agent on that computer calls into the ePolicy Orchestrator server. However, if you wish, you can launch the sensor manually so that it displays in a command window on the client computer. This may be useful for troubleshooting purposes. To do this after the sensor is installed, run the `SENSOR.EXE` from the command line with the `--console` runtime command line option to open the sensor in a DOS command dialog box.

Rogue System Detection sensor command line installation

You can install the Rogue System Detection sensor from the command line. To do this, run the `SETUP.EXE` installer from a command line.

Command line switches supported for the Rogue system sensor are:

Table 4-3 Sensor installation command line switches

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 Rogue System Detection server.
-d	C:\Program Files\Network Associates	The installation folder where the rogue system sensor will be installed.

Uninstalling the sensor

Occasionally, you may need to remove the sensor from selected computers. If you do, make sure that you don't remove the only sensor in a given network broadcast segment, as ePolicy Orchestrator will no longer be able to detect computers there. If you do remove the only sensor in a given network segment, be sure to deploy another one to a different system.

Removing the sensor from the console using the sensor deployment task

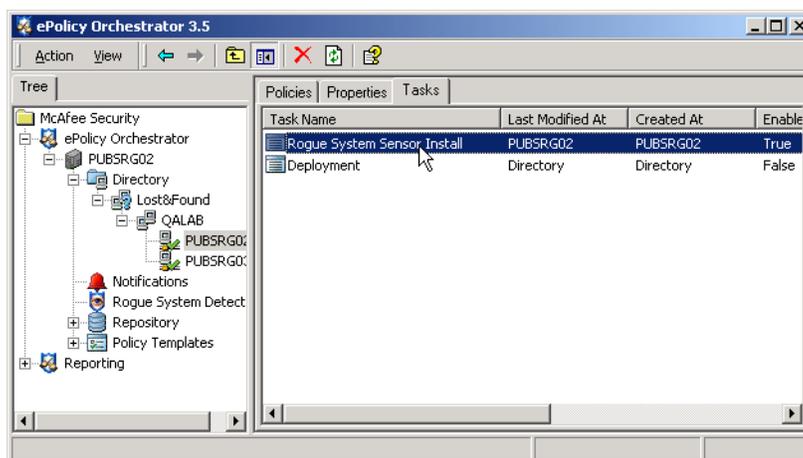
When you use the **Subnet List** to deploy rogue system sensors to computers from the ePolicy Orchestrator server, ePolicy Orchestrator creates a **Rogue System Sensor Install** task for that computer. You can use this task to remove the sensor, similar to the way you use the default Deployment task to remove anti-virus or security products such as VirusScan Enterprise from a client computer.

You can use the ePolicy Orchestrator Deployment client task in the console to remove a sensor from a particular computer, if the sensor was deployed via ePolicy Orchestrator.

To use the deployment task from the ePolicy Orchestrator console to remove a sensor:

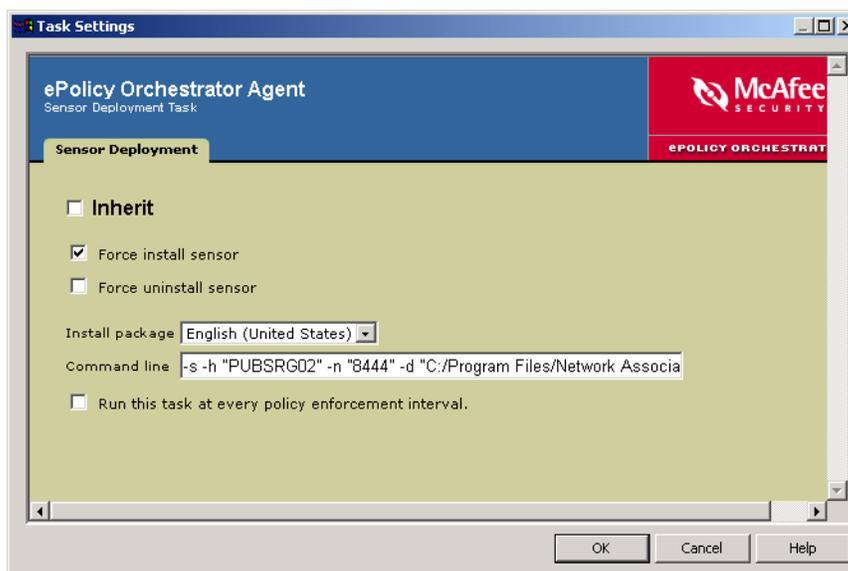
- 1 In the ePolicy Orchestrator **Directory**, select the computer from which you want to remove the sensor.
- 2 In the upper details pane of the console, click the **Tasks** tab and double-click the **Rogue System Sensor Deployment** task.

Figure 4-10 The rogue system sensor deployment task is separate from the default Deployment task



- 3 In the ePolicy Orchestrator Scheduler dialog box, deselect **Inherit** and make sure that **Enable** is selected under **Schedule Settings**.
- 4 Click **Settings**.

Figure 4-11 Task Settings for rogue system sensor install deployment task



- 5 Deselect **Inherit** to enable task setting options.
- 6 Deselect **Force install sensor** and select **Force uninstall sensor**.
- 7 Click **OK** to save the setting changes.
- 8 Click **OK** to close the ePolicy Orchestrator Scheduler.

The ePolicy Orchestrator agent will uninstall the sensor at the next ASCI.

Uninstalling the sensor manually using Add/Remove Programs

You can uninstall the Rogue System Detection sensor from the client using the Windows **Add/Remove Programs** utility.

To uninstall a sensor using the Windows **Add/Remove Programs** utility:

- 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* and click **Add/Remove**.
- 3 Click **Yes** when prompted to begin the uninstallation.

Uninstalling the sensor manually from the command line

You can uninstall the Rogue System Detection sensor using the Windows command line. When uninstalling by running SETUP.EXE from the command line, specify the `-x` command line switch to uninstall the sensor.

Specifying the `-x -s` command lines together uninstalls the sensor in silent mode.

5

Deploying Anti-Virus and Security Software

Use ePolicy Orchestrator to install products on computers

In addition to managing client anti-virus and security products, ePolicy Orchestrator allows you to deploy, or install, these products centrally from the ePolicy Orchestrator server. To do this, you can use the ePolicy Orchestrator server to send a product deployment package across the network to client computers. The deployment package then installs the software on the client. Once the product, such as VirusScan Enterprise or Desktop Firewall, is installed on the client, you can use ePolicy Orchestrator to manage the products by doing things such as scheduling DAT updates and scan tasks.

You can set these before deployment, or you can use the default policies and modify them after deployment.

What is covered in this chapter

- *About deploying products with ePolicy Orchestrator.*
- *Check in product deployment packages to the master repository.*
- *Check in NAP files to manage new products*
- *Use the deployment task to install products on clients*

What this chapter does not cover

Information in this section covers using ePolicy Orchestrator to deploy and manage anti-virus and security products generally. It covers the basic procedures used to deploy product packages and use the ePolicy Orchestrator interface to set product policies. It also covers creating client tasks to run on client computers.

It does not provide details on product-specific policy or task options. For details on configuring policies and client tasks for a particular product you can manage through ePolicy Orchestrator, see the appropriate *Configuration Guide* for that product.

Additionally, you manage your ePolicy Orchestrator agents deployed in your network using policies. However, managing agent policies is not covered here, but rather in the agent section. See *Chapter 4, Deploying Agents, SuperAgents, and Sensors* for more information about deploying agents.

About deploying products with ePolicy Orchestrator

You can use ePolicy Orchestrator to deploy anti-virus and security products, such as VirusScan Enterprise, Desktop Firewall, or GroupShield, to client computers in your network. To do this, you must first check in a special type of file, called a *package catalog* file, for each product you want to deploy with ePolicy Orchestrator. The package catalog file contains the installation files for the client product compressed in a secure format that ePolicy Orchestrator uses to push to client computers and install.

So, using ePolicy Orchestrator to deploy products to clients is a two-step process:

- 1 [Check in product deployment packages to the master repository.](#)
- 2 [Use the deployment task to install products on clients.](#)

You only need to perform these steps if you plan to use ePolicy Orchestrator to centrally deploy these products to your managed clients. If you plan to use a different deployment method and will use ePolicy Orchestrator only to manage product policies once they are already installed, you can skip this section.

Other ways to deploy client products

You may not be able to, or not want to, use ePolicy Orchestrator to deploy products or agents to the client computers to be managed. For example, there may be another department in your organization responsible for installing client software, and you plan to use ePolicy Orchestrator to manage policies for those products after they are installed. Or, you may prefer to use other network tools in your organization, such as Microsoft SMS or Tivoli, that you already use to install products on client computers. Maybe you want to install products manually or use network login scripts. You can use any of these other methods to deploy products to your clients, and then use ePolicy Orchestrator to manage those products after they are deployed.

The rest of this section only covers using ePolicy Orchestrator to deploy client software products in detail.

Check in product deployment packages to the master repository

Check in PKGCATALOG.Z product deployment package files to the master repository to be able to deploy them using ePolicy Orchestrator. You can manually check in any product package to the master repository that you plan to deploy through ePolicy Orchestrator.

What product deployment packages are installed with the ePolicy Orchestrator server?

Only two product deployment packages are installed with ePolicy Orchestrator when you install ePolicy Orchestrator server and console:

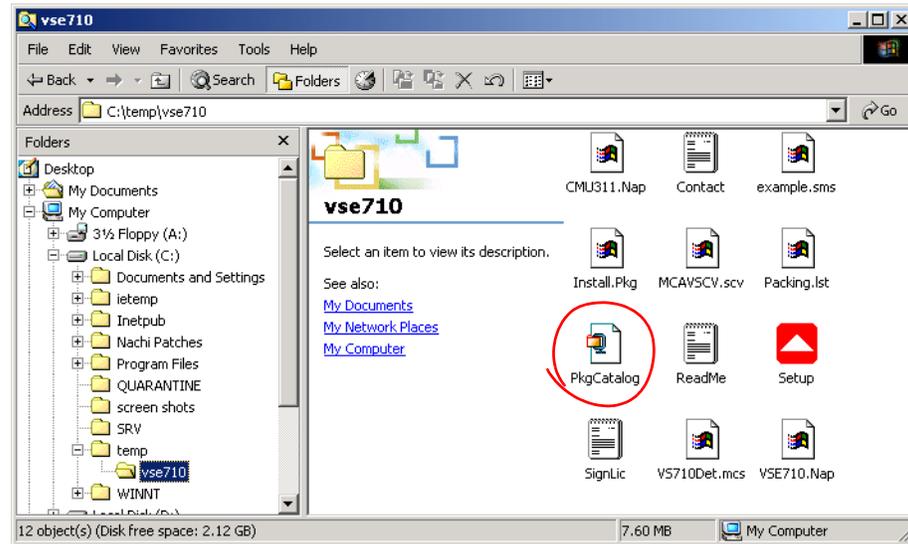
- ePolicy Orchestrator agent
- System Compliance Profiler

For all other software that you plan to deploy, or install, using ePolicy Orchestrator, you must first check in the corresponding deployment package.

Where do I find the PKGCATALOG.Z file?

Product deployment packages exist as a package catalog file called PKGCATALOG.Z. Every product that is released by McAfee and is deployable through ePolicy Orchestrator will include a PKGCATALOG.Z file. Usually, the package catalog file is located in the same folder as the other product installation files, either on the product CD or in the product installation ZIP file available on the McAfee product download site.

Figure 5-1 The PKGCATALOG.z file is included in the product download ZIP available from McAfee

**Use McAfee Installation Designer to create custom deployment packages for VirusScan Enterprise**

Like all product deployment packages created by McAfee and shipped with product releases, the VirusScan Enterprise package installs on client computers with all product default settings. You may want to significantly change the default settings to suit your needs. While you can change these through the ePolicy Orchestrator policy pages after you have installed VirusScan Enterprise on client computers in your network.

However, you may find it more efficient to create a customized VirusScan Enterprise deployment package that includes all your customized settings. Use the McAfee Installation Designer to do this. McAfee Installation Designer is a free utility available from McAfee that allows you to create custom deployment packages for VirusScan Enterprise.



Consider creating a customized VirusScan Enterprise deployment package if you are performing a very large deployment and you want to make significant changes to the product settings. Including all these setting changes in the deployment package can reduce the network traffic generated by sending the policy changes over the network from the ePolicy Orchestrator server to the agent.

Be sure to change the policies too! If you do this, don't forget to also make all your custom VirusScan Enterprise policy changes in the VirusScan Enterprise policy pages in the ePolicy Orchestrator console *before* deploying. If you don't, the agent on the client computer will change all your customized settings back to the defaults!

The Installation Designer creates a PKGCATALOG.Z file for VirusScan Enterprise contains all the customized settings. You can check this deployment package into your master repository to deploy with ePolicy Orchestrator.

The free McAfee Installation Designer utility is included with VirusScan Enterprise product CD and is also available for download from the McAfee web site.

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 updates from unsigned or untrusted sources.

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.

Checking in PKGCATALOG.Z product packages to the master repository:

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. See [Use Pull tasks to update the master repository from a source repository on page 107](#) and [Replicating the master repository contents to distributed repositories on page 139](#) for more information on these tasks.

To check in a product deployment package:

- 1 Locate the `PKGCATALOG.Z` package catalog file you want to check in. See [Where do I find the PKGCATALOG.Z file? on page 90](#).
- 2 Copy the entire contents of the folder containing the package catalog, not just `PKGCATALOG.Z` file itself, and save it to a temporary folder on your ePolicy Orchestrator server.



You must copy *all* the files in the `PKGCATALOG.Z` folder, and not just the `PKGCATALOG.Z` file itself, or the package check-in will fail.

- 3 From the ePolicy Orchestrator **Directory**, select **Repository**.
- 4 In the right-hand details pane under **AutoUpdate Tasks**, click **Check in package** to launch the **Check-in package** wizard.

Figure 5-2 Begin checking in a product deployment package to the master repository



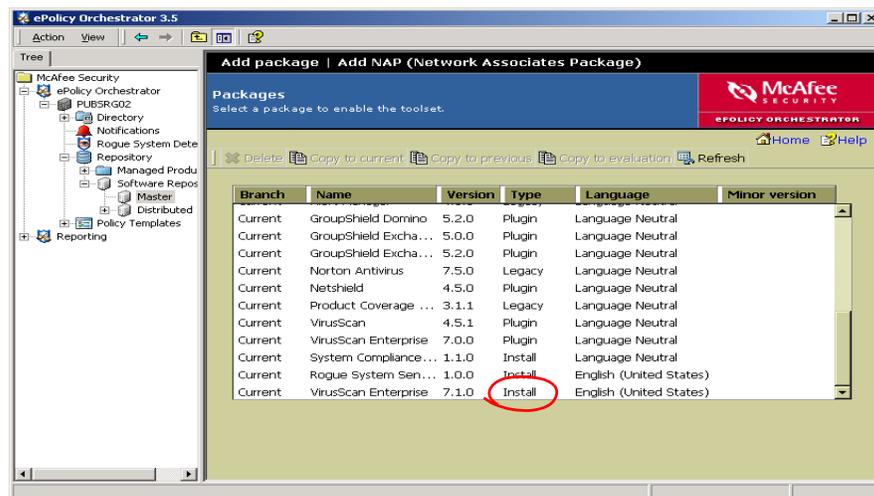
- 5 Click **Next** to open the package type dialog box.
- 6 Select **Products or updates** for the package type and click **Next**.
- 7 Type the full path or browse to and locate the PKGCATALOG.Z package catalog file that you saved in a temporary folder in [Step 1](#).
- 8 Click **Next** to view the package check-in summary information.
- 9 Click **Finish** to begin checking in the package. Wait a few minutes while the package checks in.
- 10 Click **Close** after the package check-in completes.

Confirming what product packages are in your master repository

After you check in the package, you can confirm the correct package and version has been added to your master repository. To do this:

- 1 In the ePolicy Orchestrator **Directory**, navigate to **Repository | Software Repositories | Master**.

Figure 5-3 Confirm that a deployment package was added to the repository



- 2 In the right-hand details pane, scroll through the list until you find the product name and version listed in the table for the product package you added.

Replicate packages checked into master repository to distributed repositories

If you are using distributed repositories in your network, be sure to perform a repository replication to copy the deployment package from the master repository to any distributed repositories you have. When you run the ePolicy Orchestrator deployment task to deploy a product to client computers, clients that receive updates from a distributed repository will get the product package from that distributed repository rather than the master. See [Chapter 7, Update Large Networks with Distributed Repositories](#) for more information on distributed repositories and replicating to them.

Check in NAP files to manage new products

ePolicy Orchestrator server installs with a set of policy pages for major supported products that are available when your version of ePolicy Orchestrator was released. At some point you will probably need to put new products under ePolicy Orchestrator management, or manage new versions of existing software. To manage these new products or product versions, you must first add the appropriate NAP file for that product to the software repository. You need to do this if, for example, McAfee releases a newer version of a product, such as VirusScan Enterprise or Desktop Firewall, that you will want to deploy in your network and manage with ePolicy Orchestrator.

Where can I find the *.NAP file for a new product I want to add to the repository?

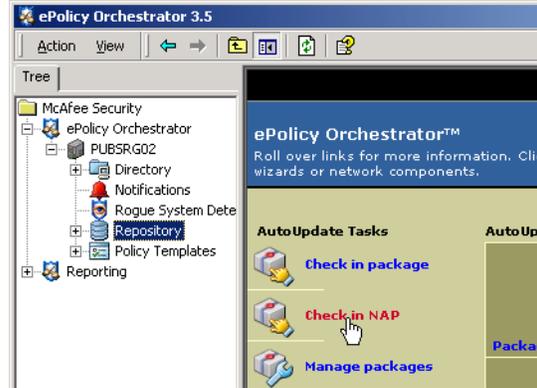
McAfee releases NAP files for all anti-virus and security products supported by ePolicy Orchestrator. The NAP file for a given product is available with the other installation files for that product. These can be either on the product CD or in the product ZIP file if you downloaded the installation files from the McAfee web site. The NAP file always has a .NAP file extension and is named with a product name code and version number, such as VSE750.NAP or DFW800.NAP for VirusScan Enterprise 8.0i and Desktop Firewall 8.0, respectively.

Policy pages are *not* added to the master repository; they are stored on the ePolicy Orchestrator server. Because of this, NAP files are not replicated to distributed repositories or updated to client computers.

To check in a NAP file to the ePolicy Orchestrator server:

- 1 Locate the appropriate product NAP file, either on the product CD or in the installation ZIP file downloaded from the McAfee web site, and save it to a temporary folder accessible from the ePolicy Orchestrator server.
- 2 Select **Repository** in the left-pane console **Tree** view of the ePolicy Orchestrator console.
- 3 Select **Check in NAP** from the right-hand details pane.

Figure 5-4 Check in the VirusScan Enterprise 7.1 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 in [Step 1](#) on your hard drive, and click OK.

Wait a few moments while ePolicy Orchestrator loads the product NAP file. Once completed, it will appear in the policy list.

Use the deployment task to install products on clients

Once you have checked in the product package, you can use the client deployment task to have the ePolicy Orchestrator server install the product on client computers in your **Directory**. The deployment task is a unique client task created automatically when ePolicy Orchestrator installs. You can use this deployment task to install any product that is deployable through ePolicy Orchestrator.

For more information on other client tasks or on client tasks in general, see [Configure client on-demand scans and update tasks on page 174](#). You can use the deployment task to install those products for which you have already checked in a product deployment package file. See [Check in product deployment packages to the master repository on page 89](#).

How much of my Directory should I deploy to at once?

You can run the product deployment task at any site, group, or individual computer in your **Directory**. While it is possible to run the deployment task once at the **Directory** level, McAfee does not recommend doing this. This is especially true if your organization is large and you are deploying workstation products such as VirusScan Enterprise or Desktop Firewall. This could mean deploying to tens of thousands of clients all at once. In addition to potentially overwhelming the ePolicy Orchestrator server or your network, deploying to too many computers can make troubleshooting problems overly complicated.

Instead, for workstation deployments, plan a phased roll-out to install products to groups of computers 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 installs, and troubleshoot any problems with individual computers. See [Chapter 13, Getting Started with Reporting](#) for more information on reports.

Deploy server products to individual computers

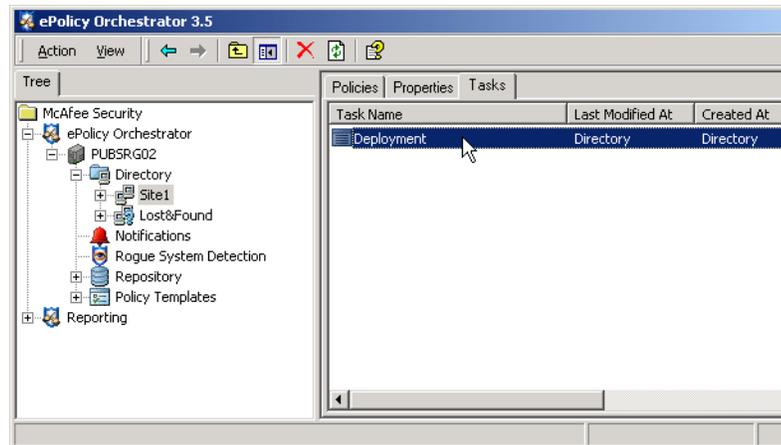
If you chose to deploy server-based McAfee products, such as GroupShield for e-mail servers or WebShield SMTP for gateway servers, you will probably want to deploy them to specific computers in your **Directory**, rather than groups or sites. Typically, there is only one or a few such servers in a site.

How to deploy products using the product deployment task

To deploy products using the product deployment task:

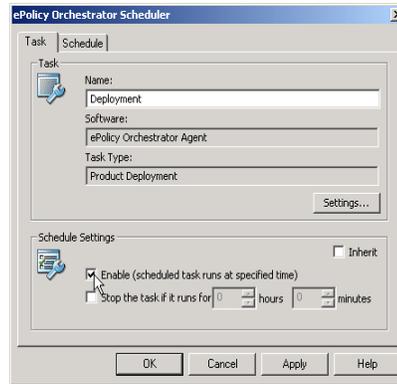
- 1 In the left-pane console tree of the ePolicy Orchestrator console, select the site, group, or individual computer in your **Directory** to which you want to deploy the product.
- 2 In the right-hand details pane, select the **Task** tab and then double-click the **Deployment** task in the task list.

Figure 5-5 Select the Deployment task for the selected node in the Directory



- 3 Once the ePolicy Orchestrator Scheduler opens, click the **Task** tab and deselect **Inherit** under **Schedule Settings**.

Figure 5-6 Enable the deployment task



4 Under **Schedule Settings**, select **Enable (scheduled task runs at specified time)**. The task will not run unless you enable it here.

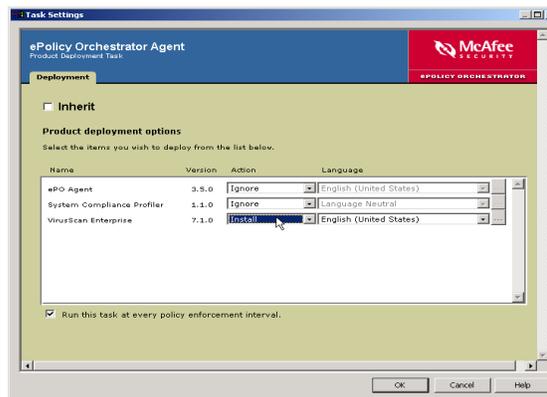
5 Click the **Settings** button.

6 On the **Deployment** page, 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 package file. See [Check in product deployment packages to the master repository on page 89](#).

7 Set the **Action** for the product you want to deploy to **Install**.

Figure 5-7 Set Action to Install for specific products you want to install when the deployment task runs



8 If you want to specify command line install options, click **...** and type 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.

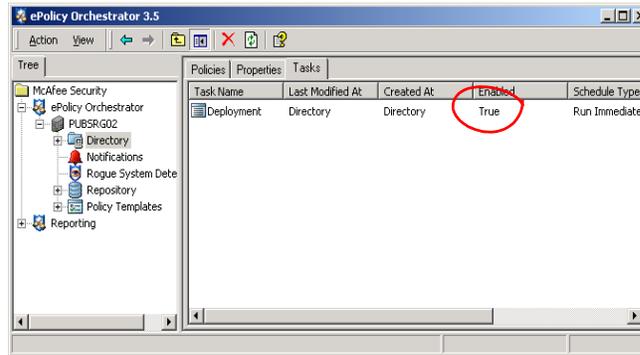
10 On the ePolicy Orchestrator Scheduler dialog box, click the **Schedule** tab.

11 Deselect **Inherit** to enable scheduling options.

- 12 To run the task once from the **Schedule Task** drop-down list, select **Run Immediately**.
Alternatively, you can schedule it to run at a later time.
- 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**.

Figure 5-8 The VirusScan deployment task is configured and enabled



Once configured, the deployment will occur 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 [Sending manual agent wakeup calls on page 150](#) for more information on agent wakeup calls.



SECTION 2

Creating an Update Infrastructure

Your anti-virus protection is only as good as your latest update. Use source, master, and distributed repositories to make sure that your client computers throughout your network can always update with the latest DATs, engines, software patches, and upgrades. Especially if your network is very large or complex, creating a reliable and efficient update repository infrastructure takes time and planning. However, once created, updating can nearly run on auto-pilot. Most importantly, a good updating infrastructure is essential for dealing effectively with virus outbreaks when they occur.

[Chapter 6, Keeping DATs and Engines Up-to-Date](#)

[Chapter 7, Update Large Networks with Distributed Repositories](#)

6

Keeping DATs and Engines Up-to-Date

Configure software repositories and tasks to deploy updates regularly

Getting agents and anti-virus products deployed to all the computers in your network is only the first step in protecting them from viruses and malicious code. Your anti-virus software is only as good as its latest virus definition signature files, or DATs, and its anti-virus engine. If your DAT files or engine are out of date, even the best anti-virus software won't be able to detect new viruses. It is therefore critical that you develop a robust updating strategy to keep your client anti-virus DAT and engine files in your network as up to date as possible.

ePolicy Orchestrator's software repository architecture makes this process easier, helping automate many aspects of distributing DAT and engine updates to client computers in your network. You can configure and run a variety of updating tasks that give you control over exactly how and when your clients are updated. You can also schedule these tasks to run at specific times or at regular intervals to fully automate regular weekly DAT updating.



Invest time in developing an update architecture now to save time later!

It will take time to come up with the best way to use ePolicy Orchestrator to update DATs and engines on clients in your network. McAfee recommends investing this time early to carefully plan a robust updating strategy. Having such a robust updating architecture in place maximizes your anti-virus effectiveness, and makes fighting a virus outbreak much easier.

What's in this chapter

This chapter focuses on configuring your master and source repositories for maintaining the latest DAT and engine versions, and then using client tasks to distribute those updates to your client computers. The next chapter discusses creating distributed repositories. You will likely want to use these, especially if your organization is large or is spread out geographically, to maximize network efficiency with updating. However, regardless of whether you use distributed repositories or not, you will need to first configure your master and source repositories. After configuring your master and source repositories, then create and configure distributed repositories, if you need them. See [Chapter 7, Update Large Networks with Distributed Repositories](#) for details on distributed repositories.

This chapter contains the following topics:

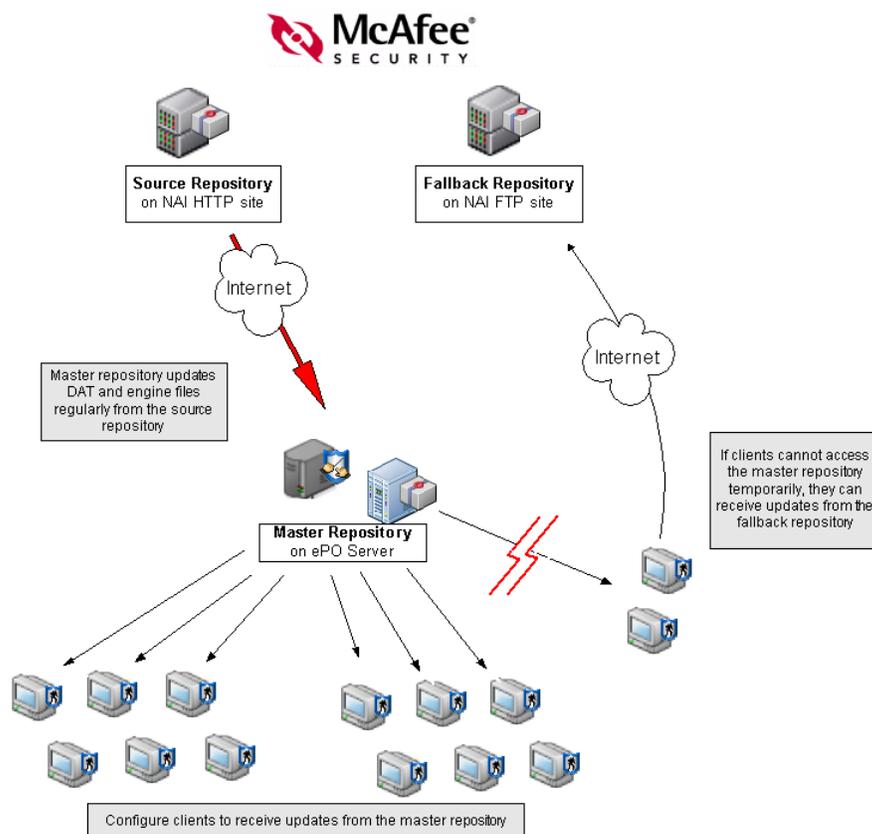
- [About master, source, and fallback repositories.](#)
- [Define a source repository to update DATs and engines.](#)
- [Use Pull tasks to update the master repository from a source repository.](#)
- [Manually check in engine, DAT and EXTRA.DAT updates.](#)

- *Distributing DAT and engine updates to clients.*
- *Evaluate new DATs and engines before deploying to your whole organization.*

About master, source, and fallback repositories

This section discusses the relationship between the master, source and fallback software repositories. You will likely want to use all three in creating a robust updating strategy with plenty of redundancy to guarantee your clients are getting DAT updates when they need them.

Figure 6-1 How the source, master, and fallback repositories work together



Master Repository

The master software repository is the central place where you maintain the latest versions of anti-virus and network security software that you deploy and manage with ePolicy Orchestrator. Client computers are configured to regularly collect updates, such as new DATs or patches and service packs for anti-virus software, from the master repository. You can only have one master repository for each ePolicy Orchestrator server.

Source Repository

Update your master repository regularly with the latest full DAT and engine files from a source repository. McAfee releases updated DATs weekly to address new viruses, and you will need to make sure your master repository always has the latest DATs and engine updates so you can use ePolicy Orchestrator to distribute them to your clients. The default ePolicy Orchestrator source repository is the McAfee FTP download site, but you can change the source repository or even configure multiple source repositories if you need to.

Source repositories are not required. You can download DAT and engine updates yourself and check them in to your master repository manually. However, using a source repository, especially the default NAIHttp or NAIftp source repositories, helps automate this.

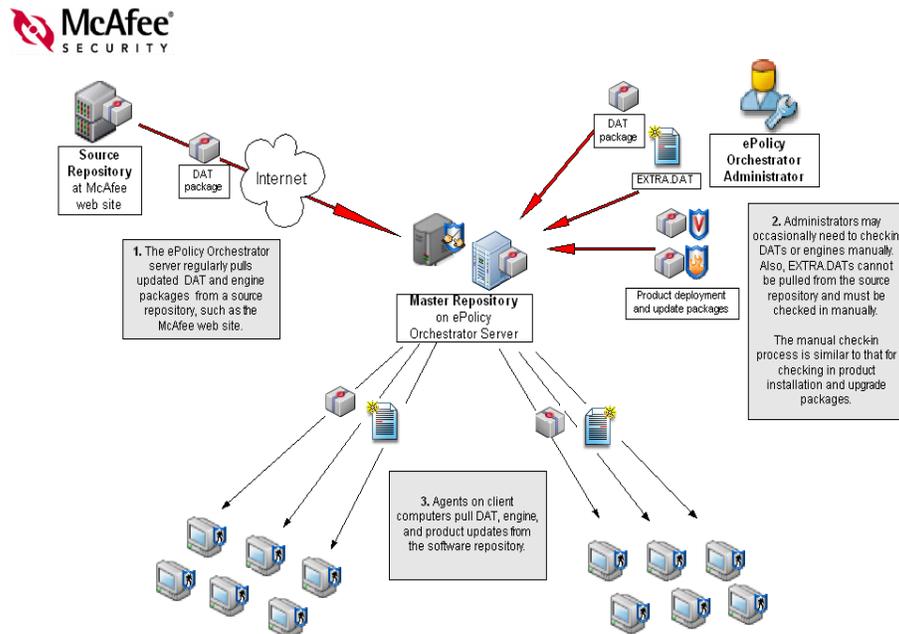
Fallback Repository

Occasionally, client computers may not be able to access master or distributed repositories for updates. Network outages, downed servers, virus outbreaks, and other things can cause this to happen. The fallback repository is where client computers can go in an emergency to get DAT and engine updates when they cannot get them from anywhere else. So, even when your master repository is unavailable, client computers can remain stay up-to-date. The default fallback repository is the McAfee FTP download site (NAIftp). You can only define one fallback repository.

How to keep the master repository DATs and engines up to date

The master repository contains several kinds of data which you add in several different ways.

Figure 6-2 Pull DAT and engine updates from the source repository, or manually check them into the master repository



- DAT and engine update files for your anti-virus software. These can be pulled from a source repository, such as the McAfee web site, or checked into the master repository manually.
- Product and product update packages that you will distribute to client computers using ePolicy Orchestrator. These can include product installation packages, such as for VirusScan Enterprise. They can also include patches, service packs, and other updates to these products.
- Policy (NAP) pages, which are used to manage client products such as VirusScan Enterprise, Desktop Firewall.

See [Manually check in engine, DAT and EXTRA.DAT updates on page 112](#) for more details about checking in and managing product packages.

About repository branches

You can maintain three versions, or branches, of DAT or engine 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 particular branches when running or scheduling update and deployment tasks to be able to distribute these different versions to different parts of your network.

Current branch

The current branch is the main repository branch for all packages. For product deployment packages, such as the product package for installing VirusScan Enterprise on your clients, can only be added to the Current branch.

Evaluation branch

You may want to test new DAT and engine updates with a small number of test clients or in one or two network segments, before deploying them to your entire organization. Specify the Evaluation branch when checking in new DATs and engines into the master repository, and then deploy them to a small number of test computers. After monitoring the test computers for several hours, you can add the new DATs to your Current branch and deploy them to your entire organization. See [Evaluate new DATs and engines before deploying to your whole organization on page 123](#) for complete details on how to use the Evaluation branch feature.

Previous branch

When you use the Previous branch, ePolicy Orchestrator saves last week's DAT and engine files into a previous folder before adding the new ones to the Current branch. This way, in the rare event that you experience a problem with the new DAT or engine files, you have a copy of a previous versions that you can re-deploy to your clients if necessary. ePolicy Orchestrator only saves the most immediate previous version of each file type, rather than save all previous versions.

You can enable the previous branch feature by selecting **Move existing packages to the 'previous' branch** when you add new DATs and engine files to your master repository. The option is available both when you pull updates from a source repository or when you manually check in packages to your master repository. See [Manually check in engine, DAT and EXTRA.DAT updates on page 112](#) for more information.

Define a source repository to update DATs and engines

The source repository is the location from which you update your master repository with new DAT and engine files. McAfee posts updated DAT files to its HTTP and FTP web sites regularly, at least once per week. The regular DATs are posted weekly on Wednesday evening GMT, but sometimes several times a week, especially if many new viruses are discovered. It is important to update your master repository with these new DATs as soon as they are available from McAfee.

Configuring ePolicy Orchestrator to pull these new DATs directly from the McAfee web site is the best way to ensure you're getting your updates as soon as possible. To do this, make the McAfee web site the Source Repository. By default, the ePolicy Orchestrator source repository is the McAfee HTTP download web site (**NAIHttp**) located at:

<http://update.nai.com/Products/CommonUpdater>

The McAfee web site contains DAT files and engine files only. It does not contain EXTRA.DATs, product deployment packages, service packs, or other kinds of updates.

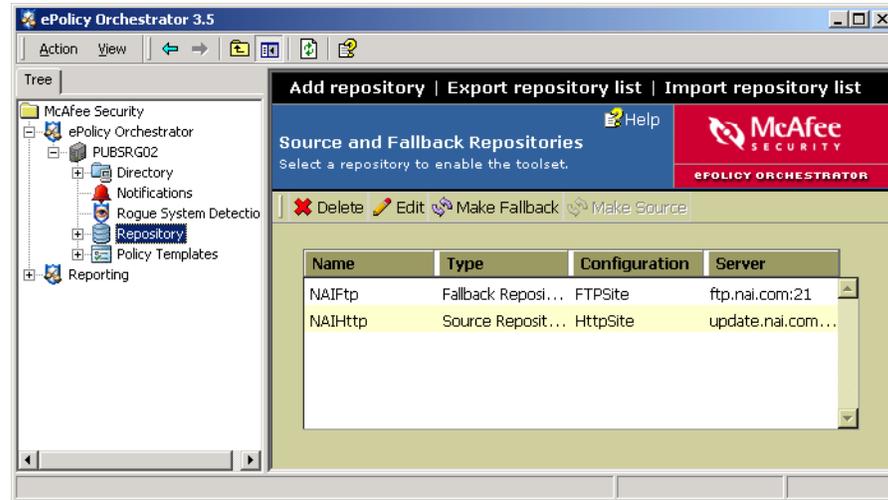
Define or change the default source and fallback repositories

You must be a global administrator to define, change, or delete source or fallback repositories. You can change settings or delete existing source repositories or the fallback repository.

To view or change your source and fallback repository configurations:

- 1 In the left-hand **Tree** of the ePolicy Orchestrator console, select **Repository**.
- 2 In the right-hand details pane, select **Source Repository** to access the **Source and Fallback Repositories** dialog box.

The **Source and Fallback Repositories** page lists the source and fallback repositories you have configured. By default, the McAfee FTP site is the fallback and the McAfee HTTP site is the source. McAfee recommends that you keep the default source and fallback repositories unless you have particular reasons for changing them.

Figure 6-3 Modify the existing default source and fallback repositories**Edit existing source or fallback repositories**

Modify URL address, port number, and download authentication credentials for existing source repositories or the fallback repository.

If you do need to edit source or fallback repository setting information, you can do this from the **Source and Fallback Repositories** page. To do this:

- 1 From the **Source and Fallback Repositories** page, select the repository you want to edit from the list.
- 2 Click **Edit** to open the **Edit Repository** dialog box.
- 3 Edit the configuration information as needed.
- 4 On the **Options** tab, click **Verify** to confirm that the ePolicy Orchestrator server can locate the source repository.
- 5 Click **OK** when done to save the changes.

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 default HTTP source repository to use the FTP site instead, and the default FTP fallback repository to use HTTP. Rather than recreate and reconfigure the repository, you can switch these two with one click. You must be a global administrator to define source or fallback repositories.

To make an existing source repository the fallback, select it from the list in the **Source and Fallback Repositories** dialog box and select **Make Fallback**. To make the existing fallback repository a source instead, select it in the list and select **Make Source**.

Removing source or fallback repositories

You can delete source or fallback repositories, for example if you want to create a new one or if you plan to check in DAT and engine updates manually. If you do delete a source or fallback repository, be sure to create a new one to replace it. Having correctly configured source and fallback repositories is essential to ensuring your master repository, and therefore your clients, always has the most up-to-date DAT and engine files. You must be a global administrator to remove source or fallback repositories.

To remove a source or fallback repository from the list:

From the **Source and Fallback Repositories** dialog box:

- 1 Click once on a repository listed in the table to select it.
- 2 Click **Delete**.

Add source repositories

You must be a global administrator to define source repositories. To add a source repository:

- 1 Log on to the desired ePolicy Orchestrator server using a global administrator user account.
- 2 In the console tree under **ePolicy Orchestrator | <SERVER>**, select **Repository**.
- 3 In the details pane under **AutoUpdate Tasks**, click **Add source repository**. The **Add repository** wizard appears.
- 4 Click **Next** to open the repository configuration dialog box.

Figure 6-4 Add repository wizard – repository configuration dialog box



- 5 In **Name**, type a descriptive name for this repository. Repository names must be unique.
- 6 In **Type**, select **Source Repository**.

- 7 Specify the type of server or path (FTP, HTTP, or UNC) where the repository resides, then click **Next**.
- 8 In the protocol configuration dialog box, provide the address and port information of the repository, then click **Next**.

Figure 6-5 Add repository wizard — FTP protocol configuration dialog box

- If you selected **FTP** in [Step 7](#), type the web address in **URL** and the FTP port number in **Port**.
 - If you selected **HTTP** in [Step 7](#), type the web address in **URL** and the HTTP port number in **Port**.
 - If you selected **UNC** in [Step 7](#), 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 296](#).
- 9 Provide the download credentials used by client computers 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.
 - a If you selected **FTP** in [Step 7](#), select **Use anonymous login** or type the user account information in **User name**, **Password**, and **Re-Enter Password**.

If you selected **HTTP** in [Step 7](#) 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 7](#), select **Use Logged On Account** or type the user account information in **Domain**, **User name**, **Password**, and **Confirm password**.
 - b To authenticate the user account you specified, click **Verify**.
 - 10 Click **Finish** to add the repository to the repository list.
 - 11 Click **Close** after the repository has been added.

Use Pull tasks to update the master repository from a source repository

You can use source repositories to make updating DAT and engine files easier. Engine files and especially DATs will need to be updated often, much more often than any other kind of update, such as a product patch, service pack, or new version. McAfee updates DAT files every week, and you will want to deploy these to the clients on your network as soon as possible to protect them against the latest viruses.

What you need to do is:

- 1 [Configure proxy server settings.](#)
- 2 [Schedule a regular Repository Pull server task.](#)
- 3 [Run a Pull Now task to update the master repository immediately.](#)

Configure proxy server settings

If you are using the McAfee HTTP or FTP web site as your source repository, the ePolicy Orchestrator server must be able to access the Internet to pull DAT and engine updates to the master repository. If your organization uses proxy servers for connecting to the Internet, you must make sure ePolicy Orchestrator uses the proxy servers. The master repository uses these settings to retrieve packages from source repositories through a proxy server.

You can use the proxy server settings in Internet Explorer or specify custom proxy server settings in the ePolicy Orchestrator console. McAfee recommends using the Internet Explorer proxy settings.

You must also configure your client computers to use proxy servers to be able to access the fallback site.

Using Internet Explorer proxy server settings

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.

To do this:

- 1 [Configure Internet Explorer proxy settings.](#)
- 2 [Configure ePolicy Orchestrator to use Internet Explorer proxy settings.](#)

Configure Internet Explorer proxy settings

To confirm that Internet Explorer's proxy settings are configured correctly, open an instance of Internet Explorer from your ePolicy Orchestrator server and browse to some publicly accessible web site, such as your organization's home page or to www.google.com. If you can access these sites, your proxy settings are correct.

If you have not yet done so, configure your Internet Explorer LAN connection and proxy configuration:

- 1 Open an Internet Explorer browser window.
- 2 Select **Tools | Internet Options**.
- 3 Click the **Connections** tab and 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** to open the **Proxy Settings** dialog box.
- 6 Type proxy information into the appropriate fields, especially for HTTP and FTP if you plan to use the default source and fallback repository sites.
- 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 will allow you to correctly view certain HTML-based sections of the ePolicy Orchestrator console interface.
- 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 confirm that this is the case, or if you're not sure, do the following:

- 1 In the left-hand **Tree** of the ePolicy Orchestrator console, select **Repository**.
- 2 In the right-hand details pane, select **Configure proxy settings**.
- 3 In the **Edit proxy** dialog box, make sure the **Use Internet Explorer proxy settings** option is selected.
- 4 Click **OK**.

Manually configure proxy settings in ePolicy Orchestrator

You can 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 don't use a proxy server.

To manually configure ePolicy Orchestrator proxy settings:

- 1 In the left-hand **Tree** of the ePolicy Orchestrator console, select **Repository**.
- 2 In the right-hand details pane, select **Configure proxy settings**.
- 3 In the **Edit Proxy** dialog box, 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**.
- 4 Click the **Servers** tab. The **Servers** tab doesn't appear until you select **Manually configure the proxy settings**.
- 5 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.

- 6 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 computers separated by a semi-colon (;).
- 7 Click the **Authentication** tab.
- 8 Configure the proxy authentication settings as appropriate, depending on whether you will pull updates from an HTTP or FTP repositories, or both.
- 9 Click **OK** to save your proxy settings.

Schedule a regular Repository Pull server task

It is a good idea to create a scheduled pull task so that your master repository is updated automatically and regularly. The scheduled pull task will execute automatically at whatever interval you specify. For example, you can schedule a weekly repository pull task that will pull new DAT and engine updates to your master repository, for example at 5:00 am every Thursday.

Once you have updated your master repository, you can push these updates out to the agents installed on client computers in your network to make sure they all have the latest anti-virus protection. McAfee updates its regular DAT files each week, so you should create a scheduled repository pull task to pull updates at least that often.

Things to consider when scheduling a pull task

Consider bandwidth and network usage. If you have enabled global updating and have deployed SuperAgents as McAfee recommends, the pull task will automatically trigger a repository replication task to all distributed repositories followed by a client update tasks. You may want to schedule all these to occur at night when network usage is lower.

McAfee releases its regular DATs each Wednesday evening GMT. If you schedule a weekly pull task, schedule it to run at some time shortly after this. If you schedule a daily task, set the time late enough so that the pull task will get the new DATs.

If you are not using the global updating feature, schedule additional tasks to make sure the updates are replicated to any distributed repositories you have set up, if any, and also any client update tasks.

Creating and scheduling the pull task

You must be a global administrator to schedule pull tasks. To schedule a repository pull task:

- 1 In the ePolicy Orchestrator console tree, select **Repository**.
- 2 In the **Repository** page, select **Schedule pull tasks** to open the **Configure Server Tasks** page.
- 3 Select **Create task** to open the **Configure New Task** wizard.

Figure 6-6 Create a scheduled pull task to pull updates from the McAfee web site

- 4 Under **Task Settings**, type a descriptive name into the **Name** field, such as *Weekly Repository Pull task*.
- 5 Select **Repository Pull** from the **Task type** drop-down menu.
- 6 Make sure **Enable task** is set to **Yes**. The task will not run unless you enable it.
- 7 Select the frequency from the **Schedule Type** drop-down list. McAfee recommends you run the task daily, but no less frequently than weekly.
- 8 Expand the **Advanced schedule options** and schedule the exact day and time for the task to run.
- 9 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 NAIHttp default source repository and also the NAIftp 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** to pull the DATs into your master repository's Evaluation branch. See [Evaluate new DATs and engines before deploying to your whole organization on page 123](#). If you do not use the evaluation branch, select **Current**. You probably will not ever pull new DATs into the **Previous** branch. See [About repository branches on page 102](#) for information about branches.
- 12 If you have older versions of McAfee products, such as VirusScan 4.5.1 for Windows 9X computers, 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. To replace packages in the current branch with the packages you are checking in, deselect **Move existing packages to the 'previous' branch**.

14 Click **Finish**. Wait a moment while the task is created.

The new pull task will be added to the task list on the **Scheduled Tasks** tab. It shows the date and time the next time it will run and that it is enabled.

Run a Pull Now task to update the master repository immediately

Scheduling a regular daily pull task is the best way to make sure your master repository always has the latest DATs and engine updates. Occasionally, however, you may need to update your master repository manually. For example, the McAfee AVERT team may release full DATs early if particularly fast-spreading viruses have appeared in the wild. If this happens, you probably won't want to wait until your next scheduled pull. Instead, you may want to initiate a manual source repository pull to add the new DAT or engine files to your master repository immediately.

While it is often easier to use a Pull Now task to update DAT and engines, you can also download and check in these updates to the master repository manually. You may occasionally need to do this if a pull task fails for whatever reason. Also, you cannot use a pull task to add EXTRA.DAT files to your master repository. You must check these in manually. See [Manually check in engine, DAT and EXTRA.DAT updates on page 112](#) for more information on how to do this manually.

To initiate a manual repository pull:

- 1** From the ePolicy Orchestrator console, select **Repository** in the left-hand tree.
- 2** In the details pane under **AutoUpdate Tasks**, click **Pull now** to launch the **Pull Now Wizard**.
- 3** In the first screen of the **Pull Now Wizard**, click **Next**.
- 4** Select the source repository from the list of available repositories and click **Next**. If you have not changed the source repository, the default is the McAfee HTTP site.
- 5** Select the repository branch.

If you use the Evaluation branch feature for testing DATs and engines before deploying to your entire organization, select **Evaluation** to pull the DATs into your master repository's Evaluation branch. See [Evaluate new DATs and engines before deploying to your whole organization on page 123](#). If you do not use the evaluation branch, select **Current**. You probably will never pull new DAT or engine updates into the **Previous** branch.

See [About repository branches on page 102](#) for information about branches.

- 6** If you have older versions of McAfee products, such as VirusScan 4.5.1 for Windows 9X computers, 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. It is a good idea to do this, in case you encounter problems with new DATs and need to roll back to a previous version. This is very rare, but it can happen.
- 8** Click **Finish** to begin the pull. Wait a few moments while the pull task executes.
- 9** Click **Close**.

You can confirm that the DATs have been updated by viewing the contents of the master repository and confirming that the DAT version number is the most current. The most recent DATs and engines are listed on the McAfee web site at <http://www.nai.com>.

Manually check in engine, DAT and EXTRA.DAT updates

In addition to updating the weekly DAT files, McAfee posts occasional EXTRA.DAT files to address specific viruses that have appeared in the wild since the last weekly DAT update. The EXTRA.DAT virus signature will be included in the next regular weekly DAT release. However, some viruses can spread very quickly. For these viruses, that McAfee AVERT ranks as a high or medium risk, you should manually download and distribute the EXTRA.DAT update before waiting for the next regular DAT update.

If you are pulling weekly DAT and engine updates from a source repository as McAfee recommends, be aware that pull tasks do not get EXTRA.DAT updates. You can only distribute EXTRA.DAT updates with ePolicy Orchestrator if you check in the EXTRA.DAT manually and then deploy it to your clients.

You must be a global administrator to check in packages.

This section includes the following information:

- [About DAT and engine package types.](#)
- [Checking in PKGCATALOG.Z DAT packages or EXTRA.DAT files.](#)

About DAT and engine package types

You can check these DAT or engine package types into the master repository

Figure 6-7 DAT and engine packages you can check into the master repository

Package type	Description
Virus definition (DAT) files.	The regular, weekly DATs released each week by McAfee.
Virus scanning engine.	The updated scanning engine for McAfee anti-virus products, such as VirusScan Enterprise. Engines are usually updated ever 3-4 months.
SuperDAT (SDAT*.EXE) files.	Contains both DATs and engine together in one update package. Note: Since SuperDAT packages can be large, and since you won't update the engine as often as you update DATs, McAfee recommends updating DATs and engines separately to save bandwidth.
Supplemental virus definition (EXTRA.DAT) files.	Supplemental DATs that address one or a few specific viruses that have appeared in the wild since the last weekly DATs were posted. Depending on the severity of the virus, you may want to deploy an EXTRA.DAT immediately, rather than wait until that signature is added to the regular weekly DATs. Note: EXTRA.DATs are not available as PKGCATALOG.Z package files, although you can still deploy them through ePolicy Orchestrator.

Where can I get the DAT or engine PKGCATALOG.Z file?

The weekly DATs and engine are available on the McAfee web site in a package format that is deployable through ePolicy Orchestrator.

To download these packages:

- 1 From your ePolicy Orchestrator server, go to the McAfee update site at <http://www.nai.com>.
- 2 Select **Download Anti-Virus Updates**.
- 3 In the **Download Anti-virus Updates (DATs)** table, select the **DAT Package for use with ePO 3.0**. Don't select the regular weekly DATs by accident—you cannot distribute those with ePolicy Orchestrator.
- 4 Download and save the DAT PKGCATALOG.Z package file to a temporary folder on your ePolicy Orchestrator server.
- 5 If you want to download the engine package, select the **Engine Package for ePO 3.5** from the **Engine Updates** table.

Where do I get EXTRA.DAT files?

EXTRA.DAT supplemental DATs are not available in a PkgCatalog format, but you can still check them into the repository and distribute them through ePolicy Orchestrator. EXTRA.DATs are also available on the McAfee update site.

Things to think about with product deployment packages

To save bandwidth, McAfee recommends that you check in DAT and engine packages separately instead of checking in a SuperDAT package that combines these updates.

EXTRA.DAT files are not collected as part of a scheduled repository pull task. If you are using a source repository from which to pull DAT and engine updates, you must get and check in EXTRA.DAT files separately.

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. 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 updates from unsigned or untrusted sources.

Legacy product support

Existing (or legacy) 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** client task to install product updates.

If the update location you specify in the **AutoUpdate** or **AutoUpgrade** task settings is a distributed software repository being managed by ePolicy Orchestrator, you need to enable legacy product support when you check the corresponding package into the master repository. Doing so, copies the packages into both directory structures. This flexibility enables you to continue to support legacy products; for example, NetShield 4.5; using **AutoUpdate** and **AutoUpgrade** tasks. For instructions, see [Check in product deployment packages to the master repository on page 89](#).

Package versioning and branches

You can add DAT and engine packages to one of three branches in the master repository: evaluation, current, or previous. For more information about using branches with DAT and engines, see [About repository branches on page 102](#) and especially [Evaluate new DATs and engines before deploying to your whole organization on page 123](#).

Checking in PKGCATALOG.Z DAT packages or EXTRA.DAT files

Once you have the DAT package, engine package or EXTRA.DAT files, you can use the ePolicy Orchestrator console to manually check them into the master repository. You cannot check packages into your master repository while pull or replication tasks are executing.

To check in a DAT or engine package file or EXTRA.DAT to the master repository:

- 1 Locate the EXTRA.DAT you want to check in and save it to a temporary folder on your ePolicy Orchestrator server.
- 2 From the ePolicy Orchestrator **Directory**, select **Repository**.
- 3 In the right-hand details pane under **AutoUpdate Tasks**, click **Check in package** to launch the **Check-in package** wizard.
- 4 Click **Next** to open the package type dialog box.
- 5 Select **Extra.dat** for the package type and click **Next**.
- 6 Type the full path or browse to and locate the EXTRA.DAT file from step 1 that you saved in a temporary folder.
- 7 Click **Next** to view the package check-in summary information.
- 8 After you've admired your check-in summary information long enough, click **Next** to configure the repository branch options.
- 9 Most likely, you will select **Current** to check in EXTRA.DAT files to the current branch so you can distribute them to all your clients as soon as possible.

However, if you are evaluating all DATs, including EXTRA.DATs, before deploying to your entire organization, select **Evaluation**. See [Evaluate new DATs and engines before deploying to your whole organization on page 123](#) for more information on using the evaluation branch to test DATs. You will never check in EXTRA.DAT files into the previous branch.

- 10 If you have older versions of McAfee products, such as VirusScan 4.5.1 for Windows 9X computers, 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 EXTRA.DAT check-in. Wait a few moments while the update completes.
- 13 Click **Close** after the package has been checked in.

Distributing DAT and engine updates to clients

Once you have configured your master repository and created a strategy for keeping it up-to-date with the most current DAT and engine files, you will need to plan how to distribute those DAT and engine updates to your client computers. ePolicy Orchestrator offers you two mechanisms for doing this.

A summary of each DAT update method follows below. Full details on how to implement each of these follow. While each method is designed to work independently, you can also use them together to add redundancy to your DAT and engine update strategy. Some computers may be shut down or logged off and not receive an update, so having a backup is a good idea. For example, even if you use global updating to distribute updates immediately, you can still create a scheduled client update task to update at regular times.

Global updating

Global updating is a feature in ePolicy Orchestrator 3.0 that can automatically update all your client computers 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 to have managed products, such as VirusScan Enterprise 7.1, perform an immediate update task.

Scheduled client agent update task

Where as global updating updates clients immediately when new DAT or engines are checked into the master repository, a scheduled client update task runs at a set frequency, such as daily or weekly. When it runs, it updates clients with the DAT and engine versions that have been most recently checked into the master repository.

The following sections cover how to distribute DAT updates to clients:

- [Use global updating to automatically distribute updates to all clients immediately on page 115](#)
- [Create and schedule a daily DAT and engine client update task on page 118](#)
- [Confirm that clients have updated to the latest DATs on page 122](#)

Use global updating to automatically distribute updates to all clients immediately

Global updating is a feature in ePolicy Orchestrator that automates distributing DATs and/or engines to all your clients. When global updating is enabled, every time you make changes to your master repository, ePolicy Orchestrator automatically replicates the contents to distributed repositories, if you have them. Then it alerts all agents deployed in your network to have managed products, such as VirusScan Enterprise 7.1, perform an immediate update task. From checking in the changes to your master repository to your last client computer receiving its update should take no longer than one hour.

Configuring global updating is a two-step process. Once configured, it occurs automatically. To enable global updating:

- 1 [Deploy SuperAgents for global updating broadcast wakeup call.](#)

2 [Enable global updating on ePolicy Orchestrator server.](#)

About global updating

When you use global updating, replication to distributed repositories and client updating are all automated. These happen without you having to create and schedule replication tasks for updating distributed repositories, if you have them, or creating Agent update tasks. Checking in a DAT or engine file into your master repository is enough to trigger a global update; all the rest happens automatically.

Use global updating for aggressive DAT and engine updating

Global updating is a great way to make sure clients are updating immediately when new DATs or engines are available in master repository. However, replicating to distributed repositories and updating clients that often can also generate significant network traffic. You must decide if the need for speedy updating is important enough to tolerate the extra load on your network.

Global updating uses the SuperAgent wakeup call

To enable and use global updating, you must have at least one SuperAgent deployed in each subnet. The global updating feature uses the SuperAgent broadcast wakeup call to wakeup other agents located in the same subnet. These other agents won't know that an update is available if there is no SuperAgent in the subnet to alert them. See [Deploying SuperAgents to distribute agent wakeup calls on page 75](#).

Selective global updating new in ePolicy Orchestrator 3.5

Use selective global updating to configure exactly what kind of updates should trigger the global update.

The global updating feature can be very useful in a virus outbreak situation. Assume that McAfee's AVERT team has posted updated DATs in response to a newly-discovered virus in the wild. 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 DATs for all computers running active, communicating agents on your network within one hour.

Deploy SuperAgents for global updating broadcast wakeup call

SuperAgents are required for global updating to work. Global updating uses SuperAgents to send a broadcast wakeup call to alert all clients that a new update is available. Therefore, before configuring global updating, first deploy at least one SuperAgent to each subnet in your network. [Deploying SuperAgents to distribute agent wakeup calls on page 75](#).

In addition to the broadcast wakeup call feature for waking up agents, SuperAgents can also serve as distributed software repositories. While global updating works with SuperAgent repositories if you decide to use them, it does not require them. Global updating will replicate to any distributed repositories you have created and configured. See [Creating SuperAgent distributed repositories on page 132](#) for more information on SuperAgent distributed repositories.

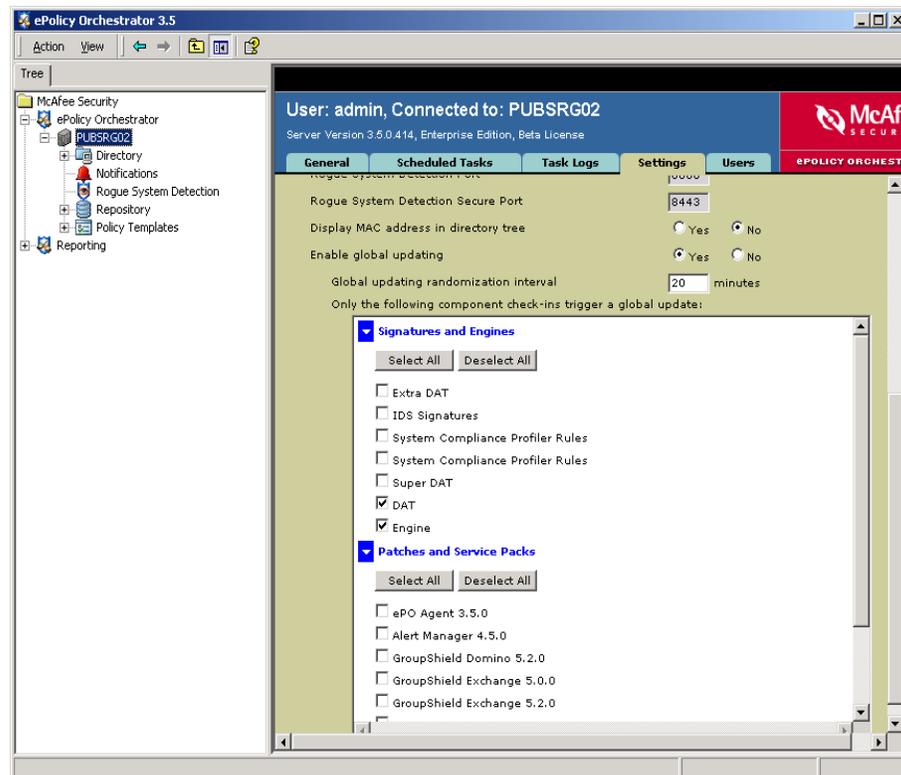
Enable global updating on ePolicy Orchestrator server

Once you have deployed SuperAgents throughout your network, you can enable global updating on your ePolicy Orchestrator server. Global updating is a feature that you can turn on or off from the ePolicy Orchestrator console. When turned on, changes to your master repository trigger automatic replication to distributed repositories, if any, followed by a SuperAgent wakeup call to your entire **Directory**. The SuperAgents will in turn wake up agents in their local subnets so that those agents can call into the server for updates.

To enable global updating on the ePolicy Orchestrator server:

- 1 In the ePolicy Orchestrator console Tree, select your ePolicy Server server (ePOServer in [Figure 6-8](#)).
- 2 In the upper right-hand details pane, select the **Settings** tab.
- 3 At the bottom of the Server Settings page, set **Enable global updating** to **Yes**.

Figure 6-8 Enable global updating on the ePolicy Orchestrator server.



- 4 Change the randomization interval, if desired.
- 5 Under **Select components for update**, select which components you want to allow to trigger an update.

Global updating only triggers if new packages for the components specified here are checked into the master repository. Select these components carefully, as this can have a big effect on how often global updating occurs, and therefore how much network traffic ePolicy Orchestrator generates. Typically, you should enable global updating only for critical updates such as DATs and engines.

- 6 Click **Apply Settings** at the top of the **Server Settings** page to save the changes.

Once enabled, global updating will trigger the next time you check in updates for the components you specified.

Create and schedule a daily DAT and engine client update task

You can create and configure client update tasks from the ePolicy Orchestrator console to help manage how and how often client computers update DATs and engines from your master repository. If you are not using global updating, then creating these client update tasks are the only way you can control client updating from the ePolicy Orchestrator server.

Even if you are using the global updating feature described in the previous section, it is not a bad idea to create a daily client update task too. Having some redundancy in updating using different methods is a good way to ensure that your clients receive DAT and engine updates frequently and regularly.

About creating and configuring client update tasks

Below are some things to consider when scheduling a daily DAT and engine client update task:

- While you can configure client tasks at any level in your **Directory**, McAfee recommends creating a DAT and engine update task at the **Directory** root that inherits to all sites and groups. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact of having all clients update at the same time. Also, for large networks with offices in different time zones, running the task at the **Local** system time on the client, rather than at the same time for all clients, helps balance network load.
- If you use distributed repositories and have scheduled replication tasks to update them, schedule regular client update tasks to begin at least an hour or two *after* the scheduled replication task completes. Updating from a distributed repository won't do any good unless you schedule the update for after the repository has been updated. See [Replicating the master repository contents to distributed repositories on page 139](#).
- How often you update is up to you. However, McAfee recommends running DAT client update tasks *at least* once a day. Even though McAfee usually releases regular DATs once a week, they may be released early if there's an outbreak. Also, you may manually check in EXTRA.DAT or even full DAT updates during the week, especially if there is a new virus outbreak. Also, client computers may be offline and miss the scheduled task; running the task frequently ensures these computers get the update soon.
- To maximize bandwidth efficiency, 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 DATs and have it run several times a day. In addition, create a second task to update both DATs and engines, and schedule it to run once a week or even once a month. Engines are released only once very few months; updating them more often than that is just wasting network bandwidth.

- Create and schedule additional update tasks for products that do not use the Common Management Agent (CMA) for Windows used in products like VirusScan Enterprise, Desktop Firewall, and GroupShield. These other products can be older products like VirusScan 4.5.1 that use a different update mechanism, or non-Windows products like NetShield for Novell NetWare that do not use the Windows Agent for updating.
- You may want to create two update tasks for your main workstation applications, such as VirusScan Enterprise, to make sure they all get updated. Schedule one to run daily or several times a day (see below). Schedule a second one to **Run Immediately**. This second task runs once for each computer in your **Directory** the first time the agent calls into the server. This can be useful if clients are offline at the scheduled update time; the second update task ensures they update immediately when they come on line, rather than wait for the next time the scheduled task runs. Existing agents will run the scheduled agent update task every day. Any new systems that come on line will run the immediate task as soon as they install and call into ePolicy Orchestrator for the first time.

To create a scheduled ePolicy Orchestrator agent update task

You can follow the procedure in this section to create and configure ePolicy Orchestrator agent update tasks. The procedure specifically describes configuring a daily update task to update DATs only. You can follow this same procedure and adjust configuration to suit your own needs, for example modifying how frequently an update runs or what components are updated.

To create a scheduled client update task to update DAT files:

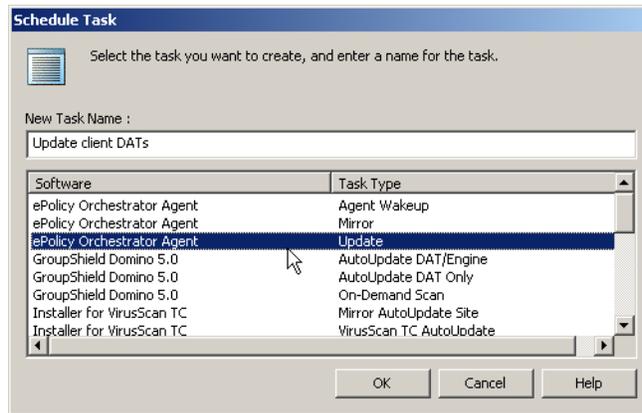
- 1 In the left-pane console tree, right-click the **Directory** and select **Schedule task**.

Figure 6-9 Create a new scheduled client update task at the Directory level to update all clients in your Directory



- 2 In the **Schedule Task** dialog box, type a name into the **New Task Name** field, such as *Daily client DAT update task*.

Figure 6-10 Create an ePolicy Orchestrator Agent update task to update DATs and engine files

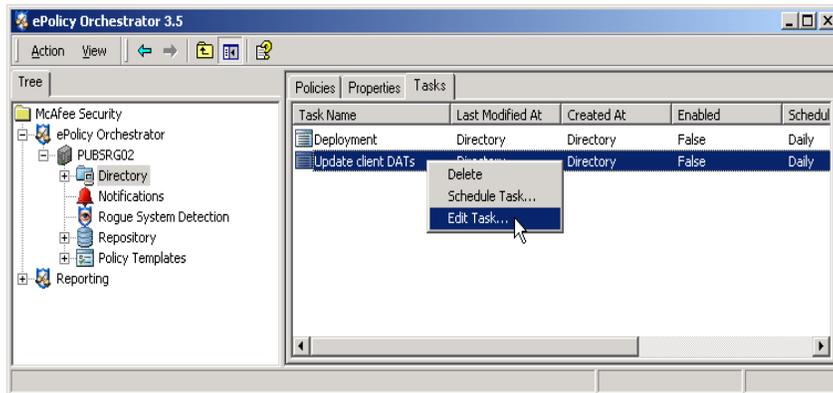


- 3 In the software list, select **ePolicy Orchestrator Agent Update** to create an update task for products like VirusScan Enterprise and Desktop Firewall that use the Common Management Agent (CMA).
- 4 Click **OK**.
- 5 Press **F5** to refresh the console and make the new task appear in the list in 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.

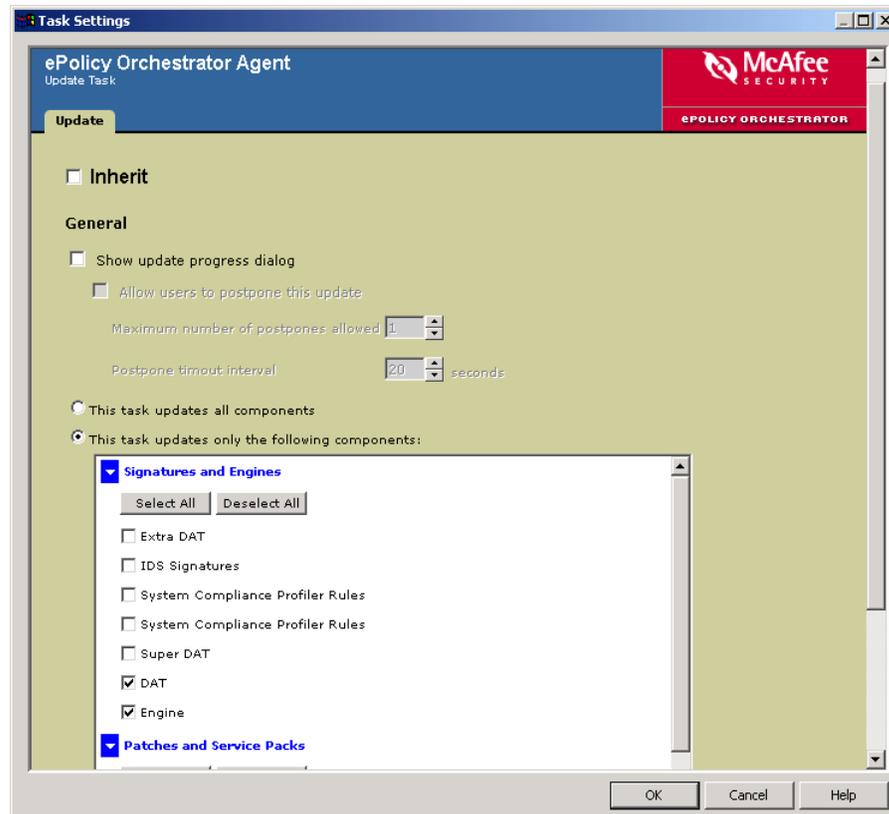
- 6 Right-click the new task in the task list and select **Edit Task**.

Figure 6-11 Edit the newly-created update task to run immediately



- 7 Deselect **Inherit** under the **Schedule Settings** section of the ePolicy Orchestrator Scheduler dialog box.
- 8 Select **Enable (specified task runs at specified time)**. The task does not run unless you first enable it here.
- 9 Click **Settings** to configure task settings.

Figure 6-12 Configure client update task settings



- 10 On the **Task Settings** dialog box for the agent update task, deselect **Inherit** to enable configuration options.
- 11 Leave the **Show update progress dialog** option unselected to hide updating on the client computer. McAfee recommends not allowing end-users on client computers to see and potentially interrupt updating in this way.
- 12 Under **Select components for update**, select specific components that should be updated for the task.
- 13 Click the **Schedule** tab and deselect **Inherit**.
- 14 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.

There are many configurable scheduling options when scheduling the client update task.

- 15 Click **OK** to close the **Task Settings** dialog box.
- 16 Click **OK** to close the **ePolicy Orchestrator Scheduler**.

Agents will get the new update task the next time they communicate with the ePolicy Orchestrator server. The client update task will run at the next occurrence of the scheduled date and time. Each client will update from the appropriate repository depending on how the update policies for that client's agent are configured. See [Using the agent policy pages to set policies on page 153](#).

Confirm that clients have updated to the latest DATs

You can use the ePolicy Orchestrator console to confirm that the DAT and engine versions in your master repository or installed on clients are the latest and most up-to-date.

Identify the latest DAT and engine versions available from McAfee

Go to the McAfee web site DAT and engine download page and read the DAT or engine version listed in the table.

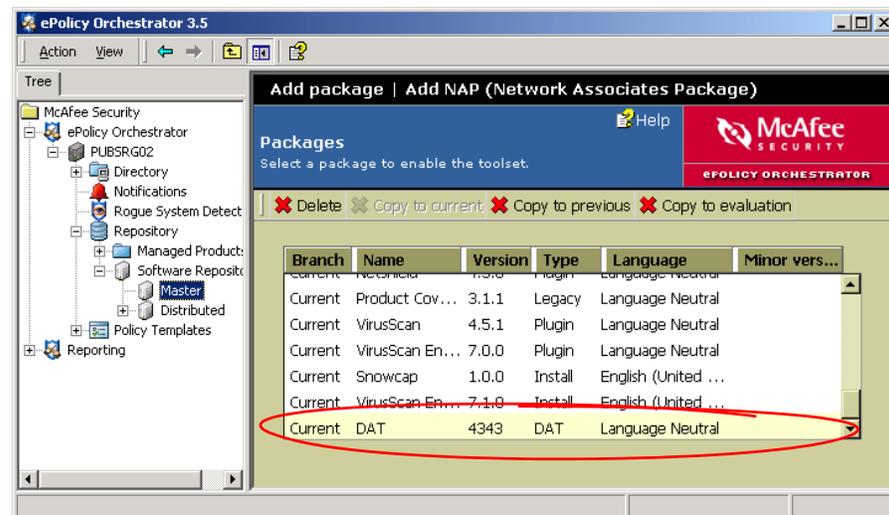
Alternatively, you can also just perform a manual Pull Now task to pull the latest DAT and engine updates from your source repository, and then read that version number right from your master repository. See [Run a Pull Now task to update the master repository immediately on page 111](#) for details on running a Pull Now task. If it turns out you already had the latest DAT files in your master repository, the Pull task stops automatically and informs you that your master repository is already up to date.

Confirm latest DAT and engine versions in master repository

First, check the DAT version that is currently checked into your master repository. These are the DATs that should now be on your client computers after they updated. To do this:

- 1 From the ePolicy Orchestrator console **Tree**, select **Repository | Software Repositories | Master**. The right-hand details pane displays the list of packages currently checked in to the master repository.
- 2 Scroll to the bottom of the **Packages** list and locate the **Current DAT** version, which will be some number like 4306.

Figure 6-13 Confirm DAT or engine package versions in the master repository



Confirm DAT and engine versions on client product properties

Next, check the DAT versions used by client software, such as VirusScan Enterprise, from the ePolicy Orchestrator console. Note that the console will 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 ePolicy Orchestrator console, select any computer in your **Directory** that has recently been updated.

- 2 In the right-pane window, select the **Properties** tab.
- 3 In the **Properties** page, 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.

Evaluate new DATs and engines before deploying to your whole organization

You may want to test weekly DAT and engine updates on a few client computers before deploying them to your entire organization. Once you have evaluated them for several hours or a day and they function without problem you can deploy them to your entire network.

You can do this without ePolicy Orchestrator if you want. For example, you could download the weekly DATs from the McAfee web site yourself and manually install them on several test computers running anti-virus software, such as VirusScan Enterprise. Once you are satisfied they function without problem, you can run a Pull Now task or manually check in DATs to add the DATs to your master repository. Then use ePolicy Orchestrator to push them out to all your managed clients. This is relatively easy to do, but it also involves many manual steps.

Use the Evaluation branch to help automate new DAT testing

Another way to do this is let ePolicy Orchestrator help automate the evaluation process for you. You can schedule synchronized pull and update tasks that use only the **Evaluation** branch of the master repository. Then you can designate a small site or group in your **Directory** as a test environment and configure clients in that group to only update from the **Evaluation** branch. When you are satisfied the new DATs work in your test group, simply move the DATs to your **Current** repository branch. The next time clients in the rest of your **Directory** perform a client update task, they will update with the new DATs.

Follow these steps to automate DAT testing using the Evaluation branch in ePolicy Orchestrator. Most of these steps you will only need to do once when you configure your evaluation updating strategy. The only step you must manually perform during each update is [Step 5](#).

To use the Evaluation branch to test DATs:

- 1 *Create a scheduled pull task to use the evaluation branch.*
- 2 *Designate a group in your Directory 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 client computers during the DAT evaluation period each week.*
- 5 *Move the new DATs from the evaluation branch to the current branch.*
- 6 *Let replication and update tasks update with the new DATs.*

Create a scheduled pull task to use the evaluation branch

Create a schedule pull task that pulls updates into the **Evaluation** branch of your master repository. Schedule it to run after McAfee releases updated weekly DATs, usually no later than 2:00 am GMT on Thursday each week. See [Schedule a regular Repository Pull server task on page 109](#) for details on specifying the evaluation branch when scheduling pull tasks.

If you use distributed repositories, be sure to also schedule a repository replication task that runs shortly after your scheduled pull task completes and *before* your scheduled client update task runs.

Designate a group in your Directory to update from the evaluation branch

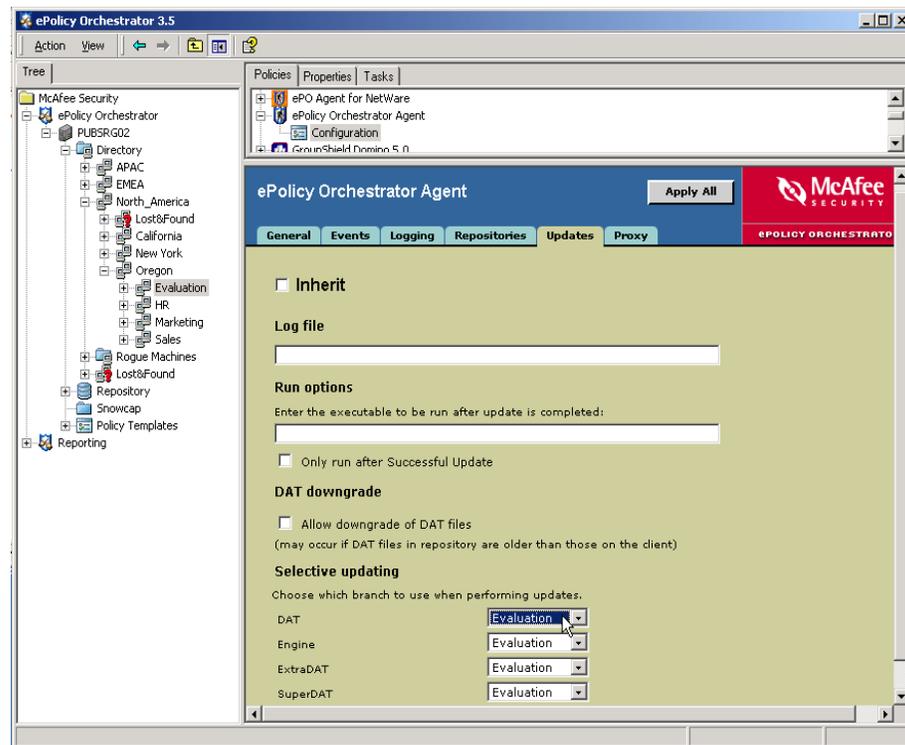
Select a group (or site) in your ePolicy Orchestrator **Directory** to serve as an evaluation group, and configure the updating agent policies for that group to use only the evaluation branch. This group will update with the latest DATs each week from the **Evaluation** branch of the repository. Leave the updating policies for the rest of your **Directory** to pull from the default **Current** branch.

You can of course configure any node in your **Directory** to use the Evaluation branch for updating; either a site, group, individual computer, or even the entire **Directory**. You must decide which computers or group of computers you want to use to evaluate DATs, and set the agent policies appropriately for only those computers. Organizing the test computers into a **Directory** group makes this easier.

To configure a group in your **Directory** to receive updates from the Evaluation branch:

- 1** In the **Directory**, select the group you have designated as the evaluation group.
- 2** On the **Updating** tab of the agent policies for the evaluation group, deselect **Inheritance** to enable policy options.
- 3** Under **Repository Branch Update Selection**, select **Evaluation** from each drop-down list to update all DATs and engine updates only from the Evaluation branch.

Figure 6-14 Configure agent policies for your group of test computers to update only from the Evaluation branch



4 Click **Apply All** to save the change.

The policies will take affect the next time the agent calls into the server. The next time the agents update, as per the configuration of a scheduled agent update task you will configure below, they will update only from the evaluation branch.

Schedule a client update task for your evaluation group to update from the evaluation branch

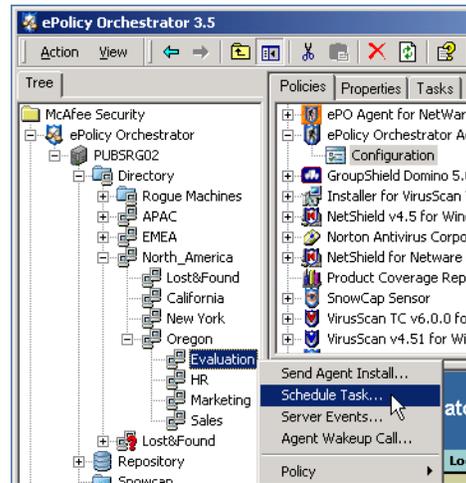
Create a scheduled ePolicy Orchestrator Agent Update task at your evaluation group level that updates DATs and engines only from the Evaluation branch of your repository. Schedule it to run one or two hours after your scheduled pull task is scheduled to begin.

Creating the evaluation update task at the evaluation group level causes it to run only for that group. You must create a separate update task, probably at the **Directory** level, to update the rest of your network from the current branch after you have evaluated the DAT and engine updates. [Create and schedule a daily DAT and engine client update task on page 118](#) for details on creating this task.

To create this update task for your evaluation group:

- 1** Right-click your evaluation group in the ePolicy Orchestrator **Directory** and select **Schedule Tasks**.

Figure 6-15 Schedule an update task at the group level to update only your test clients with the new DATs or engines



- 2 In the **Schedule Task** dialog box, type a name such as *Evaluation update*.
- 3 Select **ePolicy Orchestrator Agent Update** from the list of available software task types and click **OK**.
- 4 In the upper details pane, select the **Tasks** tab. Your new *Evaluation update* task should appear in the list of available tasks. Note that this task is only available at your evaluation group level or below.
- 5 Schedule and enable the update task to run a short time after your scheduled evaluation pull task completes. See [Create and schedule a daily DAT and engine client update task on page 118](#) for details on configuring an agent update task.

Once configured, the update task will run at the day and time you specified.

Monitor the client computers during the DAT evaluation period each week

Watch the client computers in your evaluation group for several hours after they have updated with the new DATs.

When you are satisfied the new DATs work correctly on your test clients, you can feel safe distributing them to your entire network.

Move the new DATs from the evaluation branch to the current branch

This is the manual step you must do each week. Once you are sure the DAT files are sound, copy them from the Evaluation branch to the Current branch of your master repository. Adding them to the current repository branch makes them available to your daily client update task. The next time the update task runs, it will see the new DAT files in the current folder, and distribute them to all your clients.

To copy new DATs from the Evaluation branch to the Current branch:

- 1 In the ePolicy Orchestrator 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 DATs that are saved in your master repository.

The list should show two sets of DATs; last week's DATs that are still in the Current branch and the new DATs you just downloaded that are in the Evaluation branch. Before you finish copying the new DATs to the Current branch, be sure to first copy the old DATs in the Current branch to the Previous branch. You may need to roll back DATs from the previous branch.

- 4 Select the **Current** DATs in the list by selecting them and then select **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 package.
- 7 Select the new DATs in the **Evaluation** branch in the list.
- 8 Select **Copy to current**.
- 9 Click **Close** after package has been copied.

Let replication and update tasks update with the new DATs

Once the new DATs or engines are added to the current branch of your master repository, they are available to your entire network. Scheduled replication tasks will automatically update any distributed repositories if you have them.

Also, your daily update task, which is most likely set to use the current branch, will update all your clients the next time it runs with the new DAT files. See [Distributing DAT and engine updates to clients on page 115](#) for more information about creating and configuring this task.

Moving or deleting DAT and engine packages

This section contains information about manually working with DAT and engine packages in the master repository. You may occasionally be required to manually delete or move packages between repository branches.

The topics covered here are:

- [Manually moving DAT and engine packages between branches](#)
- [Deleting DAT or engine packages from the repository](#)

Manually moving DAT and engine packages between branches

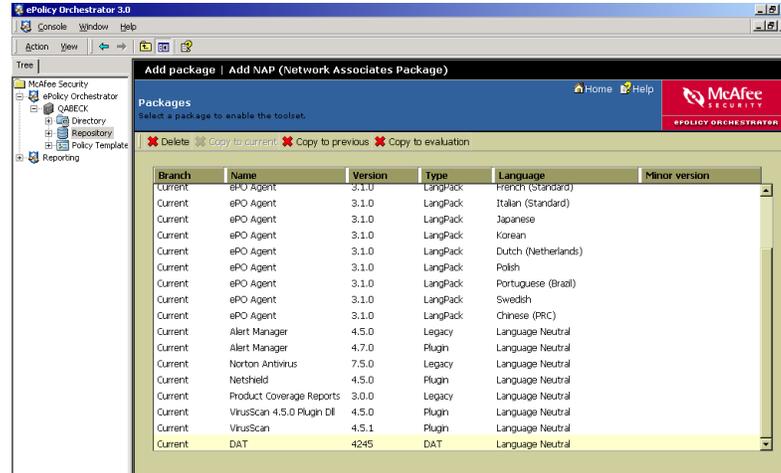
Use this procedure to move packages between the evaluation, current, and previous branches after they have been checked into the master repository. You might do this if you are using the Evaluation branch to test DAT file and engine updates (see [Evaluate new DATs and engines before deploying to your whole organization on page 123](#)). As another example, if you are manually checking in new DATs to the Current branch, you may want to copy the old DATs to the Previous branch.

For more information on branches, see [About repository branches on page 102](#). You must be a global administrator to move packages between branches.

To move a package from one branch to another:

- 1 In the ePolicy Orchestrator console tree, select **Repository**.
- 2 In the details pane under **AutoUpdate Tasks**, click **Manage packages**. The **Packages** page appears.

Figure 6-16 The Packages page shows the packages checked into the master repository



- 3 Select the desired package, then click **Copy to current**, **Copy to Previous**, or **Copy to evaluation** as needed. The **Copy package** wizard appears.
- 4 Click **Next** to open the copy options dialog box.
- 5 If you have older products deployed in your network, such as VirusScan 4.5.1, select **Support legacy product update** to make the package available to both old and newer products.
- 6 To delete the selected package after it has been moved to the new branch, select **Delete original after copy**.
- 7 Click **Finish** to move the package.
- 8 Click **Close** after package has been moved.

Deleting DAT or engine packages from the repository

You must be a global administrator to delete packages from the repository. As you check in new DATs each week, they replace the older versions or move them to the previous branch, if you are using the previous branch. However, you may occasionally want to manually delete DAT or engine packages from the master repository.



Do not manually delete packages from repositories outside of the ePolicy Orchestrator interface console, such as in Windows Explorer.

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

- 1 In the ePolicy Orchestrator console tree, select **Repository**.
- 2 In the details pane under **AutoUpdate Tasks**, click **Manage packages**. The **Packages** page appears.

3 Select the desired packages you want to remove, then click **Delete**.

This will remove the packages from your master repository.

7

Update Large Networks with Distributed Repositories

Create distributed repositories for remote offices and sharing network load

If your organization is large and you have offices in different geographic areas connected by WAN, VPN, or other lower-bandwidth connections, you will probably want to use distributed repositories. A distributed repository is a copy of the master repository on your ePolicy Orchestrator server that is located in another part of the network. You can use the ePolicy Orchestrator console to schedule regular replication tasks to keep distributed repositories up-to-date with the latest contents of the master repository. You can configure the clients in the remote domains to get their updates from a distributed repository located in the local LAN, rather than getting updates across a WAN directly from the ePolicy Orchestrator server.

ePolicy Orchestrator supports several different kinds of distributed repositories, so you can use the kind that works best in your network. One master repository and ePolicy Orchestrator server can support dozens or even hundreds of distributed repositories.

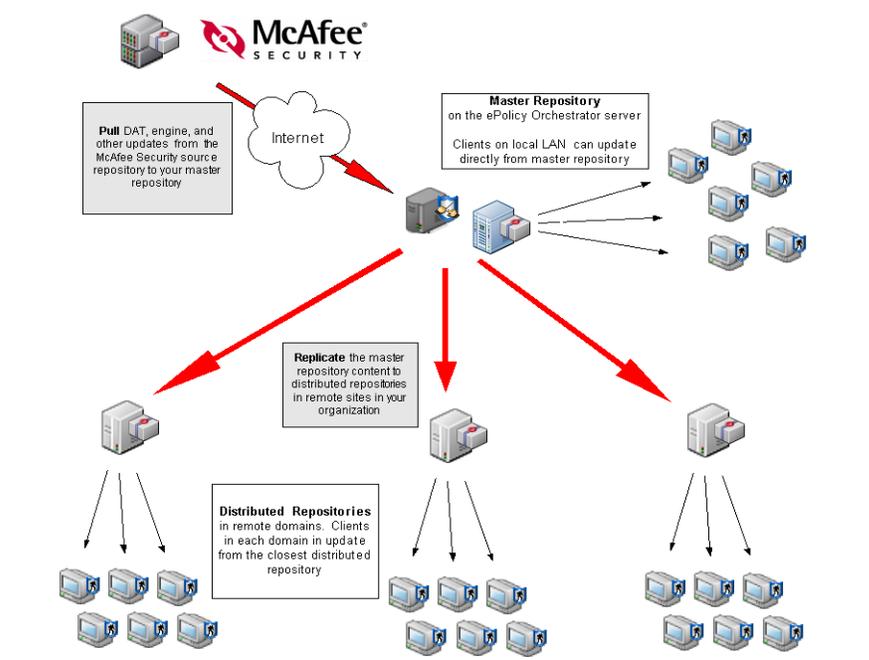
This section contains the following information:

- [About distributed repositories.](#)
- [Create distributed repositories.](#)
- [Replicating the master repository contents to distributed repositories.](#)
- [Configure agent policies to use appropriate distributed repository.](#)
- [Using local distributed repositories that are not managed through ePolicy Orchestrator.](#)
- [Managing the SITELIST.XML repository list](#)

About distributed repositories

Distributed repositories are copies of your master repository, and contain all the DAT, engine, or product update packages that are saved in your master repository. As you update your master repository, either by using Pull tasks to update DATs and engines, or by checking in package files, ePolicy Orchestrator replicates the updates to the distributed repositories. You can configure client computers in remote sites to go to the distributed repository for updates.

Figure 7-1 Distributed repositories



How do distributed repositories save bandwidth?

Using distributed repositories allow you to balance load when you have a large LAN with thousands of clients. During an outbreak situation, you may want to have all your clients update at the same time. Having several distributed repositories allows you to balance network load, rather than having them all update from one server.

In a large organization with parts of your organization separated geographically, using distributed repositories helps limit network traffic in the low-bandwidth sections of your network. For example, say you want to update full weekly DATs to a remote office with 100 client computers that is located in another country. Assume the remote network is connected to your local LAN by a WAN link. If you create a distributed repository and configure those clients to update from it, you copy the DAT package, which is usually about 3 MB, once across the WAN to the distributed repository. Then, all the clients update their DATs from the distributed repository located in the same LAN.

If you did not create a distributed repository in the remote LAN, each of the 100 clients in that LAN would have to get their DAT update from the master repository, pulling the 3MB DAT package across the WAN 100 times!

Which computers in my network should I use as distributed repositories?

You should be able to use an existing server to host the distributed repository, do not need to use a dedicated computer for the distributed repository. Ideally, the computer should be a server and large enough to have many client computers connect to it for updates. Servers are better than workstations because they are more likely to be running all the time.

About the SITELIST.XML repository list

The repository list is an XML file containing a list of all the update repositories you are managing through ePolicy Orchestrator. These include any source or fallback repositories, the master repository, and any distributed repositories you have created. The repository list location and network credential information that client computers use to select the nearest repository from the list and retrieve updates from them.

The ePolicy Orchestrator server sends the repository list to the agent during agent-to-server communication. You can also export it to a file and manually deploy, then apply it to client computers using command-line options.

Types of distributed repositories

ePolicy Orchestrator supports several different kinds of distributed repositories, and different replication protocols for keeping each up-to-date with the latest updates in your master repository. You will need to determine what kind of distributed repository works best in your network. You can use any of these types, or several or all of them together.

- SuperAgent repositories.
- FTP or HTTP servers.
- UNC share folders.
- Mapped drives (local drives).
- Non-managed repositories.

Create distributed repositories

To use distributed repositories in your ePolicy Orchestrator deployment, first create the distributed repository location to host the repository. The process for creating distributed repositories varies depending on what kind of distributed repository you chose.

- [Creating SuperAgent distributed repositories](#). You can use computers with SuperAgents installed on them as distributed repositories.
- [Creating FTP, HTTP, and UNC global distributed repositories](#). Create folders on existing servers and use them to host distributed repositories.

It is also possible to create and use distributed repositories outside of that are not created or managed by ePolicy Orchestrator, and have client computers update from them. Creating and maintaining these distributed repositories is not covered here. McAfee does not recommend using non-managed repositories if possible. For more information on using these, however, see [Using local distributed repositories that are not managed through ePolicy Orchestrator on page 143](#)

Creating SuperAgent distributed repositories

In addition to using SuperAgents to send broadcast wakeup calls to other agents during a global update, you can also use SuperAgents as distributed repositories for updating.

Why use SuperAgent repositories instead of HTTP, FTP, or UNC repositories?

SuperAgent repositories have several advantages over other types of distributed repositories making them easier to create and configure. First, you don't need to manually create folder locations on the host computer before adding the repository to the repository list. Simply enable the SuperAgent repository feature from the agent policies for a given computer, and ePolicy Orchestrator creates the required subfolders. Second, you don't need to manually enable sharing on the SuperAgent repository folder. Client computers updating from the SuperAgent repository can access the folder. Third, SuperAgent repositories don't require that you specify replication or updating credentials. Once the SuperAgent is installed and enabled on the computer, ePolicy Orchestrator can replicate repository contents to that SuperAgent, and other agents can update from it. ePolicy Orchestrator uses a proprietary network protocol called SPIPE to replicate updates to SuperAgent distributed repositories.

What's the difference between a SuperAgent and a SuperAgent repository?

You may use SuperAgents only to distribute broadcast agent wakeup calls during a global update. See [Deploying SuperAgents to distribute agent wakeup calls on page 75](#). In addition to this, SuperAgents can also function as distributed repositories.

To use the SuperAgent broadcast wakeup call for alerting other agents to call into the ePolicy Orchestrator server, SuperAgents need to be deployed one per broadcast segment. In most networks this is synonymous with a network subnet. However, it is not necessary that a SuperAgent repository be located in the same broadcast segment for a client computer to be able to update from it. For updating, a client computer only needs to be able to reach the computer hosting the SuperAgent repository on the network.

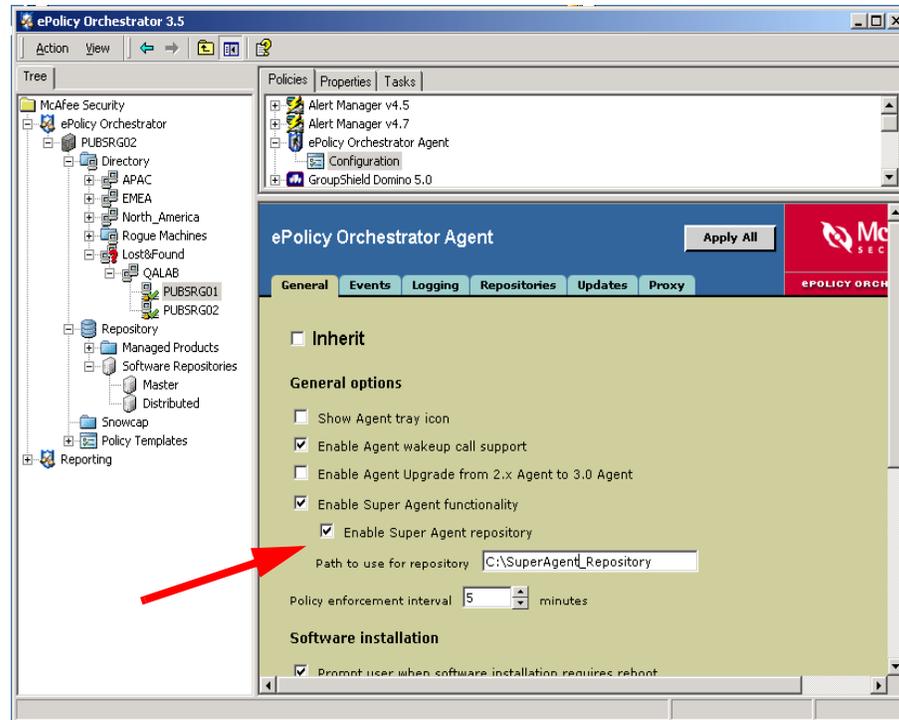
Computers hosting SuperAgent repositories may need to be more powerful than computers that host only SuperAgents used for broadcast wakeup calls. If you plan to use SuperAgent repositories, make sure the computer you create them on is large enough to allow however many client computers you have to update from it, potentially simultaneously in an outbreak situation.

Use the agent policy page to create a SuperAgent distributed repository

Create a SuperAgent distributed repository by converting any regular ePolicy Orchestrator agent into a SuperAgent repository. The procedure below assumes you have first deployed agents to clients in your network and have added them to your **Directory**. Also, you can convert existing SuperAgents into SuperAgent repositories.

To create a SuperAgent distributed repository:

- 1 Identify the client computer that you want to use as a SuperAgent repository.
- 2 Find the client computer in your ePolicy Orchestrator **Directory** and select it.
- 3 In the right-hand upper details pane, select **ePolicy Orchestrator Agent | Configuration**.
- 4 In the lower details pane, select the **General** tab of the **ePolicy Orchestrator Agent** policy page.
- 5 Deselect **Inherit** to enable configuration features.
- 6 Select **Enable SuperAgent functionality**. This turns the regular agent into a SuperAgent.

Figure 7-2 Turn an existing agent into a SuperAgent repository**7** Select **Enable SuperAgent repository**.

- 8** Type a folder path location for the repository. This is the location where the master repository copies updates during replication. You can use standard Windows variables, such as <PROGRAM_FILES_DIR>. If the folder name does not already exist on the computer, it is created.

Client computers updating from this SuperAgent repository will be able to access this folder. You do not need to manually enable file sharing.

9 Click the **Apply All** button at the top of the policy page.

The SuperAgent repository is created the next time the agent on the target computer calls back to the ePolicy Orchestrator server and gets the policy change. When the distributed repository is created, the folder you specified is created on the computer if it was not already created. If ePolicy Orchestrator cannot create the folder for whatever reason, it creates one of the two default folders:

- <DOCUMENTS AND SETTINGS>\ ALL USERS\APPLICATION DATA\NETWORK ASSOCIATES\FRAMEWORK\DB\SOFTWARE
- <AGENT INSTALLATION PATH>\DATA\DB\SOFTWARE

In addition, the location is added to the SITELIST.XML list of repositories managed by ePolicy Orchestrator. This makes the site available for other clients in your **Directory** to use for updating.

Deleting SuperAgent distributed repositories

Use the procedure to remove SuperAgent distributed repositories from the repository list and delete their contents. Changes take effect during the next agent-to-server communication.

- 1 On the **General** tab in the ePolicy Orchestrator Agent | Configuration policy page, deselect **Inherit**.
- 2 Deselect **Enable SuperAgent repository**.
- 3 Click **Apply All** to save the current entries.

The SuperAgent repository will be deleted and removed from the repository list. Note that the agent will still function as a SuperAgent as long as you leave the **Enable SuperAgent functionality** option selected.

Creating FTP, HTTP, and UNC global distributed repositories

You can use existing FTP, HTTP, or UNC file servers to host distributed repositories and have clients update from them. These allow you to use standard protocols and existing servers to host your distributed repositories.

Creating these kinds of distributed repositories is a multi-step process:

- 1 *Create a folder location on an existing FTP, HTTP, or UNC server.*
- 2 *Enable folder sharing for UNC and HTTP sites.*
- 3 *Create a distributed repository in ePolicy Orchestrator that references the folder.*

Details on each of these steps follows below. Note that you must be a global ePolicy Orchestrator 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 computer that will host the distributed repository. For UNC shares, simply create the folder on the computer and enable sharing.

For FTP or HTTP locations, 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 on how to create a site.

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 be able 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. Note that this is for replication purposes only. Client computers configured to use the distributed repository will update using the appropriate protocol (HTTP, FTP, or UNC) and do not require folder sharing.

To create a shared folder for an HTTP or UNC distributed repository folder:

- 1 From the computer on which you plan to host the distributed repository, locate the folder you created using Windows Explorer.
- 2 Right-click the folder and select **Sharing**.
- 3 On the **Sharing** tab, select **Share this folder**.

- 4 Configure Share Permissions as needed. Client computers updating from the repository only require `READ` access, but administrator accounts, including the account used by the ePolicy Orchestrator server service to replicate data, require `WRITE` access. See your Microsoft Windows documentation on how to configure appropriate security settings for shared folders.
- 5 Click **OK**.

Create a distributed repository in ePolicy Orchestrator that references the folder

Once you have created the folder to use as the repository, 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 From the left-pane console tree of the ePolicy Orchestrator console, click **Repository**.
- 2 Select **Add distributed repository** from the right-hand **Repository** pane.
- 3 Click **Next** at the first page of the wizard.
- 4 Type a name into the **Name** field. Note that this is how the distributed repository name appears in the repository list in the ePolicy Orchestrator console. It does not have to be the specific name of the server or folder that actually hosts the repository.

Figure 7-3 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, either **FTP**, **HTTP**, or **UNC**, depending on what kind of repository you are creating.
- 7 Click **Next**.
- 8 On the next wizard page, enter the address location information for the FTP, HTTP, or UNC site, depending on what you selected in [Step 6](#).

For FTP or HTTP sites, type the URL address information in the **URL** field, such as `HTTP://MyRepository`. This is the site you created in your web server (see [Create a folder location on an existing FTP, HTTP, or UNC server on page 135](#)). 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 computer name and epoShare is the name of the UNC shared folder you created.

9 Click **Next**.

10 On the download credentials page, enter authentication credential information as needed for clients that will update from the repository. Read-only permissions are sufficient for clients to be able to download updates from the distributed repository.

The options available on the download credentials page vary depending on what kind of repository you're creating.

Type	Client download credential information
FTP	Select Use anonymous login or type the user account information in User name , Password , and Re-Enter Password .
HTTP	If the HTTP server requires authentication, select Use Authentication , then type the user account information in User name , Password , and Re-Enter Password .
UNC	Select Use Logged On Account or type the user account information in Domain , User name , Password , and Confirm password .

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 clients using the authentication information you provided (or that no authentication is necessary if you did not provide any).

Figure 7-4 Your distributed repository works!



If your site is not verified, check that you typed the URL or path correctly on the previous page 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 copies, or replicates, DATs, engine files, or other product updates from the master repository to the distributed repository. These credentials must have **Read and Write** permissions in the domain where the distributed repository is located.

Type	Replication credential information
FTP	If you selected FTP , type the user account information in User name, Password, and Re-Enter Password .
HTTP	Type the UNC share name of the physical folder hosting the repository in Replication UNC . Use this format: \\<COMPUTER>\<FOLDER>. You can use system variables to define this location. Note: 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 Domain, User name, Password, and Re-Enter Password .
UNC	Type the user account information in Domain, User name, and Password fields .

- 14** Click **Verify** to test that your ePolicy Orchestrator server can write to the shared folder on the remote computer. 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**.

Changing FTP, HTTP, UNC distributed repositories after they are created

You can change configuration information about distributed repositories after you have created them. Use this procedure to change the settings of global distributed repositories.

- 1** In the ePolicy Orchestrator Console Tree, select **Repository | Software Repositories**. This displays the list of configured repositories, including all distributed repositories and the master repository.
- 2** Select a distributed repository in the list and click **Edit**.
- 3** Change configuration and authentication options as needed.
- 4** Click **OK** to save the current entries.

Deleting HTTP, FTP, or UNC distributed repositories

Use the ePolicy Orchestrator console to delete HTTP, FTP, or UNC distributed repositories. Doing this removes them from the repository list and removes the distributed repository contents on the server.

You must be a global administrator to delete distributed repositories.

- 1** In the ePolicy Orchestrator Console Tree, select **Repository | Software Repositories**. This displays the list of configured repositories, including all distributed repositories and the master repository.
- 2** Select the distributed repository from the list and click **Delete**.

Replicating the master repository contents to distributed repositories

Once you have created distributed repositories, you must use replication tasks to have ePolicy Orchestrator copy the contents of the master repository to the distributed repository. Client computers update from the closest distributed repository. Unless you have replicated master repository updates to all your distributed repositories, some client computers that update from distributed repositories may not get them. Therefore, it is essential to make sure all your distributed repositories are up to date so clients in every corner of your network can download the latest updates.

If you have enabled global updating, repository replication happens automatically; you do not need to use replication tasks when global updating is enabled. See [Use global updating to automatically distribute updates to all clients immediately](#) on page 115 for details on global updating.

Full vs. incremental replication

You can select an incremental or full replication. Incremental only copies the new updates in the master repository that are not yet in the distributed repository. A full replication copies the entire contents of the master repository. An incremental replication uses less network bandwidth; a full replication is more complete.



McAfee recommends running a daily incremental replication task and a weekly full replication task. This maximizes network bandwidth efficiency by only updating essential, incremental changes during the week. It also guarantees completeness by forcing a complete replication on a regular basis. Create and enable two scheduled replication tasks to do this, one incremental replication task that occurs daily and a full replication task that occurs weekly.

Scheduled replication vs. manual Replicate Now

This section covers using replication tasks:

- [Schedule a daily repository replication server task](#)
- [Run a manual Replicate Now task to update distributed repositories immediately](#)

Schedule a daily repository replication server task

Scheduling a regular Repository Replication server task is the best way to ensure that your distributed repositories are up to date with the latest changes in your master repository. You may update your master repository often, either through Pull tasks from a source repository or through manually checking in DAT, engine or product update packages. Scheduling a daily replication task ensures that client computers that get their updates from a distributed repository will also be able to get these changes.

To create a daily scheduled replication task:

- 1 In the ePolicy Orchestrator console Tree, select **Repository**.
- 2 In the **Repository** page, 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 menu.
- 6 Make sure **Enable task** is set to **Yes**.
- 7 Select **Daily** from the **Schedule Type** drop-down list. You can schedule tasks to run at other frequencies, too.
- 8 Expand the **Advanced schedule options** and schedule the day and time for the task to run.

If you are using a source repository to update your master repository, schedule your replication task for one hour after your scheduled pull task begins. This should give the pull task enough time to complete. Depending on your network and Internet connections, your pull task may require more or less time, so set your replication task start time accordingly.

- 9 Click **Next** at the top of the page.
- 10 Select **Incremental replication** and 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 shows the exact date and time when the task will run, according to the schedule criteria you specified.

Run a manual Replicate Now task to update distributed repositories immediately

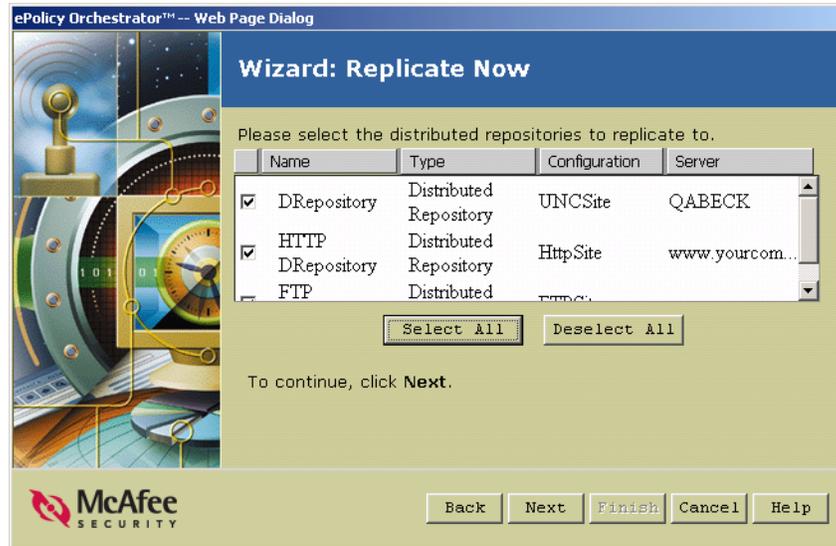
Configuring scheduled replication tasks is an easy way to automate replication to your distributed repositories. Occasionally, however, you may make changes to your master repository that you want to replicate to distributed repositories immediately, rather than wait for the next scheduled replication. For example, you may check an EXTRA.DAT update into your master repository to address a virus outbreak. Since you will want to distribute this DAT update as quickly as possible to your network, run a manual Replicate Now task to copy the update to your distributed repositories.

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 do this:

- 1 From the left-pane console **Tree** of the ePolicy Orchestrator console, click **Repository**.
- 2 In the right-pane details **Repository** page, click **Replicate now** to open the **Replicate Now** wizard.
- 3 Click **Next** at the first page of the wizard.
- 4 Click **Select All** to replicate to all your distributed repositories.

Figure 7-5 Select the distributed repositories to replicate to



If you only need to replicate to individual distributed repositories, you can select them from the list. If you are not sure which distributed repositories need to be updated, replicate to them all.

- 5 Click **Next** and select **Incremental replication** on the final wizard page.

If it is the first time you are replicating to a distributed repository, it will be a full replication even if you select incremental replication. Subsequent incremental replications will replicate only incremental changes.

- 6 Click **Finish** to begin replication. Wait a few minutes for replication to finish. Replication time varies depending on the changes to the master repository and the number of distributed repositories you are replicating to.
- 7 Click **Close** to close the wizard window.

After replication is complete, you can initiate an immediate client update task so client computers in remote sites can get updates from the distributed repositories. See [Create and schedule a daily DAT and engine client update task on page 118](#) for details.

Configure agent policies to use appropriate distributed repository

New distributed repositories are added to the SITELIST.XML repository list containing all available distributed repositories. The agent on the client computers updates the SITELIST.XML repository list every time it communicates with the ePolicy Orchestrator server. The agent performs repository selection each time the agent (**McAfee Framework Service**) service starts (for example, when the client computer is turned off and on) and when the repository list changes.

How the agent selects which repository to use for updating

By default, the agent can attempt to update from any repository in its SITELIST.XML repository list. The agent can use a network ICMP ping or subnet address compare algorithm to find the distributed repository with the fastest response time. Usually, this will be a distributed repository that is closest to the client on the network. For example, a client computer in a remote site far from the ePolicy Orchestrator server will probably select a local distributed repository. By contrast, an agent in the same LAN as the ePolicy Orchestrator server will probably update directly from the master repository, which is the closest repository.

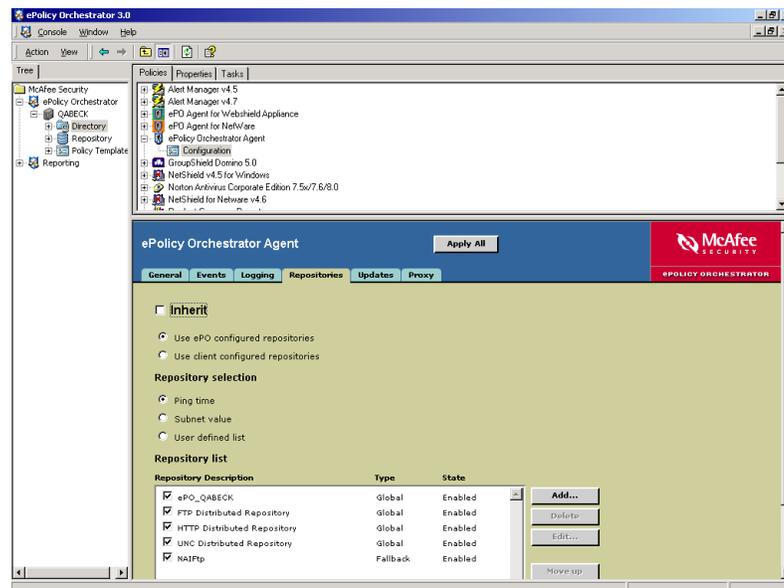
You can also tightly control which distributed repositories agents will use for updating by enabling or disabling specific distributed repositories in the agent policy. However, McAfee does not recommend doing this. Allowing agents to update from any distributed repository ensures they will get the update from somewhere. Using a network ICMP ping, the agent will probably update from the closest distributed repository anyway.

Changing how agents select repositories

Use the options on the **Repository** tab of the agent policy pages to customize how agents select distributed repositories. You can configure this at any level in your **Directory**.

- 1 On the **Repositories** tab in the ePolicy Orchestrator Agent | Configuration policy page, deselect **Inherit**.

Figure 7-6 Repositories tab in the ePolicy Orchestrator Agent | Configuration policy page



- 2 Select **Use ePO configured repositories**.
- 3 Under **Repository selection**, specify the method to use 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 computers 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 computers to select distributed repositories.
 - 6 Click **Apply All** to save the current entries.

Using local distributed repositories that are not managed through ePolicy Orchestrator

In some cases, you may need to create and maintain distributed repositories that are not managed by ePolicy Orchestrator. For example, your organization may have a remote office where the local admin wants to maintain control and doesn't want to let an ePolicy Orchestrator replication task automatically copy content to a server there. Or, your organization may already use other network tools or scripts for copying files between servers and you prefer to use that method for keeping distributed repositories up-to-date.

Either way, you or a site admin can manually create a FTP, HTTP, UNC or Local Directory (Mapped Drive) distributed repository and regularly update it with DAT, engine, or product updates. Since this distributed repository is not included in the master site list on the ePolicy Orchestrator server, ePolicy Orchestrator will not update it using Replication tasks. Instead, the local site admin will need to keep the repository up-to-date manually.

Then, you can use the ePolicy Orchestrator console or a remote console to configure client computers in a particular site or group in the **Directory** to update from it.



McAfee recommends that you manage all distributed repositories through ePolicy Orchestrator if possible. Managing distributed repositories with ePolicy Orchestrator and using scheduled replication tasks to update them frequently is the best way to ensure they are up-to-date, and therefore that clients updating from them have the latest updates. Only use non-managed distributed repositories if your network or organizational structure does not allow them to be managed by ePolicy Orchestrator.

Create a distributed repository manually and keep it up-to date

Create a UNC, FTP, or HTTP folder location on a computer (preferably a server if you have one) that will host the distributed repository. See your operating system or HTTP or FTP server software documentation for more information on how to do this.

Once the site is created, you must keep it up-to-date manually. Do this by adding update content, such as DAT and engine packages, to the site as needed. The simplest way to do this is to manually copy the contents of the master software repository folder on the ePolicy Orchestrator server and paste it to your distributed repository location you created.

To do this:

- 1 Copy or zip all files and sub-directories in the master software repository folder from the ePolicy Orchestrator server. By default, this is at the following location on your ePolicy Orchestrator server:

C:\Program Files\Network Assoc\PO3.5.0\DB\Software

- 2 Paste or unzip the copied files and subfolders in your distributed repository location on the distributed repository computer.

For example, say you have a UNC share repository folder at C:\UNC_Distr_Repo on the distributed repository server named //MyDistrServer. You would copy the contents of the .DB/Software folder, including all files and subfolders, on the ePolicy Orchestrator server to the UNC folder. Your finished folder hierarchy on the distributed repository would look something like:

//MyDistrServer/UNC_Distr_Repo/DB/Software/...

When you point client computers at the //MyDistrServer/UNC_Distr_Repo distributed repository to get updates (see below), the updater will automatically find the appropriate DAT, engine, or product updates in the correct subfolder.

Configure clients to use a non-managed distributed repository

Once you have created the location, use the ePolicy Orchestrator console to configure updating properties for computers in that site to use the distributed repository. Ideally, you have all the computers that would use this distributed repository grouped into one site or group in your **Directory**. That way, you can do this once at the site or group level and it will inherit to all child computers.

To configure clients to use a non-managed distributed repository:

- 1 In the ePolicy Orchestrator console **Directory** tree, select the site or group that should use the non-managed distributed repository.
- 2 In the right-hand details pane, select **ePolicy Orchestrator Agent | Configuration** to view the policy pages for the ePolicy Orchestrator agent.
- 3 In the lower details pane, click the **Repositories** tab.
- 4 Deselect **Inherit** to enable configuration options.
- 5 By the **Repository List**, click **Add**.
- 6 On the **Repository Options** dialog box, type a name in the **Repository** text field. Note that this is the name that appears in the ePolicy Orchestrator console; it does not have to be the exact name of the repository location.
- 7 Under **Retrieve files from**, select the type of repository.
- 8 Under **repository configuration**, type the location you created (see above) using the appropriate syntax for the repository type. For example, a UNC repository might look like "//ComputerName/UNCFolderName". An HTTP repository might be "http://MyDistrRepo".
- 9 Type a port number if you don't want to use the default port 80.
- 10 Configure authentication credentials as appropriate, if needed.
- 11 Click **OK** to save the new distributed repository.

12 At the top of the policy pages, click **Apply All** to save the policy change.

The repository is added to the Repository List. The type is **Local** to indicate it was not created in the ePolicy Orchestrator server Repository interface and is therefore not managed by ePolicy Orchestrator. When a non-managed ePolicy Orchestrator repository is selected in the **Repository List**, the **Edit** and **Delete** buttons are enabled to allow you to change the repository from the policy pages.



You cannot edit or delete ePolicy Orchestrator-managed distributed repositories that you created using the ePolicy Orchestrator console Repository interface from the agent policy pages in this way.

Managing the SITELIST.XML repository list

The SITELIST.XML file contains the repository list, which contains location and configuration information for all software repositories used with ePolicy Orchestrator. These include source and fallback repositories, the master repository, and any distributed repositories you have created.

You can use the ePolicy Orchestrator console to import an existing repository list, either from a previous installation of ePolicy Orchestrator or from another McAfee product, such as VirusScan Enterprise. You can also use the console to export your current repository list to an external XML file. This can be useful to backup your repository list in case you need to reinstall the ePolicy Orchestrator server at some point. Exported repository lists can also be manually imported to other products, such as VirusScan Enterprise, when you install them.

Importing a SITELIST.XML repository list

You may need to import a repository list at some point, either one from a previous installation of ePolicy Orchestrator or from McAfee AutoUpdate Architect (MAA).

Before you uninstall McAfee AutoUpdate Architect, make a backup copy of the SITEMGR.XML file located in the installation directory and store it in a safe location. The default location of the McAfee AutoUpdate Architect installation directory is:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\MCAFFEE AUTOUPDATE ARCHITECT
```

You cannot import a repository list (SITELIST.XML) that was exported from McAfee AutoUpdate Architect or ePolicy Orchestrator for this purpose.

You must be a global administrator to import the repository list from McAfee AutoUpdate Architect.

- 1** In the ePolicy Orchestrator 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 will be viewable from the **Master and Distributed Repositories** page. Make changes to the repositories in this list as needed.

Exporting the repository list to a file

Use this procedure to export the repository list (SITELIST.XML) to a file for manual deployment to client computers or for import during the installation of supported products. For more information, see [Managing the SITELIST.XML repository list on page 145](#).

You must be a global administrator to export the repository list.

To export a repository list:

- 1** In the ePolicy Orchestrator 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** at the first screen.
- 4** Type the path where 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 (SITELIST.XML) to the location you specified.

Once you have exported the repository list (SITELIST.XML) 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 client computers, then apply the repository list to the agent (for example, using third-party deployment tools and logon scripts). For more information, see [Agent installation command-line options on page 73](#).



SECTION 3

Managing Policies for Agents and Products

Manage policies and schedule regular client tasks to keep ePolicy Orchestrator agents and security products up and running.

Chapter 8, Managing Deployed Agents

Chapter 9, Managing Product Policies and Running Client Tasks

Chapter 10, Determining Compliance

8

Managing Deployed Agents

Manage policies and agent-to-server communication to keep agents running

The agent is the component that collects and sends information between the ePolicy Orchestrator server, repositories, and managed client computers and products. How you configure the agent and its policy settings determines how it functions and facilitates communication and updating in your environment.

This chapter is divided among the following topics:

- [About the agent-to-server communication interval \(ASCI\)](#)
- [Sending manual agent wakeup calls](#)
- [Using the agent policy pages to set policies](#)
- [Viewing properties of the agent and products from the console](#)
- [Checking agent logs](#)
- [Working with the agent from the client computer](#)

About the agent-to-server communication interval (ASCI)

The agent to server communication interval (ASCI) is an agent policy setting that determines how often the agent calls into the ePolicy Orchestrator server for updated instructions. The default ASCI is 60 minutes, but you can configure a different ASCI.

During the ASCI communication, the agent and server exchange information using SPIPE, a proprietary network protocol used by ePolicy Orchestrator for secure network transmissions. At every ASCI, 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 client computer.

About Full and Minimal Properties

The agent sends the complete set of properties during the initial agent-to-server communication. After the initial communication, the agent sends only those properties that have changed since the last agent-to-server communication. However, the agent sends the complete set again if the properties version on the agent and ePolicy Orchestrator server differ by more than two.

The set of properties sent varies depending on whether you specified that the agent collect full or minimal properties.

If you specify to collect the full set of properties, the agent collects:

- System properties — Information about the computer hardware, software, and corresponding settings including the processor speed, operating system, time zone, and the most recent date and time that properties were updated.
- Product properties — Product properties include general properties such as the installation path, virus definition (DAT) file version number, and product version number. Product properties also include specific policy settings you may have configured for each product.

If you specify to collect only minimal properties, the agent collects only general product properties.

Recommended ASCI for different connection speeds

The default ASCI is 60 minutes, but you can use the agent policy page to set the ASCI to anything you want. Be mindful, however, that the 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 ePolicy Orchestrator server over WAN, VPN or other slower network connections. For these agents, you may want to set a less frequent ASCI. The following table lists the recommended ASCI for several common network connection speeds.

Table 8-1 Recommended ASCI settings

Network Size	Recommended ASCI
Gigabit LAN	60 minutes
100MB LAN only	60 minutes
WAN	360 minutes
* Dial-up or RAS	360 minutes
10MB LAN only	180 minutes
Wireless LAN	150 minutes
* When you connect to a corporate intranet via dial-up or RAS, the agent detects the network connection and communicates to the ePolicy Orchestrator server.	

Ten minute initial ASCI after agent startup or when policies are old

If the agent service is stopped and restarted, the agent calls in to the server at a randomized interval within ten minutes. The second ASCI after startup occurs at a randomized interval on the ASCI as set in the agent policy (default is 60 minutes). Subsequent calls occur at the regular ASCI with no randomization.

You can skip the initial ten-minute, randomized ASCI if the last agent-to-server communication occurred within the time period (default is 24 hours) you specify. For example, if users turn off their computers at night, agents will initially communicate to the server randomly over the ASCI length instead of 10 minutes.

For instructions on setting this as part of agent policy, see [Using the agent policy pages to set policies on page 153](#).

Sending manual agent wakeup calls

You can prompt agents on selected client computers to contact the ePolicy Orchestrator server immediately. For very large networks, you can use a randomization interval avoid having all agents in your network call back to the server at the same time. Using the randomization interval spreads out the wakeup calls over a configurable time period, such as one hour.

About sending agent wakeup calls

Agent wakeup call uses ICMP ping

The agent wakeup call, whether run manually or as part of an agent wakeup task, is an ICMP PING command sent from the ePolicy Orchestrator server. Many network routers block ICMP traffic between subnets by default. If your network is configured this way, using agent wakeup calls will not be able to wake up any computers located outside the local subnet where the ePolicy Orchestrator server is installed. If your network is configured in this way, do not use agent or agent wakeup calls. Use the regular agent ASCII, which uses the SPIPE protocol for all communication.

Sending SuperAgent wakeup calls

The procedure for sending a SuperAgent wakeup call is very similar to sending a regular agent wakeup call. The only difference is that you select **Send SuperAgent wakeup call** for the wakeup type, instead of selecting **Send Agent wakeup call** to wake up a regular agent.

See [Deploying SuperAgents to distribute agent wakeup calls on page 75](#) and [Use global updating to automatically distribute updates to all clients immediately on page 115](#) for more information about using SuperAgents.

Send a one-time manual agent wakeup call

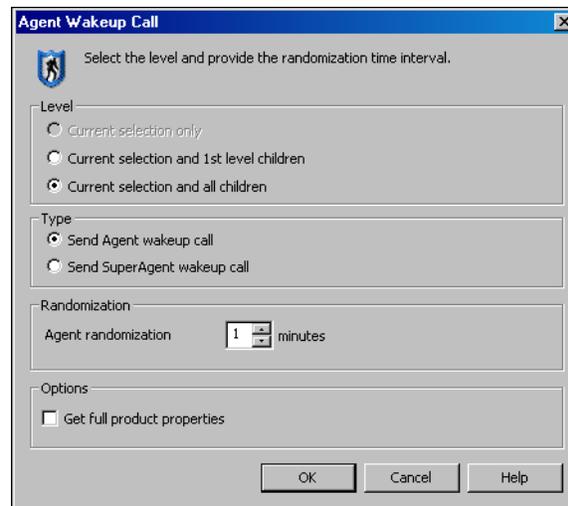
You can send a manual agent wakeup call to any site, group, or individual computer in your **Directory**. This is useful when you have made policy changes or checked in updates to the master repository and you want agents to call in for an update.

Before sending the agent wakeup call to a selected **Directory** node, make sure that wakeup support for that node is enabled (it is by default). To enable wakeup call support, select **Enable Agent wakeup call support** on the **General** tab of the **ePolicy Orchestrator Agent | Configuration** policy pages. For more information, see [Using the agent policy pages to set policies on page 153](#).

To send an agent wakeup call:

- 1 In the ePolicy Orchestrator **Directory**, right-click the desired site, group, or computer, then select **Agent Wakeup Call**. The **Agent Wakeup Call** dialog box appears.

Figure 8-1 Agent Wakeup Call



- 2 Select the **Level** at which you want to send the agent wakeup call. Typically, you will want to send to the default, which is the selected node and all children.
- 3 Under **Type**, select **Send Agent wakeup call**.
- 4 Accept the default (1 minute) or type a different **Agent randomization interval** (0 - 60 minutes). If you type 0, agents on all selected computers respond immediately.
- 5 Typically, the agent only sends 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 wakeup call.

Creating a scheduled client task to wake up the agent

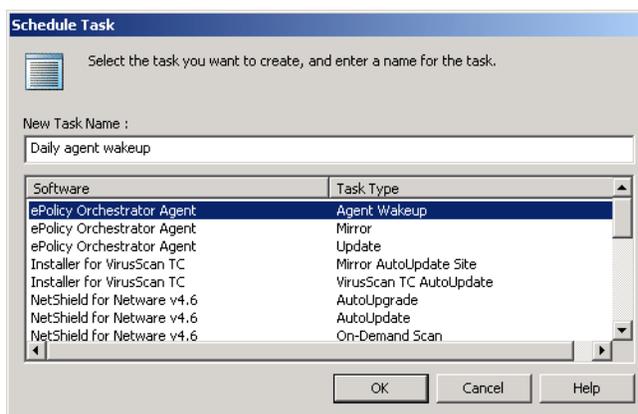
By default, agents use the ASCII setting to call into the ePolicy Orchestrator server for policy changes or other updates at a regular interval. You can also schedule regular agent wakeup tasks from the ePolicy Orchestrator console to initiate agent-to-server communication. If network traffic is a concern in your environment, using an agent wakeup task instead of setting an ASCII gives you some flexibility to reduce unnecessary network traffic between the agent and server by giving you greater control of when the communication occurs.

If you want or need to disable ASCII communication for whatever reason, you can schedule regular agent wakeup calls to alert agents to call into server for updates. You can schedule agent-to-server communication instead of using the agent-to-server communication interval (ASCII). To disable the ASCII, see [Using the agent policy pages to set policies on page 153](#).

To create a scheduled agent wakeup client task:

- 1 In the console tree, right-click the desired site, group, or computer and select **Schedule Task**.
- 2 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 8-2 Create an ePolicy Orchestrator Agent Wakeup task to wakeup agents regularly



- 3 Select ePolicy Orchestrator Agent | Agent Wakeup from the list of available tasks, then click **OK**.
- 4 Press **F5** to refresh the console and make the new task appear in the list in 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.

- 5 Right-click the new task in the task list and select **Edit Task** to edit the task in the ePolicy Orchestrator Scheduler.

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.

- 6 Under **Schedule Settings** on the **Task** tab of the ePolicy Orchestrator Scheduler dialog box, deselect **Inherit**.
- 7 Select **Enable** to define the scheduling options. If you do not select this, the task will not start.
- 8 Click the **Schedule** tab of the ePolicy Orchestrator Scheduler dialog box to specify when the task runs.
- 9 Deselect **Inherit**.
- 10 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.
- 11 Click **OK** when you have finished configuring and scheduling the task.

When done, the scheduled task appears in the list of available tasks in the **Task** tab for the selected **Directory** node. Note that the **Enabled** flag is now set to **True**. The task will run at the next scheduled time.

Using the agent policy pages to set policies

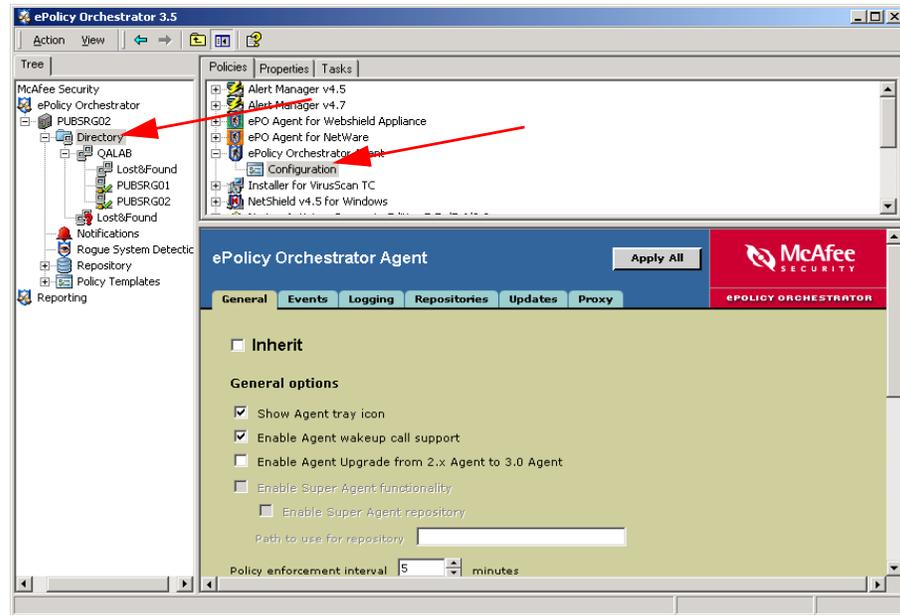
You can configure agent policies to enforce on client computers. You can set policies differently for different console tree items.

To configure agent policy:

- 1 In the ePolicy Orchestrator console **Directory**, select the desired site, group, single computer, or the entire **Directory**

The **Policies**, **Properties**, and **Tasks** tabs appear in the upper details pane.

Figure 8-3 Set policies for specific nodes in the Directory



- 2 Select the **Policies** tab in the upper details pane, then expand **ePolicy Orchestrator Agent | Configuration**. The agent configuration policy pages are divided among six tabs: **General**, **Events**, **Logging**, **Repositories**, **Updates**, and **Proxy**.

The policy settings you can configure are described, tab by tab, as instructions for setting the policy are described.

General

The general tab allows you to configure the following agent policies.

Figure 8-4 General tab

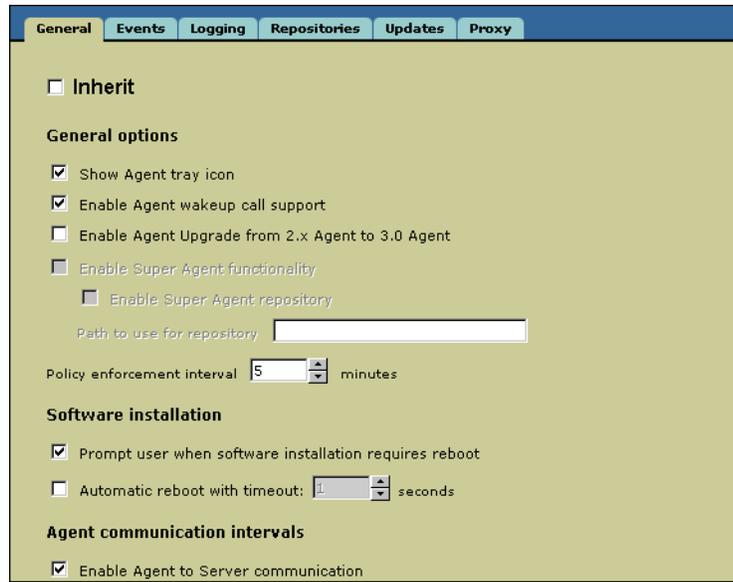


Table 8-2 General agent policies

Property	Description
General policies	
Show Agent tray icon	Show the agent tray icon in the system tray of the client computer.
Enable Agent wakeup call support	Allows you to send manual agent wakeup calls to force the agent to call into the server, rather than make the agent wait for the next ASCII. Manual (or scheduled) agent wakeup calls can be very useful for pushing changed policies or new DATs to computers immediately, or when you want to receive properties and events from the agent.
Enable Agent Upgrade from 2.x Agent to 3.5 Agent	When enabled, older 2.x agents that report to this server are upgraded at the next ASCII.
Enable SuperAgent functionality	Turns the existing agent into a SuperAgent. See Deploying SuperAgents to distribute agent wakeup calls on page 75 . Once an agent is a SuperAgent, you can also make it a SuperAgent repository. This turns the computer where the SuperAgent is installed into a distributed software repository that other computers can come to for DAT, engine, or software updates. See Creating SuperAgent distributed repositories on page 132 for more information.
Policy enforcement interval	How often the agent checks that the policies set from NAP policy pages in the ePolicy Orchestrator console are actually in effect on the client computer. The agent can enforce policy software settings on itself or any other supported software, such as VirusScan Enterprise, Desktop Firewall, or GroupShield. Note: Since the agent policy enforcement occurs locally on the client computer, enforcing often does not generate network traffic.
Software installation	

Table 8-2 General agent policies

Property	Description
Prompt user when installation requires reboot	Let the end-user on the client computer know when a reboot is required during software install. Especially when using ePolicy Orchestrator to deploy, or push, the agent or anti-virus products such as VirusScan Enterprise, to client computers, the installation occurs silently without the end-user knowing. However, if the install requires a reboot as occasionally happens, alerting the end-user makes sure they have time to save unfinished work.
Automatic reboot with timeout	Force client computer reboot after the specified timeout period.
Agent communication intervals	
Enable agent-to-server communication	Enable regular agent-to-server communication using the secure SPIPE protocol. Caution: This is the primary mechanism for how agents communicate with the ePolicy Orchestrator server. Never disable this unless you have specific reasons for doing so.
Agent communication interval (ASCI)	The period of time for the ASCI interval, in minutes. The agent will call back to the ePolicy Orchestrator once at every interval, sending properties back to the server and collecting new policy changes. In setting this interval, you must balance the need for security and up-to-dateness on clients with your networks bandwidth limitations. The more often the interval, the more up-to-date the client but also the more network traffic that is generated. See About the agent-to-server communication interval (ASCI) on page 148 for more information.
Set policy agent trigger for 10-minute ASCI	Set a threshold for outdated policies, in days, to trigger a 10-minute ASCI. For any agents with policies older than this threshold, a 10 minute ASCI is used until the policies are updated.
Full or minimal properties	Chose whether to send full agent properties or only incremental properties at every ASCI.

Enable immediate forwarding of client events

The agent and other anti-virus or security software on the client computer generate software events constantly during normal operation. These can range from informational events about regular operation, such as when the agent enforces policies locally or when VirusScan Enterprise starts an on-demand scan. These events are logged by the agent and sent to the server at every ASCI and stored in the database. A typical deployment of ePolicy Orchestrator in a large network can generate thousands of these events an hour. You wouldn't want to see every one of these events.

Some events, however, are of a higher severity and you will want to know about them immediately. You can configure the agent to forward certain critical events immediately to the ePolicy Orchestrator server. An example of such a critical event is when VirusScan Enterprise or, especially, GroupShield detects a virus and fails to clean or move it.



Note that the types of events you forward from the agent to the server affect how alert notifications are generated. You can use ePolicy Orchestrator’s Notification feature to create alert notifications, such as sending e-mails to alert key people in your organization, when events occur. The alert notification feature in ePolicy Orchestrator 3.5 uses these events forwarded from the agent to trigger notification rules you have configured. Disabling immediate event forwarding means alerts won’t trigger immediately, but rather at the next agent ASCII. See [Chapter 12, ePolicy Orchestrator Notification](#) for more information.



McAfee recommends enabling immediate event forwarding if you plan on using global updating to distribute critical updates. Update events are assigned critical severity, and you will want to be alerted to these immediately to be able to troubleshoot problems. For more information, see [Use global updating to automatically distribute updates to all clients immediately on page 115](#).

The following table lists the Event policies for the agent.

Table 8-3 Event agent policies

Property	Description
Enable immediate uploading of events	Allows the agent to forward events of the severity you specify to the ePolicy Orchestrator server immediately when they occur.
Report any events of severity	Set the severity threshold for what events are forwarded immediately to the ePolicy Orchestrator server. Typically, you will only want to send the most important events to reduce network traffic.
Interval between immediate uploads	To reduce network traffic, especially during a virus outbreak, you may want to set an interval for immediate event uploads.
Maximum events per immediate upload	The maximum total number of individual events to allow in one upload.

Logging

These options allow you to configure policies for how the agent activity is logged.

Table 8-4 Logging agent policies

Property	Description
Enable agent log	Choose whether to Enable agent log. Selecting this checkbox enables logging of agent activity log (agent_<computer>.xml) file.
Message limit	Specify a limit on the number of messages recorded in the agent log. On average, 200 messages results in a file about 16kb in size.
Enable detailed logging	Enable the detailed agent activity log agent_<computer>.log. This detailed log file can grow very large. We recommend enabling detailed logging only when you are troubleshooting a specific communication problem.
Enable remote access to log	Allows administrators to view the log file when not at the client computer. See Viewing the agent activity log files remotely on page 159 .

Repositories

These options allow you to configure policies for how the agent uses software repositories for updating. The list of available repositories includes the master, source, fallback, and any distributed repositories you have configured.

Configuring what repositories the agent uses for updating is covered in detail in another section. See [Configure agent policies to use appropriate distributed repository on page 141](#) for complete details on how to use this policy page.

Updates

These options allow you to configure policies for how the agent performs updates.

Table 8-5 Updating agent policies

Property	Description
Log file	Enter the path (desired location) for the update log file. This file logs update activity.
Run options	Enter the path to any executable you want to run on the client computers after updates are performed, and select whether to run the executable only after successful updates
Allow downgrade of DAT files	Select to allow the agent to update with DATs from the ePolicy Orchestrator repository, even when those DATs are older than the DATs already installed on the client. Checking this option is necessary if you need to "roll back" DATs to a previous version. If you do need to roll back DATs, select this option, perform the rollback, and then deselect this option again so you don't accidentally install old DATs in the future.
Repository Branch Update Selection	If you are using the Previous or Evaluation repository branches for DAT and engine updates, configure which repository branch the agent should update from. By default updating occurs from the Current branch. See About repository branches on page 102 for more information on branches. See Evaluate new DATs and engines before deploying to your whole organization on page 123 for more information on how to update agents from the Evaluation branch.

Set custom proxy server settings

McAfee recommends that you allow agents to use the default proxy server policy settings, if at all possible. This default setting is **Use Internet Explorer Proxy Settings**, which allows the agent use the current proxy server location and credential information currently configured in the Internet Explorer browser installed on that computer.

However, you may need to use ePolicy Orchestrator to configure custom proxy server settings for computers in your network. For example, maybe they use a different browser and don't have Internet Explorer installed.

Use the **Proxy** tab of the agent policy pages to configure agent proxy settings. Select **Don't use proxy** if the computers don't use a proxy and access the Internet directly.

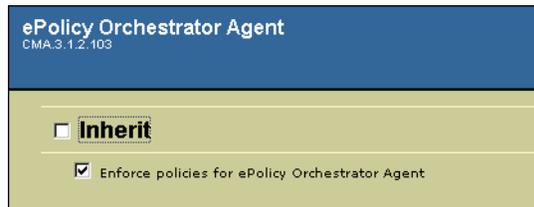
To configure proxy server settings manually for the agent, select **Manually configure the proxy settings** and then enter the appropriate location and login credential information for HTTP and FTP proxies.

Enforcing the agent policy

Once you've configured the policy settings on the ePolicy Orchestrator Agent | Configuration policy pages to your needs, you must select to enforce these policy settings before they are applied. Once you select to enforce the policy settings, they are enforced at the next ASCI.

- 1 On the Policies tab, select ePolicy Orchestrator Agent. The ePolicy Orchestrator Agent policy page appears in the lower details pane.

Figure 8-5 ePolicy Orchestrator Agent policy page



- 2 Deselect Inherit.
- 3 Select Enforce Policies for ePolicy Orchestrator Agent.
- 4 Click Apply to save the current entries.

Viewing properties of the agent and products from the console

You can use the ePolicy Orchestrator console to view current properties for a particular computer. These properties list basic system information, such as operating system, network IP address, RAM and processor speed. They also list properties for the agent and McAfee anti-virus or security products installed on that computer.

Especially when troubleshooting problems, it is a good idea to check computer policies to confirm that policy changes you have made in the console are actually being enforced on the client. The agent sends properties back to the server at each ASCI, allowing you to see system properties on client computers from the ePolicy Orchestrator console.

How are properties different from policies?

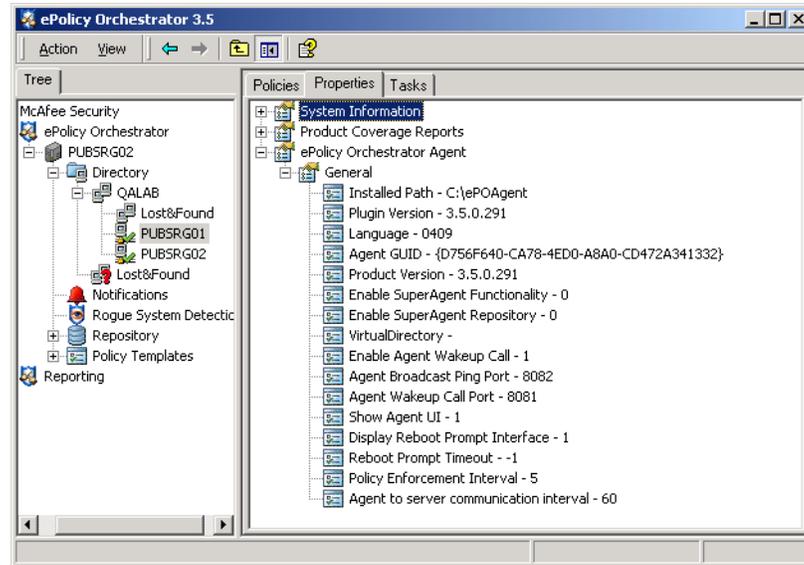
Policies are the rules you configure for the agent or for specific products in the policy pages on the ePolicy Orchestrator server. When the agent enforces these policies on the client computer, they become properties. Properties are the settings that are actually in affect on the client computer.

Viewing agent properties

To view the properties the agent collects for selected computers in the **Directory**:

- 1 In the console tree, select the desired computer.
- 2 In the upper right details pane, click the **Properties** tab to display properties for the selected computer.

Figure 8-6 View Properties for selected computers in the Directory



- Expand property types to view details on specific properties. Properties for the agent are listed under the **ePolicy Orchestrator Agent**.

Checking agent logs

Checking the log files generated by the agent can be a useful way to check on agent status or troubleshoot problems. There are two log files that record agent activity, the agent activity log and the detailed activity log. These log files are located in the agent installation folder, along with the agent executable files.

The Agent activity log is an XML file named `AGENT_<COMPUTER>.XML` where `<COMPUTER>` is the NetBIOS name of the computer where the agent is installed. This log file stores the same messages that appear in the **ePolicy Orchestrator Agent Monitor** dialog box, which can be viewed on the client in the agent user interface. 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.

Detailed agent activity log (`AGENT_<COMPUTER>.LOG`) file.

This log file, intended for troubleshooting purposes only, also stores the same messages that appear in the **ePolicy Orchestrator Agent Monitor** dialog box, plus troubleshooting messages. This file has a 1mb size limit. When this log file reaches 1MB, a backup copy is made (`AGENT_<COMPUTER>_BACKUP.LOG`).

You can configure the level of logging of agent activity. For instructions, see [Using the agent policy pages to set policies on page 153](#).

Viewing the agent activity log files remotely

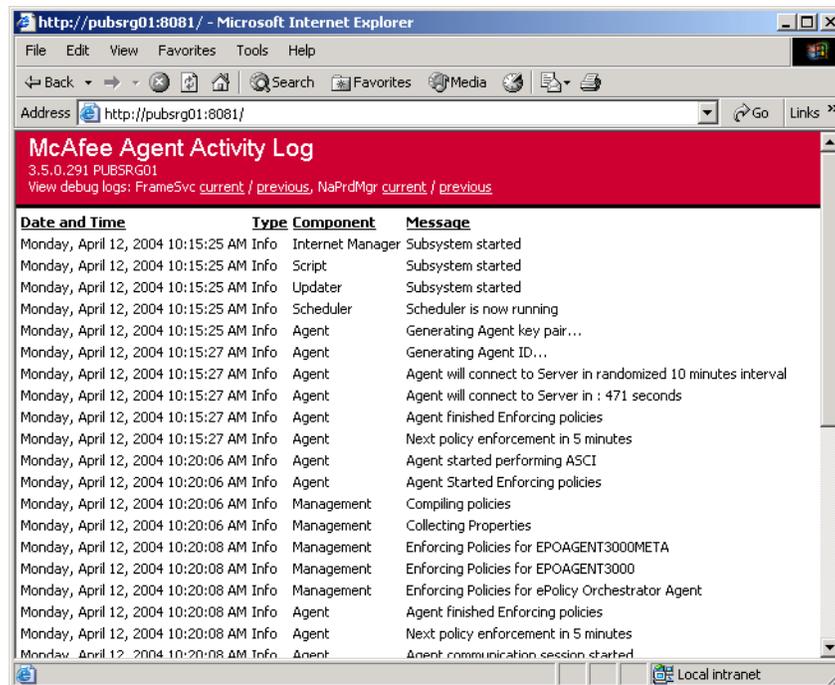
You can view the agent activity log file on the client computer remotely through a web browser. This can be useful when you are at the server and want to check status on the client in real time.

To view the log in a browser, type the computer name and port number the agent uses for wakeup call. You specified the agent wakeup port number when you installed the ePolicy Orchestrator server; the default is 8081. You can view what your agent wakeup call port is for a selected computer by checking the **ePolicy Orchestrator Agent | General** properties. See [Viewing properties of the agent and products from the console on page 158](#).

To view the activity log file remotely:

- 1 Open a web browser and type the computer name and port number used for agent wakeup call. The format should be as follows: `http://MyComputer:8081/`

Figure 8-7 Viewing the agent activity log remotely through a Web browser



- 2 To view the detailed agent activity log file, click **current** to view either the FrameSvc.exe or NaPrdMgr.exe logs 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, it is possible to use the ePolicy Orchestrator console to set the agent policies to disable remote viewing of the log file. If you can't view the log remotely, try checking that the **Enable remote access to log** option is selected on the **Logging** tab of the agent policy pages. For details, see [Using the agent policy pages to set policies on page 153](#).

Working with the agent from the client computer

You can control every aspect of the agent functionality from the ePolicy Orchestrator console on the ePolicy Orchestrator server. You can also perform selected tasks from the computer where the agent is installed.

This section covers some of these tasks:

- Using the agent user interface on the client computer
- Command Agent command-line options.

Using the agent user interface on the client computer

If you can get to the client computer where the agent is installed, you can view and manage some aspects of the agent functionality through the agent interface. The interface is accessible by right-clicking the agent icon in the system tray on the client computer.

Figure 8-8 Right-click the Agent icon in the system tray to expose menu options



Note that this is only available if you have changed the agent policy by selecting the Show Agent tray icon option from the agent policy page ([Using the agent policy pages to set policies on page 153](#)). This option is not selected by default.

You can use the agent system tray icon to perform selected agent tasks locally on client computers.

You can access the following dialog boxes and commands from the agent system tray icon.

- Run an update task with the Update Now command.
- Using the Agent Status Monitor to view logs and do stuff.
- View agent settings.
- View the version number of the agent and installed security products.

Run an update task with the Update Now command

Select **Update Now** to have the agent perform 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, and virus definition (DAT) files.

Using the Agent Status Monitor to view logs and do stuff

Right-click the agent system tray icon and select **Status Monitor** to open the agent Status Monitor. The Status window shows whether the agent is running and displays recent activity in the activity log window. This is the same XML activity log that you can view from the server through a Web browser.

You can also use the agent Status Monitor to perform selected agent tasks:

Select the **Status Monitor** to view the Agent activity log in real time:

Table 8-6 Agent Status Monitor options

Task Option	Description
Collect and Send Props	Send full properties to the server. This updates the properties displayed in the console. See Viewing properties of the agent and products from the console on page 158 .
Send Events	Immediately sends events to the server.
Check New Policies	Agent calls into the server to see if any policies have changed. If so, it downloads the new policy settings.
Enforce Policies	Enforces policies set on the server locally on the client computer.
Agent Settings	View selected agent settings.
Save contents	Saves the current contents of the agent activity log file.

View agent settings

Right-click the agent system tray icon and select **Settings** to view selected agent settings, such as the unique agent ID, the user name of the currently logged in user, the policy enforcement interval and ASCII.

You cannot change these settings here. To make changes to any of these settings, change the agent policies from the agent policy pages.

View the version number of the agent and installed security products

Right-click the agent system tray icon and select **About** to view the version information for the McAfee software installed on the client computer. This can be very useful when troubleshooting problems with installing new agent versions or confirming that the version of the agent actually installed is the same as the version displayed in the agent properties. In addition, the **About** dialog box displays the version information for other McAfee products installed on the client computer, such as VirusScan Enterprise.

Command Agent command-line options

You can use the Command Agent (CMDAGENT.EXE) to perform selected agent tasks remotely. CMDAGENT.EXE is on the client computer when the agent is installed. You can perform these same tasks locally on client computers using this program or the agent system tray icon.

The CMDAGENT.EXE file is located in the agent installation folder, which by default is:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK
```

Table 8-7 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.

9

Managing Product Policies and Running Client Tasks

Manage anti-virus and security products deployed in your network

Managing products installed on client computers in your network centrally from the ePolicy product policies is an essential feature of ePolicy Orchestrator. Policies are the configuration settings for the agent and each product that can be managed via ePolicy Orchestrator. These settings determine how the product behaves on client computers. For example, you can specify which types of files that you want VirusScan Enterprise 7.0 to scan or ignore.

You can set these before deployment, or you can use the default policies and modify them after deployment.

What is in this chapter

- [About policies and ePolicy Orchestrator.](#)
- [Using policy pages to manage product settings.](#)
- [Remove policy pages for unused products from the Repository](#)
- [Copying, exporting, and importing policies](#)
- [Reset the default policy settings](#)
- [Configure client on-demand scans and update tasks](#)

About policies and ePolicy Orchestrator

A policy is a set of software configuration settings that you configure through the ePolicy Orchestrator console and then enforce in software on your clients. Policies determine how the software on the client behaves.

Policy configuration options are different for each product. The interface in the ePolicy Orchestrator console for centrally configuring these policies is the Network Associates Package (NAP) pages. There is a separate NAP for each product you are managing through ePolicy Orchestrator. To be able to manage these products, you must first add the NAP policy pages for the appropriate product and version to the master repository. See [Check in NAP files to manage new products on page 93](#).

The set of options differs depending on the product being managed. For example, the policies for VirusScan Enterprise include the configuration options for the On-Access Scanner, the On-Demand Scanner, updating, how much of the interface to expose on the client computer, and others. Each of these configuration settings are stored within a policy. In short, a policy should reflect the desired configuration of the target system.

Policy inheritance

Policy inheritance determines whether the policy settings for any one console tree item in the **Directory** are taken from the item directly above it. All policy pages come with a set of default policy settings. All items under the **Directory** inherit these settings by default. You can modify the settings as needed for each site or group or even for each computer, then apply the new settings to all groups and computers underneath.

Each policy page contains an **Inherit** checkbox. If this box is deselected, the console tree item to which this policy page applies no longer inherits the settings for this page from the console tree item above it.

How policies are enforced on the client computer

When you change policies using the ePolicy Orchestrator consoles, those changes are added to the product configuration on the actual client computer the next time a client calls into the ePolicy Orchestrator server. This length of time is determined by how you configured the agent-to-server communication interval (ASCI), which is 1 hour by default. So, changing a policy in the ePolicy Orchestrator console will take effect on the client within an hour at the latest.

Once the policy is sent to the client at the next ASCI communication, the agent then enforces that policy locally in the client software at a regular interval. This enforcement interval is determined by the **Policy enforcement interval** setting on the agent NAP file; this is 5 minutes by default.

How new policy settings are enforced on client computers varies slightly depending on whether you are managing McAfee or Norton AntiVirus products. Policies for McAfee products are enforced immediately on the policy enforcement interval and the agent-to-server communication interval (ASCI). There is a delay of up to three minutes after the policy enforcement interval and the agent-to-server communication interval (ASCI), before policies for Norton AntiVirus products are enforced. This is because 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. Norton AntiVirus products read the GRC.DAT file approximately every three minutes.

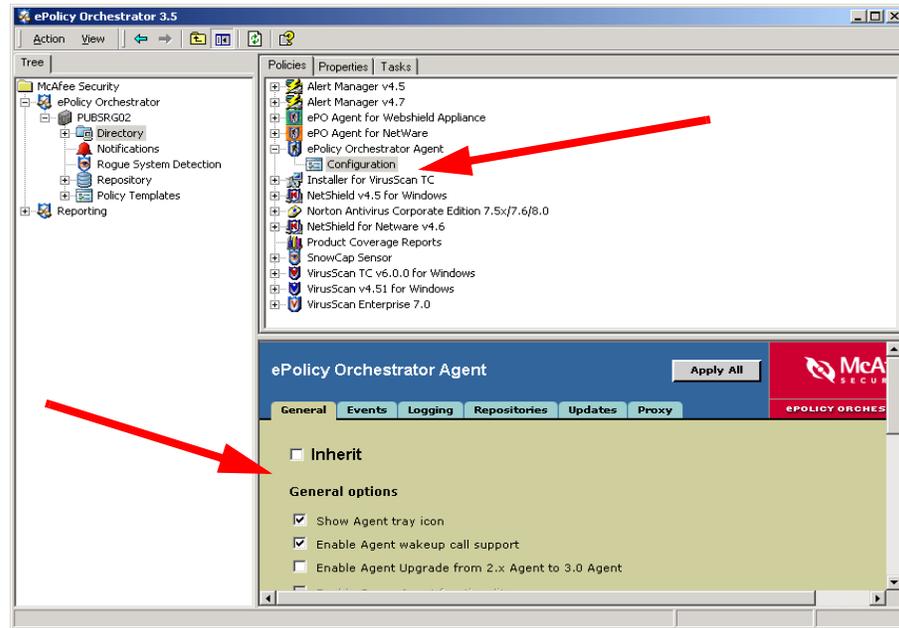
Using policy pages to manage product settings

Use ePolicy Orchestrator policy pages to manage configuration settings for security products installed and running on client computers in your network.

In addition to managing policy settings, you can also create, configure, and schedule client tasks, such as anti-virus on-demand scans or product update tasks. See [Configure client on-demand scans and update tasks on page 174](#) for more information about how to use ePolicy Orchestrator to run client tasks.

ePolicy Orchestrator installs with a set of policy pages, or Network Associates Package (NAP) files. These include the latest releases of common anti-virus and security products, the ePolicy Orchestrator agent, and others. The policy pages allow you to manage policies for those products through the ePolicy Orchestrator console. Any time you change a policy, that change is picked up by the client software the next time the agent calls in to the ePolicy Orchestrator server.

Figure 9-1 The Policies tab shows available policy pages (NAP) for products. The details pane shows policy options for the selected policy page



You can set product policies at any level of your **Directory**, such as at the site or group level or even for individual computers. The **Policies** tab in the upper details pane shows the policies for the currently selected branch in the **Directory**.

List of complete NAP files installed with the ePolicy Orchestrator server

- Alert Manager 4.5
- Alert Manager 4.7
- ePO Agent for WebShield Appliance
- ePO Agent for NetWare
- ePolicy Orchestrator Agent
- Installer for VirusScan TC
- NetShield 4.5 for Windows
- Norton Antivirus Corporate Edition 7.5x/7.6/8.0
- NetShield for NetWare 4.6
- System Compliance Profiler 1.1
- Rogue System Sensor
- VirusScan TC 6.0 for Windows
- VirusScan 4.5.1 for Windows
- VirusScan Enterprise 7.0
- VirusScan Enterprise 7.1
- VirusScan Enterprise 8.0

See the appropriate *Configuration Guide* for complete details on all policy options for major McAfee anti-virus and security products like VirusScan Enterprise, Desktop Firewall, and GroupShield. These configuration guides are available on your product CD or on the McAfee web site. Furthermore, many of the configuration options in the policy pages simply reflect what you can configure in the product interface; see the *Product Guide* for each product for additional information on the features.

Viewing the version number of policy pages

You must use the appropriate version of the policy pages NAP file to set policies for a product.

You cannot manage policies for other versions of the product with a particular NAP file. For example, to set policies for VirusScan Enterprise 8.0i, you must use the 8.0i NAP file.



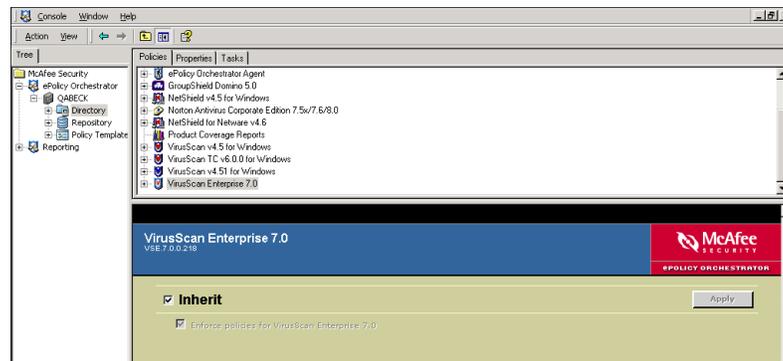
Remove NAP files from the ePolicy Orchestrator server for older products that you no longer manage. ePolicy Orchestrator allows you to check in different NAP files for different versions of the same product, such as VirusScan Enterprise 7.0, 7.1, and 8.0i. It can get confusing trying to keep track of which policies you're supposed to set for which products in which parts of your **Directory**.

For example, if you migrate all of your workstations and servers to VirusScan Enterprise 8.0i, delete the old NAP files for VirusScan Enterprise 7.0 and 7.1.

To determine the version number of policy (.NAP) pages that are in the **Repository**:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 In the console tree under **ePolicy Orchestrator | <SERVER>**, select **Directory** then click the **Policies** tab in the upper details pane.
- 3 Select the desired product (for example, **VirusScan Enterprise 7.0**). The corresponding policy page appears in the lower details pane.
- 4 The version number (for example, **VSE.7.0.0.216**) appears below the product name.

Figure 9-2 Version number of policy pages

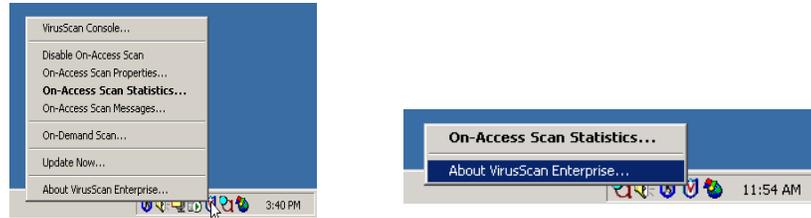


Policy Change Example: change default policies for VirusScan Enterprise

To illustrate changing product policies, this section shows how to modify policies for VirusScan Enterprise 7.x to hide some of the product interface on the client computer. By default, VirusScan Enterprise installs with full interface options available on the client. You may want to hide some of these options to prevent some users from easily changing settings or purposefully or accidentally disabling features.

To demonstrate how to do this, we'll use a simple example: changing the policies for workstations to install VirusScan Enterprise 7.1 with minimal user interface. Servers will keep the default policy, which is to display the full interface. [Figure 9-3](#) demonstrates the difference.

Figure 9-3 VirusScan Enterprise server and workstation interface

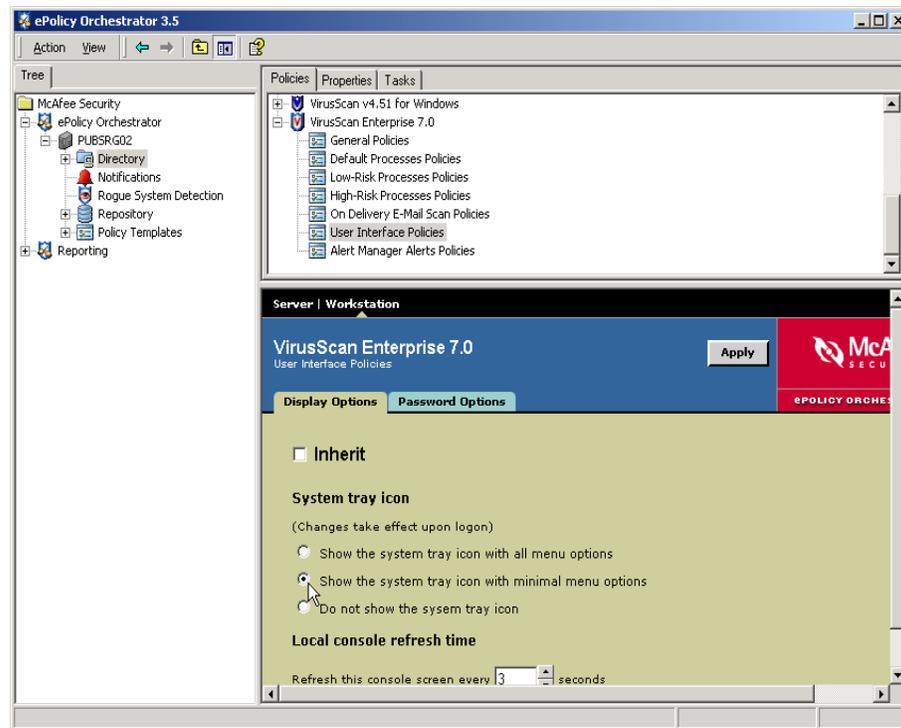


We'll change the policies for all workstation computers to hide most of the interface. For servers, we will leave the default policy, which installs VirusScan Enterprise with the full menu options available in the system tray. Also, in this example we'll make the change at the **Directory** level, which inherits to all sites, groups and computers in your **Directory**.

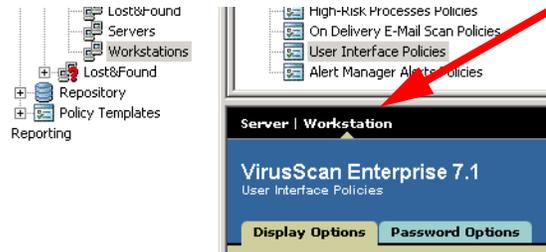
To change the VirusScan Enterprise policies for workstations:

- 1 From the left-tree pane console tree, click the **Directory**.
- 2 In the right-hand details pane, click the **Policies** tab and select **VirusScan Enterprise 7.1** to expand policies.
- 3 Select the **User Interface Policies** policy page.
- 4 Deselect **Inherit** to enable user interface policy options.
- 5 Select **Show the system tray icon with minimal menu options**.

Figure 9-4 Use the VirusScan Enterprise policy pages to change workstation policy to only display a limited interface.



- 6 Make sure the operating system switch is set to **Workstation**.

Figure 9-5 Make sure the Server / Workstation switch is set correctly

The **Server | Workstation** switch allows you to set separate policies for servers and workstations without using **Directory** groups. ePolicy Orchestrator detects the operating system on the client computer and applies the right policy.

- 7 Click **Apply** to save the changes.

The policy change takes effect on clients the next time the client computer calls in to the ePolicy Orchestrator server.

Once again, this example only serves to illustrate how to use the ePolicy Orchestrator console interface to change policies. For complete information on changing product policies, see the appropriate *Configuration Guide* for that product, or consult the regular product documentation.

Remove policy pages for unused products from the Repository

Use this procedure to remove policy pages that you no longer want to manage via ePolicy Orchestrator. You may need to do this, for example, if you upgrade to a newer version of a client product, such as upgrading to VirusScan Enterprise 8.0i from an older version, such as VirusScan Enterprise 7.1. Having extra NAP files in your policy pages can clutter your ePolicy Orchestrator console. Having multiple NAP files for different versions of the same product, such as VirusScan Enterprise 8.0.i, can be confusing. Remove the NAP file for the older version so you don't set policies for the wrong product version by accident!

Keep a neat console by deleting NAP files for any products you are not managing with ePolicy Orchestrator.

To delete a NAP file:

- 1 From the ePolicy Orchestrator Tree, locate the product NAP file policy pages to delete by selecting **Repository | Managed Products | <Platform> | <Product Name>**.

Depending on what you are removing, you may remove a NAP at the product name or product version level. If you have NAP files for multiple versions of the same product, each is saved in the version subfolder beneath the product folder. Be sure to select the right level to remove only the correct product and version.

- 2 Right-click desired **Managed Products** subfolder and select **Remove**. The Remove option is only available if there is in fact a NAP saved in the folder.

- 3 Click **Yes** when asked whether you want to remove the selected software.
- 4 Refresh the ePolicy Orchestrator console by right-clicking the **Directory** node and selecting **Refresh**.

The policy pages are removed from the list of available product policies on the **Policies** tab of the details pane. In addition, removing the policy pages for a specific product version removes any client tasks specific to that product from the list of available client tasks.

Copying, exporting, and importing policies

Setting the right agent or product policies to best suit your network can be a time-consuming process involving experimentation and trial and error. Once you get them right, you don't want to have to re-create them if you don't need to. This section contains information on how you re-use existing policies you have spent time perfecting in other parts of your **Directory**.

What's in this section

- [Copying policy settings from one Directory node to another](#)
- [Exporting policies to a file or policy template](#)
- [Importing policies from a file or policy template](#)

Copying policy settings from one Directory node to another

You can copy and paste policy settings between branches in the **Directory**. You may spend time working in the policy pages customizing policy settings for the agent or for VirusScan Enterprise for a particular group or site. These policies may apply to another site or group. Rather than re-enter the policy changes on the second node, you can copy the customized policy and paste it into the new node.

If you may want to copy policies and paste them to several other **Directory** branches, you can use the procedure in this section. However, in that case, you may find it easier to export the customized policies once to a file or policy template and then import them into target branches.



You must be a global or site administrator to copy or paste policies.

When you paste policy settings to another console tree item, inheritance for that console tree item is turned off, but remains unchanged for items underneath it. Therefore, console tree items that have inheritance turned on, below the one to which policy settings are pasted, will inherit the new settings during the next agent-to-server communication.

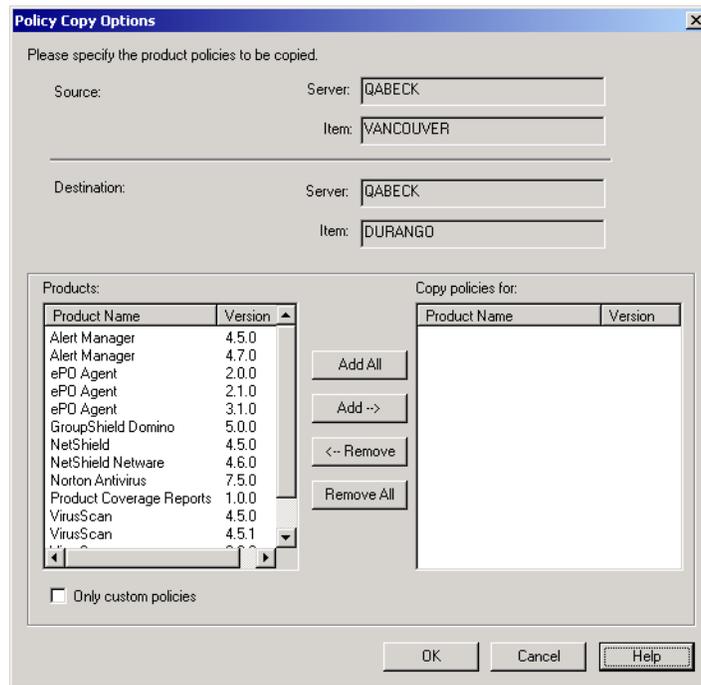
How to copy policies from one Directory node to another

To copy and paste policy settings from one branch to another:

- 1 Log on to the desired ePolicy Orchestrator server.

- 2 Right-click the desired branch in the **Directory** at which you want to copy the policies and select **Policy | Copy**.
- 3 Locate the target branch in the **Directory** to which you want to paste the policies. This can be any site, group or individual computer in the **Directory**.
- 4 When you find the target, right-click it and select **Policy | Paste**. The **Policy Copy Options** dialog box appears.

Figure 9-6 Policy Copy Options dialog box



- 5 Verify that the **Server** and **Item** for the **Source** and **Destination** are correct before you continue.
- 6 Select policies for specific products that you want to paste to the target branch. To do this, click the product policy in the **Products** list and then click **Add** to move it to the **Copy policies for** list.
- 7 To copy only those policy settings that differ from the inherited settings, select **Only custom policies**. Otherwise, all policy settings are copied.
- 8 Click **OK** when done.

Exporting policies to a file or policy template

You can export and import your custom product-policy settings to and from policy files or policy templates. These allow you to create a customized set of policy settings that you can reuse in other parts of your **Directory**. They also allow you to define enterprise-wide policy settings that can be easily applied to any ePolicy Orchestrator server.

Whether other ePolicy Orchestrator administrators need access to these settings affects whether you choose policy files or policy templates. Since the procedure for exporting is similar, both options are covered together in this section.

About exporting policies to a file

Exporting policies to a file saves the policy information to an external file, and the exported policy file is not directly viewable in the ePolicy Orchestrator console. Global administrators can send the policy file to local site administrators who can import it into their portions of the **Directory**.

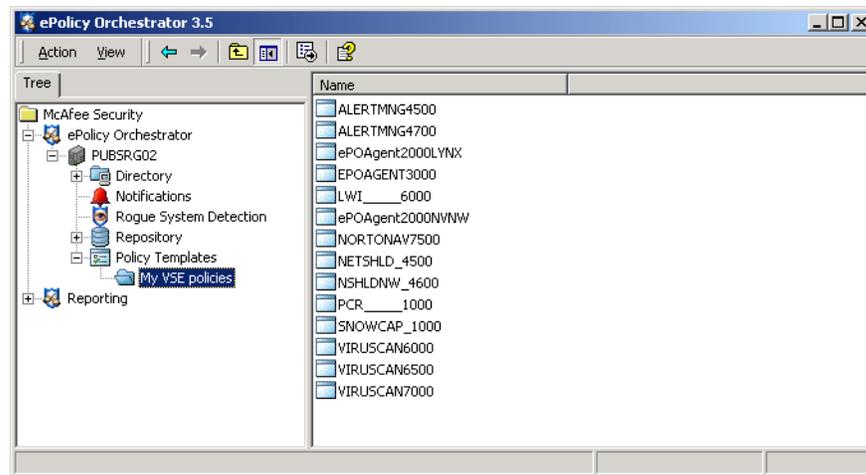
You can also import policies from a file on another ePolicy Orchestrator server. For example, if you have an evaluation deployment of ePolicy Orchestrator in a test network, you can test customized policies in the test deployment. Exported policies can be imported on your production server. Policy files are also useful for backing up customized policy settings; if policies are changed accidentally or you need to re-install the ePolicy Orchestrator server for whatever reason, you can import customized policies rather than have to re-create them from scratch.

Policy files cannot be accessed via the ePolicy Orchestrator console or remote consoles. They must be saved and managed outside of the console interface.

About exporting policies to a policy template

Saving customized policies in a policy template saves the template to the ePolicy Orchestrator database. The policy template is available in the **Policy Templates** section of the ePolicy Orchestrator console, and global and local site administrators can import the settings from the policy template into any branch of the **Directory**.

Figure 9-7 Export customized policies to a policy template in the database



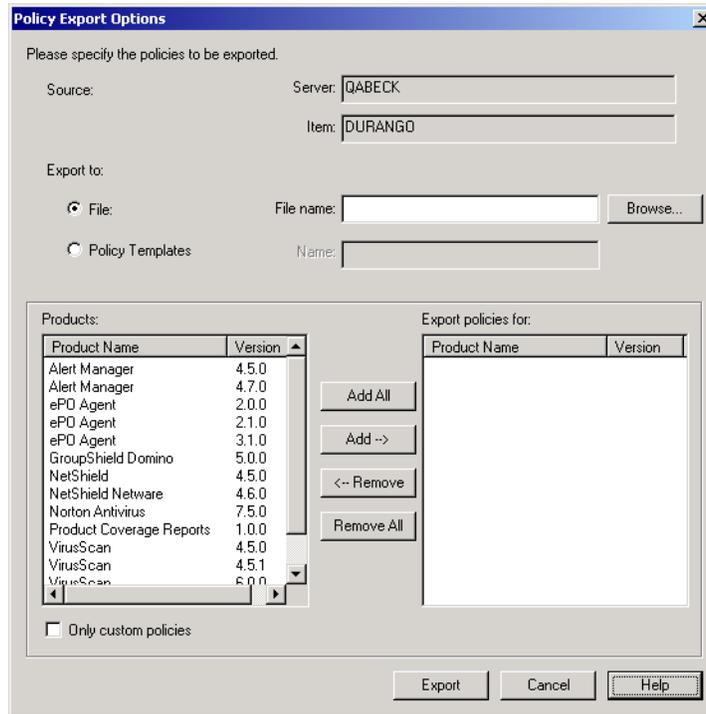
Since policy templates are saved in the database, you cannot use them on other ePolicy Orchestrator servers. They are therefore also not effective ways for backing up customized policies; they will be lost if you need to uninstall the ePolicy Orchestrator server.

To export policies to a file or policy template

- 1 Locate the branch in the ePolicy Orchestrator **Directory** from which you want to export policies.

- 2 When you have found the branch, right-click it and select **Policy | Export**. The **Policy Export Options** dialog box appears.

Figure 9-8 Policy Export Options dialog box



- 3 Under **Export to**, select **File** or **Policy Templates**.
- 4 Type a file name or template name, depending on what type you are exporting to.
- 5 Select policies for specific products that you want to export. To do this, click the product policy in the **Products** list and then click **Add** to move it to the **Copy policies for** list.
- 6 Select **Only custom policies** to export only those policy settings that differ from the inherited settings.
- 7 Click **Export** to save the policies.

If you exported to a file, the file is saved to the hard drive. If you export it to a policy template, it is saved to the database.

Importing policies from a file or policy template

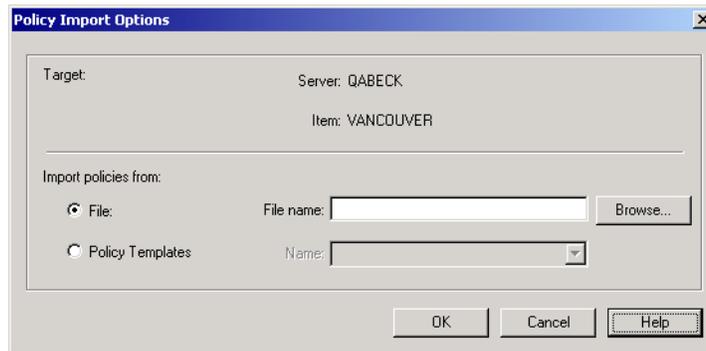
Use this procedure to import policies to a branch of the **Directory**, either from an exported file or a policy template in the database. You must be a global or site administrator to import and export policies.

To import policy settings for selected products via a policy template:

- 1 Locate the branch in the ePolicy Orchestrator console **Directory** tree into which you want to import the policies.
- 2 When you have found the branch, right-click it and select **Policy | Import**.

- 3 Click **OK** at the warning dialog box.

Figure 9-9 Policy Import Options dialog box



- 4 In the **Policy Import Options** dialog box under **Import policies from**, select **File** or **Policy Template**. If you selected **File**, type the location of the policy file or browse to it and select it. If you selected **Policy Template**, select a template from the drop-down list displaying all policy templates currently saved in the database.
- 5 Click **OK**. Wait a moment while the policy is imported.

Once completed, you can confirm that the policies imported by checking the appropriate policy pages for the products or products.

Reset the default policy settings

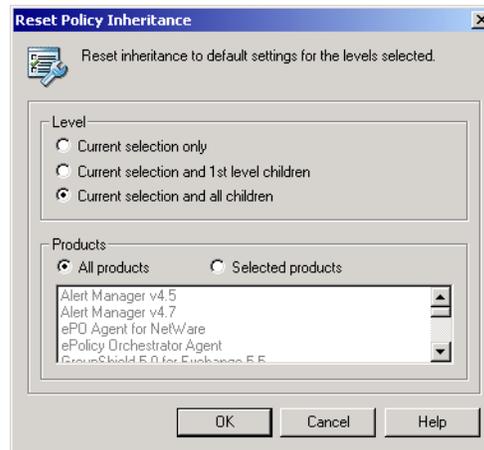
You may need to reset policies that you have changed. The ePolicy Orchestrator **Directory** allows you to easily reset policies for all or selected products at any level in the **Directory**.

You can also restore the default policy settings on any policy page by selecting **Inherit**, then clicking **Apply**.

To reset policies for selected products to their original settings:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 Right-click the desired **Directory**, **<SITE>**, **<GROUP>**, or **<COMPUTER>**, then select **Policy | Reset Inheritance**. The **Reset Policy Inheritance** dialog box appears.

Figure 9-10 Reset Policy Inheritance dialog box



- 3 Select the **Level** at which you want to restore the default policy settings.
- 4 Specify whether you want to reset the default settings on **All products** or **Selected products**.
- 5 If you choose **Selected products**, select the desired products from the **Products** list.
- 6 Click **OK**. Changes take effect during the next agent-to-server communication

Configure client on-demand scans and update tasks

In addition to allowing you to customize policies for products deployed in your network using the policy pages, the ePolicy Orchestrator console also allows you to configure client tasks that run on the client computers. These are the same tasks you might configure to run through the product interface; ePolicy Orchestrator console allows you to create, schedule and configure them all from the console.

You can schedule tasks on the ePolicy Orchestrator server that run on specified client computers. You can define tasks to run on the computers of the entire **Directory**, of a specific site or group, or on individual computers. Before creating and scheduling tasks, you must understand how task inheritance works in ePolicy Orchestrator.

This section contains the following topics:

- [About running client tasks in ePolicy Orchestrator.](#)
- [Creating a scheduled client on-demand scan task for VirusScan Enterprise.](#)
- [Client task scheduling options.](#)
- [Changing client tasks.](#)
- [Deleting client tasks.](#)

About running client tasks in ePolicy Orchestrator

What policy pages, or NAP files, you have installed on your ePolicy Orchestrator server, determine which tasks are available. For example, the VirusScan Enterprise 7.0 on-demand scan task is available because that NAP file is automatically loaded when you install the ePolicy Orchestrator. If you delete any of the installed NAP files, you will remove any tasks associated with that product.

Typically, the tasks are product-specific and relate either to:

- Running on-demand anti-virus scans. These are for anti-virus products like VirusScan Enterprise 7.x, NetShield 4.5 for Windows NT, and VirusScan 4.5.1.
- Running product-specific update and upgrade tasks for those products that don't use the integrated Common Management Agent (CMA). The products tend to be non-Windows products or older products built before CMA.

Client tasks covered in other parts of this guide

Some client tasks that deal with other aspects of ePolicy Orchestrator are covered in other sections of this guide. These are

- The **ePolicy Orchestrator Agent Update** task used to update DATs and engines for products that use the CMA updating architecture. See [Create and schedule a daily DAT and engine client update task on page 118](#).
- The default product deployment task, used to install products on client computers. See [Use the deployment task to install products on clients on page 94](#).
- Agent wakeup task. Used when you want to schedule the ePolicy Orchestrator server to wakeup agents at regular intervals using an ICMP PING. See [Sending manual agent wakeup calls on page 150](#).

Tasks inherit through the Directory like policies do

Tasks created for a level of the **Directory** inherit by default to all children below the level where you created the task. Task inheritance determines whether the client task settings for any one console tree item in the **Directory** are taken from the item directly above it. When you turn off inheritance for an item, tasks scheduled for the item above it are ignored and the new task is scheduled for all items below it, if they items below have inheritance turned on.

Which tasks do I need and when should I schedule them?

Which specific tasks you need to create will depend on several factors. Which tasks you create depends on which products you have deployed in your network and are managing their policies with ePolicy Orchestrator. When you want to schedule each task depends on how you want to balance network performance when the tasks run. For example, you may want to schedule a VirusScan Enterprise on-demand scan task on a critical e-commerce web server for the middle of the night local time, and lower the CPU usage throttle to 20% to minimize server performance.

See [Things to do on a daily or weekly basis to stay prepared on page 270](#) for ideas on what kinds of tasks you can and should schedule to run on a regular basis.

Creating a scheduled client on-demand scan task for VirusScan Enterprise

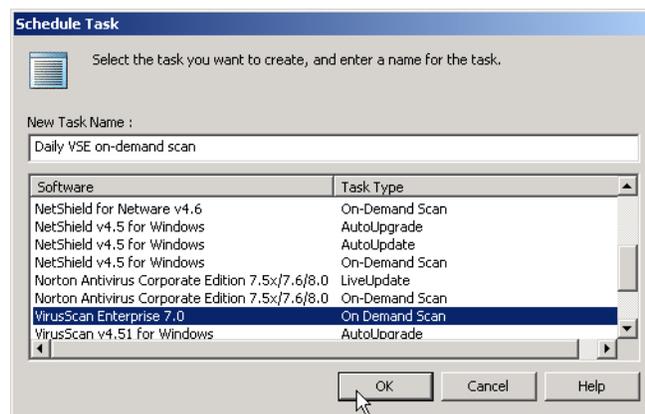
You can create tasks using any of the default task types available in the ePolicy Orchestrator **Schedule Task** dialog box. Again, what task types that are available depend on what product NAP files are in the software repository. The process for creating and scheduling client tasks is similar, regardless of which type of task you create. This section covers creating a scheduled on-demand scan task for VirusScan Enterprise to illustrate the basic procedure for creating tasks. Using on-demand anti-virus scans is an important part of your anti-virus strategy, and you will likely need to create and schedule this task through ePolicy Orchestrator if you have VirusScan Enterprise deployed.

This example creates the task at the **Directory** level so that it takes effect throughout the entire **Directory**. You can create tasks at lower levels in your **Directory** if it only applies to specific sites or groups.

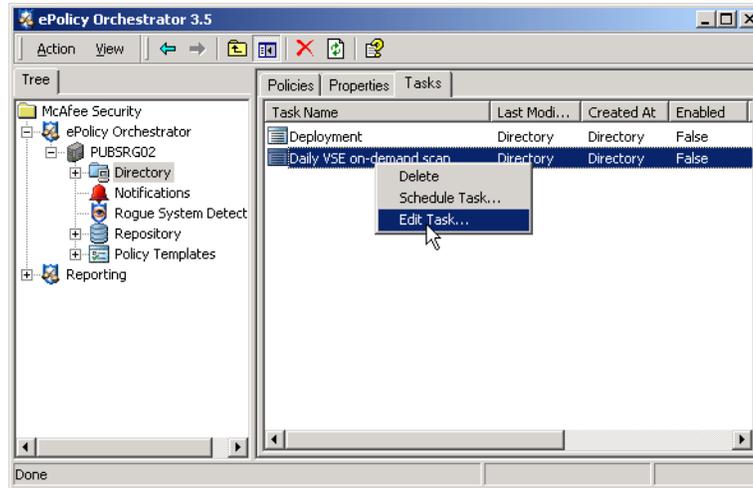
To create a client on-demand scan task for VirusScan Enterprise:

- 1 In the left pane of the ePolicy Orchestrator console, select the **Directory** root and select **Schedule Task**.
- 2 In the **Schedule Task** dialog box, type a descriptive name for the task you are creating, such as *Daily VirusScan Enterprise on-demand scan*. Select **VirusScan Enterprise On Demand Scan** for the software and task type.

Figure 9-11 Create and name the new VirusScan Enterprise on-demand scan task



- 3 Click **OK** to add the new task.
- 4 Refresh the ePolicy Orchestrator console, either by right-clicking the **Directory** node and selecting **Refresh**, or by clicking 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 in the task list and select **Edit Task**.

Figure 9-12 Edit the newly created task to run immediately

- 6 On the **Task** tab of the ePolicy Orchestrator Scheduler dialog box, deselect **Inherit** to enable task options.
- 7 Select **Enable**. The task will not run unless you enable it.
- 8 Click **Settings** to configure the on-demand scan settings.

This is the step that is unique to each task type. In the case of a VirusScan Enterprise on-demand scan, the settings page includes anti-virus scanning configuration options, such as what local drives to scan, what kind of files to scan or not scan, and what to do if viruses are detected. Details on configuring a specific type of task are not covered here. For details on task settings, see the product documentation, such as the VirusScan Enterprise Product Guide. For major products, see the Configuration Guide for ePolicy Orchestrator 3.5 for the product.

- 9 Click **OK** when you are done configuring the scan task settings.
- 10 On the ePolicy Orchestrator Scheduler dialog box, click the **Schedule** tab and deselect **Inherit** to enable scheduling options.
- 11 Select **Daily** and specify a **Start Time**. Since on-demand scans are processor-intensive and may affect system performance on the client computer, you might consider scheduling it to run during non-business hours, such as late at night. Also, if you have other scheduled tasks, such as DAT update tasks, coordinate schedules appropriately. For example, you can schedule your on-demand scan to start after a DAT update is complete to ensure the scan is using the latest DATs.

There are many options for scheduling a client task. See [Client task scheduling options on page 178](#) for details.

- 12 Click **OK** when finished modifying schedule and task setting information to save the task.

The new On Demand scan appears in the list of created... tasks. Make sure that it is enabled

Client task scheduling options

There are many options when scheduling a client task. The table below lists them and includes some suggestions on when you might consider using a specific option.

Table 9-1 Client task scheduling options

Scheduling option	Description
Stop the task if it runs for	On the Schedule Settings section of the Task tab. To limit the length of time the task can run before it is cancelled.
Schedule Task	Set the type of schedule, such as daily, weekly, or when the client computer is turned on.
Start Time	The time of day when the task should begin running.
GMT Time or Local Time	Select local time to run the task at the scheduled interval at the client computer system time. This is useful for scheduling processor-intensive tasks, such as on-demand anti-virus scans, to run during non-business hours. Selecting GMT will run the task when the Start Time occurs GMT (Greenwich Mean Time). Using this option will cause the task to run at the same time for all your clients, regardless of the local system time on the client.
Enable Randomization	The task does not run at exactly the specified start time. Instead, it starts after a random, specified time.
Run missed task	Ensures that the task is started if the client computer is shutdown or otherwise not available during the scheduled start time. Selecting this option runs the task the next time the client computer becomes available.
Delay missed task by	On the Advanced Schedule Options dialog box. When running missed tasks, selecting this option sets a delay after the client computer becomes available before the missed task runs.
Start Date / End Date	On the Advanced Schedule Options dialog box. Enter start and end dates if you only want the task to run within a specific time window of a few days or weeks. This may be a good idea if you only need the task to run temporarily and then never more.
Repeat Task	On the Advanced Schedule Options dialog box. Use this option to run a task multiple times in the same day. To do this, check Repeat Task and then set the repeat interval appropriately. Typically, you might do this to run a client update task several times a day, especially if there are lots of new viruses appearing in the wild. You can also schedule the task to repeat during other intervals, such as weekly or monthly.

Changing client tasks

You can edit settings or schedule information for any task that you have already created and configured.

To edit a client task configuration:

- 1 Locate the branch in the ePolicy Orchestrator console **Directory** at which you want to change the task information.
- 2 In the right-hand upper details pane, click the **Tasks** tab.
- 3 Right-click the task in the list of available tasks that you want to edit and select **Edit task**.
- 4 Deselect **Inherit** to enable configuration options.

- 5 Edit any setting or schedule information as needed. See the example in [Creating a scheduled client on-demand scan task for VirusScan Enterprise on page 176](#) for details.
- 6 Click **Apply** and **OK** to save the edited task.

The changes to the client software will be picked up the next time the agents call in to the ePolicy Orchestrator server.

Deleting client tasks

You can delete any client task you have created that you no longer want to run on your client computers. This could be a one-off client task you scheduled to Run Once and is now complete. It could also be an on-demand scan or update task for an older product you are no longer using. For example, you may stop using VirusScan 4.5.1 on client computers and NetShield 4.5 on servers after you have migrated both to the latest version of VirusScan Enterprise. In this case, you could delete any client tasks you had created for NetShield or VirusScan 4.5.1.

You cannot delete the default deployment task used to install anti-virus and security products through the ePolicy Orchestrator console. See [Use the deployment task to install products on clients on page 94](#).

To delete client tasks you have created but no longer need:

- 1 Locate the branch in the ePolicy Orchestrator console **Directory** at which you created the task. You can only delete tasks at the same level at which you created them.
- 2 In the right-hand upper details pane, click the **Tasks** tab.
- 3 Right-click the task in the list of available tasks that you want to edit and select **Delete**.
- 4 Click **Yes** at the warning dialog box.

10

Determining Compliance

Limit vulnerabilities by maintaining minimum software versions, patches and service packs

Most of the virus and worm outbreaks today attack known vulnerabilities in common operating systems. Usually, these are vulnerabilities for which the operating system makers have released patches or Service Packs to provide protection against. However, it has been a very difficult task for administrators to keep all of their computers up-to-date with such patches and Service Packs, and even harder still to find computers on the network which are not compliant with these.

Similar problems can occur in large networks with keeping all computers compliant with anti-virus software, virus definition (dat) files, engine versions.

ePolicy Orchestrator 3.5 comes with several new features that help you ensure that the managed computers in your environment are compliant with your security policy:

- System Compliance Profiler
- Compliance Check server task
- ePolicy Orchestrator Notification

System Compliance Profiler

System Compliance Profiler's features include:

- 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").
- Complete integration with McAfee ePolicy Orchestrator, for centralized administration and host-based compliance reporting.
- 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 computers to determine whether they comply with policies that you set up. Policies consist of rules, each of which tells the software to look for a specific file, registry key, patch, or service on scanned computers. Computers that meet all of your rule criteria are in compliance with your policies. Computers that do not meet rule criteria have rule violations.

You can use System Compliance Profiler to create graphical and tabular reports that show which network computers do and do not comply with company policies.

System Compliance Profiler integrates into the McAfee ePolicy Orchestrator management software. This means that you use ePolicy Orchestrator to configure and deploy the software.

System Compliance Profiler works by installing remote scanning software on each computer that you want to monitor. This scanning software periodically scans for files, registry keys, patches, and services, and then relays the information it collects back to ePolicy Orchestrator. Once the software finishes its scans and reports back, you can use System Compliance Profiler and ePolicy Orchestrator to run reports based on the collected data.

Compliance Check server task

The Compliance Check server task allows you to schedule a task that can run one or more compliance rules that check your managed computers for compliance with specified:

- DAT version.
- Engine version.
- Agent version.
- VirusScan version.

The ability to create multiple rules allows you to configure separate rules (there for separate standards of compliance) for computers with different operating system and for computers that have communicated with the ePolicy Orchestrator server within a given number of days.

For each rule you must also define a threshold that, when crossed, an event is generated and sent to ePolicy Orchestrator Notification. You can define the threshold as a percentage of target computers being non-compliant, and/or a specific number of the target computers being non-compliant. For example, you can define the rule to send an event when either 15% of the target computers are not compliant with the rule, or when 50 computers are not compliant.



You must have a rule configured in ePolicy Orchestrator Notification to send an event when a **Non-compliant computer detected** event is received from the **ePO server**.

To create a compliance task and the rules associated with it:

- 1 Log on to the ePolicy Orchestrator server.
- 2 Select the ePolicy Orchestrator server in the console tree, then select the **Scheduled Tasks** tab in the details pane.

- 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 **Advanced schedule options**, configure the **Start time**, **Start date**, **End date** (if necessary), and how often you want to repeat the task if it fails.
- 10 Under **Advanced 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** at the top of the page and go to [Configuring compliance rules on page 182](#).

Configuring compliance rules

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 computers 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 Choose to apply this rule to computers 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.



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 Notification to send a notification message to the desired individuals when such events are received. For information and instructions, see [ePolicy Orchestrator Notification on page 224](#).

ePolicy Orchestrator Notification

When System Compliance Profiler or the Compliance Check server task generate events, it is ePolicy orchestrator Notification that informs you when the server receives those events.

The ePolicy Orchestrator Notification feature allows you to configure rules that, when the conditions are met, send a notification message to specified recipients. These notification messages can be sent via standard e-mail, SMS, text pager, or SNMP trap. You can also configure a rule to execute external commands when its conditions are met.

Among many other types of events, rules can be configured to send notification messages (or execute external commands) based on events the server receives from System Compliance Profiler, Rogue System Detection, and the **Compliance Check** server task.

For more information and instructions, see [ePolicy Orchestrator Notification on page 224](#).



SECTION 4

Dealing Proactively with Events

Two new features in ePolicy Orchestrator 3.5 help you to deal proactively with anti-virus events. Rogue System Detection allows you to detect and remediate computers on your network that are not under ePolicy Orchestrator management. Notifications allow you to create automatic alerts for client events to inform network administrators when critical security events occur.

Chapter 11, Rogue System Detection

Chapter 12, ePolicy Orchestrator Notification

11

Rogue System Detection

Find and remediate unmanaged computers in your network

This chapter introduces the new Rogue System Detection feature for ePolicy Orchestrator 3.5. By the time you read this, it is assumed you have already deployed rogue system sensors to your network. See [Deploying Rogue System Detection sensors on page 78](#) for more information about deploying sensors to your network.

What is in this chapter

The following topics are included in this chapter:

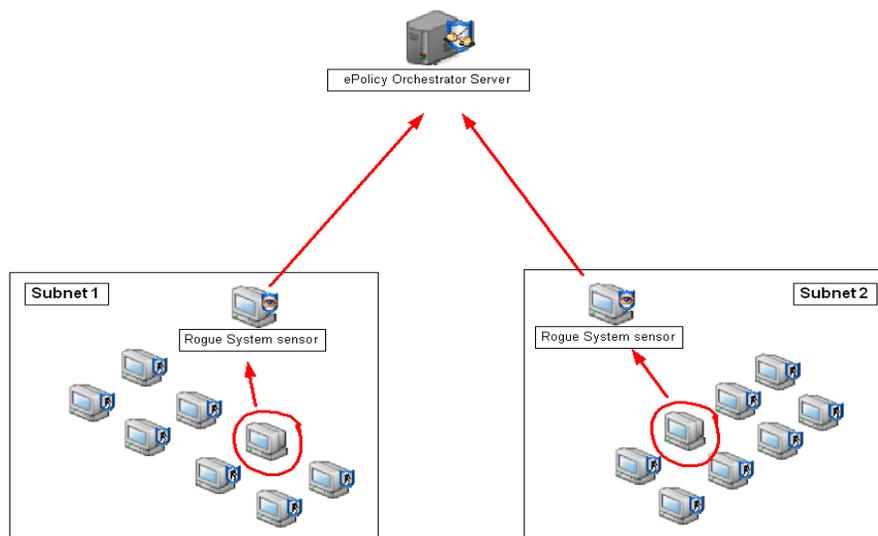
- [About Rogue System Detection](#)
- [Monitor detected systems and deployed sensors](#)
- [Configure Rogue System Detection sensor policies](#)
- [Take manual actions on detected rogues](#)
- [Configure automatic responses for specific events](#)
- [Configure third party command line executables to use in automatic responses](#)
- [View status of actions taken and view event history](#)
- [Customize the Rogue System Detection server and interface](#)
- [Frequently Asked Questions](#)

About Rogue System Detection

Even though you already use ePolicy Orchestrator to manage your anti-virus policies, your protection is only as good as your coverage. Diligently deploying agents to the computers you know about on your network and keeping their DAT and engine files up-to-date is only 90% of the battle. The final critical step is making sure you are covering every device that connects to your network that should have an agent installed. In any network, there are inevitably a small number of computers which do not have an ePolicy Orchestrator agent on them at any given time. These can be computers that frequently log on and off the network, such as test servers, laptop computers brought from home, or wireless devices. End-users can uninstall or disable agents on their own computers. 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 computer 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 computer has connected to the network.

Figure 11-1 Rogue system sensors detect computers without agents and report back to the ePolicy Orchestrator server.



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 computer has an active agent installed and is managed by ePolicy Orchestrator. If the new computer 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 pushing an ePolicy Orchestrator agent to the computer.

Topics covered in this section

- [About the rogue system sensor](#)
- [The Rogue System Detection server](#)
- [About system status and rogue type](#)
- [Overview of the Rogue System Detection interface](#)

About the rogue system sensor

The sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect the computers, 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.

How the sensor interfaces with your network

To detect systems on the network, the sensor utilizes WinPCap, an open source packet capture library. Using WinPCap, the Rogue System Detection sensor captures network layer two broadcast packets sent by computers connected to the same network broadcast segment. The sensor listens for and parses 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 that part of the network.

The Rogue System Detection sensor is a passive listener; it does not actively probe the network to search for which devices are connected. Instead, it listens for network broadcast messages sent out across the network.

Intelligent filtering of network traffic

The Rogue System Detection sensor implements intelligent filtering of network traffic to ignore “chatter” 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 those devices that are part of the local network. For example, if a computer on the network happens to be browsing Yahoo, packets will appear on the local network with the IP address of yahoo.com. Since the purpose of the Rogue System Detection sensor is to detect computers on your local network only, it ignores all unicast packets since their sources cannot be guaranteed to be a local system.

Since the computers on your network send broadcast packets all the time, the sensor needs to be “smart” about how often it sends information back to the Rogue System Detection server for processing. For instance, the Rogue System Detection sensor will detect 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 swamped with sensor detection messages. 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.

To this end, the sensor further implements filtering on systems it has already detected according to the following rules:

- The sensor always reports any system the first time it is detected on the network.
- The sensor adds the MAC address of every system it detects to the packet filter, so that it will not be 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 will again be removed from the filter, causing those hosts to be re-detected and re-reported to the server.

Gathering data on detected systems and communicating to the server

Once the sensor detects a system located on the local network, it attempts to gather as much information about that system as it can from the information contained in the network packet. The information gathered includes DNS name, operating system version, and NetBIOS information such as domain membership, NetBIOS 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 then sends this message via secure HTTPS to the Rogue System Detection server for processing. Once the message is received by the Rogue System Detection server, the server queries the ePolicy Orchestrator database to determine whether the computer is a rogue.

To help tune sensor operation to save bandwidth in large deployments, you can configure how often the sensors send detection messages to the server. You can allow the sensor to send every detection event to the server immediately. Or, you can have the sensor cache detection events for a given time period, such as 1 hour, and then send a single message containing all the events from that time period. See [Configure Rogue System Detection sensor policies on page 197](#) for more information on customizing the sensor in this way.

Note that the sensor makes no determination about system rogue status. It simply detects systems connected to the network and reports these detections back to the rogue system server located on your ePolicy Orchestrator server.

The Rogue System Detection server

The Rogue System Detection server consists of a number of servlets running within the Apache Tomcat web server. The rogue system servlets and the Tomcat web server are installed and started when you install the ePolicy Orchestrator server. The servlets collect detection messages sent by the sensors deployed on your network and maintain tables in the ePolicy Orchestrator database for detection information. The server also hosts the Rogue System Detection interface that is viewable in the ePolicy Orchestrator console.



The TOMCAT.EXE Rogue System Detection server is a separate process from the ePolicy Orchestrator server service, and runs regardless of whether the ePolicy Orchestrator server is running or not.

When a sensor detects a new system on the network and informs the server, the server queries the ePolicy Orchestrator database to determine whether that system is listed in it. If a system is in the ePolicy Orchestrator database, that means the system has an active ePolicy Orchestrator agent running on it. This is a managed system. If the system is not listed in the ePolicy Orchestrator database, then that system does not have an active ePolicy Orchestrator agent installed and could mean that the system is a rogue system.

You can view detection data collected by the Rogue System Detection server from within the ePolicy Orchestrator console. To do this, select **Rogue System Detection** in the ePolicy Orchestrator console tree.

About system status and rogue type

Machine Status and Rogue Type are both important concepts to understand dealing with how ePolicy Orchestrator classifies what is a rogue system. Every system detected by sensors and is listed in the **Machine List** has system status and, if the status is rogue, a rogue type. These classifications are very useful for grouping computers in the **Machine List** table, and you can use status and rogue type as criteria for triggering automated responses. See [Configure automatic responses for specific events on page 207](#).

Machine status for detected systems

Every system detected by a rogue system sensor has a basic status of Managed, Rogue, Exception, or Inactive. This state is shown in the **Status** column of the **Machine List**.

Table 11-1 Types of Machine Status

Machine Status	Description
Managed	The computer that is listed in the ePolicy Orchestrator database as having an active agent installed and running. The vast majority of computers in your Machine List should have a status of managed.
Rogue	A computer that is not listed in the ePolicy Orchestrator database and therefore doesn't have an agent on it.
Exception	A computer you have flagged as an exception. An exception system is a piece of network equipment, such as a network router, switch, or printer, that you know does not require an agent.
Inactive	A computer 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 computers that have been shut down or disconnected from the network.

About rogue type: when a rogue is not necessarily a rogue

Machines in **Rogue** or **Inactive** state also have a Rogue Type. These may be computers that are not listed in the database, but are also not necessarily true rogues at a given point in time. Rogue types give you greater flexibility and control in defining what exactly is a rogue in your network.

For example, a new computer may have just come on line and the agent was installed with a network login script. Since the initial agent call to the server may take up to ten minutes, the rogue system sensor will likely detect the computer before the agent communicates with the server and that computer is added to the database as a managed computer. In this case, the computer would be classified as a rogue, even though it is not really a rogue as it already has an agent. If you configure automatic responses or automatic e-mail alerts for rogue detections, specifying a reasonable grace period can help you minimize false positive rogue detections like this.

For this reason, the rogue type **Rogue (In Grace Period)** allows you to specify a grace period, such as one hour, within which newly detected computers are not yet classified as true rogues. This is very useful if you configure automatic responses, such as e-mail alerts or an immediate agent push when rogues are detected, to avoid triggering a false positive alert.

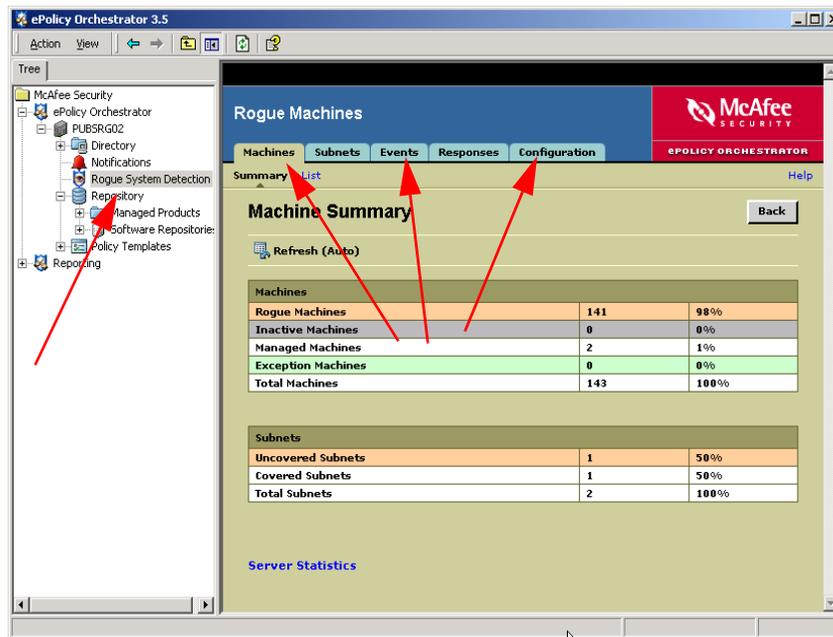
Table 11-2 Rogue Types

Rogue Type	Description
No Agent	The detected computer has no agent installed. This is the most common rogue type.
Grace Period	<p>You can define a grace period for a length of time after a system is detected and before it is classified as a rogue. This can be useful if you have many computers that join and leave the network. It is also useful if you use login scripts to install the agent when new computers log onto the network. In this case, the rogue system sensor will detect the new computer before the newly-installed agent has called into the server for the first time. Using the grace period allows you to create a time buffer to avoid false positive rogue detections for computers that are not really rogues.</p> <p>The grace period is disabled by default, so all systems that are detected by sensors and are not listed in the database are immediately classified as Rogue (No Agent). You might consider enabling the grace period if you have configured automatic responses that are triggered by the rogue detection event that are generating many false positives.</p> <p>To enable the grace period:</p> <ol style="list-style-type: none"> 1 Select Rogue System Detection in the ePolicy Orchestrator console tree. 2 Click the Configuration tab to view the Basic Configuration page. 3 Select Rogue machine grace period and specify a time period. 4 Click Apply at the bottom of the page to save the change.
Inactive Agent	<p>The detected computer has an agent installed, but it has not called into the ePolicy Orchestrator server for some configurable period of days, 7 days by default.</p> <p>To change the inactive agent period, change the ePO agent timeout parameter on the Basic Configuration page of the Configuration tab.</p>
Alien Agent	<p>The detected computer has an agent installed, but the agent does not report into your ePolicy Orchestrator 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 into your network could have an alien agent. This rogue type is distinct as you probably would not want to take action on these computers 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>
Managed	For computers in the Inactive status only. The computer has not been detected by a sensor in a while, but when last detected it did have an agent.

Overview of the Rogue System Detection interface

The Rogue System Detection interface consists of a series of tabbed HTML pages in the details pane of the ePolicy Orchestrator console. The interface is accessible via a **Rogue System Detection** node in the ePolicy Orchestrator console tree.

Figure 11-2 Select Rogue System Detection in the console tree to access the interface. Use tabs to access different features.



Each tab contains a different feature of the Rogue System Detection interface. See the following sections of this guide for detailed information on using the tabs of the interface.

Viewing table data in Rogue System Detection

Most of the information displayed in the Rogue System Detection interface is in tables, such as the **Machine List** or **Subnet List**. These tables display data from the ePolicy Orchestrator database and share similar configurable features that allow you to customize what and how they display.

Filter table data by status

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.

Refresh table data

Use the **Refresh** button to immediately refresh the table data. This can be particularly useful when you are performing tasks that cause the data to change rapidly. For example, deploying a sensor to a new subnet adds many newly-detected systems to the ePolicy Orchestrator database. However, you must refresh the Machine List periodically to see the new data in the table.

Furthermore, the tables by default refresh automatically at a configurable rate. You can either disable this feature or change the refresh rate. See [Customize the Rogue System Detection server and interface on page 217](#) for details about automatic refresh.

Configure table to show or hide specific kinds of data

Click **Configure Table** to access the **Columns and Column Order** page for a given table, such as the **Machine List** or **Subnet List**. Select and move items between the **Available columns** and **Selected columns** lists to customize which columns appear in the table. Use the **Up** and **Down** buttons to change the column display order; the first item listed in the **Selected Columns** list is listed in the first column of the table.

Sort a table by a column

Click any hyperlinked table heading, in blue font, to sort the table by that column.

Help

Each page in the Rogue System Detection interface includes a **Help** link in the upper right corner of the page. Click it to open the Online Help file and view information about the current page.

Set custom filters for system and subnet lists

You can set customized filters for the **Machine List** and **Subnet List** to filter what information is displayed in each. Create a custom filter if the other filters available in the **Filter** drop-down list don't 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 either the **Machine List** or **Subnet List**:

- 1 From the appropriate page (**Machine List** or **Subnet List**), select **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.

Note that **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, such as **All** to display all systems, by selecting another filter from the **Filter** drop-down list. The custom filter settings are saved until you change them.

Monitor detected systems and deployed sensors

The **Machine List** and **Subnet List** provide a snapshot of your network protection at any given time. After you have finished your initial deployment of rogue system sensors and configured the server to your liking, you will probably spend most of your day-to-day time using Rogue System Detection on the **Machine Summary**, **Machine List**, and **Subnet List** pages.

You should try to check these pages daily or at least weekly to monitor the completeness of your coverage. Typical regular tasks might include deploying ePolicy Orchestrator agents to new rogues and making sure all your network subnets have active rogue system sensors on them.

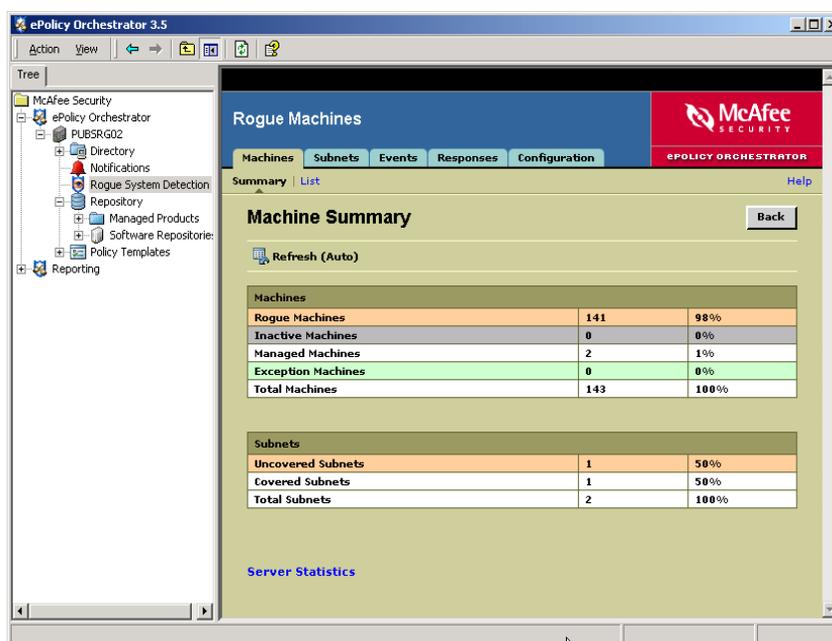
This section contains detailed information on the following topics:

- [View summary information about your Rogue System Detection coverage](#)
- [View the list of systems detected on your network](#)
- [View details about specific detected systems](#)
- [Monitor your sensors deployed to network subnets](#)

View summary information about your Rogue System Detection coverage

When you launch the Rogue System Detection server interface in the ePolicy Orchestrator console, you see the **Machine Summary** page. This page shows a summary of your current Rogue System Detection coverage.

Figure 11-3 View summary of Rogue System Detection coverage



The **Machine Summary** provides a high-level summary of which computers on your network are currently flagged as rogues, exceptions, or managed and which network subnets have rogue system sensors installed on them.

The **Machines** table shows how many of fall into one of four categories. You can click any row in the Machine table to see the complete list of all systems of that type that have been detected by rogue system sensors.

The four system types are:

- **Rogues.** The number of rogue systems on your network. Rogue systems are computers that are not currently managed by ePolicy Orchestrator but should be. This number should be as close to zero as possible. In most cases, computers listed as rogue should either have an agent deployed to them or be flagged as an exception.

- **Exceptions.** Number of systems that you have flagged 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.** The number of systems on your network that currently have active ePolicy Orchestrator agents running on them.
- **Inactive.** Machines listed as inactive are those that have not been detected by a sensor in a user-configurable time period, by default 3 days. These are usually computers that have been shut down or are no longer connected to the network.

The Subnets summary table shows all the network subnets represented in the ePolicy Orchestrator database. These subnets are grouped into either:

- **Covered.** There is at least one active rogue system sensor installed on a computer located in this subnet.
- **Uncovered.** There is no active sensor on any computer in this subnet. This can mean no sensor was ever installed or that a sensor has been disabled or uninstalled, or that all computers running sensors have been shut down.

View the list of systems detected on your network

The **Machine List** page shows a list of all the systems on your network that have been detected by the Rogue System Detection sensors.

Figure 11-4 View a list of systems detected on your network

The screenshot shows the ePolicy Orchestrator 3.5 interface. The left-hand navigation tree includes 'McAfee Security', 'ePolicy Orchestrator', 'PUBSRG02', 'Directory', 'Notifications', 'Rogue System Detection', 'Repository', 'Policy Templates', and 'Reporting'. The main content area is titled 'Rogue Machines' and features a 'Machine List' table. The table has columns for 'Status', 'Friendly Name', 'IP', and 'Last Detect Time'. The first two rows are 'Managed' systems (PUBSRG01 and PUBSRG02), and the remaining rows are 'Rogue' systems with various names and IP addresses. Below the table, there are controls for 'Check All', 'Uncheck All', and pagination information: '144 items in 15 pages. Go to page: 11'. At the bottom, there is a 'Checked machines:' section with a dropdown menu set to 'Add to ePO tree' and a 'Run' button.

Status	Friendly Name	IP	Last Detect Time
Managed	PUBSRG01	172.16.39.228	3/17/04 8:31:27 AM
Managed	PUBSRG02	172.16.39.164	3/17/04 8:21:00 AM
Rogue	QA-MWYMAN	172.16.39.48	3/17/04 8:31:29 AM
Rogue	QA-MWYMAN2	172.16.39.209	3/17/04 8:36:19 AM
Rogue	RIESCIENT	172.16.39.212	3/17/04 8:01:36 AM
Rogue	RIESSERVER	172.16.39.37	3/17/04 8:57:22 AM
Rogue	RIESTEST3	172.16.39.171	3/17/04 8:46:16 AM
Rogue	RLL-EN-WIN2KSRV	172.16.39.116	3/17/04 8:42:28 AM
Rogue	RLL-EN-WINXPP	172.16.39.124	3/17/04 8:21:31 AM
Rogue	SHALEYDEV	172.16.39.219	3/17/04 8:18:08 AM

Machines have a status of either Managed, Rogue, Inactive, or Exception. Use the **Filter** to filter what systems are displayed in the **Machine List**. For example, to find out what computers need to have ePolicy Orchestrator agents installed on them, set the filter to Rogue to show only rogue systems.

You can select systems in the list and perform manual actions on them, such as deploying an ePolicy Orchestrator agent or adding the computer to the **Directory**. To do this, select an action from the **Checked machines** drop-down. See [Take manual actions on detected rogues on page 201](#) for more information.

Group machines in the Machine List by subnet

You can sort the system list table to group machines by subnet address. To group systems by subnet in the **Machine List**:

- 1 In the Rogue System Detection interface, click the **Configuration** tab.
- 2 Under **UI Related**, select **Sort machines by network subnet**.
- 3 Click **Apply**.

For more information on what you can do from the Machine List:

- [Take manual actions on detected rogues on page 201](#).
- [Configure automatic responses for specific events on page 207](#).
- [Flag systems that don't need agents as Exceptions on page 205](#).

View details about specific detected systems

From the **Machine List**, click any computer listed in the table to view detailed information on that computer that is stored in the ePolicy Orchestrator database. This includes information about the computer such as operating system, IP address, and network domains to which it belongs. It also includes information about its status (rogue, managed, or exception) and when it has been last detected by a rogue system sensor. In the **Comments** field, you can type notes about this computer that will be saved in the database.

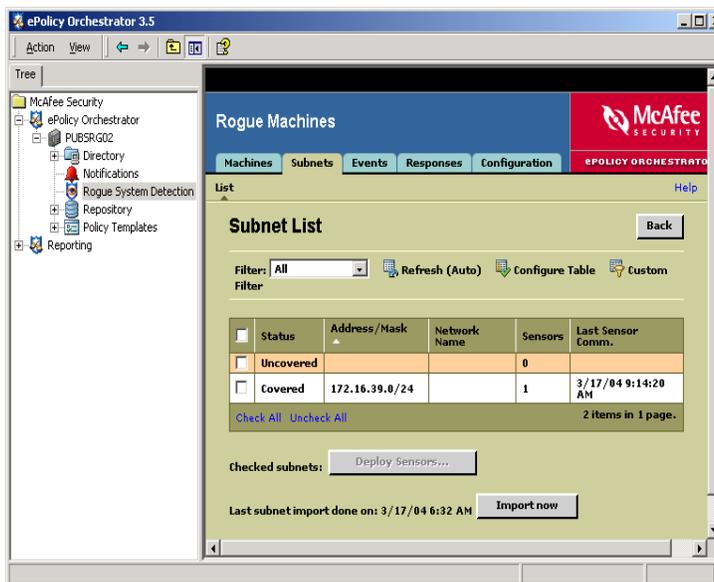
Any of these fields can also be displayed in the **Machine List** table. Use the **Configure Table** feature on the **Machine List** page to add any of these fields to the machine list table.

The **Events and Actions for this machine** section lists the event and action history for this computer. These include:

- Any ePolicy Orchestrator events that have occurred on this computer, such as rogue system detected, sensor install, or ePolicy Orchestrator agent pushed.
- Any automatic or manual Rogue System Detection actions that have been taken in response to events.

Monitor your sensors deployed to network subnets

The **Subnet Coverage** page shows all the network subnets that are represented in your ePolicy Orchestrator database, which records where you have ePolicy Orchestrator agents deployed.

Figure 11-5 View which of your network subnets have active sensors deployed to them

Each subnet listed in the table receives a status of *Covered* if there is an active rogue system sensor installed on a computer in that subnet. A subnet is *Uncovered* if there is currently no sensor deployed there. You can drill down on each Subnet to view details about the computers in that subnet by clicking once on a row in the table. This displays a **Subnet Details** page listing all the computers in that subnet that currently have an active ePolicy Orchestrator agent running on them.

Deploy sensors to uncovered subnets

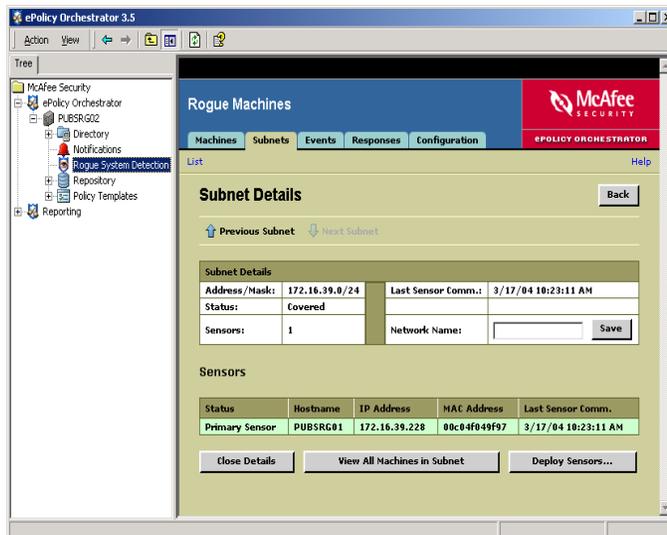
If a subnet is listed as *Uncovered*, deploy a sensor to it by checking the corresponding checkbox for the subnet and clicking **Deploy Sensors**. Follow the **Sensor Deployment** wizard to either manually select computers to which to deploy sensors or have ePolicy Orchestrator automatically select computers to host sensors.

Sensor deployment is covered in detail in the chapter dealing with deploying agents. See [Deploying Rogue System Detection sensors on page 78](#) for more details on deploying rogue system sensors.

View subnet details about a particular subnet

From the **Subnet List** page, you can click any subnet listed in the table to view detailed information on that selected subnet, including which computers in that subnet currently have Rogue System Detection sensors installed on them.

Figure 11-6 Subnet details



Configure Rogue System Detection sensor policies

You can set sensor properties for all sensors deployed by the Rogue System Detection server by using the Rogue System Detection sensor properties pages in ePolicy Orchestrator. This is similar to the way you can set policies for a deployed product like VirusScan Enterprise or the agent. The Rogue System Detection policy pages are installed on the ePolicy Orchestrator server when you install the server.

See [Deploying Rogue System Detection sensors on page 78](#) for more details about deploying sensors on computers in your network.

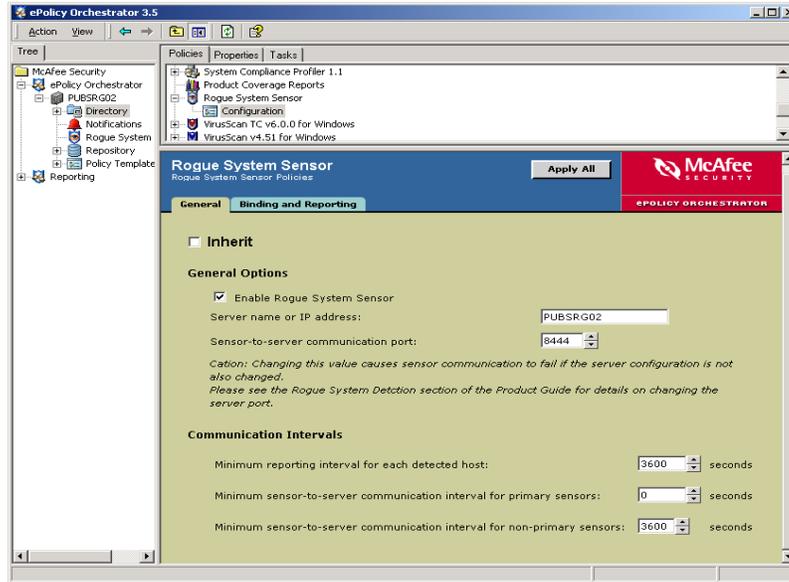
How to set sensor policies

Set the sensor policy configurations the same way you would for the ePolicy Orchestrator agent or any security product installed on computers in your network. Do this through the policy pages in the Rogue System Sensor NAP file that is installed when you install the ePolicy Orchestrator server. Policies you set at higher levels of the **Directory**, such as at the **Directory** root, inherit to lower-level groups or individual computers.

To configure sensor policies:

- 1 From the **ePolicy Orchestrator Console**, select **Directory**. To set policies at a lower level, select a site or group within the **Directory**.
- 2 In the upper details pane, select the **Policies** tab and select **Rogue System Sensor | Configuration**.
- 3 On the **General** tab of the **Rogue System Sensor Policies** page, deselect **Inherit** to enable configuration options.

Figure 11-7 Configure Rogue System Detection policies



- 4 Change any sensor properties you wish on the **General** or **Binding and Reporting** tabs. See the tables on the following pages for descriptions of these parameters.
- 5 Click **Apply All** when finished to save your changes.

In most cases, using the default policies is recommended. If, however, your specific network requirements require, you can change any of the policy settings as needed.

What sensor policies you can configure

Use the rogue system sensor policy pages to change sensor configuration. The policy pages consist of **General**, **Sensor**, and **Subnet** tabs. The following sections detail which policies you can set on each of these pages.

General sensor properties

On the **General** tab, configure sensor-to-server communications parameters.

Table 11-3 General Rogue System Detection sensor properties

Property	Description
Enable Rogue System Sensor	When this is selected, as it is by default, the rogue system sensor is enabled after it is installed and begins reporting detections to the ePolicy Orchestrator server. This happens the first time after the sensor is installed that the agent on that computer calls into the server. If you want to disable the sensor by stopping the sensor service on the client computer, deselect this option. You may do this if you only want sensors to function for certain periods of time and otherwise be disabled.
Server name or IP address	The name or IP address of your ePolicy Orchestrator server, which also hosts the Rogue System Detection server. When you install ePolicy Orchestrator, this value is automatically set to the name of the computer on which you installed ePolicy Orchestrator.

Table 11-3 General Rogue System Detection sensor properties

Property	Description
Sensor-to-server communication port	<p>The port number used for sensor-to-server communication. Unless you specified a different value when you installed the ePolicy Orchestrator server, this is port number 8444 by default.</p> <p>If you change the sensor port number here, you <i>must</i> also change it in the Tomcat SERVER.XML configuration file in the ePolicy Orchestrator installation folder. See Change sensor-to-server port number in SERVER.XML on page 221 for more information on how to do this.</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. By default this is set to one hour (3600 seconds).</p> <p>This feature can be used to reduce network traffic by limiting the number of times the sensor reports on computers that it already knows about. A given computer likely sends network broadcasts many times in an hour, and is detected by the sensor each time. But the computer's managed status doesn't change that often, so the sensor doesn't need to report the same information to the server at each detection. To save network bandwidth, the sensor will only update detection information for a given computer once within this time period.</p>
Minimum sensor to server communication interval for primary sensors	<p>How long, in seconds, the sensor waits before sending system detection events to the server. If used, the sensor caches multiple detection events and sends them to the server together in a single batch message. When set to the default of 0, the sensor forwards each detection event to the server immediately as a separate message.</p> <p>This is useful if you want 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, or non-primary, sensor should sleep before checking with the server to see if it should startup or continue sleeping.</p> <p>This parameter is useful when you have multiple sensors deployed on the same subnet as McAfee recommends. The ePolicy Orchestrator server periodically switches which sensor is the Primary Sensor and which are sleeping, or Inactive Sensors. Inactive sensors ping the server once during this interval to check whether they should become active.</p> <p>Note the difference between an <i>inactive</i>, or non-primary, sensor and a <i>disabled</i> sensor. An inactive sensor is running but is in sleep mode, so it does not report detections to the server. A disabled sensor, controlled by the Enable Rogue System Sensor policy, is one whose SENSOR.EXE service has been stopped by the ePolicy Orchestrator agent.</p> <p>See About deploying the ePolicy Orchestrator agent on page 57 for more information about primary and inactive sensors. Also see the Maximum number of primary sensors per subnet feature in Customize the Rogue System Detection server and interface on page 217</p>

Configure what NIC the sensor binds to and which detections it reports to the server

On the **Binding and Reporting** tab of the Rogue System Detection sensor policy pages, you can configure two things:

- The network subnets that the sensor reports on.
- If you install the sensor on a computer with multiple Network Interface Cards (NIC), you can specify which NICs the sensor binds to.

Table 11-4 Rogue System sensor binding and reporting properties

Property	Description
Only listen on an adapter if its IP address is included on a network found during installation	Force the sensor to only report detections occurring in the subnet where the sensor was installed. For example, if the sensor is installed on a computer with IP address 192.168.13.100, then it will only report on detections that occur in the 192.168.13.0/24 subnet. This can be useful if the sensor is installed on a laptop that may move between subnets within your network or travel to different networks, such as a home network. You may not want the sensor to report detections in any of these other subnets. The sensor is active when the laptop is connected to that network, but becomes inactive otherwise, such as when connecting from a different subnet in the network, at home, or in a hotel.
Only listen on adapters whose IP addresses are included in the following networks	If you install the sensor on a computer with multiple Network Interface Cards (NIC), specify the IP address range that includes the NIC you want the sensor to bind to. The elements of the list are formatted in standard network address notation using the following format: xxx.xxx.xxx.xxx/##. For example, 192.168.13.0/24 indicates a subnet including computers with IP addresses 192.168.13.1 - 255 and a subnet mask of 255.255.255.0.
Do not listen on adapters whose IP addresses are included in the following networks	If you install the sensor on a computer with multiple NICs, specify the IP address range for any NICs that you do not want the sensor to bind to. Use the same network address notation as for the subnets. Note: If a subnet address is included in both the included subnet and excluded subnet lists, that subnet is excluded (the latter overrides the former).
Do not report systems whose IP address is outside of the sensor's network	If selected, as it is by default, the sensor only reports detections to the server for systems that belong to the same network subnet as the computer where the sensor is installed. If not selected, the sensor reports on all computers it detects regardless of which network subnet they belong to. The sensor can detect computers 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. However, even if you have configured your routers in this way, you might find it easier to keep track of your sensors by deploying one to each subnet. You would then select this option to force the sensors to only report on their local subnet.

Rogue System Detection sensor command line options

In addition to configuring sensor policies through the Rogue System Sensor policy pages in the ePolicy Orchestrator console, you can also run command line options from the client computer. The following table lists the runtime command line options for the sensor.

Table 11-5 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]"	<p>Overrides the ServerName config setting in the registry that you specified during installation.</p> <p>Note: This parameter will only take affect when running in command line mode, which requires the --console command line switch as well.</p> <p>Sample syntax:</p> <pre>sensor.exe --server "MyServerName" --console</pre>
--port "[server port]"	<p>Overrides the ServerPort configuration setting in the registry that you specified during installation.</p> <p>Note: This parameter will only take affect when running in command line mode, which requires the --console command line switch as well.</p> <p>Sample syntax:</p> <pre>sensor.exe --port "8081" --console</pre>
--console	Forces the sensor to run as a normal command-line executable; otherwise it must be run as an NT service.

Take manual actions on detected rogues

You can perform actions on one or more systems listed in the **Machine List**. For example, you may want to push an agent to a new rogue computer or flag computers for later follow-up action. In addition to these manual actions, you can configure automatic responses that can be triggered by a detection event. For more information, see [Configure automatic responses for specific events on page 207](#).

What's covered in this section

This section covers some of the common actions you can take on computers in the **Machine List**. The topics covered here are:

- [Types of manual actions](#)
- [Push agents to rogue systems](#)
- [Add computers to the ePolicy Orchestrator Directory.](#)
- [Flag specific systems for later follow-up action.](#)

- [Flag systems that don't need agents as Exceptions](#)

Types of manual actions

The following table lists the manual actions you can take on selected systems in the Machine List. Some of these are covered in greater detail in following sections.

Table 11-6 Actions available for manual actions

Action	Description
Add to ePO tree	Adds a computer node to a Rogue System site beneath the Directory . You can manually place the computer into an appropriate site or group.
Mark for Action	Flags the detected computer as Mark for Action in the Machine List. See Flag specific systems for later follow-up action on page 205 for more information.
Mark as Exception	Flags selected computers as Exception machines in the Machine List. See Flag systems that don't need agents as Exceptions on page 205 for details on exception machines.
Push ePO Agent	Have the ePolicy Orchestrator server push an agent to the selected computer. See Push agents to rogue systems on page 202 for more information.
Query ePO agent	Queries the newly-detected system to see whether there is an ePolicy Orchestrator agent installed on it. This query is required if you want to be able to use the Alien Agent rogue type in your Machine List . See About system status and rogue type on page 189 for more information on the alien agent rogue type. Create an automatic response for this 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 into your network, they will show up as rogues even if they have an agent from another ePolicy Orchestrator server installed. See Configure automatic responses for specific events on page 207 .
Remove Host	Hides the detected system in the Rogue System Detection Machine List but does not delete it from the database.
Send ePO Server Event	Forwards <i>Rogue System Detection</i> and <i>Subnet Uncovered</i> events to the Notification server. This is required if you plan to use the new Notification feature in ePolicy Orchestrator 3.5 to automatically send e-mail alerts for rogue detection events.
Unmark for Action	Unmarks computers that you have already flagged for follow up using Mark for Action .
Unmark as Exception	Unmarks computers that you have already flagged as Exceptions using the Mark as Exception action.

Push agents to rogue systems

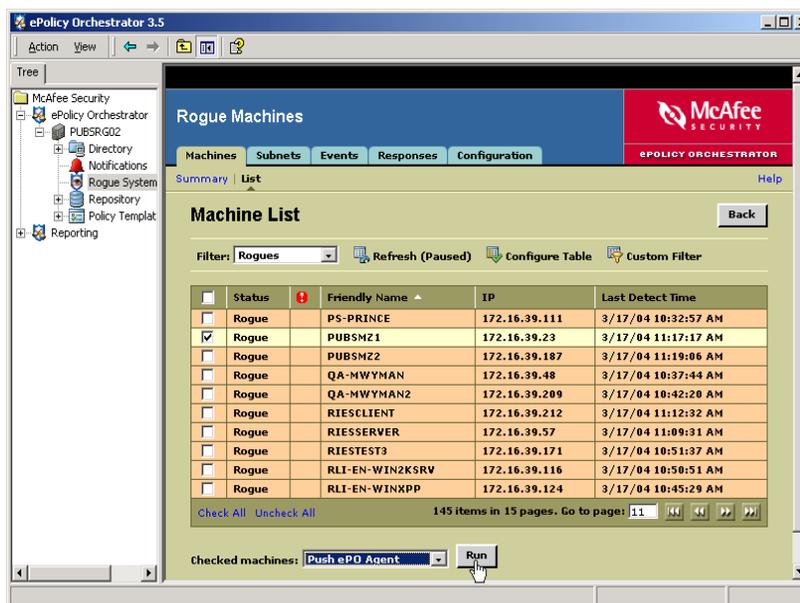
One of the most important features of Rogue System Detection is the ability to easily push ePolicy Orchestrator agents to newly-detected rogue computers. You can do this right from the **Machine List**. After the agent is installed, ePolicy Orchestrator adds the computer to the **Directory**. If you are using IP filtering, the computer is automatically added to the right site or group for its IP address. See [About IP address filters and sorting on page 42](#).

The agent push uses the ePolicy Orchestrator server push technology. Depending on your network, you may or may not be able to deploy agents to clients in this way. See [Using ePolicy Orchestrator to deploy the agent on page 60](#) for more details on using the ePolicy Orchestrator console to push agents.

To push agents from the **Machine List** of the Rogue System Detection interface:

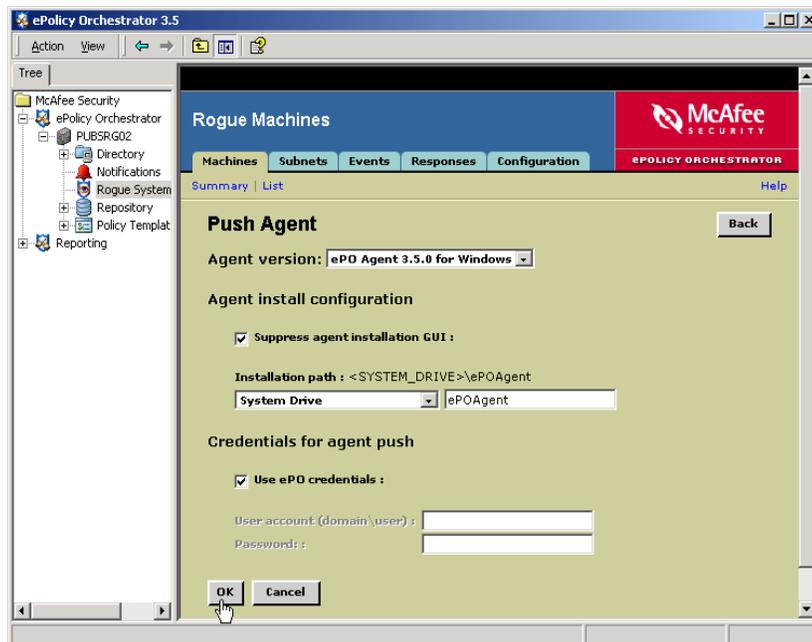
- 1 Click the **Machines** tab and click **List** to display the **Machine List**.
- 2 Find the target computer in the table and select it by clicking its checkbox.
- 3 In the **Checked machines** drop-down list, select **Push ePO Agent** and click **Run**.

Figure 11-8 Deploy an agent to a rogue computer in the Rogue System Detection Machine List



- 4 On the **Push Agent** page, specify any changes to the default installation configuration you wish.

Figure 11-9 Configure agent installation parameters for deployment



You can configure the following:

Table 11-7 Rogue System Detection Push Agent parameters

Parameter	Description
Agent version	A drop-down displaying the agent installation packages you have checked into your master software repository. By default, the only option is the ePolicy Orchestrator 3.5 Agent.
Suppress agent installation GUI	By default, the agent installs in silent mode. Unchecking this box (not recommended) displays the ePolicy Orchestrator agent installation GUI on the client computer.
Installation path	The agent installation folder. By default this is C:\ePOAgent.
Credentials for agent push	Make sure that the credentials you specify have domain administrator privileges in the target computer's network domain and also local administrator rights to the target computer. By default, this parameter is set to use the admin credentials for the ePolicy Orchestrator server service that you specified when installing the server. If these credentials do not have the sufficient rights for agent installs, deselect Use ePO credentials and enter appropriate user name and password.

5 Click **OK** to begin the agent deployment.

After clicking **OK**, you arrive at the **Response Progress** page on the **Responses** tab of the Rogue System Detection interface. Your agent push action is listed in the table and the **End Time** field is empty. When the agent installation is complete and the agent has called back to the ePolicy Orchestrator server, the **End Time** value is populated to signify that the agent push is complete.

Eventually, the status for the targeted computer in the **Machine List** changes from **Rogue** to **Managed** when the system is redetected.

Once the agent has been installed and communicated this back to the ePolicy Orchestrator server, the server adds the computer to the **Directory**. Refresh the **Directory** by right-clicking **Directory**, then selecting **Refresh**.

Add computers to the ePolicy Orchestrator Directory

You can add computers listed in the Rogue System Detection **Machine List** to the ePolicy Orchestrator **Directory**. New computers are added to a special site, and you can manually move them or use IP sorting to move them to the appropriate site or group.

To do this:

- 1 On the **Machines** tab, select **Machine List**.
- 2 Select computers you want added to the ePolicy Orchestrator **Directory** by checking the corresponding checkbox.
- 3 Select **Add to ePO tree** from the **Checked machines** drop-down list and select **Run**.

You arrive at the **Action Progress** table on the **Events** tab, which contains a new entry for the computer you have just added to the ePolicy Orchestrator **Directory**. If you open the ePolicy Orchestrator tree, you can see that the computer has been added to a **Rogue Machines** site beneath the **Directory | Lost&Found**.

Flag specific systems for later follow-up action

In some cases, you may not want to do anything to a particular computer from the ePolicy Orchestrator console. Instead, for example, you may simply want walk over to the computer and troubleshoot an issue. You can flag specific computers in the **Machine List** with a  action icon to serve as a reminder that further action is required with this computer.

To do this:

- 1 On the **Machines** tab, select **Machine List**.
- 2 Select computers for which action is required by checking the corresponding checkbox.
- 3 Select **Mark for Action** from the **Checked machines** drop-down list and select **Run**.

The computer is flagged with an  action icon in the **Action** column of the **Machine List** table. You can sort the Machine List table on the **Action** column or filter it with a **Mark For Action** custom filter.

You can also unflag any systems marked for action by selecting them in the **Machine List** table, selecting **Unmark for Action** from the **Checked machines** drop-down list and clicking **Run**.

Flag systems that don't need agents as Exceptions

Some of the systems that the Rogue System sensors detect, such as network switches, routers, or printers, do not require agents and therefore are not rogues. You can flag these systems as **Exceptions** to indicate they are not managed by ePolicy Orchestrator but are also not rogues. You can then easily sort or filter the Machine List to hide these Exception machines so you can focus on finding and remediating real rogues.

You can also configure rules for automatic responses to classify certain computers as Exceptions. See [Configure automatic responses for specific events on page 207](#) for more information.

This section contains the following topics

- [Flag specific systems as exceptions.](#)
- [Import and export exceptions from and to an XML file.](#)

Flag specific systems as exceptions

You can set an exception for a system listed in the **Machine List** in a state of either *Rogue* or *Inactive*. Machines in a *Managed* state already have an ePolicy Orchestrator agent installed on them and therefore are never going to be exceptions.

To flag a specific computer or computers as an Exception:

- 1 On the **Machine List**, click the checkbox for one or more systems.
- 2 From the **Checked machines** drop-down list, select **Mark as Exception** and click **Run**.
- 3 Refresh the **Machine List** to see that the state for the selected system has been changed to **Exception**.

You can unflag systems that have already been flagged as exceptions by checking them and then clicking **Unflag as Exception**.

Import and export exceptions from and to an XML file

Creating your exception list can be a labor-intensive process, often done by manually flagging one computer at a time as an exception. To prevent you from having to re-do this work if you need to reinstall the ePolicy Orchestrator server, you can save your exceptions list to an XML file. This XML exceptions list preserves your exceptions information so you can re-import it easily if needed.

Export exceptions list

Exporting your current list of exception systems to an XML file will include all systems from your Machine List that you have flagged as exceptions at that time. To export your current list of exceptions to an XML file:

- 1 From the Rogue System Detection interface, click the **Configuration** tab.
- 2 Click **Export** under **Exceptions List Import / Export** at the bottom of the **Configuration** 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 exceptions list from an XML file

You can also re-import an exceptions list. The exception list import does not overwrite all data in your Rogue System Detection database, but rather only for those systems that are listed in the exception list. When you do this, be aware that the import overwrites exception information for computers in the list. For example, if *machine A* is listed in your current Rogue System Detection database as a rogue, but in your XML exception list as an exception, when you import the exception list the status of *machine A* will change to exception.

To import an exported exception list from an XML file:

- 1 From the Rogue System Detection interface, click the **Configuration** tab and select **Basic Configuration**.
- 2 Under **Exceptions List Import / Export** at the bottom of the page, type the full path and filename into the text box or browse to the exceptions list XML file on your hard drive.
- 3 Click **Import**.

You can go to the **Machine List** and refresh your browser to see the newly imported exception data reflected in the table.

Configure automatic responses for specific events

You can configure automatic responses in the Rogue System Detection interface so that ePolicy Orchestrator responds automatically to the rogue system detection events. There are two 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.** There is a subnet in your network that does not have a rogue system sensor installed.

These automatic responses can be alerts, like sending an e-mail to a network administrator notifying him or her of the new detection. They can also be server actions, such as automatically adding newly-detected computers to the **Directory** or deploying an ePolicy Orchestrator agent to a newly detected rogue system. The automatic responses will occur within one minute of the event being triggered.

What is in this section

This chapter covers the following topics.

- [Types of Rogue System Detection automatic responses.](#)
- [Configure automatic e-mail alerts for new rogue detections](#)

Types of Rogue System Detection automatic responses

Rogue System Detection allows you to configure responses that can include any number of actions to be taken when one of these events is triggered.

An automatic response can contain one or more of these actions. For example, if you configure a response to push an ePolicy Orchestrator agent to newly-detected systems, you may also want to send an e-mail to ePolicy Orchestrator or network administrators to follow up on the agent installation.

The following table lists the actions you can configure as part of an automatic response. These are the same actions that you can perform manually on selected systems in the Machine List. See [Take manual actions on detected rogues on page 201](#) for more details.

Table 11-8 Actions available for automatic responses

Action	Description
Add to ePO tree	Adds a computer node to a Rogue System site beneath the Directory . You can later manually place the computer into an appropriate site or group.
Mark for Action	Flags the detected computer as Mark for Action in the Machine List. This is the automatic equivalent of manually flagging computers for follow up action. See Flag specific systems for later follow-up action on page 205 for more information.
Mark as Exception	Flags computers as exceptions that meet the specified conditions. See Flag systems that don't need agents as Exceptions on page 205 for details on exception systems. 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 as Exception and add a condition to trigger 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 computers. In this case, you can use the OUI Org condition to trigger an automatic response to flag machines as exceptions if the system's MAC address contains a specific vendor code.
Push ePO Agent	Have ePolicy Orchestrator push an agent to the computer. See Chapter 4, Deploying Agents, SuperAgents, and Sensors and also Push agents to rogue systems on page 202 for more information on pushing agents with ePolicy Orchestrator.
Query ePO agent	Queries the newly-detected system to see whether there is an ePolicy Orchestrator agent installed on it. This query is required if you want to be able to use the Alien Agent rogue type in your Machine List . See About system status and rogue type on page 189 for more information on the alien agent rogue type. Create an automatic response that uses this action to query all new rogues for an ePolicy Orchestrator agent if you have multiple ePolicy Orchestrator servers in your network.
Remove Host	Probably not used in automatic responses.
Send E-mail	See Configure automatic e-mail alerts for new rogue detections on page 208 .
Send ePO Server Event	Forwards <i>Rogue System Detection</i> and <i>Subnet Uncovered</i> events to the Notification server. This is required if you plan to use the new Notification feature in ePolicy Orchestrator 3.5 to automatically send e-mail alerts for rogue detection events.
Unmark for Action	Probably not used in automatic responses.
Unmark as Exception	Probably not used in automatic responses.

Configure automatic e-mail alerts for new rogue detections

Probably one of the most common automated tasks you will use 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 computers so you can take appropriate remediation.

When should I use Notification and when should I use Rogue System Detection?

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.



Configure all your e-mail alerts in the Notification feature 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.

Configure generic rogue detection e-mail alerts in the Notifications interface

In most cases, consider using the new Notifications feature in ePolicy Orchestrator 3.5 to configure e-mail alerts for rogue system detection events. Configuring e-mail alerts here will work if you will always send rogue system detection alerts to the same people. Also, managing all your automatic e-mail alerts in one place can make it easier to maintain them. See [Chapter 12, ePolicy Orchestrator Notification](#) for detailed information on creating e-mail alerts.

Basically, to use the Notifications feature to configure e-mail alerts for rogue detection events, do the following:

- 1 Configure an automatic response in the Rogue System Detection interface to send rogue system detection events to the Notification server.
- 2 Configure an e-mail alert in the Notifications interface to send e-mail notifications to network or security administrators.

Configure audience-specific e-mail alerts in Rogue System Detection interface

Because of the way the Rogue System Detection feature is designed, you have more flexibility with your e-mail alerts in the **Rogue System Detection** interface than in the **Notifications** interface. 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, you may want to do this if you have different IT personnel responsible for different parts of your network or for different types of computers, such as workstations or servers. You can create separate, targeted e-mail alerts that go to different people depending on the IP address, or send an e-mail alert for a newly-detected server to one IT team responsible for servers and another to a second team responsible for workstations.

How to configure e-mail alerts in Rogue System Detection

To configure an automatic response to send an e-mail alert:

- 1 [Configure Rogue System Detection to use your e-mail server.](#)
- 2 [Add recipients to automatic response contact list.](#)
- 3 [Create and configure an automatic e-mail response.](#)

Configure 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 the Rogue System Detection server will use for sending e-mail alerts. Rogue System Detection communicates with the e-mail server via SMTP over TCP/IP.

Usually, the ePolicy Orchestrator server should be able to send SMTP messages to the e-mail server as long as it can reach the e-mail server on the network. To test this connectivity, ping the e-mail server from your ePolicy Orchestrator server. Depending on your e-mail server configuration, there may be additional requirements. For example, the ePolicy Orchestrator may need to reside in the same NT domain as the e-mail server. Consult your network documentation to troubleshoot 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 Rogue System Detection interface, click the **Configuration** tab and select **Basic Configuration**.
- 2 Under **E-mail alerting**, type the name of your e-mail server in the **Mail server** text box.
- 3 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 will be bounced back to this address. You may need to access this e-mail account occasionally to troubleshoot or track undelivered Rogue System Detection e-mail alerts. It would probably be the address of the mail administrator for the selected SMTP server, or some other system administrator.

- 4 At the bottom of the **Basic Configuration** page, click **Update** to save the change.

Add recipients to automatic response contact list

Manage the list of recipients for rogue detection e-mail alerts from the **E-mail Contacts** table. For example, if you want to configure an automatic response to send an e-mail to a network administrator when a new rogue system is detected, you must first add the network administrator's e-mail information to the **E-mail Contacts** table.

This table lists the e-mail contacts you have added for both Rogue System Detection and other ePolicy Orchestrator 3.5 alert notifications. E-mail contacts added in either interface are available in both. See [Chapter 12, ePolicy Orchestrator Notification](#) for more information on using alerts with the new Notifications feature.

To add a new e-mail contact for a rogue system detection alert:

- 1 In the Rogue System Detection interface, click the **Configuration** tab and select **E-mail Contacts**.
- 2 Click **Add Contact** above the list of current contacts.
- 3 Type a name or short description for the new contact in the **Name** field.
- 4 Type the e-mail address for the contact into the **E-mail address** field. Make sure you type the complete and correct e-mail format, such as `MyEmail@example.com`.
- 5 Click **Add**.

You must add a separate contact for each e-mail address to which you might send e-mail alerts. If you will want to send some e-mail alerts to many recipients, you might want to create a distribution list on your e-mail server and then create a Rogue System Detection e-mail contact for that address instead.

Contacts you create appear in the list of available contacts. You can now select this contact when configuring automatic responses to specific events, such as sending e-mail when a new rogue system is detected.

Create and configure 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.

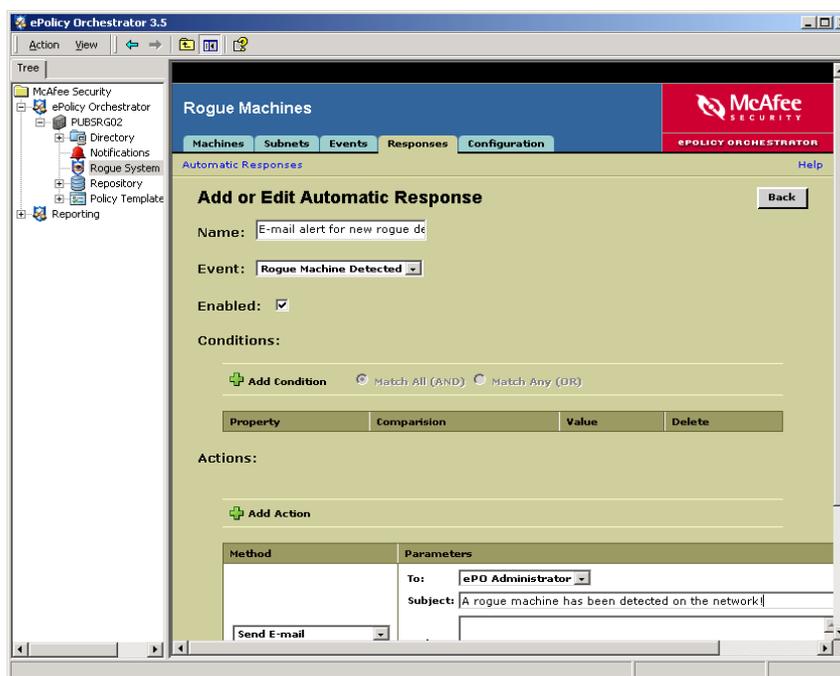


You can also choose to configure ePolicy Orchestrator Notification to send notification e-mail messages based on Rogue System Detection events. For more information, see [Chapter 12, ePolicy Orchestrator Notification](#).

To create an automated e-mail response for this event:

- 1 In the Rogue System Detection server web interface, click the **Responses** tab.
- 2 Click **Add Automatic Response**.

Figure 11-10 Create an automatic e-mail response



- 3 Type a short description of the response in the **Name** field. This name displays in the list of available automatic responses on 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 the server triggers a rogue system detection event.

If desired, you add one or more conditions that must be met before the automated 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.

- 6 To add conditions, select **Add Condition** and then configure property and the value for that property.
- 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. See [Add recipients to automatic response contact list on page 210](#).

9 Type your e-mail message in the **Subject** and **Body** fields.

If you want, 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 follow the previous steps, starting at [Step 7](#), for each additional contact.

11 Click **OK** to save the new automatic response.

The new automatic response is live once it has been added to the response list. The next time that the event associated with that response occurs, Rogue System Detection will automatically initiate the configured automatic response.

Configure third party command line executables to use in automatic responses

You can run any command-line executables to gather additional information about systems detected by Rogue System Detection. You can run these executables as part of an automated response to a rogue system detected or uncovered subnet event, or you can run them manually. In order to run, these executables must be installed on the ePolicy Orchestrator server.

This section covers the following topics:

- [About using executables in responses](#)
- [How to configure an executable for an automatic response](#)

About using executables in responses

You can only run command-line executables in this way; you cannot run executables with a Windows GUI. Some common executables you may want to use are listed below.

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.

NMAP.EXE Network Mapper

NMAP stands for “Network Mapper” and is a free, open-source utility for performing security audits of individual computers and entire networks. Features include network-wide ping sweep, port scan, and operating system detection. An advantage of NMAP is that it more information is returned — it can identify operating system type and other information about non-Windows computers; whereas,

the Rogue System Detection sensor can only identify operating system type for Windows-based systems. This more specific information provided by the NMAP integration are put into the appropriate host field.

See <http://www.insecure.org/nmap> for more information.

NSLOOKUP.EXE comes with Windows

A simple utility that looks up information on specific computers using the DNS name server. This utility can be useful when the Rogue System Detection sensor is unable to resolve DNS name information for certain computers. For example, you could create an automatic event with a condition that tests if the DNS name field of a detected computer is “ ” (blank), run NSLOOKUP.EXE to see if the DNS server has the computer name.

The Nslookup command-line tool is installed on Windows computers if you have the TCP/IP protocol installed, typically installed in the System32 folder.

How to configure an executable for an automatic response

To configure a command line executable for use with an automatic response, do the following:

- 1 *Make a registered executable available to Rogue System Detection.*
- 2 *Configure the executable command line.*
- 3 *Use the command line as part of an automated response.*

See the following sections below for more details on each of these steps.

Make a registered executable available to Rogue System Detection

Before you can configure a command line tool, you must register it with Rogue System Detection. This ensures that only the executable applications you want can be used and also allows you to make the executable available for other ePolicy Orchestrator administrators to use or to easily add it to automatic responses.

To register an executable with ePolicy Orchestrator:

- 1 Install the executable, if it is not already, on the computer hosting your ePolicy Orchestrator server.
- 2 In the Rogue System Detection interface, click the **Configuration** tab and select **External Commands**.
- 3 On the **External Commands** page, select **Add Registered Executable**.
- 4 In the **Add or Edit Registered Executable** page, type a descriptive name for the executable in the **Name** field.
- 5 Type the full path or browse to the location of the EXE file for this executable.

6 Click **Add**.

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.

Configure the executable command line

Once you have added a registered executable through the Rogue System Detection interface, you can configure command line options for it. To do this:

- 1** In the Rogue System Detection interface, click the **Configuration** tab and select **External Commands**.
- 2** On the **External Commands** page, select **Add Command Line**.
- 3** In the **Add or Edit Command Line** page, type a descriptive name for the command in the **Name** field.
- 4** Select the executable to use for this command line from the drop-down list of registered executables that have been made available to Rogue System Detection.
- 5** Type arguments in to 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 in your command. These are available in the **Variables** drop-down list.
- 6** Click **Add** when finished.

The command line 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, so you can include it as an action as part of an automatic response.

Use the command line as part of an automated response

Once configured, the registered command line 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.

View status of actions taken and view event history

The Rogue System Detection interface allows you to check the history of events that have occurred, such as the rogue detection event. Also, you can view the status of actions you have taken, such as manually pushing an agent or deploying a sensor.

This section covers the following topics:

- [View the status of in-progress actions.](#)
- [View Rogue System Detection event history](#)

View 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 computers, by watching the status from the **Events | Action Progress** page. 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 pushing a sensor to a specific computer, that response is added to the table.

Figure 11-11 View responses that are in-progress

The screenshot shows the McAfee ePolicy Orchestrator 3.5 interface. The main content area is titled 'Rogue Machines' and has tabs for 'Machines', 'Subnets', 'Events', 'Responses', and 'Configuration'. The 'Events' tab is selected, and the 'Action Progress' sub-tab is active. A summary bar indicates 'In Progress: Push Agent: 0 | Deploy Sensor: 0 | Total: 0'. Below this is a filter dropdown set to '(All)' and buttons for 'Refresh (Auto)', 'Configure Table', and 'Purge'. A table of actions is displayed below, with columns for Action, Action Status, Description, Start Time, and End Time.

<input type="checkbox"/>	Action	Action Status	Description	Start Time	End Time
<input type="checkbox"/>	ePO Agent Push	Completed Successfully	Pushing ePO agent to system PUBSRG02	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 PUBSRG02 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 PUBSRG01 as an exception.	2004-01-11 11:02:23.91	2004-01-11 11:02:23.93
<input type="checkbox"/>	Unmark as Exception	Completed Successfully	Unmarking host PUBSRG01 as an exception.	2004-01-11 11:02:23.89	2004-01-11 11:02:23.9
<input type="checkbox"/>	Unmark as Exception	Completed Successfully	Unmarking host PUBSRG02 as an exception.	2004-01-11 11:02:23.86	2004-01-11 11:02:23.87

The **Status** column shows whether the response is complete or still in progress. The response is in progress until the **Status** column displays as **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**.

Dismiss old events to filter the Event History table

If the table becomes too big, you can remove old or unimportant events no longer requiring attention from the **Event History** table. To do this:

- 1 Select one or more events by checking the corresponding checkbox.
- 2 Click the **Dismiss** button.

Dismissed events will be removed from the **Event History** table, but will remain in the database so you can use them in queries and reports.

Purge dismissed events from the database

If your database grows too big 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. You can dismiss events either from the Event History table on the **Events** tab, or from the Events and Actions for this system table on the **Machine Details** page.



Purging events removes them from the database permanently, and you will never be able to reclaim the purged event data in reports or queries. Event history can provide very valuable information in troubleshooting problems with specific computers or subnets. Therefore, purge dismissed events only if you are certain the event information is no longer needed or if your database grows so big that it causes performance problems.

Other places you can view event information in Rogue System Detection

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** table on the **Responses** tab.

Also, you can view the event history for a particular computer by clicking that computer in the **Machine List**. The **Events and Actions for this machine** table at the bottom of the page lists all the events that have occurred for this computer that are still in the database.

Display Action details

Click any action listed in the **Action Progress** table to view more detailed information on that action.

View 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.

Rogue Machine Detection and **Subnet Uncovered** events may trigger automatic responses, if you have created and configured responses to automatically respond to these events. See [Configure automatic responses for specific events on page 207](#).

The events that the Rogue System Detection server can generate are:

- **Rogue Machine Detection.** A sensor has detected a computer that is not in the ePolicy Orchestrator database. This probably means the computer does not have an ePolicy Orchestrator 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 computers to the ePolicy Orchestrator **Directory** tree. Click these events in the **Event History** table to view event details for the event, which shows the specific action taken to generate the event.
- **Subnet Uncovered.** A subnet that was covered by one or more Rogue System Detection sensors is now uncovered again. This can occur if the sensors have been uninstalled or stopped. The Subnet Uncovered event occurs only once the first time that the uncovered subnet becomes uncovered.

- **Agent Push Failed.** You have pushed an Agent to a rogue system from the Rogue System Detection Machine List, but the agent failed to install on the client computer.
- **Sensor Push Failed.** You have pushed a sensor to a computer from the Subnet List, but the sensor failed to install successfully on the target computer.
- **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.

Dismiss old or unneeded events from the Event History table

If the Event History table becomes too cluttered with old or unimportant events, you can remove them from the table. To do this, select one or more events by checking the corresponding checkbox, and then click **Dismiss**.

Purge dismissed events from the database

You may want to regularly purge the database of old, dismissed events. To do this:

- 1 Set the **Event History** table filter to show only dismissed events by selecting **Dismissed Events** from the **Filter** drop-down list. This activates the **Purge Dismissed** button.
- 2 Click **Purge Dismissed**.
- 3 Set the table filter back to something other than **Dismissed Events** to view current events that are still in the database.

View details of a particular event

Click any event listed in the **Event History** table to view more detailed information on that event, including any automatic actions that have been triggered by it.

Customize the Rogue System Detection server and interface

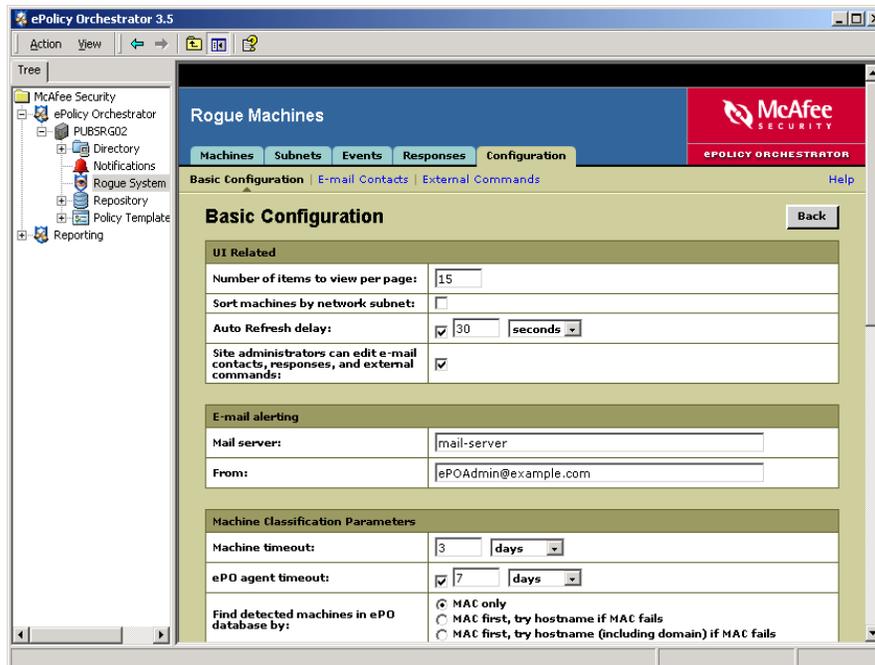
This section contains the following topics:

- [Use Configuration tab to customize server and interface](#)
- [Change sensor-to-server port number in SERVER.XML](#)

Use Configuration tab to customize server and interface

Customize several features of the Rogue System Detection interface on the **Configuration** tab.

Figure 11-12 Customize the Rogue System Detection interface



From here, you can customize the interface display in the following ways.

UI Related

Parameter	Default Value	Description
Number of items to view per page	15	The number of rows that appear on a single page in any of the Rogue System Detection tables, such as the Machine List or Subnet List. Once you have sensors deployed in your network, the Machine List, for example, can become very large. While you can display hundreds of rows in a table if you wish, you may find it easier to navigate the list if you keep the number to less than 20.
Sort systems by network subnet	Disabled	Enabling this feature keeps systems listed in the Machine List organized by subnet. Once enabled, sorting occurs within the subnet grouping only.
Auto Refresh delay	Enabled at 30 seconds	Auto refresh automatically refreshes the Rogue System Detection tables at a configurable time period. When auto refresh is enabled, the refresh status is listed as Refresh (Auto) above each table. If this is disabled, you must manually click the Refresh button above a table to refresh the data in that table.

E-mail alerting

Parameter	Default Value	Description
Mail server	mail-server	The name of the e-mail server to use for the e-mail alert automatic response.
From	from@example.com	The return e-mail address for the ePolicy Orchestrator server that should appear in the From field of e-mail alert messages.

Machine Classification Parameters

Parameter	Default Value	Description
Machine timeout	4320 minutes (3 days)	The period since the last time the computer was detected by a Rogue System Detection sensor after which a computer is listed as <i>Inactive</i> in the Machine List. The default is 3 days (entered in minutes) to allow for weekends, when users may shut down computers but those computers are not necessarily inactive.
ePO agent timeout	7 days	The amount of time after which an agent is considered inactive, if it has not reported to the ePolicy Orchestrator server. This affects whether a system is classified as rogue or managed; managed systems whose agents have stopped responding for the configured time period, but are still detected on the network by sensors, will be considered rogue.

Parameter	Default Value	Description
Find detected systems in ePO database by	MAC only	<p>When a detected system is processed by the Rogue System Detection server, one of the first things it must do is try to find that host in the ePolicy Orchestrator database. You can configure how it interrogates the database to find this.</p> <p>The options include:</p> <ul style="list-style-type: none"> ■ MAC only ■ MAC first, try hostname if MAC fails ■ MAC first, try hostname (including domain) if MAC fails <p>This parameter is useful when you have computers, such as laptops, that connect to the network by multiple methods (for example, Ethernet and a wireless card). Using this parameter allows you to ensure such computers don't appear as different computers depending on the method of connection. However, using this parameter can also result in false positives. Selecting MAC first, try hostname (including domain) if MAC fails option can reduce such false positives.</p>
Rogue system grace period	Disabled	<p>The time period at which a rogue system exists in the Rogue (In Grace Period) status before being classified as a Rogue (No Agent). See About system status and rogue type on page 189.</p> <p>There may a lag after the grace period expires and before the rogue system detected event triggers. This depends on what your sensor reporting interval is (default is 60 minutes).</p>

Sensor Parameters

Parameter	Default Value	Description
Sensor timeout	90 minutes	The period 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 Subnet List to <i>Inactive</i> .
Maximum number of primary sensors per subnet	Disabled	<p>The maximum number of sensors that report to the Rogue System Detection server, if there are multiple sensors deployed in the same subnet. The Rogue System Detection server automatically chooses which sensors to use as the primary sensors.</p> <p>McAfee recommends having at least two primary sensors per subnet.</p>
Maximum active time period for a primary sensor	12 hours	Rogue System Detection automatically changes the primary sensors at this interval. This is to avoid relying on any one sensor for too long.

Change 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. If you do only change the port number in the policy pages, you will break sensor-to-server communication. See [Configure Rogue System Detection sensor policies on page 197](#) for more information on changing sensor policies.



There are several `SERVER.XML` configuration files in different subfolders on the ePolicy Orchestrator server. Be sure you edit the one in the Tomcat subfolder only.

To change the port in the Tomcat `SERVER.XML` file:

- 1 Browse to the `SERVER.XML` file for the Tomcat server. By default, this file is installed in:

```
C:\Program Files\Network Associates\ePO\3.5.0\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 `TOMCAT.EXE` service on your ePolicy Orchestrator server.

Configuring Rogue System Detection for ePolicy Orchestrator Notification

You can configure ePolicy Orchestrator Notification to send notification messages based on certain events from Rogue System Detection events as well as the with the Automatic Response feature of Rogue System Detection. (For more information about using Automatic Response to send e-mail messages, see [Configure automatic e-mail alerts for new rogue detections on page 208](#).)

There are certain 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**.

For information and instructions on using Automatic Response to send e-mail messages, see [Configure automatic e-mail alerts for new rogue detections on page 208.](#))

ePolicy Orchestrator Notification

- Centralized alerting for all events types.
- Throttling and aggregation of messages.
- Ability to send SNMP traps as well as e-mail messages.

To configure to send notification messages from ePolicy Orchestrator Notification for Rogue System Detection events you must:

- [Configure an automatic response to send server events.](#)
- [Create a Notification rule based on Rogue System Detection events.](#)

Configure an automatic response to send server events

To configure an automatic response to send ePolicy Orchestrator server events:

- 1 Log on to the ePolicy Orchestrator server.
- 2 Click **Rogue System Detection** in the console tree.
- 3 Select the **Responses** tab in the details pane.
- 4 Click **Add Automatic Response**. The **Add or Edit Automatic Response** page appears.
- 5 Specify a **Name** for the automatic response. For example, **Send event to Notification**.
- 6 Select an **Event** for which to configure the automatic response. We recommend selecting **Any Event**.



Rogue System Detection can only send two events to ePolicy Orchestrator Notification: **Rogue Machine Detected** and **Subnet Uncovered**.

- 7 Add any desired conditions.
- 8 In the **Actions** section, under **Method**, change the default method to **Send ePO Server Event**.
- 9 Click **OK**.

Create a Notification rule based on Rogue System Detection events

Create a notification rule to send notification messages based on Rogue System Detection events. For instruction on notification rule creation, please see, [Creating and editing rules.](#)



ePolicy Orchestrator Notification can only send notification messages (regarding Rogue System Detection) based on ePolicy Orchestrator server events.

However, 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**.

We also recommend utilizing the aggregation and throttling features for all rules.

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 point product by ePolicy Orchestrator. For information, see [Deploying Rogue System Detection sensors on page 78](#).

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. For more information see, [Take manual actions on detected rogues on page 201](#) or [Configure automatic responses for specific events on page 207](#).

What happens when a sensor is deployed – in terms of agents and point products getting installed?

Sensor deployment does not affect the installation of agents and other point products. However, from the ePolicy Orchestrator console, the sensor can only be deployed to a system that already has an agent.

The sensor is simply another point product.

12

ePolicy Orchestrator Notification Configure rules to alert you to events on your network

The ePolicy Orchestrator Notification feature can alert you to any events that occur on the managed computers 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) when specific events are received and processed by the ePolicy Orchestrator server. The ability to specify the event categories which 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 ePolicy Orchestrator notifications, see [Product and component list on page 244](#).

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 (PUP) 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 computer 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, computers are found that are not up to date 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.

Using this feature

Using this feature requires that you perform four steps:

- 1 [Understanding how it works on page 225](#) — Before planning how you should configure your rules, you need to understand how the feature functions with your **Directory** and the rest of your network.
- 2 [Planning on page 231](#) — Before configuring the feature or creating its rules, you should consider how this feature can be best implemented in your environment.

- 3 [Configuring ePolicy Orchestrator Notification on page 231](#) — Before creating notification rules, define a contact list from which you select the recipients of notifications for each rule, and decide whether to allow site administrators to view global rules and the notification log.
- 4 [Creating and editing rules on page 235](#) — Define or modify the rules that generate notifications when events are processed by the ePolicy Orchestrator server.

Understanding how it works

Before you plan the implementation of ePolicy Orchestrator Notifications, you should understand how this feature works with ePolicy Orchestrator and its **Directory**.



This feature does not follow the inheritance model of ePolicy Orchestrator policy enforcement.

When events occur on computers in your environment, they are delivered to the ePolicy Orchestrator server, the notification rules (associated with the group or site that contains the affected computers and each parent above it) are applied to the events. If the conditions of any such rule are met, a notification message is sent per the rule's configurations.

This design allows you to configure similar (or very different) rules at the different levels of the console tree that may have different:

- Thresholds used to send a notification message. For example, a site administrator may want to be notified if viruses are detected on 100 computers within 10 minutes on the site, but a global administrator may not want to be notified unless viruses are detected on 1000 computers within the same amount of time within the entire environment.
- Recipients for the notification message. For example, you may want just the individual site administrator to receive a notification message if a specified number of virus detection events occur within his or her site. You may also want every site administrator to receive a notification message if a specified number of virus detection events occur within the whole **Directory**.

This section includes:

- [Throttling and aggregation on page 226](#).
- [Notification rules and the Directory scenarios on page 226](#).
- [Default rules on page 228](#).

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 Notification 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 235](#).

Notification rules and the Directory scenarios

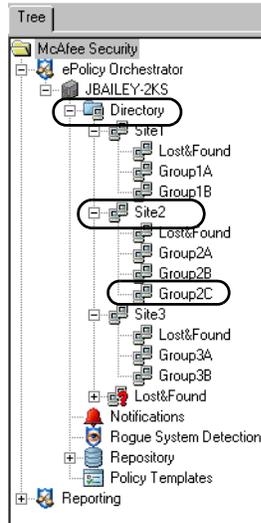
To show how this feature functions with the **Directory**, two scenarios are used.

For both scenarios, we can assume that each group, site, and the **Directory** of the console tree has a similar rule configured. These rules are each configured to send a notification message when 100 virus infection events have been received from any product within 60 minutes.

Scenario one

For this scenario, 100 virus infections are detected in **Group2C** within 60 minutes on a certain day.

Conditions of these rules configured at **Group2C**, **Site2**, and the **Directory** are met, sending notification messages per the rules' configurations.

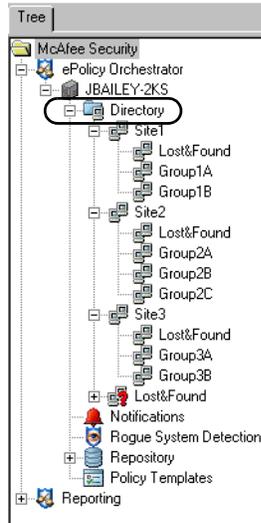
Figure 12-1 Console tree

Scenario two

For this scenario, 50 virus infections are detected in **Group2C** and 50 virus infections are detected in **Group3B** within 60 minutes on a certain day.

The **Directory** is the only node whose rule can be applied to all 100 events, so only this rule of the Director sends notification messages based on these 100 events.

Figure 12-2 Console tree



Default rules

To make implementing this feature easier, we've provided six default rules which you can enable to use this feature immediately while you familiarize yourself with abilities of ePolicy Orchestrator Notification.



Once enabled, these 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.

Daily unknown product notification

This rule sends a notification message when an event is received from any unknown product. This rule sends a notification message at most once a day.

Daily unknown category notification

This rule sends a notification message when an event of an unknown category is received from any product. This rule sends a notification message at most once a day.

Virus detected and not removed

This rule sends a notification message:

- When **Virus Detected and Not Removed** events are received from any product.
- When the number of events exceeds 1000 within an hour.
- At most once every two hours.

- With the source computer IP address, actual threat names, and actual product information, if available.

Virus detected heuristics and not removed

This rule sends a notification message:

- When **Virus Detected (Heuristic) and Not Removed** events are received from any product.
- When the number of events exceeds 1000 within an hour.
- At most once every two hours.
- With the source computer IP address, actual threat names, and actual product information, if available.

Repository update or replication Failed

This rule sends a notification message:

- When any **Repository Update Failure** or **Repository Replication Failure** events are received.

Non-compliant computer detected

This rule applies to an ePolicy Orchestrator server task (**Compliance Check**) that actually contains four rules that check for compliance on: **DAT file version**, **Engine version**, **Agent version**, and **VirusScan version**. This rule can only send one event per each of these four rules each time the task runs. A **Non-compliant Computer Detected** event represents a collection of all computers found for a given rule.

This rule sends a notification message:

- When a **Non-compliant Computer Detected** event is received.
- Once per each rule of the server task.

Getting started with the default rules

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 ePolicy Orchestrator Notification on page 232](#).
- Ensure the recipient e-mail address is the one with which you desire to receive e-mail messages. For more information, see [E-mail contacts list on page 233](#).

Determining when events are forwarded

The ePolicy Orchestrator server receives notifications from the Common Management Agent (CMA). You must configure its policy pages to either forward events immediately to the ePolicy Orchestrator server or only at agent-to-server communication intervals.

If you choose to have events sent immediately, 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 ePolicy Orchestrator Notification when the events occur, configure the agent to send them immediately.

If you choose not to have events sent immediately, then the agent only forwards events that are designated by the issuing product as high priority. Other events are only sent at the agent-to-server communication intervals.

To set the ePolicy Orchestrator agent policy:

- 1 Log in to the ePolicy Orchestrator server.
- 2 Select the **Directory**, or the desired site, group, or computer, then select the **Policies** tab in the upper details pane.
- 3 Select **ePolicy Orchestrator Agent | Configuration** in the upper details pane.
- 4 In the lower details pane, select the **Events** tab.
- 5 Deselect **Inherit**.
- 6 Configure the following policy options:

Event forwarding

Select **Enable immediate uploading of events** to enable the agent to forward events to the server immediately.



We recommend enabling immediate event forwarding if you plan on using global updating to distribute critical updates. Update events are assigned critical severity. For more information, see [Use global updating to automatically distribute updates to all clients immediately](#) on page 115.

Deselect this option to have the agent forward events only at the next ASCI. If this option is selected, you must specify:

- The lowest severity of events you want sent to the server in **Upload events of priority <SEVERITY> and above**. (For example, if you select **Minor**, then all events with a severity of Minor or more severe get forwarded to the server.)
 - The event forwarding interval in **Interval between immediate uploads**. The quantity of time you select here determines the highest frequency that events are forwarded. (For example, if you select **5 minutes** then the agent forwards events to the server every five minutes at most.)
 - The maximum number of events to send at a time in **Maximum events per immediate upload**. (If the number of events exceeds this limit, the remaining events are sent during the next event forwarding interval.)
- 7 Click **Apply All** to save these settings and changes will take effect during the next agent-to-server communication.

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, then all events are forwarded. This is the default setting.

If you want to select which events are forwarded on an immediate:

- 1 Log on to the ePolicy Orchestrator server.
- 2 Select the desired ePolicy Orchestrator database server under **Reporting** in the console tree and log on to it.
- 3 Select **Events** in the console tree under the database server.
- 4 Select the **Filtering** tab in the details pane.
- 5 Select **Send only the selected events to ePO** on the **Filtering** tab.
- 6 Select the desired events in the list and click **Apply**.

Planning

Before creating the rules that send notifications, it can save you time to plan:

- 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 244](#).
- Who should receive which notifications. For example, it may not be necessary to notify the site administrator of site B about a failed replication task 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 ePolicy Orchestrator Notification

To use this feature, you need to configure:

- [Basic configurations of ePolicy Orchestrator Notification on page 232](#) — 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 233](#) — This is the list from which you select recipients for notification messages.
- [SNMP servers on page 234](#) — 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 trigger a notification message.
- [Configuring external commands on page 235](#) — You can specify a list of external commands to run when the conditions of a rule are met.

Basic configurations of ePolicy Orchestrator Notification

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 Log on to the ePolicy Orchestrator.
- 2 Select **Notifications** under the desired **Directory** in the console tree.
- 3 Select the **Configuration** tab in the details pane, then click **Basic Configuration**.

Figure 12-3 Basic Configuration page

- 4 Under **UI Related**, choose:
 - **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.
 - **Allow site administrators to view rules outside of their site** — If selected, site administrators can view global rules and notifications. If deselected, site administrators can only view site rules and notifications, and cannot filter them.



Site administrators can never edit global rules.

- 5 Under **UI Related**, 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.

- 6 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.

To configure the e-mail contacts list:



It is not necessary to create a contact list, but you may find it more convenient.

- 1 Log on to the ePolicy Orchestrator.
- 2 Select **Notifications** under the ePolicy Orchestrator server in the console tree.
- 3 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 12-4 Add or Edit E-mail Message page

- 4 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 computers in your environment.

To use this feature:

- [Adding SNMP servers on page 234.](#)
- [Importing .MIB files on page 234.](#)



You do not need to make other configurations or start any services to set up 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 Log on to the ePolicy Orchestrator.
- 2 Select **Notifications** under the **Directory** in the console tree.
- 3 Select the **Configuration** tab in the details pane, then click **SNMP Servers**. Then **SNMP Servers** page appears displaying a list of the SNMP servers currently added.
- 4 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, just click the server in the list and the settings of this server appear.

Deleting an SNMP server from ePolicy Orchestrator Notifications

To delete an SNMP server from ePolicy Orchestrator 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\Network Associates\ePO\3.5.0\MIB
```

This file allows your network management program to decode the data in the SNMP traps sent by ePolicy Orchestrator 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 ePolicy Orchestrator notification rules to execute an external command when the rule is triggered. You must first add the registered executable before adding the command line that references the executable.



You can only configure registered executables on the ePolicy Orchestrator 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 a specific location on your computer.

To create the external commands list:

- 1 Log on to the ePolicy Orchestrator.
- 2 Select **Notifications** under the desired **Directory** in the console tree.
- 3 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.
- 4 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.

- 5 Type a **Name** for the external command.
- 6 Type or **Browse** to the external command you want the rule to execute when triggered.
- 7 Click **OK** to add the external command to the list.
- 8 Repeat [Step 4](#) through [Step 7](#) 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:

- [Step one: Describing the rule on page 236.](#)
- [Step two: Setting filters for the rule on page 237.](#)
- [Step three: Setting thresholds of the rule on page 238.](#)
- [Step four: Configuring the notifications for the rule on page 239.](#)

Step one: Describing the rule

The Describe Rule page allows you to:

- Define the **Directory**, site, or group for which the rule applies.
- Name and describe the rule.
- Set a priority for the notification message.

To begin creating or editing a rule:

- 1 Log on to the desired ePolicy Orchestrator server and select **Notifications** in the console tree.
- 2 In the details pane, select the **Rules** tab.
- 3 *If you want to create a new rule*, click **Add rule**. The **Add or Edit Notification Rule** wizard appears.

Figure 12-5 Describe Rule page

If you want 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** page, 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 ePolicy Orchestrator server must be unique. For example, if one site administrator creates a rule named **Emergency Alert**, then 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**.**Step two: Setting filters for the rule**

On the **Set Filters** page:

1 Select the **Products** whose events trigger this rule.

Figure 12-6 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
Unknown Product
Virex
VirusScan
VirusScan PDA
WebShield

Select All
Deselect All

Categories: Categories selected below Any category

Any selected

Access Protection rule violation detected and blocked
Access Protection rule violation detected and NOT blocked
Buffer Overflow detected and blocked
Buffer Overflow detected and NOT blocked
Intrusion detected
Normal operation

Select All
Deselect All

Threat or rule name: (Any)

2 Select **Categories** of events that trigger this rule.

Both the **Products** and **Categories** selections must be true for the rule to trigger 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 should use.

a Select an operator from the drop-down list.

- b Type any text for the operator act on. For example, the name of a virus.

For example, if you select **Contains** as the operator, then type **nimda** in the text box, then events are scanned for any line of text that contains **nimda** within it.



If you choose to filter on a threat name, then the **Products**, **Categories**, and the **Threat name** selections must all be true for the rule to send a notification message.

- 4 Click **Next**.

Step three: Setting thresholds of the rule

The **Set Thresholds** page allows you to define when the rule triggers 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 12-7 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 may also choose to send a notification when the specified conditions met. These conditions may include:
 - a **When the number of affected computers** is a defined number of computers
 - b **When the number of events** is a defined number of events.
 - c Either (by selecting both options).



You can select *one* or *both* of these options. For example, you can set the rule to send a notification if the number of affected computers 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**.

Step four: Configuring the notifications for the rule

You can choose to 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 notification of notification message to add.*
 - **Standard E-mail** — Select this option to create a subject line and body message to send to someone to an individual via e-mail message.
 - **SMS** — Select this option to define a brief message to send to a specified cell phone with SMS functionality.
 - **Text Pager** — Select this option to 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 to include in the notification is not represented, the information was not available in the event file.

- c Click **Save**, then go to [Step 5](#).
- 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 either the **Subject** or **Body** button 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 to include in the notification 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 *If you want to add an external command to be executed when the rule is triggered*, 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

The ePolicy Orchestrator feature also 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
- Notification list

Notification summary

The **Notification Summary** page allows you to view, a summary of the number of notifications sent by product or category:

- 1 Log on to the ePolicy Orchestrator.
- 2 Select **Notifications** under the desired **Directory** in the console tree.
- 3 Select the **Log** tab, then click **Summary**.
- 4 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
- 5 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 selected to allow reviewers and site administrators to view all notifications and rules, then site administrators and site reviewers are limited to viewing only notifications and rules for their sites.

- 6 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 appear.

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 Log on to the ePolicy Orchestrator.
- 2 Select **Notifications** under the desired **Directory** in the console tree.
- 3 Select the **Log** tab, then click **List**.
- 4 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, then 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, these can include:

- Time notification sent
- Notification rule name
- Rule priority
- Rule site

■ First event time	■ Rule defined at
■ Actual number of events	■ Actual products
■ Number of computers	■ Selected products
■ Affected computer IP addresses	■ Actual categories
■ Affected computer names	■ Selected categories
■ Source computers	■ Actual threat or rule names
■ Notification status	■ Selected threat or rule names
■ Notification type	■ Message subject
■ Event IDs	■ Event descriptions
■ Affected objects	■ 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 Notification 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 Log on to ePolicy Orchestrator.
- 2 Select **Notification** in the console tree.
- 3 Select the **Log** tab, then **List** in the details pane.
- 4 Click **Custom Filter**. The **Custom Filter** page appears.
- 5 Click **Add Condition**.
- 6 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.
 - **Received products** — Select **Received products** from the **Property** drop-down list, **contains** or **does not contain** from the **Comparison** drop-down list, then the product with which 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 with which 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 with which 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 with which you want to filter from the **Value** drop-down list.
- 7 Repeat [Step 5](#) and [Step 6](#) as needed until all conditions by which you want to filter the list are represented.
 - 8 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. Here is a list of products and components for which you can configure rules, and a list of all possible event categories.

Products and Components Possible Event Categories

Dr. Ahn	Access Protection rule violation detected and blocked
Desktop Firewall	Access Protection rule violation detected and NOT blocked
Entercept	Banned content or file detected and NOT removed
ePO Server	Banned content or file detected and removed
ePO Agent	Computer placed in quarantine mode
GroupShield Domino	E-mail content filtered or blocked
GroupShield Exchange	Encrypted/corrupted file detected and removed
System Compliance Profiler	Firewall rule triggered
Symantec NAV	Virus detected (heuristic) and NOT removed
NetShield	Virus detected (heuristic) and removed
NetShield for NetWare	Unwanted program detected (heuristic) and NOT removed
PortalShield	Unwanted program detected (heuristic) and removed
Stinger	Intrusion detected
ThreatScan	System Compliance Profiler rule violation
Unknown product	Non-compliant computer detected
Virex	Normal operation
VirusScan	On-access scan disabled
VirusScan PDA	Policy enforcement failed
WebShield	Repository update or replication failed
LinuxShield	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
	Virus detected and 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 only be sent once per a 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 during 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 the following notification targets: E-mail (including standard SMTP, SMS, and text pager), SNMP servers (via SNMP v1 traps), and any external tool installed on the ePO server. During the creation of a rule, you can define any combination of these notification formats for each rule you create.



SECTION 5

Stay Prepared with Periodic Maintenance

Perform regular maintenance tasks on a daily or weekly basis to keep ePolicy Orchestrator running smoothly over the long haul. Get started with running reports in ePolicy Orchestrator to monitor the health of your deployment. Maintain the **Directory** of managed computers as your network changes. Perform routine maintenance tasks on your ePolicy Orchestrator database to optimize performance and secure important data. Lastly, this section offers some suggestions and tips for staying prepared against virus outbreaks, as well as how to deal with them when they occur.

[Chapter 13, Getting Started with Reporting](#)

[Chapter 14, Maintaining the Directory](#)

[Chapter 16, Maintaining ePolicy Orchestrator Databases](#)

[Chapter 15, Preparing for and Managing Virus Outbreaks](#)

13

Getting Started with Reporting

An introduction to running reports with ePolicy Orchestrator

You can produce reports and queries for a group of selected client computers. You can also limit report results by product or computer criteria; for example, product name, product version number, or operating system. You can export reports into a variety of common file formats to distribute to key people or groups in your organization.

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 part of the ePolicy Orchestrator console tree is included in the report.
- Set a **Data Filter**, by using logical operators, to define precise filters on the data returned by for 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.

What is and is not covered in this chapter

This chapter contains an introduction to reporting only. It does not go into great detail about how reports work in ePolicy Orchestrator, or about advanced reporting features such as defining filters and writing custom reports and queries. For additional details on running reports in ePolicy Orchestrator, see the *Reports and Queries Implementation Guide*.

The topics covered in this section are:

- [About pre-defined reports in ePolicy Orchestrator](#)
- [How to generate a report in ePolicy Orchestrator](#)
- [Viewing report results in the report window](#)
- [Print or export reports into publishable formats](#)
- [Running Queries to get detail](#)
- [Saving filtered reports and queries as templates](#)
- [Writing custom reports in Crystal Reports](#)

About pre-defined reports in ePolicy Orchestrator

The ePolicy Orchestrator agent on the client systems communicates a variety of useful information back to the server. This information is stored in the reports database. You can run reports and queries against this stored information.

There are over 40 pre-defined reports that come with ePolicy Orchestrator. The default reports fall into two main categories: Coverage reports and Infection reports. In addition to the reports that available through ePolicy Orchestrator, you may also create your own report templates with the help of Crystal Reports 8.0.

What is the report repository?

The report repository contains both the pre-defined reports and queries that come with ePolicy Orchestrator and also any custom reports and queries you create yourself.

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 to 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, the administrator can easily view anti-virus policy compliance. Coverage reports provide snapshots of the anti-virus protection that is currently active on your computers. These reports are based on the computer and product property information stored in the server's database.

Examples of coverage information include what anti-virus product has been deployed and what version of DAT and engine files are installed on which clients. Compliance reports can help illustrate graphically problems you may be having with your ePolicy Orchestrator coverage, such as with getting DAT updates to particular computers. Run these reports and review them frequently to look for areas to improve your ePolicy Orchestrator coverage.

Infection reports show which viruses have been detected

Infection reports, by contrast, alert you to actual virus detections that may have occurred in your network. These reports can list which computers have the most virus detections (most likely your e-mail servers running GroupShield or Internet gateway running WebShield). They can list which specific viruses are being detected, and what actions were taken by the anti-virus software deployed in your network.

View summary information and drill down to detail

Another benefit when using ePolicy Orchestrator is the ability to receive both summary and detailed information from the same report. In this section, we will look at different reports and drill down into the reports for detailed analysis.

Summary reports can also be very 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. Most people are stunned to learn how many viruses ePolicy Orchestrator is routinely detecting, cleaning or removing.

Control access and filter results

You can control what visibility the different ePolicy Orchestrator users, such as global administrators or site reviewers, have into report information. Site administrators and site reviewers can only report on those client computers in sites to which they have rights.

How to generate a report in ePolicy Orchestrator

There are several ways in which you can control what data 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 computers 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.)

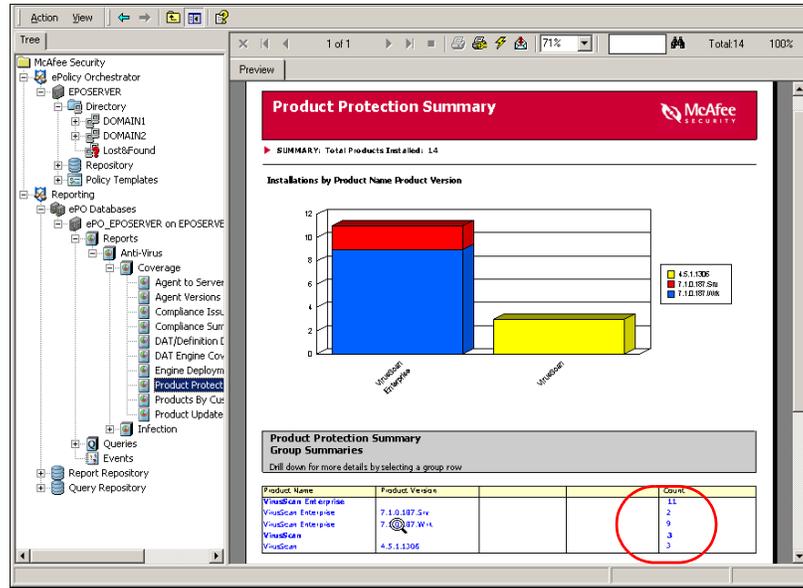
Once the results of a report appear, you can then perform a number of tasks on the data. You can view details on desired report data. (For example, to determine which client computers do not have a compliant version of VirusScan installed on them.) Some reports even provide links to other reports, called 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.

Generating a Product Protection Summary report

To run a *Product Protection Summary* report:

- 1 From the left-pane 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 in to the database, type your MSDE `sa` 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.

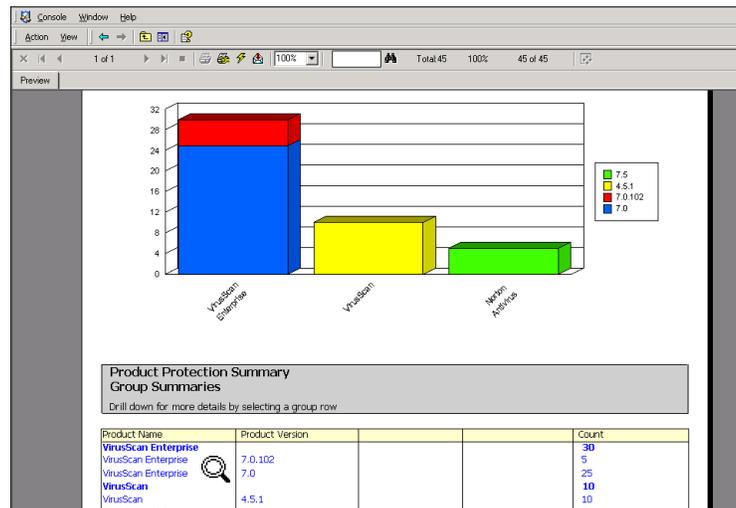
Figure 13-1 The Product Summary Report results show VirusScan Enterprise successfully installed on all servers and workstations



Viewing report results in the report window

The results of reports appear in the report window. You 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.

Figure 13-2 Highlighting report data



Select bits to drill down to.

If no additional data is listed, you've reached the details section of the report for the selected data.

Figure 13-3 Viewing details on report data

Product Protection Summary
Group Summary and Details

DRILLDOWN PATH: Product Name: VirusScan Enterprise > Product Version: 7.0.102

Product Name	Product Version	Count
VirusScan Enterprise	7.0.102	5

Page

Directory Path	ComputerName Username	Agent Version Contact Engine DAT	IPAddress DomainName OS Version Language
Directory_AVTest_WorkStations60.S1	Agents55.S1_AgentVer10.0.0.S1, AV45.S1,VirusScan2FW-10.S1,Engine45.S1,DAT8.S1		
Comp_Computer1.DAT8.S1	VirusScan Enterprise 7.0.102 SP1 HF1	3.0.123 2002-12-15 12:12:12	4.1.44 4.0-4136 Extrabab
Comp_Computer2.DAT8.S1		3.0.123 2002-12-15 12:12:12	0409

Print or export reports into publishable formats

After generating a report, you can print it to a network printer or export it to any number of standard formats such as an Adobe PDF document, Microsoft Excel spreadsheet, or HTML web page. Distributing reports or making them available for viewing is an important part of on-going ePolicy Orchestrator administration. Post a daily summary report on DAT compliance or top 10 viruses to a corporate web site. Distribute a weekly PDF report detailing virus infection and security information to key people in your organization to help remediate problems.

Some common export formats are:

- Adobe PDF
- Crystal Reports (RPT)
- Data Interchange Format (DIF)
- Microsoft Excel
- HTML and XML
- Text, Tab-delimited text
- Rich Text and Microsoft Word.

How to export a report data to other file formats

- 1 After running the report, click **Export** on the report toolbar.
- 2 In the **Export** dialog box, select the desired export **Format**.
- 3 Click **OK**. The **Choose Export File** dialog box appears.
- 4 Specify the name and location of the file, then click **Save**.

Running Queries to get detail

Queries provide a specific, single view. A query can either be a group summary or a detailed point view. They run faster than reports but do not support drilling down and some filtering.

Queries display data in a raw tabular form. They support **Directory** filtering and the creation of new user SQL queries. But do not support data filtering, drilling down, and the subreport features of reports.

In addition to the predefined queries that are available, you can also create your own custom queries if you have some experience writing SQL. In addition, you can refresh query data or go to specific rows in a query.

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 computers in a selected site or group, set a **Directory** filter.
- 3 In the console tree under **Reporting | ePO Databases | <DATABASE SERVER> | Queries | <QUERY GROUP>**, right-click **<QUERY>**, then select **Run**.
- 4 The resulting query appears in the details pane.
- 5 If you want 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**.
- 6 If you want 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.

Saving filtered reports and queries as templates

To save the selections you made in the **Current Protection Standards**, **Enter Report Inputs**, and **Report Data Filter** dialog boxes as a report template:



You can also save the selections you made in the **Enter Report Inputs** dialog box at the same time that you are making them.

- 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 location to which you want to store it temporarily, then click **Save**.
- 6 Add the Report Template file to the **Report Repository**.

Writing custom reports in Crystal Reports

ePolicy Orchestrator 3.5 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. Neither the *Product Guide* nor the *Reports and Queries Implementation Guide* go into detail about how to use Crystal Reports to write custom reports and queries. For information on how to do that, consult your Crystal Reports documentation.

14

Maintaining the Directory

Perform regular maintenance tasks to ensure the Directory accurately reflects the computers currently on your network

Performing regular maintenance on your **Directory** will likely be one of the tasks you will do most frequently in ePolicy Orchestrator on a daily or weekly basis. Making sure that the **Directory** is accurate and up-to-date makes doing all the other on-going things in ePolicy Orchestrator, such as pushing regular updates and running reports, much easier. The **Directory** is ePolicy Orchestrator's window to what is on your network. If it doesn't accurately reflect what is actually on your network, then you don't know how good your ePolicy Orchestrator coverage really is.

Over time, you will need to regularly make adjustments to the **Directory** as your network changes. Old or inactive computers that are no longer on the network need to be removed from the **Directory**, and you will need to make sure that new computers coming online are added. New computers with agents installed may appear in **Lost&Found** groups and need to be moved to the correct site or group to pick up the right policies. You may need to troubleshoot problems with specific computers.

What is covered in this chapter

- *Using Active Directory discovery*
- *Keeping imported NT domains synchronized with sites in the Directory*
- *Maintaining IP filters for sites and groups*
- *Scheduling a daily server task to find inactive agents in your Directory*
- *Use Directory Search to find computers in the Directory*
- *Manually moving nodes in the Directory*

Using Active Directory discovery

As you will recall, you can create sites and groups in the **Directory** by importing computers directly from your Active Directory containers. To ensure these sites or groups contain all of the computers actually in your Active Directory, you should periodically run the **Active Directory Computer Discovery** task to poll the Active Directory containers for new computers.

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

Use this procedure if you have created sites or groups by importing Active Directory containers when you created your **Directory**. See [Chapter 3, Creating a Directory of Managed Computers](#) for more information.

Using the Active Directory Computer Discovery task requires two steps:

- [Scheduling the Active Directory discovery task on page 255.](#)
- [Configuring Active Directory discovery mapping points on page 256.](#)

Once the task is configured, you can also run the **Active Discovery Computer Discovery** task immediately.

Scheduling the Active Directory discovery task

To schedule the **Active Directory Computer Discovery** task:

- 1 Select the desired ePolicy Orchestrator server in the ePolicy Orchestrator **Directory** tree in the left pane of the console.
- 2 Select the **Scheduled Tasks** tab in right pane of the console.

Click **Create task** to create a new task. If you chose to create an Active Directory Discovery task while in the **Active Directory Import** wizard, then select the task and click **Modify task** and the **Modify Task** page appears.

If you did not choose to create an **Active Directory Computer Discovery** task while in the **Active Directory Import** wizard, click **Create task**, and the **Configure New Task** page appears.

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

Figure 14-1 Task settings

- 4 In the **Task type** drop-down list, select **Active Directory Computer Discovery**.
- 5 Choose whether to enable or disable the task.

- 6 In the **Schedule type** drop-down list, select the desired interval to run the task, or whether to run it once or immediately.
- 7 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.
- 8 Under **Advanced schedule options**, configure the **Start time**, **Start date**, **End date** (if necessary), and how often you want to repeat the task if it fails.
- 9 Under **Advance 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** at the top of the page and go to [Configuring Active Directory discovery mapping points on page 256](#).

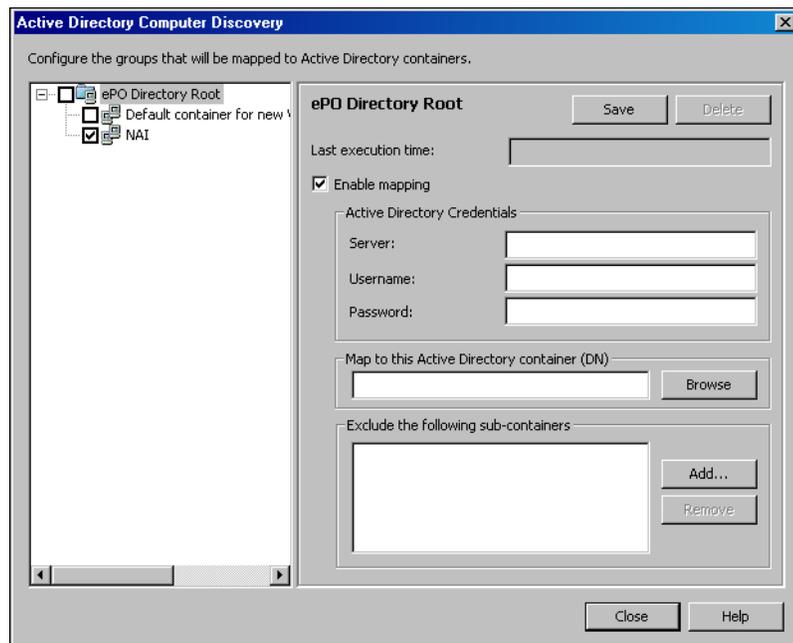
Configuring Active Directory discovery mapping points

To configure the mapping points between the ePolicy Orchestrator **Directory** root or sites and Active Directory containers:

- 1 Click **Configure Active Directory Computer Discovery** on the page that appears.

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

Figure 14-2 Active Directory Computer Discovery



- 2 Select the ePolicy Orchestrator **Directory** root or the desired site in the left pane of the dialog box that you want to map to an Active Directory container.
- 3 Select **Enable mapping** in the right pane of the dialog box, then enter the Active Directory credentials. The Active Directory credentials you enter must have read rights to the desired Active Directory container.

- 4 Under **Map to this Active Directory** container, click **Browse** and select the desired Active Directory container to map to the selected ePolicy Orchestrator item.
- 5 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 from the discovery task and click **OK**.
- 6 Once you've defined the settings for an ePolicy Orchestrator **Directory** item, click **Apply** at the top of the dialog box.



If you click **Close** before clicking **Save**, the task configurations are not applied!

- 7 If you want to map another ePolicy Orchestrator **Directory** item to an Active Directory container, select the desired **Directory** item in the left pane, and repeat [Step 3](#) through [Step 6](#).
- 8 Once you've configured and saved all mapping points for your Active Directory computer discovery task, click **Close**.

The task appears in the list of server tasks you have created. The **Next Run Time** field indicates the next time the task will run based on your schedule settings.

Running the Active Directory Discovery task immediately

You can run any server task immediately by selecting it from the list of available server tasks and clicking **Run Now**. The task will run immediately. Note that it will also still continue to run at its scheduled times.

To run the **Active Directory Discovery** task immediately:

- 1 Select the desired server in the console tree.
- 2 Select the **Scheduled Tasks** tab in the details pane.
- 3 Select the **Active Directory Discovery** task from the list of server tasks you have created.
- 4 Click **Run Now**.

Keeping imported NT domains synchronized with sites in the Directory

If you created sites (or groups) in your **Directory** by importing whole NT network domains, use ePolicy Orchestrator to periodically update the site. This ensures that the site actually contains the computers actually in that domain. You can add new computers that have recently appeared on the network to your site. You can also delete old computers no longer logged into the domain.

You can schedule a regular server task to do the synchronization, you can perform it manually, or both.

- [Schedule a regular domain synchronization server task](#)

- [Use Update Domain Directory task to synchronize specific domains manually](#)

Schedule a regular domain synchronization server task

You can create a server task to synchronize selected Windows NT domains that you have imported into the **Directory** with their counterparts on the network. If there is an existing site or group with the same name as the domain you select, the computers in the domain are added to that site or group. If the domains you select do not already exist in the **Directory**, they are automatically added as sites.

Use this procedure if you have created sites or groups by importing NT domains when you created your **Directory**. [Chapter 3, Creating a Directory of Managed Computers](#).

You can also perform this task manually.

The task does the following when adding new computers from the domain to a site:

- Adds the computers to the corresponding site or group in the **Directory**.
- Deploys the agent using the user account you provided. Pushing the agent is part of the synchronization task. When the task runs and imports new computers to the **Directory**, it automatically deploys an agent to the new computers.
- Applies policies and tasks for the site or group to these computers.

Because the agent cannot be deployed to all operating systems in this manner, you might need to manually deploy the agent to some computers. For information and instructions, see [Chapter 4, Deploying Agents, SuperAgents, and Sensors](#).

When a computer leaves a specified domain, this task removes the computer from the **Directory**.

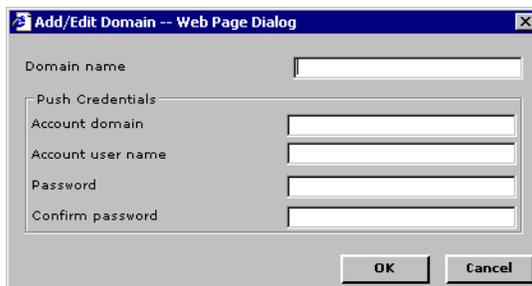
How to create a scheduled synchronize domains server task

To create a synchronize domains server task:

- 1 Select the server in the console tree, click the **Scheduled Tasks** tab in the details pane, and click **Create Task**.
- 2 Under **Task settings**, type the desired name of the task.
- 3 In the **Task type** drop-down list, select **Synchronize domains**.
- 4 Choose whether to enable or disable the 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. (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.
- 7 Under **Advanced schedule options**, configure the **Start time**, **Start date**, **End date** (if necessary), and how often you want to repeat the task if it fails.
- 8 Under **Advance 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**.

- 9 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 14-3 Add/Edit Domain dialog box



- 11 In the **Add/Edit Domain** dialog box, type domain administrator user account information as needed, then click **OK**.
- 12 To remove a domain from the task, select the domain, then click **Delete**.
- 13 Click **Finish** when done. The task appears in the **Scheduled Tasks** tab.

Use Update Domain Directory task to synchronize specific domains manually

In addition to scheduling a server task to do this, you can also manually synchronize sites or groups created by importing a Windows NT domain. Use the **Update Domain Directory** task to have ePolicy Orchestrator synchronize the computers in the site with the computers actually logged on to that domain on the network. As you update the domain, you can add computers currently in the domain but not in the selected site or group, or remove computers from your **Directory** site that are no longer in the domain. At the same time, you can also uninstall agents from all computers that no longer belong to the specified domain.



If you use the **Getting Started** wizard to import computers belonging to selected domains, you need to synchronize domains differently. For information, see [The Getting Started wizard on page 35](#).

To update your **Directory** with a Domain synchronization task:

- 1 Log on to the desired ePolicy Orchestrator server.
- 2 In the console tree, right-click the desired site or group, then select **All Tasks | Update Domain**. The **Update Domain** dialog box appears.
- 3 Click **Add All** or **Add** to move all or selected computers, respectively, from the network domain to the selected site or group.

Click **Remove All** or **Remove** to delete all or selected computers, respectively, from the selected site or group.

- 4 If you are removing computers, select **Uninstall agent from computers when they are removed from the group** to uninstall the agent when they are removed from the group.
- 5 Click **OK** when finished.

Maintaining IP filters for sites and groups

Perform regular maintenance of your IP filters to keep sites and groups organized.

- [Modifying IP filters for existing sites or groups](#)
- [Check integrity of IP filters](#)
- [Periodically sort computers by IP address](#)
- [Running an IP sort to sort computers by IP address](#)

Modifying IP filters for existing sites or groups

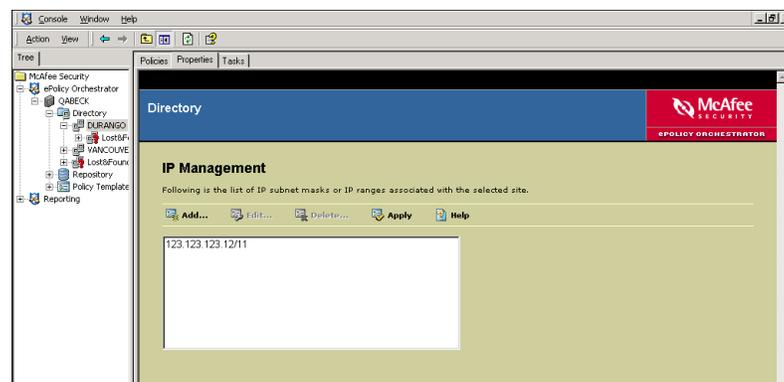
If you use IP filters in sites and groups in your **Directory**, you can assign new IP filters or change existing ones for sites and groups you have already created. You can also create these IP filters when you create your **Directory**.



If the IP filter is in place before the agents call into the **Directory** for the first time, you can use the **Sort Computers by IP** Directory task to automatically move computers from Lost&Found folders to the correct group. If the IP filter is added after the initial agent communication, you must move the computer manually from Lost&Found to the appropriate container. See [About IP address filters and sorting on page 42](#).

To view the current IP management settings for a given site or group, select it in the **Directory** and then click the **Properties** tab. The **IP Management** page shows which IP subnet masks or IP ranges have been specified for the selected site or group.

Figure 14-4 The IP Management page lists IP filters for the site or group



Adding IP filters to a site or group

You can add an IP address filter to an existing site or group. To do this:

- 1 In the ePolicy Orchestrator console, select the desired site or group in the **Directory**.
- 2 Click the **Properties** tab in the details pane to display the **IP Management** page, listing any IP filters that have already been configured for selected site or group.

- 3 Click **Add** to bring up the **Add IP Management** dialog box.

Figure 14-5 Add or change an IP Subnet mask or IP range for the selected site or group

- 4 Select **IP Subnet Mask** or **IP Range** and type the appropriate values.
- 5 Click **OK**.
- 6 On the **IP Management** page, click **Apply** to save the changes to IP filters for the selected site or group.



Your IP filter changes, additions, or deletions are not actually saved unless you click **Apply** on the **IP Management** page. If you leave the page without clicking **Apply**, your changes will be lost.

Changing IP management settings of existing sites or groups

To change the IP management settings assigned to existing sites or groups:

- 1 In the ePolicy Orchestrator console tree, select the desired site or group in the **Directory**.
- 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 Type changes to 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 assigned to existing sites or groups:

- 1 In the ePolicy Orchestrator **Directory**, select the site or group for which you want to delete an IP filter.
- 2 Click the **Properties** tab in the details pane. The **IP Management** page appears.
- 3 Select the desired IP filter from the list to highlight it.
- 4 Click **Delete**.
- 5 Click **Apply** to save the changes.

Check integrity of IP filters

Adding IP filters to sites and groups and then periodically using the **Sort computers by IP** address can help automate re-populating of the **Directory** when new computers appear on the network. Running an IP sort task automatically moves new computers to the correct site or group based on IP address. However, for IP sorting to work, all IP filters must be valid and not conflict with each other. To help you keep your IP filters valid, ePolicy Orchestrator provides an **IP integrity Check Directory** task.

IP sorting will not run if IP filters conflict between sites and groups. Therefore, run an IP integrity check any time you change IP filters or before you run an IP sort task.

How to run an IP integrity check:

- 1 In the ePolicy Orchestrator 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 computer causing the conflict appears in **List of conflicts**.

Table 14-1 Possible types of IP address conflicts

If the Type column displays...	Then the First node column displays...	And the Second node column displays...
Site	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.
Subset	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.
Overlap	The group whose IP address range or IP subnet mask overlaps with the group in the Second node column.	The group whose IP address range or IP subnet mask overlaps with the group in the First node column.

- 3 Select the conflict you want to review in **List of conflicts**. A description of the conflict displays in **Details**.
- 4 To jump to the site or group listed in the **First node** or **Second node** column, click the **First node** or **Second node** button, respectively. The **IP Management** page appears in the details pane.
- 5 To resolve conflicts, add, change, and delete IP address ranges or IP subnet masks as needed.
- 6 Repeat [Step 2](#) through [Step 5](#) until no conflicts are found.

Periodically sort computers by IP address

If you have added IP address filters to your sites and groups, you can run **Directory** tasks that sort the computers according to IP address. The task automatically moves computers to the appropriate site or group for that IP address. Computers that don't match the IP filter of a site or group are moved to a **Lost&Found** folder.

IP sorting does not work if there are any conflicts between the IP filters of different sites or groups. Run an IP integrity check on your **Directory** before running the IP sort task.

- [About sorting computers in the Directory by IP address](#)
- [Running an IP sort to sort computers by IP address](#)

About sorting computers in the Directory by IP address

The **IP Sorting** wizard uses two sorting methods:

The non-explicit sorting method is the default and sorts as follows:

- Follow the rules set by the explicit sorting method, unless one of the rules set in the non-explicit sorting methods takes precedence.
- If the computer is in a group that does not have an IP range, but that group is under a group that matches the computer's IP range, then leave it where it was found.
- If a computer resides under a group that is less appropriate than another group that has the correct IP range, the computer will be moved to the more appropriate group.

The explicit sorting method is an alternative method you can enable by inserting a new key in the `CONSOLE.INI` file. The explicit sorting method sorts as follows:

- Computer IP must match the IP range of its parent site. If no suitable site is found, the computer will be moved to the site specified by the user (global **Lost& Found** by default).
- (Optional) — If the computer belongs to a site, and no other groups are valid under that site, a new group must be created under the site **Lost&Found** before the computer can be moved to this site. The new group must be named after domain that the computer belongs to. This can only be enabled via the option in the `CONSOLE.INI` file.

The `UseExplicitLostFound` option determines how we treat systems that need to be moved to the **Lost&Found** or a site. If this option is enabled, computers are moved directly to the root of the **Lost&Found** or site. If the `UseExplicitLostFound` option is not enabled (default), and a computer needs to be moved to a site, the computer is moved to the site level **Lost&Found**.

In addition, if a computer needs to be moved to any **Lost&Found** (including the explicit move from site level), we create the computer's domain as a group under the **Lost&Found** and move the computer under the new **Lost&Found/domain** group.

Specifying explicit and non-explicit IP sorting in `CONSOLE.INI`

Use the **IP Sorting** wizard to sort computers by IP address. To specify the sorting method and rules for moving computers 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\NETWORK ASSOCIATES\EPO\3
```

If you upgraded your ePolicy Orchestrator server and console from version 2.5.1, the default location is:

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

The non-explicit sorting method and rules for moving computers are the default settings as indicated below:

```
[Sorting]
UseExplicitLostFound=0
UseExplicit=0
```

- 2 To enable the explicit sorting method or rules for moving computers, make this change:

```
[Sorting]
UseExplicitLostFound=1
UseExplicit=1
```

- 3 Save the file.

Running an IP sort to sort computers by IP address

Run the **Sort computers by IP** task periodically, such as once a week, to make sure computers are still located in the appropriate site or group for their IP address. The sort task moves computers to sites or groups based on the criteria for non-explicit or explicit sorting you have specified.

New computers that call into the server for the first time will automatically be added to the right site or group for their IP address. If, however, you define any IP filters after the initial agent-to-server communication, you must run the IP sort to re-sort the computers and move them to the appropriate site or group.

To run the IP sort:

- 1 Run an IP Integrity check on your **Directory** to confirm all IP filters are valid and don't conflict. For instructions, see [Check integrity of IP filters on page 262](#).
- 2 In the console tree, right-click the **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, select what you want the sort task to do with computers that are found to be in the wrong container for their IP address.
- 5 To exclude computers without IP management settings from being sorted, select **Ignore machines with no IP address**.
- 6 Click **Next** to sort the computers in the **Directory** using their IP management settings.
- 7 Click **Next**, then **Finish**.

Scheduling a daily server task to find inactive agents in your Directory

An inactive agent is an agent that has not communicated with the ePolicy Orchestrator server within a time period you specify. Some agents that you have deployed may become disabled or be uninstalled by end-users. In other cases, the computer hosting the agent may have been removed from the network. You should perform regular weekly searches of your **Directory** to find computers with these inactive agents.

When you find them, you can determine whether the computer is still on the network, perhaps by pinging it or passing the computer information to your IT team for follow up. If the computer is still on the network but the agent is inactive for whatever reason, you can re-install the agent. If the computer has been removed from the network, you can delete the computer from your **Directory**.



ePolicy Orchestrator provides several tools for keeping your **Directory** up-to-date, and you should use them together. Use a scheduled inactive agent maintenance server task in conjunction with a regularly scheduled Domain or Active Directory synchronization task. Also, periodically check the Rogue System Detection Machine List periodically to see what agents haven't communicated with the server in a while.

Find computers with inactive agents with a manual Directory Search

You can use the **Directory Search** feature to find inactive agents in part or all of your **Directory**. To do this, select the **Inactive ePolicy Orchestrator agents** search and specify a time period defining the inactive agent. Then you can then perform selected commands on computers found by the search. For instructions, see [Use Directory Search to find computers in the Directory on page 267](#).

Scheduling a regular Inactive Agent Maintenance server task

A more reliable way to periodically check your **Directory** for inactive agents is to schedule a regular, daily server task to find them. You can configure the task to move any computers with inactive agents to a special "Inactive Agent" group. You can then check this group periodically and take remediating action on any computers that the inactive agent task has moved there, such as deleting the computer from the **Directory** or pushing another agent to it.

To schedule a regular server task for finding inactive agents.

- 1 In the ePolicy Orchestrator console tree, select the server icon.
- 2 In the details pane, click the **Scheduled Tasks** tab in the details pane, and click **Create Task**.
- 3 In 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 14-6 Task settings

- 4 In the **Task type** drop-down list, select **Inactive Agent Maintenance**.
- 5 Enable the task by selecting **Yes** next to **Enable task**.
- 6 In the **Schedule type** drop-down list, select **Daily**. 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 14-7 Inactive Agent Maintenance Task page

- 9 To move computers with inactive agents to another group, select **Move** under **Action to perform**.
- 10 Type the name of a group to which any computers with inactive agents should be moved in **Move inactive agents to this group**. If this group doesn't already exist, it is created for you when the task runs.

11 Click **Finish** when done.

The new task appears in the **Scheduled Tasks** tab list, and the next time the task is scheduled to run is listed under **Next Run Time**. You can run the task manually at any time by selecting the task in the list and clicking **Run Now**.

Use Directory Search to find computers in the Directory

Use this procedure to quickly find computers using predefined search queries. For example, you can use the **Computers with a specific DAT version** query to find computer without the minimum level of protection. Or, you can search for a computer with a particular NetBIOS name. You can then perform selected commands on any computers found in the search, such as delete them from the **Directory** or push an agent to them.

Table 14-2 Types of Directory searches

Directory Search	Description
Computers in domain	Find a computer by NetBIOS name that also belongs to a specific network domain. Use this search instead of the generic Specific computers search if you have computers with the same name in different domains.
Computers in a specific group or site	Find a computer 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 computers with the same name in different domains.
Computers with a specific DAT version	Search for all computers currently running a specific DAT version.
Computers with a specific engine version	Search for all computers running a specific anti-virus engine version.
Duplicate computer names	Find duplicate entries of the same computer so you can remove the duplicates.
Inactive ePolicy Orchestrator agents	This is a manual search similar to the scheduled inactive agent search. See Use Directory Search to find computers in the Directory on page 267 .
Operating system	Find computers running a particular version of Windows.
Specific computers	Find specific computers by NetBIOS name.
Specific ePO agent version	Search for all computers running a specific anti-virus engine version.
Specific plugin version	Find computers with a specific plugin version.

How to perform a Directory Search

To find computers in the **Directory**:

- 1 In the ePolicy Orchestrator console tree, right-click the **Directory** or a site or group in the **Directory**, then select **Search**.
- 2 The **Directory Search** dialog box appears.
- 3 To display the path of computers, select **Get the location of each computer in the search results**.
- 4 Select the desired query in **Search for**.
- 5 For each **Field Name** listed, specify the **Operator** and **Value** to apply to the selected query.

- 6 Click **Search Now**. Computers that match the search criteria display under **Search Results**.

Select the desired computers in **Search Results**, right-click them, and select:

- **Send Agent Install** to deploy the agent. For instructions, see [Using ePolicy Orchestrator to deploy the agent on page 60](#).
- **Agent Wakeup Call** to send an agent wakeup call. For instructions, see [Sending manual agent wakeup calls on page 150](#).
- **Move To** to move computers to another site or group.
- **Delete** to remove computers from the **Directory**. (You can also remove the agent from these computers, by selecting **Uninstall agent from all connected computers**.)
- **Save As** or **Print** to save or print the search results.

Using wildcard characters to find computers

Using the **Directory Search** dialog box, you can use the following wildcard characters in conjunction with the **Operator like** to find computers in the **Directory**.

Table 14-3 List of wildcard characters

Use this character...	To find...	For example...
%	Any string of zero or more characters.	like <code>computer%</code> finds <code>computer1</code> , <code>computerNT</code> , and <code>computers</code> . like <code>%computer%</code> finds <code>computer1</code> , <code>computerNT</code> , <code>computers</code> , and <code>my computer</code> .
_	Any single character.	like <code>computer_</code> finds <code>computer1</code> and <code>computers</code> . like <code>computer__</code> finds <code>computerNT</code> .
[]	Any single character within a specified range; such as [a-f]; or set; such as [abcd].	like <code>PDX[abc]</code> finds <code>PDXA</code> , <code>PDXB</code> , <code>PDXC</code> . like <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].	like <code>PDX[^abc]</code> finds <code>PDXD</code> , <code>PDXF</code> , and <code>PDXG</code> . like <code>IT[^a-b]-Test</code> finds <code>ITD-Test</code> and <code>ITF-Test</code> .

Manually moving nodes in the Directory

Even if you have a perfectly organized **Directory** that mirrors your actual Network hierarchy, use IP filters, and you use automated tasks to regularly resynchronize your **Directory**, you may still need to manually move computers between sites or groups. For example, you may decide a certain computer should receive the policies of a different group and manually move it into that group. Or, you may need to periodically move computers from the **Lost&Found**.

If you are using IP filters in your **Directory**, make sure that the IP address information for the computer (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.

Drag and drop

You can use your mouse to drag-and-drop items from one **Directory** location to another, just as you would move files from one folder to another in Windows Explorer. When you release the item in the new location, you may see a standard message box alerting you that IP ranges may be broken. Click **OK** at this message box.

Cut and paste

To cut and paste items within the **Directory**:

- 1 In the console tree, right-click the desired group, computer, or appliance, then select **Cut**.
- 2 Right-click the site or group to which you want to move the item, then select **Paste**.
Verify the integrity of IP management settings. For instructions, see [Modifying IP filters for existing sites or groups on page 260](#).
- 3 Click **OK** at the message dialog about IP integrity.

15

Preparing for and Managing Virus Outbreaks

Strategies for keeping up-to-date and for dealing with a virus outbreak

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.

What's in this chapter

You can use ePolicy Orchestrator 3.5 to help stay prepared and then deal with virus outbreaks when they occur:

- *Things 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*

Things to do on a daily or weekly basis to stay prepared

You can use features of ePolicy Orchestrator 3.5 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 will take you some time initially to configure and schedule these tasks, 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.

Schedule server tasks to update repositories and do Directory clean up

Figure 15-1 Regular server tasks you should create and schedule

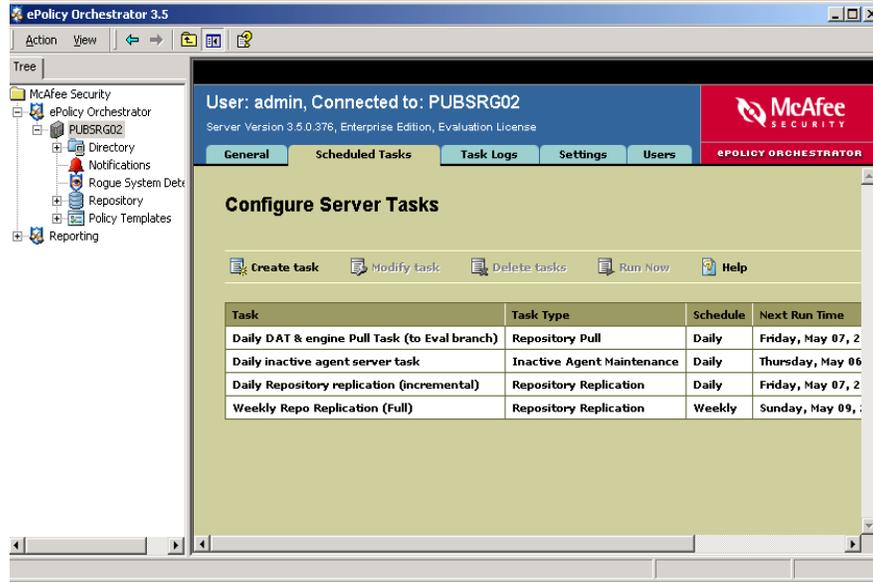


Table 15-1 Suggested server tasks

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 to run 4 times every day, starting at 1 am. Repeat task is selected to repeat the task every 6 hours, so it occurs 4 times a day.
Daily incremental repository replication	Replicates only changes to the master repository to all distributed repositories. It is scheduled to mirror the pull task by running 4 times a day, one hour after each repository pull (first one runs at 2 am).
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 Directory for computers with agents that have not communicated with the server and places them in an "InactiveAgents" group.

Schedule client update and scan tasks to keep clients protected

To keep anti-virus and security software on client computers 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.

Figure 15-2 Regular client tasks you should create and schedule

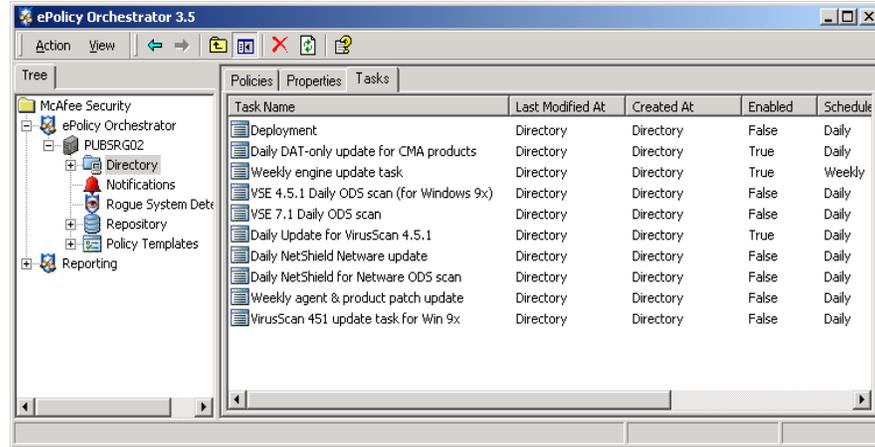


Table 15-2 Suggested client tasks

Client task	Task type	Description
Daily DAT-only client update task	ePolicy Orchestrator 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. Repeat task is selected to repeat the task every 6 hours, so it occurs 4 times a day. In the task Settings, select only DAT and EXTRA.DAT only. You will update these the most often.
Weekly engine-only client update task	ePolicy Orchestrator 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 task Settings, select only Engine .
Weekly agent patch and service pack update	ePolicy Orchestrator 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 Task Settings , select all the Service Pack and Patch types. You will update these the most often.
Daily VirusScan 4.5.1 update	VirusScan 4.5.1 for Windows AutoUpdate	Update DATs daily for Windows 9X clients 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 computers. 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 ePolicy Orchestrator 3.5 reports to determine coverage. For more information and instructions, see the *ePolicy Orchestrator 3.5 Report and Template Reference*.
- 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 computers 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 computers are compliant to the latest Microsoft patches and Service Packs.
- You have configured ePolicy Orchestrator Notification to send a message to you or others when specified events (like a virus detection) are received and processed by the ePolicy Orchestrator server.
- The Rogue System Detection feature is implemented to recognize and deploy agents to rogue computers and devices coming on to your network.
- You are performing regular, scheduled updates of products through ePolicy Orchestrator.
- You have enabled the agent wakeup call and tested the agent's communication with the computers 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. Computers 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:

- 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 computer.

- 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 computer, you must manually scan the system or computer using the command-line scanner, or use another anti-virus product.

16

Maintaining ePolicy Orchestrator Databases

Perform weekly database maintenance tasks to protect data and optimize performance

Regardless of whether you use an MSDE or SQL database with ePolicy Orchestrator, your databases will require regular maintenance over time. This ensures the database is performing well and that the data in it is protected.

Depending on your deployment of ePolicy Orchestrator, plan on spending time each week, perhaps a few hours, performing regular database backups and maintenance. Many of the tasks in this section should be done on a regular basis, either weekly or daily. Some are only required at specific times, such as when there is a problem.

You can use a combination of tools to maintain ePolicy Orchestrator databases. You will use a slightly different set of tools depending on whether you are using a Microsoft Data Engine (MSDE) 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.

What is in this section

There are tasks you should perform regularly on the ePolicy Orchestrator databases:

- *Perform daily or weekly database maintenance.*
- *Back up your ePolicy Orchestrator database regularly.*
- *Repairing events and computer names in the database.*
- *Deleting old events from the database periodically.*
- *Changing SQL Server user account information*
- *Restoring ePolicy Orchestrator databases in the event of software or hardware failure.*

Perform daily or weekly database maintenance

To keep your database from growing too large and to keep performance optimized, perform regular database maintenance on it. McAfee recommends doing this daily, if possible, or weekly at the very least. Performing this maintenance regularly can help keep the size of your database down and thereby improve database performance.

The procedure varies whether you are running an MSDE or SQL database:

- *Perform weekly maintenance on MSDE databases*

- [Perform regular maintenance for SQL Server databases](#)

Perform weekly maintenance on MSDE databases

Use the SQLMAINT.EXE utility to regularly perform clean-up and maintenance on your MSDE database. By default, the SQLMAINT.EXE utility is installed in your MSDE installation folder on your ePolicy Orchestrator server.

Run this utility at least once a week. You can use SQLMAINT.EXE command-prompt utility to perform routine database maintenance activities. It can be used to run DBCC checks, to dump a database and its transaction log, to update statistics, and to rebuild indexes.

The simple procedure below does not cover everything you can do with SQLMAINT to maintain your MSDE database, but rather the minimum you should do on your ePolicy Orchestrator database each week. See the Microsoft web site for additional information on `SQLMAINT` and what it can do for your database.

To perform MSDE database maintenance using the SQLMAINT.EXE utility, do the following once a week:

- 1 Type the following at the command prompt (the commands are case sensitive):

```
SQLMAINT -S <SERVER> -U <USER> -P <PASSWORD> -D <DATABASE> -RebldIdx 5  
-RmUnusedSpace 50 10 -UpdOptiStats 15
```

Where `<SERVER>` is the name of the ePolicy Orchestrator server, where `<USER>` and `<PASSWORD>` are the user name and password of the user account, and where `<DATABASE>` is the name of the ePolicy Orchestrator database. The default database name is `EPO_<SERVER>` where `<SERVER>` is the name of the ePolicy Orchestrator server.

- 2 Press ENTER.

Perform regular maintenance for SQL Server databases

Use SQL Enterprise Manager to perform regular maintenance of your SQL ePolicy Orchestrator database.

The simple procedure below does not cover everything you can do to maintain your SQL database in SQL Enterprise Manager. See your SQL documentation for details on what else you can do to maintain your database.

Change recovery model to simple

Set the recovery model to **simple**. This is a one-time change to your SQL Server settings, and it is very important. While MSDE databases install with the simple recovery model by default, SQL Server installs using a different recovery model that doesn't allow the transaction log to be cleaned as easily. This can cause the log to swell in size.

To change the SQL Server recovery model to simple:

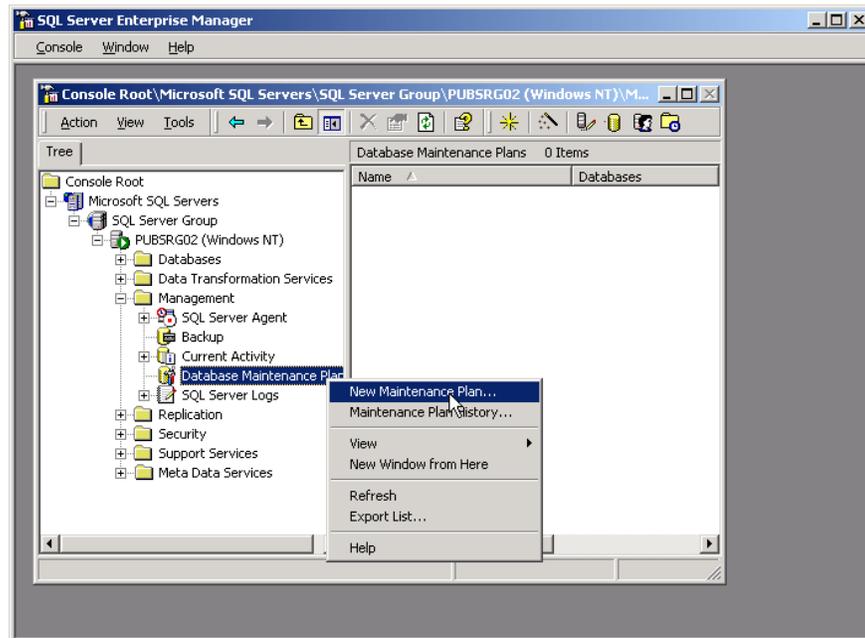
- 1 In SQL Server Enterprise Manager under **Microsoft SQL Servers | SQL Server Group | <DATABASE SERVER> | Databases** in the console tree, right-click `<DATABASE>`, then select **Properties**. The **Properties** dialog box for the selected ePolicy Orchestrator database appears.
- 2 Click the **Options** tab.

- 3 Under **Recovery**, select **Simple** in **Model**, then click **OK**.

Run the Enterprise Manager Maintenance Plan Wizard

- 1 Open SQL Enterprise Manager.
- 2 In the console tree under **Microsoft SQL Servers | SQL Server Group | <DATABASE SERVER> | Management**, right-click **Database Maintenance**, then select **New Maintenance Plan**.

Figure 16-1 Begin a maintenance plan in SQL Server Enterprise Manager



- 3 When the **Database Maintenance Plan Wizard** appears, click **Next**.
- 4 In the **Select Databases** dialog box, select **These databases**, then select the user database and deselect the system databases: **master**, **model**, and **msdb**.

The name of the user database is the name of the ePolicy Orchestrator database. The default name of ePolicy Orchestrator databases is **EPO_<SERVER>**, where **<SERVER>** is the name of the ePolicy Orchestrator server.
- 5 Click **Next**. The **Update Data Optimization Information** dialog box appears.
 - Select **Reorganize data and index pages**.
 - Select **Change free space per page percentage to**, and type **10** as the percentage.
 - Select **Remove unused space from database files**.
 - Schedule the data optimization tasks to execute during off-peak times. Click **Change** to change the default schedule.
- 6 Click **Next**. The **Database Integrity Check** dialog box appears.
- 7 Select **Check database integrity** and **Perform these checks before doing backups**.
- 8 Click **Next**. The **Specify the Database Backup Plan** dialog box appears.

- 9 Schedule the database backup tasks to execute during off-peak times. Click **Change** to change the default schedule.
- 10 Click **Next**. The **Specify Backup Disk Directory** dialog box appears.
- 11 Select **Use the default backup directory**.
- 12 Click **Next**. The **Specify the Transaction Log Backup Plan** dialog box appears.
- 13 Select **Back up the transaction log as part of the maintenance plan** and **Verify the integrity of the backup when complete**.
- 14 Schedule the transaction log backup tasks to execute during off-peak times. Click **Change** to change the default schedule.
- 15 Click **Next**. The **Specify the Transaction Log Backup Disk Directory** dialog box appears.
- 16 Select **Use the default backup directory**.
- 17 Click **Next** three times. The **Completing the Database Maintenance Plan Wizard** dialog box appears.
- 18 Click **Finish**.

Back up your ePolicy Orchestrator database regularly

McAfee recommends that you back up ePolicy Orchestrator databases regularly to protect your data and guard against hardware and software failure. You may need to restore from a backup, such as if you ever need to reinstall the server.

How often you backup depends on how much of your ePolicy Orchestrator data you are willing to lose. At a minimum, back up your database once a week, but you might want to backup daily if you have been making lots of changes to your deployment. You could also do daily backups as part of an automated nightly job. You can also spread the work by doing incremental daily backups and then a full weekly backup each week. Save the backup copy to a different server than the one hosting your live database—if your database server crashes you don't want to lose your backup too.

In addition, see [Restoring ePolicy Orchestrator databases in the event of software or hardware failure](#) on page 285.

Backing up a SQL database--see your SQL documentation

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

Backing up an MSDE database

If you are using Microsoft Data Engine (MSDE) as the ePolicy Orchestrator database, you can use the Database Backup Utility (DBBAK.EXE) to back up and restore ePolicy Orchestrator MSDE databases on the database server.



The database backup utility works while the ePolicy Orchestrator server service is running. However, McAfee recommends stopping the ePolicy Orchestrator NAIMSERV.EXE server service before beginning the backup.

You can back up and restore MSDE databases to the same path on the same database server using this utility. You cannot use it to change the location of the database. To back up ePolicy Orchestrator Microsoft Data Engine (MSDE) databases using the McAfee Database Backup Utility (DBBAK.EXE):

1 Stop the McAfee ePolicy Orchestrator 3.5 Server service and ensure that the SQL Server (MSSQLSERVER) service is running. For instructions, see the operating system product documentation.

2 Close all ePolicy Orchestrator consoles and remote consoles.

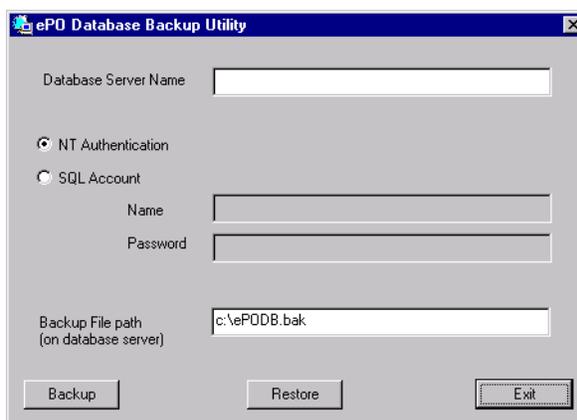
3 Start the Database Backup Utility (DBBAK.EXE). The default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0

If you upgraded the software from version 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFEE\EPO\3.5.0

Figure 16-2 Database Backup Utility



4 Type the Database Server Name.

5 Select NT Authentication or SQL Account.

If you selected SQL Account, type a user Name and Password for this database.

6 Type the Backup File path.

7 Click Backup.

8 Click OK when the backup process is done.

9 Start the McAfee ePolicy Orchestrator 3.5 Server service and ensure that the MSSQLSERVER service is running. For instructions, see the operating system product documentation.

Repairing events and computer names in the database

Every computer is assigned a unique ID called a global unique identifier (GUID). These IDs are stored with events in the ePolicy Orchestrator database and identify which client computers generated each event. In addition, it's important to track when computers are renamed. These associations are necessary to ensure that infection reports are accurate.

Certain conditions cause computers to be assigned a new ID. In these cases, the ID stored in the database no longer matches the ID assigned to the computer. You need to update the events in the database that correspond to these mismatched IDs, to ensure that infection data is reported accurately.

Here are some common examples of situations that cause computers to be assigned a new ID:

- Changing the MAC address on computers.
- Changing the network interface card (NIC) in computers.
- Renaming computers.
- Uninstalling, then reinstalling the agent. Note that agent AutoUpgrade does *not* generate a new ID.
- Using a common image of the software and hardware to build computers.
- Using a docking station with laptop computers.

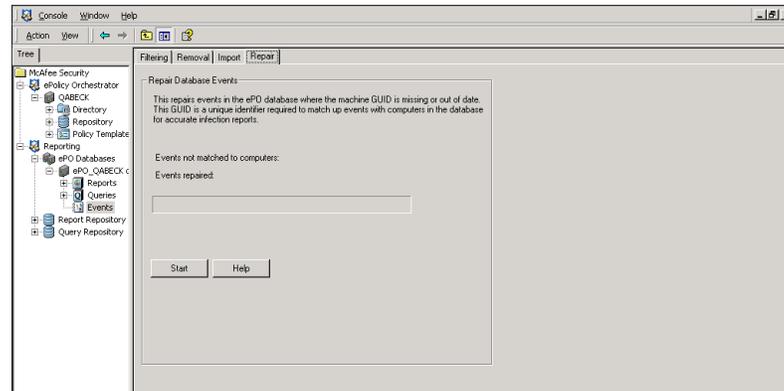
Repairing events in the database

Use this procedure to synchronize the ID in events in the selected ePolicy Orchestrator database with the IDs of computers on the network.

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

- 1** Back up the database. For instructions, see [Back up your ePolicy Orchestrator database regularly on page 279](#).
- 2** Log on to the desired ePolicy Orchestrator database server using ePolicy Orchestrator authentication.
- 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 **Repair** tab.

Figure 16-3 Repair tab



- 5 Click **Start** to synchronize the IDs in events with IDs of computers on the network.
- 6 If **Events not matched to computers** is greater than zero after the repair process has completed, you need to also repair computer names. For instructions, see [Repairing computer names associated with events in the database on page 282](#).

Repairing computer names associated with events in the database

Use this procedure whenever computer names have changed to update events with the new computer names.

- 1 Repair events in the database. For instructions, see [Repairing events in the database on page 281](#).
- 2 In your database maintenance tool (for example, SQL Server Query Analyzer), run the following SQL statement on the database for each renamed computer or create a SQL script that contains a SQL statement for each renamed computer:

```
UPDATE EVENTS SET HOSTNAME='<NEW COMPUTER>' WHERE HOSTNAME='<OLD COMPUTER>'
```

Where <NEW COMPUTER> and <OLD COMPUTER> are the current and previous computer names, respectively.

- 3 Repeat as necessary.

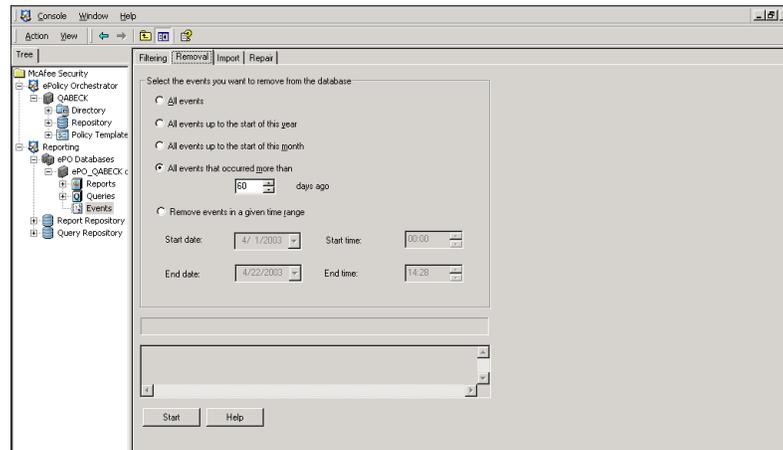
Deleting old events from the database periodically

You may want to periodically delete events from the database to keep the database size down and improve performance. Many events, especially informational and minor events, are less useful over time. Furthermore, you can and should back up the database before deleting events of any kind from the database. You can archive this database and use it later for historical reporting if you need to.

Use this procedure to delete events permanently from the ePolicy Orchestrator database.

- 1 Back up the database. For instructions, see [Back up your ePolicy Orchestrator database regularly on page 279](#).
- 2 Log on to the desired ePolicy Orchestrator database server.
- 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 **Removal** tab.

Figure 16-4 Removal tab



- 5 Select the events that you want to remove from the database.
 - **All events** — Selecting this option removes all events from the database.
 - **All events up to the start of the year** — Selecting this option removes all events before the beginning of the current calendar year.
 - **All events that occurred more than X days ago** — Selecting this option allows you to remove events older than the number of days you specify.
 - **Remove events in a given time range** — Selecting this option allows you to specify a range of dates. Any events that occurred within the date range are removed.
- 6 Click **Start** to delete the specified events from the database.

Changing SQL Server user account information

Use this procedure to change the SQL Server user account information in ePolicy Orchestrator when you make changes to the SQL Server authentication modes in another program, for example, SQL Server Enterprise Manager. Do this if you need to use a privileged SQL user account for added network security.

To change the SQL Server authentication information:

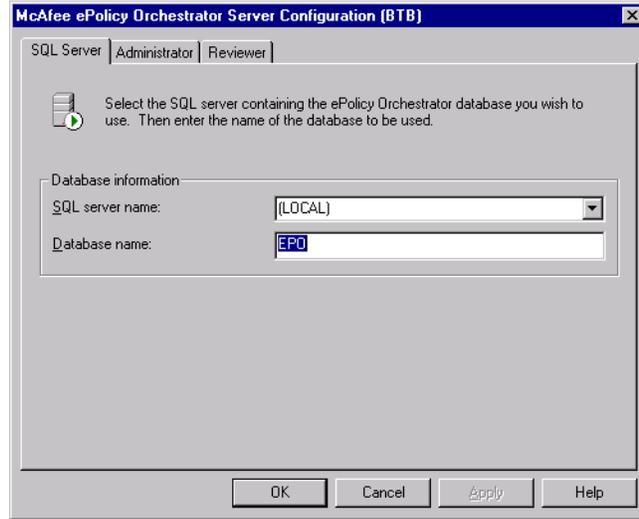
- 1 Start the Server Configuration program (CFGNAIMS.EXE). The default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0

If you upgraded the software from version 2.5.1, the default location is:

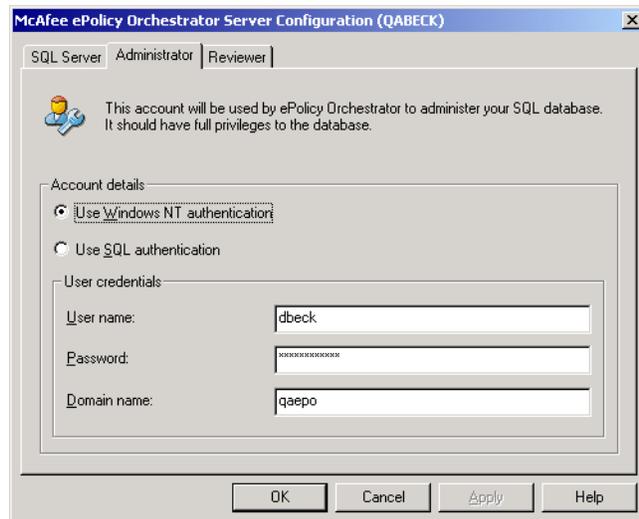
C:\PROGRAM FILES\MCAFFEE\EPO\3.5.0

Figure 16-5 Server Configuration program



- 2 In the **Server Configuration** dialog box on the **SQL Server** tab, select the desired SQL server name and **Database name**.
- 3 To change the credentials on the ePolicy Orchestrator global administrator user account, click the **Administrator** tab, then select the authentication mode. Depending on the Authentication Type you chose, make the necessary selections:
 - Type a **User Name** and **Password** of a local or domain administrator user account.
 - Type the **Domain name**.

Figure 16-6 Administrator tab in the Server Configuration dialog box



- 4 To change the credentials on the ePolicy Orchestrator reviewer user account, click the **Reviewer** tab, then select the authentication mode. Depending on the Authentication Type you chose, make the necessary selections:

- Type a **User Name** and **Password** of a local or domain administrator user account.
 - Type the **Domain name**.
- 5 Click **OK** when done.
 - 6 Restart the computer to apply the changes.

Restoring ePolicy Orchestrator databases in the event of software or hardware failure

If you have been backing up your database regularly as McAfee recommends, then restoring it is easy. You should not need to do this very often, or ever. Aside from software or hardware failure, you need to restore the database from a backup if you want to upgrade your ePolicy Orchestrator server or database server hardware.

The process varies depending on whether you are backing up a SQL or MSDE database. To restore a SQL Server database, see your SQL Server documentation.

Restoring an MSDE database from a backup

You can back up and restore MSDE databases to the same path on the same database server using this utility. You cannot use it to change the location of the database. To restore ePolicy Orchestrator Microsoft Data Engine (MSDE) databases that you backed up using the Database Backup Utility (DBBAK.EXE):

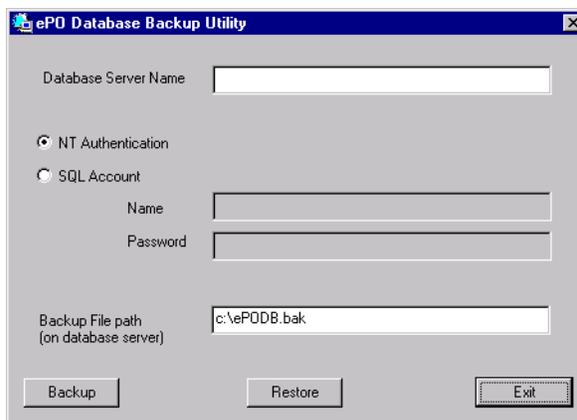
- 1 Stop the **McAfee ePolicy Orchestrator 3.5 Server** service and ensure that the **MSSQLSERVER** service is running. For instructions, see the operating system product documentation.
- 2 Close all ePolicy Orchestrator consoles and remote consoles.
- 3 Start the Database Backup Utility (DBBAK.EXE). The default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0

If you upgraded the software from version 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFFEE\EPO\3.5.0

Figure 16-7 Database Backup Utility



- 4** Type the **Database Server Name**.
- 5** Select **NT Authentication** or **SQL Account**.
- 6** If you selected **SQL Account**, type a user **Name** and **Password** for this database.
- 7** Type the **Backup File path**.
- 8** Click **Restore**.
- 9** Click **Yes** when asked whether you want to overwrite the entire ePolicy Orchestrator database.
- 10** Click **OK** when the restore process is done.
- 11** Start the **McAfee ePolicy Orchestrator 3.5 Server** service and ensure that the **MSSQLSERVER** service is running. For instructions, see the operating system product documentation.



SECTION 6

Appendices, Glossary, and Index

Appendix A, Maintenance Tools

Appendix B, Using ePolicy Orchestrator over the Internet

Appendix C, Reference

Glossary

A

Maintenance Tools

The ePolicy Orchestrator software provides some additional tools, log files, and error messages to help troubleshoot issues and record performed tasks, and who performed them.

Topics in this section include:

- [Minimum Escalation Requirements Tool](#).
- [Audit log](#).

Minimum Escalation Requirements Tool

The McAfee Minimum Escalation Requirements Tool (MERTool) is a utility that is designed to gather reports and logs for the McAfee software on your system. The tool must be launched manually and only collects information following user input. The information obtained can be used to help analyze problems.

To get more information about MERTool and access the utility, click the *MERTool* file that was installed with the ePolicy Orchestrator product.

This file is located in the installation folder. If you accepted the default installation path, this file is located in:

```
<drive>:\Program Files\Network Associates\
```

When you click the *MERTool* file, it accesses the URL for the MERTool web site. Follow the instructions on the web site.

Audit log

The ePolicy Orchestrator 3.5 software provides a log file (EPOAUDIT.LOG) that records all of the ePolicy Orchestrator tasks and which administrator or reviewer performed them.



The audit log is not supported for use with Microsoft SQL 7.

The information recorded in the log file provides accountability in your network environment.

This file logs the following administrative actions:

- | | |
|-----------------------------|--|
| ■ User login | ■ Adding or deleting a group |
| ■ Adding or deleting a user | ■ Adding or deleting a computer |
| ■ User role change | ■ Uninstalling an agent when deleting |
| ■ User password change | ■ Renaming sites, groups, or computers |
| ■ Adding or deleting a site | ■ Policy changes |

Installing the auditing feature

To install the audit log feature:

- 1 Copy the EPOAUDITINSTALL.EXE file from the ePolicy Orchestrator installation directory. The default location is:

```
C:\Program Files\Network Associates\ePO\3.5.0\Auditing
```
- 2 Log on to the computer running the SQL Server used for ePolicy Orchestrator. You must use an account with local administrative privileges.
- 3 Paste the EPOAUDITINSTALL.EXE file to a temporary location on this computer.
- 4 Execute the EPOAUDITINSTALL.EXE file.
- 5 Restart the computer, or stop and restart the SQL Server service (and all dependent services).

Reading the audit log

Log files are created for each day and are stored in `C:\ePOAudit\`.

A SQL job is scheduled to run just before midnight each day and produces a log for the entire day. The name of the file is `EPO MM.DD.YY.CSV`. Where `MM.DD.YY` is the month, day, and year of the log file.

These files can be viewed using Microsoft Excel.

Uninstalling the auditing feature

To uninstall the auditing feature, use **Add/Remove Programs** to remove **McAfee ePO Audit Logs for SQL**.

B

Using ePolicy Orchestrator over the Internet

ePolicy Orchestrator was designed for Internet use. It allows agent-to-server communication over the Internet if the firewall is configured to allow the correct range of IP addresses.

- Internet scenarios.
- Remote access via VPN and RAS.
- Corporate intranet.
- Connecting through an ISP and a firewall.
- Configuring the firewall for ePolicy Orchestrator.
- Agent-to-server communications packet size.

Internet scenarios

The following options are discussed here:

Behind a firewall

- Microsoft Remote Access Service (RAS), where a remote user (agent) dials into one of the ports to access the network behind the firewall.
- Virtual Private Networks (VPN), where remote users (agents) dial into a port provided by a commercial carrier, but access is still behind a single firewall.

Open to the Internet

- Internet Service Provider (ISP), where transactions between the user (agent) and the server cannot be contained behind a firewall because the IP address remains open to the Internet.

Remote access via VPN and RAS

Many situations require that ePolicy Orchestrator consoles or agents are deployed outside the physical perimeter of the corporate intranet. To minimize configuration and security issues, it is highly recommended that remote agents or consoles access the server via a VPN or Microsoft RAS connection. Use of proxies is not supported.

Corporate intranet

There are many network topologies in which the ePolicy Orchestrator software and its components can be deployed. The simplest deployment and the highest level of security are achieved when you deploy all of the ePolicy Orchestrator components within a particular corporate intranet, behind a single firewall. In this scenario, all components of the network topology are located in fixed physical locations, all with the appropriate access to the corporate intranet.

This topology is the simplest to implement for system administrators.

In this scenario, administrators can leverage existing corporate infrastructure to allow seamless access to ePolicy Orchestrator services. Any firewall issues are hidden by the VPN and RAS transports.

Connecting through an ISP and a firewall

Agent

The agent can access ePolicy Orchestrator servers via an ISP (Internet Service Provider) with several restrictions:

- The ISP must be able to resolve the ePolicy Orchestrator server IP address.
- The ISP can use DHCP to assign random IP addresses, which the corporate firewall must accept.
- The ePolicy Orchestrator server cannot push the ePolicy Orchestrator agent over a firewall. In this environment, the agent must be delivered via alternate media.
- The port on the firewall used for agent-to-server communication is port 80. It must be configured for incoming and outgoing agent-to-server traffic. The default value for this port is 80, but you can define a different value during server installation.
- The port on the firewall used for console-to-server communications is port 81. The default value is 81, but you can define a different value during server installation.
- The port on the firewall used for agent wakeup calls is port 8081. You can change this value dynamically using the server configuration feature, described in [Server Settings on page 186](#).

Console

Using an ISP to connect the console to the server is strongly discouraged for the following reasons:

- The ePolicy Orchestrator console cannot operate over some older firewalls, because it uses the HTTP "Keep Alive" function for many of its transactions. Removing "Keep Alive" from the console would significantly impact performance in usage scenarios where the console is "inside" the corporate intranet.
- Accessing SQL server inside the company firewall creates a significant security risk.

Configuring the firewall for ePolicy Orchestrator

Any of the following three options allows agent-to-server communications:

No firewall

- If there is no firewall, agent-to-server communication is open.

Firewall with open HTTP port

- If the HTTP port is already open in the firewall, no action is needed. Communications are open.

Firewall with no open HTTP port

- Destination rule — Create a destination rule for the firewall configuration that opens only the ePolicy Orchestrator server to communicate with the agents outside the firewall. A destination rule specifies only the ePolicy Orchestrator server IP address as the destination for incoming HTTP traffic.
- Source rule — Create a source rule in the firewall configuration that allows only designated client computers to talk to the ePolicy Orchestrator server. This allows a range of IP addresses access to the server via the port. Precautions must be made to prevent someone hijacking the IP address and using it improperly.

Agent-to-server communications packet size

Following is an example of packet sizes:

Table B-1 Typical Packet Size for Agent-to-Server Communication

Activity (per computer)	*Full Size (KB)	*Incremental Size (KB)
Agent sends properties	10	2
Agent checks for new policies (no new policies)	2	—
Agent checks for new policies (new policies)	5 – 9	—
* The packet size can vary depending on events collection.		

C

Reference

This chapter contains useful reference information on various aspects of ePolicy Orchestrator administration. The following topics are covered:

- How to read operating system data.
- Locale IDs.
- Product IDs.
- Variables.

How to read operating system data

The CMA retrieves data about the operating system of client computers from the operating system itself. For this reason, the data that appears in reports, queries, and in the computer properties is not immediately obvious. Use the table below to determine the version number that corresponds to each operating system. This table is helpful when using operating system name or version number to limit report results.

Operating System Name	Operating System Version Number	Service Pack
Windows 95	4.0	
Windows 98	4.10	1998
Windows 98 SE	4.10	2222A
Windows NT	4.0	
Windows 2000	5.0	
Windows Me	4.9	
Windows XP Professional	5.1	

Action taken numbers

When viewing queries, use this table to determine how supported anti-virus products responded to detected viruses.

Action Taken	Description	Action Taken	Description
(blank)	Unknown	59	Not Scanned
2, 3, 4	Continued Scan	60	Continued Scan
50	Cleaned	61	Deleted
51	Clean Error	62	Heuristic Error
52	Deleted	63	Moved
53	Delete Error	64	Heuristic Error
54	Excluded	65	Cleaned
55	Exclude Error	66	Heuristic Error
56	Access Denied	67	Continued Scan
57	Moved	68	Test Virus
58	Move Error	69	Scan Timed Out

Locale IDs

Occasionally, you might need to know the locale ID that corresponds to each language. The ePolicy Orchestrator software uses this ID to identify languages.

Locale ID	Languages	Locale ID	Language
0000	More than one language	0415	Polish
0404	Chinese (Traditional)	0416	Portuguese (Brazil)
0405	Czech	0419	Russian
0406	Danish	0804	Chinese (Simplified)
0407	German (Standard)	0809	English (United Kingdom)
0409	English (United States)	0810	Italian (Switzerland)
0410	Italian	040a	Spanish (Traditional Sort)
0411	Japanese	040b	Finnish
0412	Korean	040c	French (Standard)
0413	Dutch	041d	Swedish
0414	Norwegian	0c04	Chinese (Hong Kong)

Product IDs

The software uses a unique product ID to identify each version of every supported product. In some places within the software (for example, in log file entries or within directory structures), the product ID appears instead of the product name and version number. Use this table to identify the product name and version number that corresponds to each product ID.

Product ID	Product Name and Version Number
ALERTMNG4500	Alert Manager 4.5
EPOAGENT2000LYNX	Agent for WebShield appliances 2.0
EPOAGENT3000	Agent for Windows 3.0
GSDOMINO5000	GroupShield Domino 5.0.0
LWI___6000	Setup program for VirusScan TC 6.0
NAE___2100	Agent for NetWare 2.1.0
NAV___7500	Norton AntiVirus Corporate Edition 7.50, 7.51, 8.0
NETSHLD_4500	NetShield 4.5 for Windows NT
NSNW__4600	NetShield NetWare 4.6.0
PCR___1000	Product Coverage Reports 1.0
VIRUSCAN4500	VirusScan 4.5
VIRUSCAN6500	VirusScan 4.5.1, VirusScan 4.5.1 with Service Pack 1
VIRUSCAN6000	VirusScan TC 6.0
VIRUSCAN7000	VirusScan Enterprise 7.0.0

Variables

You can use these predefined variables in various dialog boxes and policy pages. You can also use system environment variables.

Client computers use the values from user environment variables, then system environment variables. For more information on environment variables, see the Windows product documentation.

The location you specify using these variables must exist on client computers.

Variable	Description
<COMPUTER_NAME>	The name of the client computer. This is the NetBIOS name on Windows computers, the DNS name on Unix computers, and NDS name on NetWare computers.
<DOMAIN_NAME>	The domain name or workgroup name to which the client computer belongs.
<PROGRAM_FILES_COMMON_DIR>	The path of the Windows common folder; for example, C:\PROGRAM FILES\COMMON.
<PROGRAM_FILES_DIR>	The path of the program files folder; for example, C:\PROGRAM FILES.
<SOFTWARE_INSTALLED_DIR>	The installation directory of the corresponding McAfee product.
<SYSTEM_DIR>	The Windows system directory; for example, C:\WINNT\SYSTEM32 or C:\WINDOWS\SYSTEM.
<SYSTEM_DRIVE>	The drive where the operating system is installed; for example, C:.
<SYSTEM_ROOT>	The path of the Windows root directory; for example, C:\WINNT or C:\WINDOWS.
<TEMP_DIR>	The Windows temporary directory; for example, C:\TEMP.
<USER_NAME>	The user name of the currently logged on user account.

Glossary

agent AutoUpgrade

The act of automatically upgrading the agent whenever a newer version is available on the ePolicy Orchestrator 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-to-server communication

Any communication that occurs between ePolicy Orchestrator agents and the ePolicy Orchestrator 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-to-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, trigger alert messages.

anti-virus policy

See *policy*.

ASCI

See *agent-to-server communication interval*.

AutoUpdate

The automatic program in the McAfee software 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.

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 ePolicy Orchestrator 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 ePolicy Orchestrator 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 ePolicy Orchestrator console.

console tree

The contents of the Tree tab in the left pane of the ePolicy Orchestrator 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 ePolicy Orchestrator 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 ePolicy Orchestrator console, which shows details of the currently selected console tree item. Depending on the console tree item selected, the details pane can be divided into upper and lower panes.

See also *upper details pane* and *lower details pane*.

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 ePolicy Orchestrator 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 ePolicy Orchestrator 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 ePolicy Orchestrator database. This can be the same computer on which the ePolicy Orchestrator server is installed or a separate computer.

ePolicy Orchestrator database

The database that stores all data received by the ePolicy Orchestrator server from ePolicy Orchestrator 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 ePolicy Orchestrator server.

See also *ePolicy Orchestrator console*.

ePolicy Orchestrator server

The back-end component of the ePolicy Orchestrator software.

See also *ePolicy Orchestrator agent* and *ePolicy Orchestrator console*.

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 ePolicy Orchestrator 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 ePolicy Orchestrator 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 ePolicy Orchestrator 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.

legacy updating

XX

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.

lower details pane

In the console, the lower-right pane, which displays configuration settings for the products listed on the **Policies** tab in the upper details pane.

See also *details pane* and *upper details pane*.

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 ePolicy Orchestrator 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*.

mirror, mirroring

The act of copying the contents of one distributed software repository to another outside of the normal replication process. This is typically used when the master repository cannot access the computer hosting the repository for some reason.

NAP file

Network Associates Package 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.

POAGAINST.EXE

See *agent installation package*.

policy enforcement interval

The time period during which the agent enforces the settings it has received from the ePolicy Orchestrator 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 ePolicy Orchestrator server, but cannot be accessed via a remote console.

See also *policy templates*.

policy pages

Part of the ePolicy Orchestrator console; they allow you to set policies and create scheduled tasks for products, and are stored on individual ePolicy Orchestrator servers (they are not added to the master repository). Also referred to as NAP files.

policy templates

Set of policy settings for one or more products that is stored in the ePolicy Orchestrator database and is available from the ePolicy Orchestrator console.

See also *policy 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

Attributes or characteristics of an object used to define its state, appearance, or value.

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 remote 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 (SITE.LIST.XML)

The SITE.LIST.XML file that is used by those McAfee anti-virus 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 ePolicy Orchestrator server that is recorded by the Windows Event Viewer. This information is not stored in the ePolicy Orchestrator 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 ePolicy Orchestrator server when needed, rather than waiting for the next agent-to-server communication interval (ASCI).

See also *agent wakeup call*.

SuperAgent

A type of ePolicy Orchestrator 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*.

task

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.

upper details pane

In the console, the upper-right pane, which contains the **Policies**, **Properties**, and **Tasks** tabs.

See also *details pane* and *lower details pane*.

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, 254
 discovery task, 255
 integration with ePolicy Orchestrator, 12
 mapping points, 256
adding
 user accounts, 27
 WebShield appliances to the Directory, 56
administrator accounts (See user accounts)
agent
 activity log, 159
 ASCII, 148
 ASCII packet size, 292
 command-line options, 162
 deploying to WebShield, 72
 distributing, using third-party deployment tools, 68
 enabling, 69
 events, 229
 installation command-line options, 73
 installation, using search feature to send agent install, 267
 interface, 161
 introduction, 8
 log, 159
 NAP, 153
 operating system data, 293
 policies, 141, 148, 153, 158
 properties, 158
 selective updating policies, 30, 124
 uninstalling, 72 to 73
 upgrading from 2.5.1, 70
 upgrading from 3.x, 70
 wakeup call, 150
agent deployment, 45, 57, 64, 67
 installing manually, 66
 to NetWare servers, 72
 to WebShield appliances, 72
 with ePolicy Orchestrator, 57, 60 to 62

 with login script, 64
Agent Monitor, 161
agent wakeup call, 150
 using search feature to send, 267
 with client task, 151
agent-to-server communication
 packet size, 292
aggregating notifications, 222, 226
appliances, adding WebShield, 56
architecture, distributed update repository, 10 to 14
ASCII (agent-to-server communication interval), 148
audience for this manual, 14
audit log, 288 to 289
auditing feature
 installing and uninstalling, 289
 overview, 13
AVERT security headquarters
 contacting, 20
 contacting if outbreak occurs, 274
 DAT file notification service, 20
 submitting a virus sample to, 18
 WebImmune, 20

B

bandwidth usage
 monitoring network performance, 272
 product deployment improvements, 10 to 14
beta program, contacting, 20

C

checking in packages, 89, 112
client tasks, 163
 agent wakeup call, 151
 changing, 178
 daily and weekly, 270
 deleting, 179
 on-demand scan, 174
 running, 175
 scheduling, 178
 update, 115
 update task, 174

 VirusScan Enterprise on-demand scan, 176
compliance check, 180
 server task, 180 to 181, 183
computer names
 finding duplicates in the Directory, 267
configuring
 external commands, 235
 notifications, 231
console (See ePolicy Orchestrator software)
console tree items
 Directory, 269
 organizing the Directory, 268
 WebShield appliances, 56
consulting services, 20
contacting McAfee, 20
conventions for DNS computer names, 82
creating
 distributed repositories, 130, 132
 notification rule based on Rogue System Detection events, 222
Crystal Reports, 253
customer service, contacting, 20
cut and paste, moving items in the Directory, 268

D

DAT file, 112
 and engine update, 118
 checking in manually, 112
 daily update, 118
 deleting from repository, 127 to 128
 evaluating, 123
 McAfee update web site, 20
 repository branches, 127
 update notification service, 20
DAT file updating, 99, 122
 from source repository, 103
 in master repository, 101
 with client task, 115
database
 changing SQL accounts, 283
 deleting events, 282

- maintaining, 276
 - MSDE maintenance, 277
 - repairing events, 281 to 282
 - restoring from backup, 285
 - SQL maintenance, 277
 - definition of terms (*See* Glossary)
 - deleting
 - client tasks, 179
 - computers from the Directory, 267
 - events from the ePolicy Orchestrator database, 282
 - user accounts, 28
 - deploying products, 89
 - deployment
 - improvement in bandwidth usage, 10 to 14
 - devices, adding WebShield appliances, 56
 - Directory
 - Active Directory, 256
 - Active Directory discovery, 254 to 255
 - add computers, 205
 - autopopulating, 49
 - create from Active Directory, 49
 - creating, 39
 - creating sites and groups manually, 53
 - Directory Search, 267
 - domain synchronization, 257 to 258
 - finding inactive agents, 265
 - importing a computer from a domain, 52, 54
 - importing a computer from a text file, 54
 - importing from Active Directory, 49 to 50
 - inheritance, 40
 - IP filters, 44, 260, 269
 - IP integrity check, 262
 - IP sorting, 42, 262
 - maintaining, 254
 - methods for creating, 48
 - moving computers, 268
 - planning, 46
 - search feature to delete computers, 267
 - synchronizing with NT domains, 259
 - updating domains, 259
 - Directory, creating
 - about, 40
 - deploy agent, 64
 - from NT domain, 51
 - from text file, 54
 - disabled agent, enabling, 69
 - distributed repositories, 130
 - about, 130, 138
 - architecture for update, 10 to 14
 - creating, 130, 132
 - FTP, HTTP, UNC, 135
 - local, 143
 - nonmanaged, 143
 - replicating to, 139 to 140
 - SuperAgent, 132
 - documentation for the product, 16
 - domain synchronization, manual, 259
 - download web site, 20
 - duplicate computer names, finding in the Directory, 267
- E**
- e-mail contact, 233
 - e-mail notifications, 208
 - enabling the agent, 69
 - engine
 - checking in manually, 112
 - deleting from repository, 127 to 128
 - repository branches, 127
 - engine updating, 99
 - from source repository, 103
 - in master repository, 101
 - ePolicy Orchestrator database
 - removing events, 282
 - ePolicy Orchestrator server, 21, 29
 - events, 33
 - logging on, 21
 - server tasks, 31
 - settings, 31
 - version, 34
 - ePolicy Orchestrator software
 - configuring the firewall for, 292
 - connecting through an ISP and firewall, 291
 - console, introduction, 9
 - new features, 10
 - events, 229
 - removing, 282
 - virus detection, 225 to 226, 274
 - exporting
 - report data to other formats, 251
 - repository list to a file, 146
 - EXTRA.DAT, 114
- F**
- fallback repository (*See* repository)
 - FAQ (frequently asked questions), 223, 245
 - feature comparison, 10 to 14
 - features, new in this release, 10
 - Active Directory integration, 12
 - ePolicy Orchestrator administrator auditing, 13
 - ePolicy Orchestrator Notification, 11
 - McAfee Enterecept integration, 14
 - Rogue System Detection, 10
 - selective updating, 14
 - support for variable MAC address, 13
 - System Compliance Profiler, 11
- G**
- getting information, 16
 - list of contacts, 20
 - within the product, 17
 - Getting Started wizard, 26, 35 to 37, 259
 - global updating, 115
 - new features, 11 to 14
 - selective updating, 30, 124
 - glossary, 297
 - groups, 260
 - from text file, 54
 - groups (*See* Directory)
- I**
- importing a computer
 - from a domain, 52, 54
 - from a text file, 54
 - inactive agents
 - finding with daily server task, 265
 - inheritance, 40
 - resetting, 173
 - installation (*See* Installation Guide)
 - installing the auditing feature, 289
 - integrity check, IP address, 260
 - Internet Service Provider (ISP), 290
 - IP address, checking integrity, 260
 - IP filters, Directory, 260
 - IP integrity check, 262
 - IP management
 - sorting computers by, 264
 - IP sorting, 262
- L**
- links to resources in the product, 17
 - local distributed repositories, 143
 - Locale IDs, 75, 294
 - login scripts, 64
- M**
- MAC address, variable, 13
 - Machine Summary page, 193
 - maintenance tools, 288
 - manuals for the product, 16
 - master repository
 - pulling from source repository, 107, 109, 111

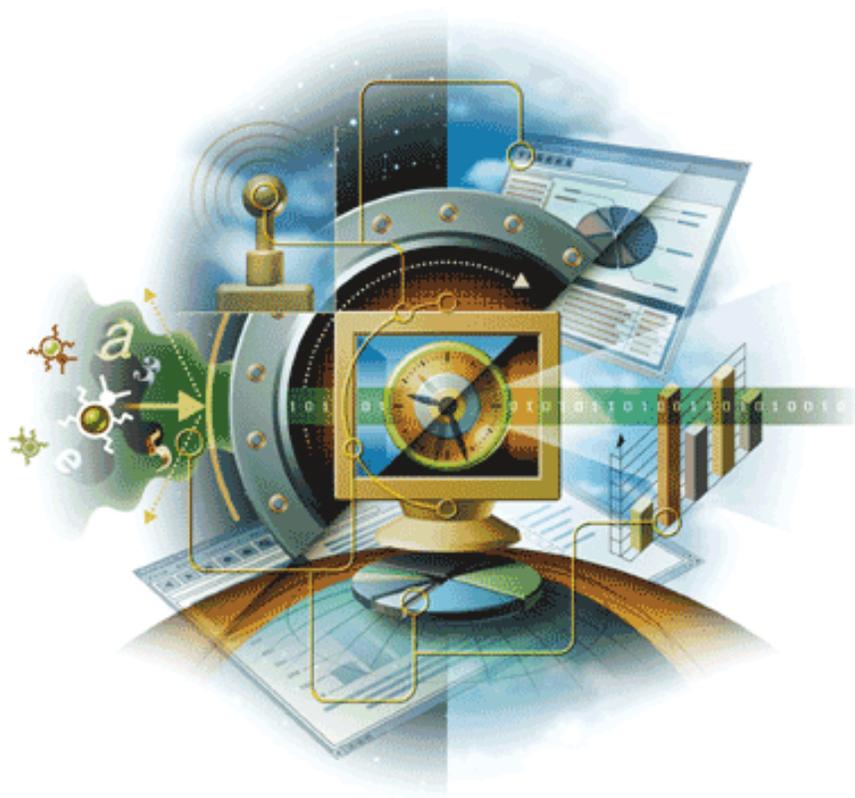
- replicating to distributed repositories, [139 to 140](#)
 - McAfee AutoUpdate Architect
 - importing repositories, [145](#)
 - McAfee University, contacting, [20](#)
 - MERtool (Minimum Escalation Requirements), [288](#)
 - Microsoft Remote Access Service (RAS), [290](#)
 - monitoring network performance, [272](#)
 - moving items in the Directory
 - via cut and paste, [268](#)
 - via search feature, [267](#)
 - MSDE database maintenance, [277](#)
- N**
- naming conventions, [82](#)
 - NAP package, [164](#)
 - checking in, [93](#)
 - defined, [303](#)
 - deleting, [168](#)
 - NetWare server, [72](#)
 - network performance, monitoring, [272](#)
 - new features, [10](#)
 - global updating, [11 to 14](#)
 - nodes (*See* console tree items)
 - notification service, DAT updates, [20](#)
 - notifications, [180 to 181](#), [183](#), [211](#), [221 to 222](#), [224](#), [226](#), [228 to 229](#), [231 to 232](#), [235](#), [242](#), [273](#)
 - aggregation, [222](#), [226](#)
 - configuring, [231](#)
 - configuring notifications, [232](#)
 - default rules, [228 to 229](#)
 - history, [240](#)
 - how they work, [225](#)
 - notification list, [240 to 243](#)
 - rules, [226](#), [235](#)
 - summary, [240 to 241](#)
 - throttling, [222](#), [226](#)
 - NT domains
 - importing to Directory, [51](#)
 - synchronizing with Directory, [257](#), [259](#)
- O**
- on-site training, [20](#)
 - outbreaks
 - preparation checklist, [272](#)
 - recognizing, [273](#)
 - overview
 - auditing feature, [13](#)
 - ePolicy Orchestrator servers, [21](#)
 - ePolicy Orchestrator software, [7](#)
 - Rogue System Detection, [190](#)
 - selective updating, [14](#)
- P**
- packages
 - checking in, [89](#), [112](#)
 - dependencies, [91](#)
 - moving between branches in repository, [127](#)
 - ordering, [91](#)
 - signing and security, [91](#), [113](#)
 - unsigned, [91](#), [113](#)
 - versioning and branches, [114](#)
 - password, changing on user accounts, [28](#)
 - pkgcatalog.z, [114](#)
 - policies, [164](#)
 - about, [163](#)
 - copying, [169](#)
 - exporting and importing, [169](#)
 - exporting to template, [170](#)
 - importing from a template, [172](#)
 - resetting inheritance, [173](#)
 - policy pages (NAP), [164](#)
 - PrimeSupport, [20](#)
 - product deployment package
 - checking in, [89](#)
 - product IDs, [295](#)
 - product information
 - documentation, [16](#)
 - resources, [16](#)
 - training, [20](#)
 - products
 - deploying, [88](#)
 - deploying with ePolicy Orchestrator, [94](#)
 - properties for products, [158](#)
 - proxy server, [107](#), [157](#)
 - Pull Now task, initiating, [111](#)
- Q**
- queries, [252](#)
 - saving as template, [252](#)
- R**
- RAS, [290](#)
 - reference information, [293](#)
 - administering ePolicy Orchestrator, [293](#)
 - locale IDs, [294](#)
 - product IDs, [295](#)
 - reading operating system data, [293](#)
 - variables, system environment and predefined, [296](#)
 - remote console, [290](#)
 - connecting through firewall, [291](#)
 - connecting to server over the Internet, [290](#)
 - corporate intranet, [149](#), [290 to 291](#)
 - removing
 - events from the database, [282](#)
 - user accounts, [28](#)
 - Replicate Now task, [140](#)
 - replicating repositories, [139](#)
 - replication tasks, [139](#)
 - initiating, [140](#)
 - reporting
 - exporting reports, [251](#)
 - generating, [249](#)
 - introduction, [247](#)
 - queries, [252](#)
 - repairing events, [281 to 282](#)
 - results, [250](#)
 - saving reports and queries as template, [252](#)
 - reports
 - about, [248](#)
 - exporting data to other formats, [251](#)
 - repository
 - about, [100](#)
 - branches, [102](#), [123](#), [127](#)
 - creating, [106](#)
 - distributed repository, [69](#)
 - nonmanaged, [143](#)
 - fallback, changing, [103](#)
 - master repository
 - deleting NAPs and products, [168](#)
 - moving and deleting packages, [127](#)
 - replication, [139 to 140](#)
 - SITELIST.XML, [145](#)
 - source repository, [105](#), [107](#), [109](#), [111](#)
 - repository list
 - exporting to a file, [146](#)
 - McAfee AutoUpdate Architect, [145](#)
 - Repository Pull task, [107](#), [109](#)
 - Repository Replication server tasks, [139](#)
 - resources for information, [16](#)
 - Rogue System Detection, [23](#), [25](#), [30](#), [78 to 82](#), [84 to 85](#), [87](#), [183](#), [185 to 188](#), [190 to 198](#), [200 to 223](#), [265](#), [273](#)
 - about, [185](#)
 - action, [215](#)
 - action status, [214](#)
 - action types, [202](#)
 - automatic e-mail notifications, [208](#)
 - automatic responses, [207](#), [212](#)
 - status, [215](#)
 - using an executable in, [213](#)
 - customizing the server, [217](#)
 - dealing with new rogues, [201](#)
 - event history, [214](#), [216](#)
 - interface, [190](#)

- Machine Summary, 193
 - sensor-to-server communication, 221
 - server, 79 to 80, 84 to 85, 186 to 188, 193, 197 to 198, 208 to 209, 211, 215 to 217, 220 to 221
 - status, 215
 - Subnet List, 80
 - using with notification, 221
 - rogue system sensor
 - about, 187
 - deploying, 57, 78, 80, 83
 - installing manually, 83
 - managing, 195
 - policies, 197 to 198
 - uninstalling, 85
- S**
- sample virus, submitting, 20
 - scheduling
 - client tasks, 178
 - domain synchronization task, 258
 - Repository Pull task, 107, 109
 - repository replication, 139
 - scheduling a daily server task, 265
 - search
 - feature, using to delete computers, 267
 - for computers in the Directory, 267
 - security certificate, 23
 - security headquarters, contacting AVERT, 20
 - selective updating
 - overview, 14
 - Send Agent Install, 62
 - server events, 33
 - server tasks
 - daily and weekly, 270
 - domain synchronization, 258
 - servers
 - introduction, 8
 - printing events, 34
 - tasks, scheduling Repository Replication, 139
 - service portal, PrimeSupport, 20
 - SITELIST.XML file, 145
 - enabling the agent, 69
 - sites
 - from text file, 54
 - IP filter, 260
 - sites (See Directory)
 - SNMP, 231, 234
 - sorting computers using IP management settings, 264
 - source repositories, 103
 - adding, 105
 - changing, 103
 - pulling from, 107, 109, 111
 - SQL
 - database maintenance, 277
 - transaction log is full, 277
 - Subnet List, 80
 - SuperAgent
 - defined, 306
 - deploying, 57, 75
 - distributed repository, 132
 - wakeup call, 75
 - synchronizing domains, 259
 - System Compliance Profiler, 89, 165, 180 to 181, 183, 224, 244, 273
- T**
- tasks
 - deleting, 179
 - domain synchronization, 258
 - finding inactive agents, 265
 - Pull Now, 111
 - repository replication, 139
 - scheduling, 178
 - Update Domain Directory, 259
 - technical support
 - accessing from the product, 18
 - contact information, 20
 - throttling notifications, 222, 226
 - training web site, 20
- U**
- uninstalling the auditing feature, 289
 - Update Domain Directory task, 259
 - updating
 - DAT file, 118
 - domains, 259
 - global, new features, 11 to 14
 - upgrading
 - agent, 70
 - web site, 20
 - user accounts, 25
 - adding and editing, 27
 - changing passwords, 28
 - deleting, 28
 - global administrator, 25
 - global and site reviewers, 27
 - removing, 28
 - site administrators, 26
 - using this guide, 14
 - utilities
 - Agent Monitor, 161
- V**
- Virtual Private Networks (VPN), 290
 - Virus Information Library, 17, 20
 - virus outbreaks, 275
 - indicators, 273 to 274
 - Internet scenarios, 290
 - network usage indicators, 273
 - preparing for, 270
 - recognizing an outbreak, 273
 - responding to an outbreak, 274
 - virus, submitting a sample
 - web site, 20
 - virus, submitting a sample to AVERT
 - from within the product, 18
 - VirusScan Enterprise
 - deploying, 88
 - deploying with ePolicy Orchestrator, 94
 - detection events, 225 to 226, 274
 - on-demand scan, 176
 - policies, 163
- W**
- WebImmune, 20
 - WebShield, 72
 - WebShield appliance, 56
 - wizard
 - Add repository, 105
 - Check-in package, 91, 114
 - Copy package, 128
 - Export repository list, 146

ePolicy Orchestrator®

Deploy and manage anti-virus and security products for your entire enterprise

version 3.5



McAfee® System Protection

Industry-leading intrusion prevention solutions



COPYRIGHT

Copyright © 2004 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Entercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Coliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Viruscan, Virusscan (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. 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.

PATENT INFORMATION

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

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 provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. • Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. • Software written by Douglas W. Sauder. • Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. • Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. • FEAD™ Optimizer™ technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In™ Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In™ HTML Export, © 2001 Stellent Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1989. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems®, Inc. © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, © 1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, © 2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors. • Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>). • Software copyrighted by Kevin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. • Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, © 2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. • Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Contents

1	Requirements and Recommendations	5
	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	10
	Non-Windows Agent requirements	10
	Operating systems language support	11
	Supported products	11
2	Pre-Installation	12
	Pre-installation best practices guidelines	12
	Installing or upgrading the database software	13
	Installing MSDE 2000 for the first time	13
	Upgrading MSDE to MSDE 2000	14
	Installing SQL Server 2000 for the first time	15
	Upgrading to SQL Server 2000	15
	Upgrading to MDAC 2.7	15
	Proxy settings	16
3	First-Time Installation	18
	Step 1: Migrating repository settings from McAfee AutoUpdate Architect	18
	Step 2: Installation preparation	19
	Step 3: Installing the database software	19
	Installing MSDE 2000	19
	Installing SQL Server 2000	20
	Installing MDAC 2.7	20
	Step 4: Installing the server and console	21
	Step 5: Installing remote consoles	28
	Step 6: Importing McAfee AutoUpdate Architect settings	29
4	Upgrading to ePolicy Orchestrator 3.5	31
	Step 1: Upgrade preparation	32
	Step 2: Upgrading the database software	32
	Upgrading MSDE to MSDE 2000	33
	Upgrading to SQL Server 2000	33
	Installing MDAC 2.7	34
	Step 3: Backing up ePolicy Orchestrator databases	35
	Microsoft SQL Server	35
	MSDE	36
	Step 4: Upgrading the server and console	36
	Step 5: Upgrading remote consoles	41
	Step 6: Migrating to a licensed version	42

5	Post-Installation Procedures	44
	Completing a first-time installation	44
	Completing an upgrade from a previous version.	44
	Checking in files manually.	45
	Uninstalling the software	45
6	Troubleshooting	47
A	Migrating to SQL Server 2000	51
	Migrating from SQL Server 7 or MSDE to SQL Server 2000	51
	Stopping the ePolicy Orchestrator server service	51
	Installing Client Tools only (SQL Server 2000)	51
	Backing up ePolicy Orchestrator 3.5 databases (MSDE users).	52
	Backing up ePolicy Orchestrator 3.5 databases (SQL Server 7 users)	52
	Installing SQL Server 2000.	54
	Configuring the ePolicy Orchestrator server.	54
	Starting the ePolicy Orchestrator server service	54
B	Settings Conversions	55
	McAfee AutoUpdate Architect 1.0 information conversion	55
	McAfee AutoUpdate 7.0 information conversion.	56
	Index	57

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 the minimum system requirements are met. The requirements for each of these components 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 10](#).
- [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** — 250MB minimum (first-time installation); 650MB minimum (upgrade); 2 GB recommended.

- **Memory** — 512MB RAM; 1 GB recommended.
- **Processor** — Intel Pentium II-class or higher; 500MHz 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 2 or later.
 - Windows 2000 Server with Service Pack 2 or later.
 - Windows Server 2003 Enterprise.
 - Windows Server 2003 Standard.
 - Windows Server 2003 Web.
- **Browser** — Microsoft Internet Explorer 6.0.
- **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** — 120MB.
- **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 1 or later.
 - Windows 2000 Professional with Service Pack 1 or later.
 - Windows 2000 Server with Service Pack 1 or later.
 - Windows NT Server 4.0 with Service Pack 6a or later.
 - Windows NT Workstation 4.0 with Service Pack 6a or later.
 - Windows Server 2003 Enterprise.
 - Windows Server 2003 Standard.
 - Windows Server 2003 Web.
 - Windows XP Professional.
- **Browser** — Microsoft Internet Explorer 6.0 or later.

Database requirements

The ePolicy Orchestrator database requirements are:

- **Database software** — Any of the following:
 - Microsoft Data Engine 7 (MSDE) with Service Pack 3.
 - Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) with Service Pack 3.



Neither MSDE 7 nor MSDE 2000 with Service Pack 3 can be installed on a backup domain controller (BDC).

- Microsoft SQL Server 2000 Standard or Enterprise Edition with Service Pack 3.
 - Microsoft SQL Server 7 Standard or Enterprise Edition with Service Pack 3 or 4.
- **Maintenance settings** — We recommend making specific maintenance settings to ePolicy Orchestrator databases. For instructions, see *Maintaining ePolicy Orchestrator databases* in the *ePolicy Orchestrator 3.5 Product Guide*.
- **Remote database server** — Microsoft Data Access Components (MDAC) 2.7.

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 computer as the ePolicy Orchestrator server, we recommend specifying a fixed memory size approximately two-thirds of the total memory for SQL Server in Enterprise Manager. (For example, if the computer has 1GB of RAM, then set 660MB as the fixed memory size for SQL Server.)
- **SQL Server licenses** — A SQL Server license 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 problems 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 10](#).

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; 166 processor or higher.
- **Free disk space (agent)** — 10MB.
- **Free disk space (products)** — Sufficient disk space on client computers for each McAfee product you plan on deploying. 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 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 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, available at no charge from Microsoft. At press time, this program and instructions for installation were available on the Microsoft web site.
- DCOM95 1.3, available at no charge 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, available at no charge from Microsoft. At press time, this program and instructions for installation were available on the Microsoft web site.



Client computers using Windows 98 SE do *not* need this program installed on them.

SuperAgent requirements

You can enable the ePolicy Orchestrator agent for Windows as a SuperAgent, which is used to communicate with other agents or 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 PC equipped with:

- **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 computers using NetWare 4.11 or 4.2 must install NW4WSOCK.EXE, available at no charge 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 works with 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 3.5 supports the management of the following products:

- McAfee Alert Manager versions 4.5 and 4.7
- McAfee ePolicy Orchestrator Agent (CMA)
- McAfee NetShield 4.5 for Windows
- McAfee NetShield for NetWare version 4.6
- McAfee VirusScan Thin Client version 6.0 for Windows
- McAfee VirusScan Enterprise versions 4.51, 7.0, 7.1, 8.0i
- Norton Antivirus Corporate Edition 7.5x, 7.6, 8.0, 8.1

2

Pre-Installation

The procedures you need to complete before installing the new version of the software depend on whether you are installing the software for the first time or upgrading from version 2.5.1. or 3.0.x. The following topics are covered here:

- [Pre-installation best practices guidelines on page 12.](#)
- [Installing or upgrading the database software on page 13.](#)
- [Proxy settings on page 16](#)

Pre-installation best practices guidelines

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 ePolicy Orchestrator database server with the latest Microsoft security updates. (Specifically, be sure to install Service Pack 3 on all MSDE 2000 and SQL Server 2000 databases.)
- **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 (for example, Desktop Firewall 8.0) on the ePolicy Orchestrator server.
- **Ports**
 - Avoid using port 80 for any HTTP communication via ePolicy Orchestrator, because it might 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 communication via ePolicy Orchestrator.
- **System Administrator account and upgrades** — If you are upgrading the ePolicy Orchestrator software, you must assign a password to the System Administrator (sa) user account. Otherwise, you cannot upgrade the software.

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 defined in Chapter 1, *Requirements and Recommendations*, go to either of the following, depending on whether you are installing for the first time or upgrading the software:

- [First-Time Installation on page 18.](#)
- [Upgrading to ePolicy Orchestrator 3.5 on page 31.](#)

If you need to install or upgrade the required database, go to the:

- [Installing MSDE 2000 for the first time on page 13.](#)
- [Upgrading MSDE to MSDE 2000 on page 14.](#)
- [Installing SQL Server 2000 for the first time on page 15.](#)
- [Upgrading to SQL Server 2000 on page 15.](#)

Installing MSDE 2000 for the first time

Typically, you would install MSDE or MSDE 2000 on the same computer 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 3.5. If you want 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, click the **Start** button, then point to **Run**. The **Run** dialog box appears.
- 3 In **Open**, type the following command:

```
"E:\SETUP\MSDE\SETUP.EXE" TARGETDIR="C:\PROGRAM FILES\NETWORK  
ASSOCIATES\EPO\" COLLATION=SQL_LATIN1_GENERAL_CP1_CI_AS  
SAPWD=<PASSWORD> REBOOT=R
```

Where `TARGETDIR` equals 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 start the installation.
- 5 To continue the installation of ePolicy Orchestrator 3.5, go to either [First-Time Installation on page 18](#) or [Upgrading to ePolicy Orchestrator 3.5 on page 31.](#)

MSDE or MSDE 2000 installed on a remote server?

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



You do not need to upgrade remote database servers using MSDE 2000 SP 3 to Microsoft Data Access Components (MDAC) version 2.7. This upgrade is performed automatically as part of the MSDE 2000 installation process.

Upgrading MSDE to MSDE 2000

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.



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 3.5 Product Guide*.

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 **Open**, type the following command:

```
SETUP UPGRADE=1 INSTANCENAME=MSSQLSERVER /1*v C:\MSDEUpgrade.Log
```



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 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` directory.

- 4 Click **OK** to start the installation.
- 5 To continue the installation of ePolicy Orchestrator 3.5, go to either [First-Time Installation on page 18](#) or [Upgrading to ePolicy Orchestrator 3.5 on page 31](#).

Remote database servers using MSDE or MSDE 2000

Typically, you would install MSDE or MSDE 2000 on the same computer as the ePolicy Orchestrator server. However, if you are using a remote database server, you must manually install or upgrade the database before you install the ePolicy Orchestrator software.



You do not need to upgrade remote database servers using MSDE 2000 SP 3 to Microsoft Data Access Components (MDAC) version 2.7, because the MSDE 2000 installation does this for you.

Installing SQL Server 2000 for the first time

If you are installing SQL Server 2000 for the first time, you must manually install it before you install the ePolicy Orchestrator software. Be sure to also 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've installed SQL Server 2000, go to [First-Time Installation on page 18](#) to continue the installation of ePolicy Orchestrator 3.5.

Upgrading to SQL Server 2000

If you want 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 before you upgrade the database software. 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.



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) 2.7. For instructions, see [Upgrading to MDAC 2.7 on page 15](#).

- If your database server is installed locally (on the same computer as the ePolicy Orchestrator server), go to [Proxy settings on page 16](#) 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 2.7](#) to continue.

- If your database server is installed remotely (on a different computer than the ePolicy Orchestrator server), go to [Upgrading to MDAC 2.7](#) to continue.

Upgrading to MDAC 2.7

Now that you have installed the database server, you must also ensure that all remote ePolicy Orchestrator servers have Microsoft Data Access Components (MDAC) version 2.7 currently installed. You must determine the version number of MDAC and upgrade to version 2.7 as needed. Because the ePolicy Orchestrator server uses version 2.7, it's important that all remote database servers use the same version to avoid performance and functionality issues.

MDAC 2.7 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 2.7 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 2.7, 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 2.7, close the dialog boxes and proceed to [Step 4](#).
- If the MDAC version number is 2.7, close the dialog boxes and proceed to [Proxy settings](#).

- 4 Run the MDAC 2.7 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 2.7 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** twice to save the current entries.

3

First-Time Installation

This chapter provides instructions to install ePolicy Orchestrator 3.5 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 3.5](#) on page 31.

This chapter is divided into the following sections:

- [Step 1: Migrating repository settings from McAfee AutoUpdate Architect.](#)
- [Step 2: Installation preparation on page 19.](#)
- [Step 3: Installing the database software on page 19.](#)
- [Step 4: Installing the server and console on page 21.](#)
- [Step 5: Installing remote consoles on page 28.](#)
- [Step 6: Importing McAfee AutoUpdate Architect settings on page 29.](#)

Step 1: Migrating repository settings from McAfee AutoUpdate Architect

If you have not been using McAfee AutoUpdate Architect, go to [Step 2: Installation preparation on page 19](#).

Although you cannot upgrade directly from McAfee AutoUpdate Architect, you can migrate its repository configuration settings to ePolicy Orchestrator 3.5. To migrate these settings, you must:

- 1 Make a backup copy of the SITEMGR.XML file and store it in a safe location until after you have installed the ePolicy Orchestrator server and consoles. The default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\MCAFFEE AUTOUPDATE ARCHITECT



If you uninstall McAfee AutoUpdate Architect without making a backup copy of the SITEMGR.XML file, you will not be able to migrate these configuration settings.

- 2 Uninstall McAfee AutoUpdate Architect with **Add/Remove Programs** in the **Control Panel**.
- 3 Go to [Step 2: Installation preparation](#).

Step 2: Installation preparation

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

- 1 Update both the ePolicy Orchestrator server computer and the ePolicy Orchestrator database server computer with the latest Microsoft security updates. (Specifically, be sure to install Service Pack 3 on all MSDE 2000 and SQL Server 2000 databases.)
- 2 Install and/or update the anti-virus software on the ePolicy Orchestrator server computer and scan for viruses.
- 3 Install and/or update firewall software (for example, Desktop Firewall 8.0) on the ePolicy Orchestrator server computer.
- 4 Notify the network staff of the ports you intend to use for HTTP communication via ePolicy Orchestrator.



Avoid using port 80 for any HTTP communication via ePolicy Orchestrator, because it might be disabled during virus outbreaks.

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

Step 3: Installing the database software

Depending on which database you plan to use, you need to complete different tasks.

If your system already meets the database requirements defined in Chapter 1, [Requirements and Recommendations](#), go to [Step 4: Installing the server and console on page 21](#).

If you need to install a required database, go to the appropriate one the following:

- [Installing MSDE 2000 on page 19](#).
- [Installing SQL Server 2000 on page 20](#).

Installing MSDE 2000

Typically, you would install MSDE 2000 on the same computer as the ePolicy Orchestrator server. However, if you want to use a remote database server, you must manually install the database before you install the ePolicy Orchestrator software.



You do not need to upgrade remote database servers using MSDE 2000 SP 3 to Microsoft Data Access Components (MDAC) version 2.7. This upgrade is performed automatically as part of the MSDE 2000 installation process.

You can also install MSDE 2000:

- As part of the ePolicy Orchestrator 3.5 Setup program. If so, go to [Step 4: Installing the server and console on page 21](#).
- Manually, prior to installing ePolicy Orchestrator 3.5. If you plan to install MSDE 2000 on a different system than the system running the ePolicy Orchestrator server, then you must install MSDE 2000 manually. If you choose to install MSDE 2000 manually, continue to [Step 1](#) one of this procedure.

To install MSDE 2000 manually:

- 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 **Open**, type the following command:

```
"E:\SETUP\MSDE\SETUP.EXE" /Q TARGETDIR="C:\PROGRAM FILES\NETWORK  
ASSOCIATES\" COLLATION=SQL_LATIN1_GENERAL_CP1_CI_AS  
SAPWD=<PASSWORD> REBOOT=R
```

Where `TARGETDIR` equals 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 start the installation.
- 5 When the installation is complete, go to [Step 4: Installing the server and console on page 21](#).

Installing SQL Server 2000

If you are installing SQL Server 2000 for the first time, you must manually install it before you install the ePolicy Orchestrator software. Be sure to also install Service Pack 3 for SQL Server 2000. For instructions, see the SQL Server product documentation.

If you are installing SQL Server remotely, verify that it is visible on the network before you install the ePolicy Orchestrator software.

Once you've installed SQL Server 2000, go to [Installing MDAC 2.7](#).

Installing MDAC 2.7

See the following topics:

- [Database servers installed locally](#).
- [Database servers installed remotely](#).

Database servers installed locally

MDAC 2.7 is installed automatically on all *local* ePolicy Orchestrator database servers, regardless of which supported database server software you are running. But if you have installed a language version of the database server, locally, other than French, German, Japanese, or Spanish, then the English language version of MDAC 2.7 is installed automatically.

If you want to install a language version of MDAC 2.7 other than these four languages (or English) they are available on the Microsoft web site.

Database servers installed remotely

If you installed either MSDE 7.0 or SQL Server 7.0 for use as a remote ePolicy Orchestrator database server, you must install MDAC 2.7 manually. Go to [Step 1](#).

Also, if you have installed a language version of the database server, remotely, other than French, German, Japanese, or Spanish, then the English language version of MDAC 2.7 is installed automatically.

If you want to install a language version of MDAC 2.7 other than these four languages (or English), they are available on the Microsoft web site.

To determine the version number of the current installation of MDAC and upgrade to MDAC 2.7, 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 2.7, close the dialogs and proceed to [Step 4](#) of this procedure.
- If the MDAC version number is 2.7, close the dialogs and proceed to [Step 4: Installing the server and console on page 21](#).

- 4 Run the MDAC 2.7 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, the MDAC 2.7 Setup program and instructions for English, French, German, Japanese, Spanish, Chinese (Simplified and Traditional), and Korean language versions were available on the Microsoft web site.

- 5 Go to [Step 4: Installing the server and console on page 21](#).

Step 4: Installing the server and console

To install the ePolicy Orchestrator 3.5 server and console:



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

- 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. For instructions, see the Microsoft product documentation.

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 3.0**.

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 When the **ePolicy Orchestrator 3.5 Setup** wizard appears, click **Next**.

5 In the **End User License Agreement** dialog box, select the appropriate license type and the country in which you purchased the software. The license type must match the license you purchased. If you are unsure which license you purchased, contact the person who sold you the software.

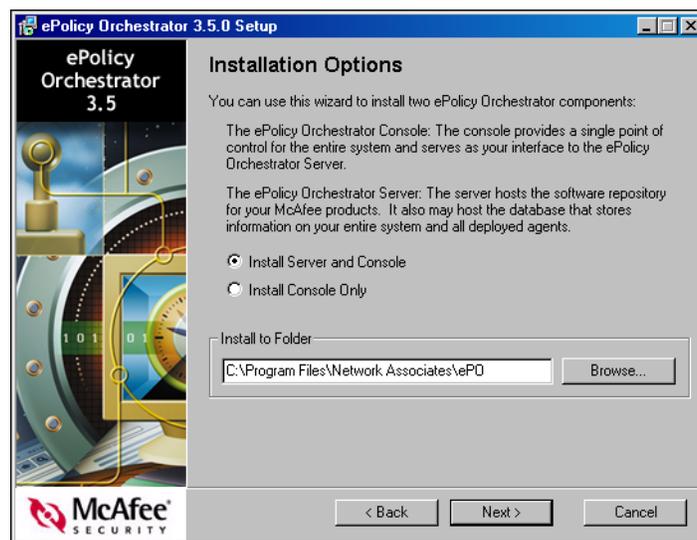


If the information in this dialog box does not display correctly, read the appropriate license agreement in the LICENSEAGREEMENT.PDF file supplied with the software.

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.

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



- In the Set Server Password dialog box, enter and verify the password you will use when logging onto this ePolicy Orchestrator server.



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

Figure 3-2 Set Server Password dialog box



- In the Server Service Account dialog box, specify the type of account to log on to the ePolicy Orchestrator server service, then click **Next**.

Figure 3-3 Server Service Account dialog box



- Use Local System Account — Specifies that the ePolicy Orchestrator server service logs on using the system account rather than a user account. Most services log on to a system account.

If you select **Use Local System Account**, you cannot use the ePolicy Orchestrator server credentials to deploy the agent. You must provide a user account that belongs to the local administrators group on the desired computers.

- **Account Information** — Specifies the NetBIOS name of the **Domain** associated with the desired domain administrator user account, and the **User Name** and **Password** of the desired user account. Available only when you deselect **Use Local System Account**.



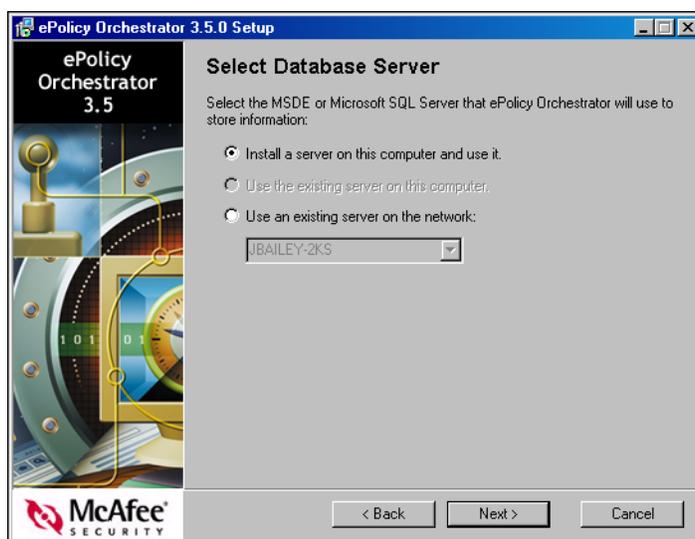
When you change the password on the account used to log on to the ePolicy Orchestrator server service after the installation, be sure to update the password for the **McAfee ePolicy Orchestrator 3.5 Server** service. For instructions, see the operating system product documentation.

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



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.

Figure 3-4 Select Database Server dialog box



- **Install a server on this computer and use it** — Installs Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) as the ePolicy Orchestrator database, using the system administrator (sa) login specified in [Step 8 on page 23](#).
- **Use the existing server on this computer** — Uses the existing MSDE, MSDE 2000, or SQL Server database server on this computer.

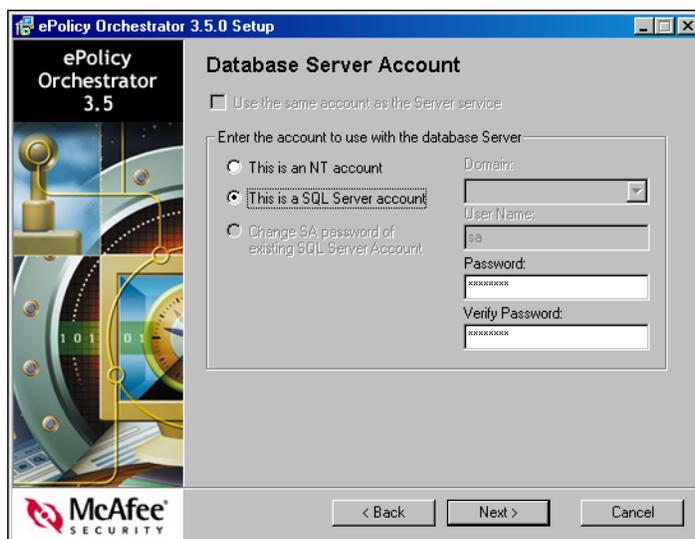
- **Use an existing server on the network** — Uses the remote database server that you specify. The drop-down list displays all remote SQL Server database servers that are in the same domain as this computer. If the desired database server doesn't appear, type its name in the list box.



If using Windows NT and you do not have MDAC 2.7 installed on the remote database servers *or* if using other operating systems and you do not have MDAC 2.5 or later installed on the remote database servers, these servers do not appear in this list.

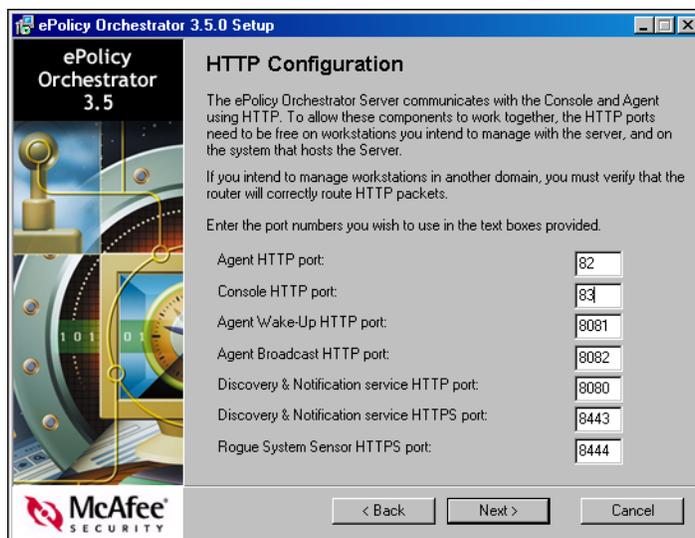
- 11 In the **Database Server Account** dialog box, specify the type of account to log on to the database server, then click **Next**.

Figure 3-5 Database Server Account dialog box



- a Select **Use the same account as the Server service** if you want to use the same account you specified for the ePolicy Orchestrator server service in [Step 9 on page 23](#). If you select this checkbox, go to [Step 12 on page 25](#).
If you deselect this checkbox, go to [Step b](#).
 - b Select whether to specify a Windows NT user account or a SQL Server user account.
 - c 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**.)
 - d Specify the **User Name** and **Password** of the desired user account.
If you selected **Install a server on this computer and use it** in the **Select Database Server** dialog box, type `sa` for the **User Name** and you must specify a password; the default password is blank.
 - e Retype the password that you specified for the user account, then click **Next**.
- 12 Specify the port numbers used for communication to and from the server, as indicated, then click **Next**.

Figure 3-6 HTTP Configuration dialog box



- **Agent HTTP port** — This is the port that the agent uses to communicate with the server.



We recommend using a port other than 80.

- **Console HTTP port** — This is the port that the console uses to communicate with the server.



We recommend using a port other than 81.

- **Agent Wake-Up HTTP port** — This is the port used to send agent wakeup calls.
- **Agent Broadcast HTTP port** — This is the port used to send SuperAgent wakeup calls.
- **Discovery & Notification service HTTP port** — This is the port used by Rogue System Detection and ePolicy Orchestrator Notification for non-SSL user interface communication and non-SSL sensor communication.
- **Discovery & Notification service HTTPS port** — This is the port used by the console to access the Rogue System Detection and ePolicy Orchestrator Notification user interfaces through an SSL-encrypted connection.
- **Rogue System Sensor HTTPS port** — The port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL.

- 13 In the **Set E-Mail Address** dialog box, enter the e-mail address you want the software to use as the recipient for the default notification rules of ePolicy Orchestrator Notification. For more information, see the ePolicy Orchestrator Notification chapter in the ePolicy Orchestrator 3.5 Product Guide.



You do not have to set this address now. If you choose not to, leave the default address in the field.

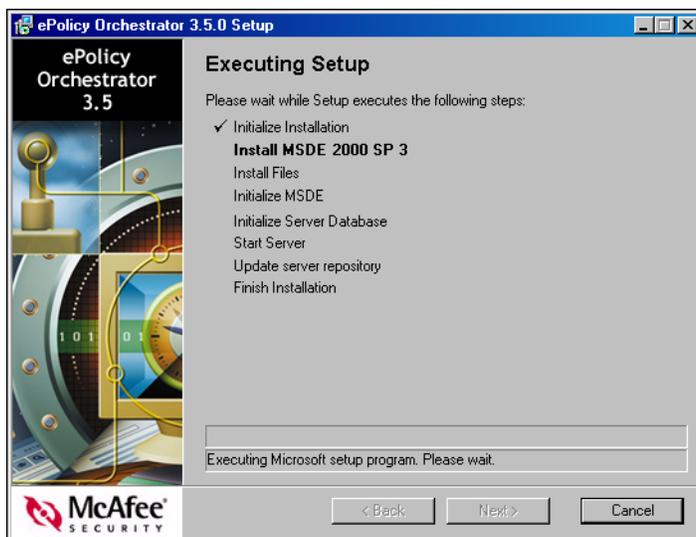
Figure 3-7 Set E-Mail Address



- 14 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, providing the installation status.

Figure 3-8 Executing Setup dialog box



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

Step 5: Installing remote consoles

The installation procedure also installs CMA on the computer.



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

To install the ePolicy Orchestrator 3.5 remote console:

- 1 Log on to the desired computer using a user account with local administrator permissions.
- 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 3.0**.

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.

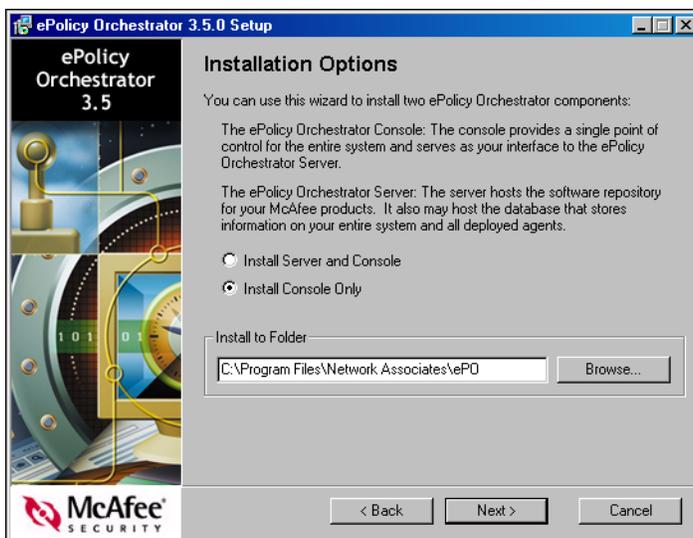
- 3 In the **ePolicy Orchestrator 3.5 Setup** wizard, click **Next** to begin the installation.
- 4 In the **End User License Agreement** dialog box, select the appropriate license type and the country in which you purchased the software. The license type must match the license you purchased. If you are unsure which license you purchased, contact the person who sold you the software.



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.

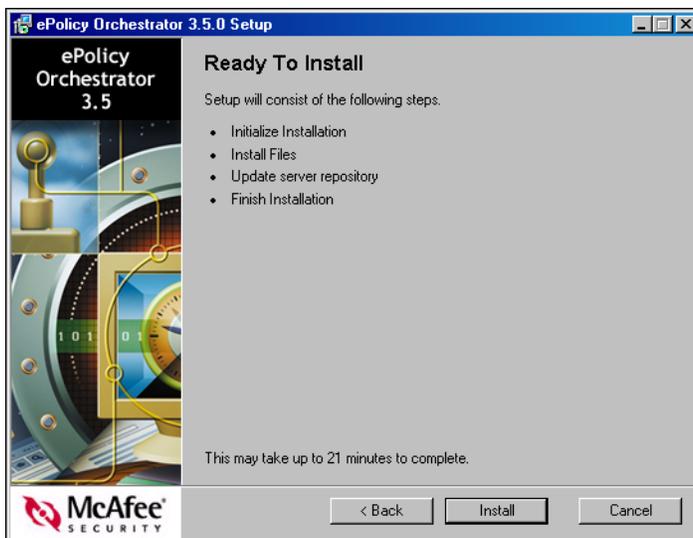
- 5 Accept the agreement and click **OK** to continue, or click **Cancel** if you do not agree to the terms and end the installation process.
- 6 In the **Installation Options** dialog box, select **Install Console** and either accept the default installation location, or click **Browse** to select a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

Figure 3-9 Installation Options dialog box



- 7 In the Ready To Install dialog box, click **Install** to begin the installation.

Figure 3-10 Ready To Install dialog box



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.

Step 6: Importing McAfee AutoUpdate Architect settings

If you are not importing repository configuration settings from McAfee AutoUpdate Architect, go to [Post-Installation Procedures on page 44](#).

To import the repository configuration settings defined in the McAfee AutoUpdate Architect 1.0 software into the ePolicy Orchestrator 3.5 software:

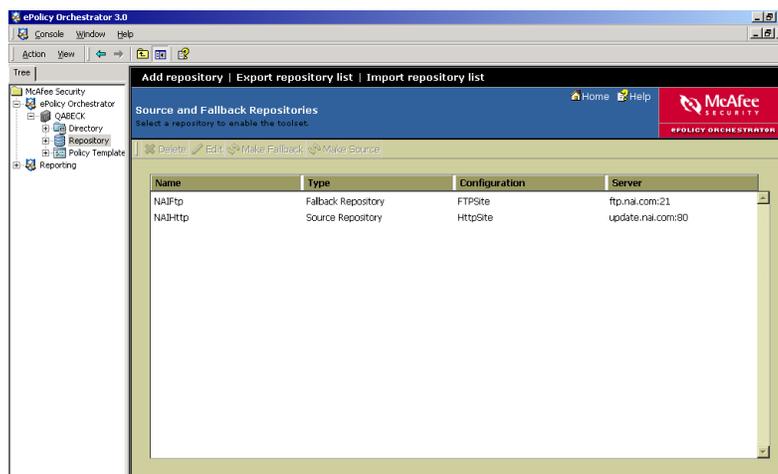
- 1 Log on to the desired ePolicy Orchestrator server using a global administrator user account.



You must be a global administrator to import the repository list from McAfee AutoUpdate Architect.

- 2 In the console tree under ePolicy Orchestrator | <SERVER>, select **Repository**.
- 3 In the details pane under **AutoUpdate Components**, click **Source Repository**. The **Source and Fallback Repositories** page appears.

Figure 3-11 Source and Fallback Repositories page



- 4 Click **Import repository list** to open the **Open** dialog box, and select the McAfee AutoUpdate Architect repository list (SITEMGR.XML) from the location you saved it prior to the installation. To see how McAfee AutoUpdate Architect policies are converted in ePolicy Orchestrator 3.5, go to [McAfee AutoUpdate Architect 1.0 information conversion on page 55](#).
- 5 Update your SITELIST.XML file or upgrade AutoUpdate 7.0 to the Common Management Agent (CMA) 3.5.
- 6 Once finished, go to [Post-Installation Procedures on page 44](#).

4

Upgrading to ePolicy Orchestrator 3.5

You can upgrade or migrate to ePolicy Orchestrator 3.5 if you are currently using:

- ePolicy Orchestrator version 2.5.1
- ePolicy Orchestrator 3.0.x
- Protection Pilot 1.0.
- Evaluation versions of ePolicy Orchestrator version 3.5.

This chapter is divided into the following sections:

- [Step 1: Upgrade preparation on page 32.](#)
- [Step 2: Upgrading the database software on page 32.](#)
- [Step 3: Backing up ePolicy Orchestrator databases on page 35.](#)
- [Step 4: Upgrading the server and console on page 36.](#)
- [Step 5: Upgrading remote consoles on page 41.](#)
- [Step 6: Migrating to a licensed version on page 42.](#)



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

Product removal

The list of products ePolicy Orchestrator 3.5 manages is different than prior versions. The following products that were supported with prior versions of ePolicy Orchestrator are no longer supported in version 3.5 and are removed from the repository when you upgrade:

- McAfee Klez/Elkern 1.x
- McAfee NetShield 4.0.3 for Windows NT
- McAfee NimdaScan 1.x
- McAfee NimdaScan 2.x
- McAfee ThreatScan 2.0 and 2.1
- McAfee VirusScan 4.0.3 for Windows
- McAfee VirusScan 4.0.3 for Windows NT

- McAfee VirusScan 4.5.0 for Windows
- McAfee GroupShield Domino 5.0.0

Step 1: Upgrade preparation

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

- 1 Update both the ePolicy Orchestrator server computer and the ePolicy Orchestrator database server computer with the latest Microsoft security updates. (Specifically, be sure to install Service Pack 3 on all MSDE 2000 and SQL Server 2000 databases.)
- 2 Install and/or update the anti-virus software on the ePolicy Orchestrator server computer and scan for viruses.
- 3 Install and/or update firewall software (for example, Desktop Firewall 8.0) on the ePolicy Orchestrator server computer.
- 4 Notify the network staff of the ports you intend to use for HTTP communication via ePolicy Orchestrator.



Avoid using port 80 for any HTTP communication via ePolicy Orchestrator, because it might be disabled during virus outbreaks.

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

- 5 Ensure a password is assigned to the System Administrator (sa) user account. Otherwise, you cannot upgrade the software. If you do not prior to the upgrade, the installation wizard prompts you to assign one.

Step 2: Upgrading the database software

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



If your system already meets the database requirements defined in chapter 1, *Requirements and Recommendations*, go to [Step 3: Backing up ePolicy Orchestrator databases](#) on page 35.

If you need to install or upgrade the required database, go to the:

- [Upgrading MSDE to MSDE 2000](#) on page 33.
- [Upgrading to SQL Server 2000](#) on page 33.

Upgrading MSDE to MSDE 2000

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 upgrade the database before you upgrade the ePolicy Orchestrator software.



Be sure to back up the existing database before you upgrade the database software. For instructions, see [Step 3: Backing up ePolicy Orchestrator databases on page 35](#).

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 select **Run**. The **Run** dialog box appears.
- 3 In **Open**, type the following command:

```
SETUP UPGRADE=1 INSTANCENAME=MSSQLSERVER /1*v C:\MSDEUpgrade.Log
```



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 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 directory.

- 4 Click **OK** to begin the installation.
- 5 When finished, go to [Step 3: Backing up ePolicy Orchestrator databases on page 35](#).

Remote database servers using MSDE or MSDE 2000

Typically, you would install MSDE or MSDE 2000 on the same computer as the ePolicy Orchestrator server. However, if you are using a remote database server, you must manually install or upgrade the database before you install the ePolicy Orchestrator software.



You do not need to upgrade remote database servers using MSDE 2000 to Microsoft Data Access Components (MDAC) version 2.7, because the MSDE 2000 installation does this automatically.

Upgrading to SQL Server 2000

To upgrade existing ePolicy Orchestrator databases from Microsoft Data Engine (MSDE) or SQL Server 7 with Service Pack 3 to SQL Server 2000, use the following procedure after you install ePolicy Orchestrator 3.5:

- 1 Stop the ePolicy Orchestrator server service.
- 2 Install SQL Server 2000 Client Tools:
 - a Insert the SQL Server 2000 CD into the CD-ROM drive of the computer. When the installation menu appears, click **SQL Server 2000 Components**.
 - b Click **Install Database Server**. When the **Welcome** wizard appears, click **Next** twice.
 - c Select **Create a new instance of SQL Server**, or **install Client Tools**, then click **Next**.

To determine the version number of the current installation of MDAC, and upgrade to MDAC 2.7, 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 2.70.xxx, close the dialogs and proceed to [Step 4](#) of this procedure.
- If the MDAC version number is 2.10.xxx, close the dialogs and proceed to [Step 3: Backing up ePolicy Orchestrator databases on page 35](#).

- 4 Run the MDAC 2.7 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, the MDAC 2.7 Setup program and instructions for English, French, German, Japanese, Spanish, Chinese (Simplified and Traditional), and Korean language versions were available on the Microsoft web site.

- 5 Go to [Step 3: Backing up ePolicy Orchestrator databases on page 35](#).

Step 3: Backing up ePolicy Orchestrator databases

Before you upgrade to version 3.5, back up all ePolicy Orchestrator databases:

- [Microsoft SQL Server on page 35](#).
- [MSDE on page 36](#).

Once your ePolicy Orchestrator databases are backed up, go to [Step 4: Upgrading the server and console on page 36](#).

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 [Step 4: Upgrading the server and console on page 36](#).

MSDE

If you are using MSDE as the ePolicy Orchestrator database, 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 server using this utility.



This tool cannot change the database location.

- 1 Stop the **McAfee ePolicy Orchestrator 3.0 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 the software from version 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFFEE\EPO\2.0

If you are upgrading from Protection Pilot 1.0, the default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\PROTECTION PILOT\1.0.0
- 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 [Step 4: Upgrading the server and console on page 36](#).

Step 4: Upgrading the server and console

You must upgrade ePolicy Orchestrator on every ePolicy Orchestrator server and console to version 3.5.



If you are upgrading from version 2.5.1 and were using AutoUpdate 7.0, you are prompted during the Setup wizard whether you want to migrate your AutoUpdate 7.0 settings to ePolicy Orchestrator 3.5. For more information about how these settings are migrating, see [McAfee AutoUpdate 7.0 information conversion](#).

This procedure upgrades the ePolicy Orchestrator server and console from ePolicy Orchestrator version 2.5.1, 3.0.x. and Protection Pilot version 1.0. This upgrade also installs the common management agent (CMA). The default location of CMA is:

- ePolicy Orchestrator 2.5.1
C:\PROGRAM FILES\NETWORK ASSOCIATES\MCAFEE\EPO
- ePolicy Orchestrator 3.0.x and ProtectionPilot 1.0.0
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO



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

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 3.5**.

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 3.5 Setup** wizard, click **Next** to begin the installation.
- 6 In the **End User License Agreement** dialog box, select the appropriate license type and the country 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, or click **Cancel** if you do not agree to the terms and end the installation process.

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 if you wish to proceed with the upgrade process, or **Cancel** to end it now.
- 9 If the AutoUpdate 7.0 policy page was in the **Repository** when you started the installation, a message appears asking whether you want to preserve the AutoUpdate 7.0 settings. Click **Yes** to migrate AutoUpdate 7.0 policies and tasks. For information about this conversion, see [McAfee AutoUpdate 7.0 information conversion on page 56](#).

- 10 In the **Server Service Account** dialog box, specify the type of account to log on to the ePolicy Orchestrator server service, then click **Next**.

Figure 4-1 Server Service Account dialog box



- **Use Local System Account** — Specifies that the ePolicy Orchestrator server service logs on using the system account rather than a user account. Most services log on to a system account.



If you select **Use Local System Account**, you cannot use the ePolicy Orchestrator server credentials to deploy the agent. You must provide a user account that belongs to the local administrators group on the desired computers.

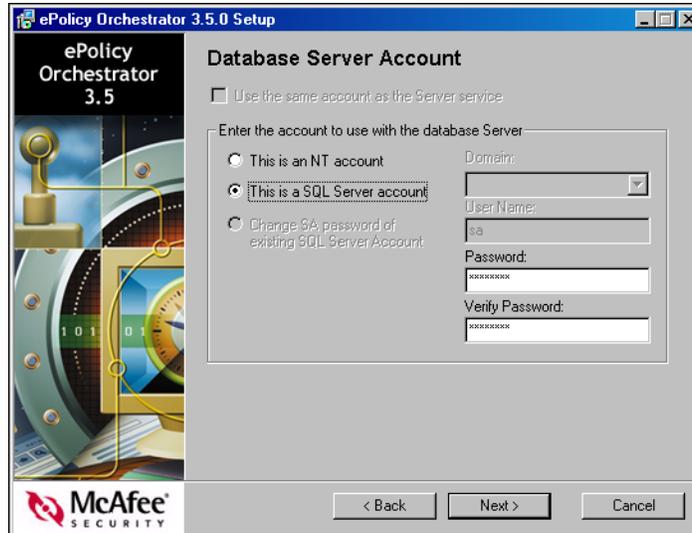
- **Account Information** — Specifies the NetBIOS name of the **Domain** associated with the desired domain administrator user account, **User Name** of the desired user account, and **Password** of the desired user account. Available only when you deselect **Use Local System Account**.



When you change the password on the account used to log on to the ePolicy Orchestrator server service after the installation, be sure to update the password for the **McAfee ePolicy Orchestrator 3.5 Server** service. For instructions, see the operating system product documentation.

- 11 In the **Database Server Account** dialog box, specify the type of account to log on to the database server, then click **Next**.

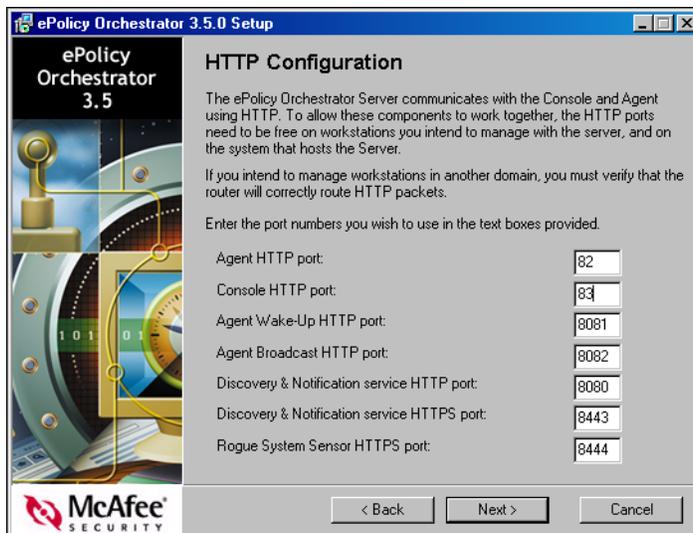
Figure 4-2 Database Server Account dialog box



- a Select **Use the same account as the Server service** if you want to use the same account you specified for the ePolicy Orchestrator server service in [Step 10 on page 38](#). If you select this checkbox, go to [Step 14](#).

If you deselect this checkbox, go to [Step b](#).
 - b Select whether to specify a Windows NT user account or a SQL Server user account.
 - c 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**.)
 - d Specify the **User Name** and **Password** of the desired user account.
- 12** 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 3.5.

Figure 4-3 HTTP Configuration dialog box



- **Agent HTTP port** — This is the port that the agent uses to communicate with the server.



We recommend using a port other than 80.

- **Console HTTP port** — This is the port that the console uses to communicate with the server.



We recommend using a port other than 81.

- **Agent Wake-Up HTTP port** — This is the port used to send agent wakeup calls.
- **Agent Broadcast HTTP port** — This is the port used to send SuperAgent wakeup calls.
- **Discovery & Notification service HTTP port** — This is the port used by Rogue System Detection and ePolicy Orchestrator Notification for non-SSL user interface communication and non-SSL sensor communication.
- **Discovery & Notification service HTTPS port** — This is the port used by the console to access the Rogue System Detection and ePolicy Orchestrator Notification user interface through an SSL-encrypted connection.
- **Rogue System Sensor HTTPS port** — The port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL.

- 13** In the **Set E-Mail Address** dialog box, provide an e-mail address to which the software sends notification messages from ePolicy Orchestrator Notification. For more information, see the *ePolicy Orchestrator 3.5 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.

- 14** 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.

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

Step 5: Upgrading remote consoles

Be sure to upgrade ePolicy Orchestrator on every ePolicy Orchestrator remote console to version 3.5. This procedure upgrades the ePolicy Orchestrator remote console from version 2.5.1 or 3.0.x and also installs the common management agent (CMA). The default location of CMA is:

- ePolicy Orchestrator 2.5.1
C:\PROGRAM FILES\NETWORK ASSOCIATES\MCAFEE\EPO
- ePolicy Orchestrator 3.0.x and ProtectionPilot 1.0.0
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO



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



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\MCAFEE\EPO\2.0

To upgrade a remote console:

- 1** Log on to the desired computer 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 3.0**.

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 3.5 Setup wizard, click **Next** to begin the installation.
- 5 In the **End User License Agreement** dialog box, select the appropriate license type and the country in which you purchased the software. The license type must match the license you purchased. If you are unsure which license you purchased, contact 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, or click **Cancel** if you do not agree to the terms and end the installation process.
- 7 In the **Ready To Install** dialog box, click **Install** to begin the installation.



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

The **Executing Setup** dialog box appears and provides 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.

Step 6: 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 45](#).

- 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 the Setup program you are using is 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 3.5**.
- 4 In the ePolicy Orchestrator 3.5 Setup wizard, click **Next** to begin the migration.

- 5 A message appears indicating that the migration was completed successfully.

5

Post-Installation Procedures

Although you've finished the Setup wizard, you still have a few steps to perform before being ready to begin using the software. The procedures you need 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 44.](#)
- [Completing an upgrade from a previous version on page 44.](#)
- [Checking in files manually on page 45.](#)
- [Uninstalling the software on page 45.](#)

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 Create the updating repositories.
- 4 Check in the products ePolicy Orchestrator is to manage. For a list of the type of files you must check in manually, see [Checking in files manually on page 45.](#)
- 5 Deploy agents to computers you want to manage with ePolicy Orchestrator.
- 6 Deploy product to the managed computers.

For instructions and information, see the *Getting Started* section of the *ePolicy Orchestrator 3.5 Product Guide*.

Completing an upgrade from a previous version

The version and product you are upgrading determines which procedures you must perform to complete your installation of ePolicy Orchestrator 3.5:

- 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 from legacy agents, full functionality is not present.
- 3 Check in and deploy any new products you wish to manage.

For instructions and information, see the *Getting Started* section of the *ePolicy Orchestrator 3.5 Product Guide*.

Checking in files manually

Files that you must check into the master repository or the **Repository** after you install the software for the first time are listed below. For more information, see the *ePolicy Orchestrator 3.5 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 3.5 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 in the **Repository** 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 regardless of whether 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.

Uninstalling the software

Use this procedure to remove the software. If you used the ePolicy Orchestrator Setup program to install MSDE, you can remove it at the same time.

- 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 48](#). Messages are listed 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 the McAfee Technical Support staff:

- Verify that you have met the minimum installation requirements. For a complete list, see [System requirements on page 5](#).
- Review the *ePolicy Orchestrator 3.5 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 text of all messages, word-for-word, and be sure to take note of any message codes that appear.
- Gather the installation log files (for server and console, SERVER.LOG; for remote console, CONSOLE.LOG.) The default location of these files is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0

If you upgraded from version 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFEE\EPO\3.5.0

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 2.5.1 or later software has not been installed on this computer. You must install version 2.0 before you can install version 3.5. If you are using version 1.0 or 1.1, see the <i>ePolicy Orchestrator 1.1 Getting Started Guide</i> or <i>ePolicy Orchestrator 2.0 Installation Guide</i> for instructions on upgrading to version 2.0.
ePolicy Orchestrator requires Internet Explorer 6.0 (version number 6.0.2600.0000) 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 or later before you install the software.
ePolicy Orchestrator Setup is already running.	The ePolicy Orchestrator 3.5 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 Password box is blank. Specify the password of the user account that you want to use.
For security reasons we do not allow blank passwords. Please enter a value in the "Verify Password" field provided.	The Verify Password box is blank. Specify the password of the user account that you want to use.
It is recommended 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 Start button, then select Help .
It is recommended that this computer have at least 128 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 Server and console requirements on page 5 or Remote console requirements on page 6 , respectively.
Microsoft Windows 2000 SP 1 is not installed. ePolicy Orchestrator recommends Windows 2000 Service Pack 1 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 Server and console requirements on page 5 or Remote console requirements on page 6 , respectively.
Please enter a value in the "Agent Broadcast communication" field.	The Agent Broadcast HTTP port 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 communication" field.	The Agent HTTP port box is blank. Specify the port number that the agent will use to communicate with the server.

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

If this message appears...	Then...
Please enter a value in the "Agent Ping communication" field.	The Agent Wake-Up HTTP port 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 communication" field.	The Console HTTP port 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 Install to Folder box is blank. Type the installation path in Install to Folder , or click Browse to select a location. The default location is: C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO
Please enter a value in the "User Name" field.	The User name 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.
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 Server and console requirements on page 5 or Remote console requirements on page 6 , respectively.
The passwords you entered do not match. Please try again.	The values you typed in Password and Verify Password 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 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.

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

If this message appears...	Then...
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. 1 Verify that the Domain, User Name , and Password you provided are typed correctly. 2 Verify that the database server is running. 3 Verify that the user account you provided is valid for the database server.
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 Domain, User Name , and Password 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

Migrating to SQL Server 2000

Migrating from SQL Server 7 or MSDE to SQL Server 2000

To migrate existing ePolicy Orchestrator databases from SQL Server 7 with Service Pack 3 or MSDE to SQL Server 2000, complete the following procedures.

- 1 [Stopping the ePolicy Orchestrator server service on page 51.](#)
- 2 [Backing up ePolicy Orchestrator 3.5 databases \(SQL Server 7 users\) on page 52.](#)
- 3 [Installing SQL Server 2000 on page 54.](#)
- 4 [Configuring the ePolicy Orchestrator server on page 54.](#)
- 5 [Starting the ePolicy Orchestrator server service on page 54.](#)

Stopping the ePolicy Orchestrator server service

Now that you have successfully installed ePolicy Orchestrator 3.5, you need to stop the ePolicy Orchestrator server service (**McAfee ePolicy Orchestrator 3.5 Server**) to ensure the data integrity while you back up the database. Depending on the operating system that you are using, this procedure varies. For instructions, see the Microsoft product documentation.

Installing Client Tools only (SQL Server 2000)

With the ePolicy Orchestrator server service stopped, you need to install the SQL Server 2000 Client Tools before you can back up ePolicy Orchestrator 3.5 databases.

- 1 Insert the SQL Server 2000 CD into the CD-ROM drive of the computer. The installation menu appears.
- 2 Click **SQL Server 2000 Components**.
- 3 Click **Install Database Server**. The **Welcome** wizard appears.
- 4 Click **Next** twice.
- 5 Select **Create a new instance of SQL Server**, or **install Client Tools**, then click **Next**.
- 6 Type a **Name** and **Company**, then click **Next**.
- 7 Click **Yes** to agree to the terms of the license agreement.

- 8 Select **Client Tools Only**, then click **Next**.
- 9 Accept the default components and subcomponents, then click **Next** twice.
- 10 Click **Finish**.

Backing up ePolicy Orchestrator 3.5 databases (MSDE users)

Now that you have installed the SQL Server 2000 Client Tools, you are ready to back up the ePolicy Orchestrator 3.5 databases. It is important to back up the database should you need to revert to using Microsoft Data Engine (MSDE). Be sure to store the backup copy of the database files (for example, EPO_<SERVER>.BAK) in a safe and secure location.

- 1 Start SQL Server 2000 Enterprise Manager.
- 2 In the console tree under **Microsoft SQL Servers**, right-click **SQL Server Group**, then select **New SQL Server Registration**.
- 3 Specify the desired SQL server, use the SQL Server authentication method, type the logon name (sa is the default) and password (blank is the default), and select a SQL Server group.
- 4 In the console tree under the SQL server you just registered | **Databases**, right-click the desired ePolicy Orchestrator database (for example, EPO_<SERVER>), then select **All Tasks** | **Backup Database**. The **SQL Server Backup** dialog box appears.
- 5 On the **General** tab, verify that the name of the ePolicy Orchestrator database appears in **Database**.
- 6 Under **Backup**, select **Database - complete**.
- 7 Under **Destination**, click **Add** to open the **Select Backup Destination** dialog box.
- 8 Select **File name**, then type the desired path or click the browse button to select a directory.
- 9 Under **Overwrite**, select **Append to media**.
- 10 Click the **Options** tab, then select **Verify backup upon completion**.
- 11 Click **OK** to save the current entries and close the **SQL Server Backup** dialog box.

A .BAK file is created.

Backing up ePolicy Orchestrator 3.5 databases (SQL Server 7 users)

Now that you have stopped the ePolicy Orchestrator server service, you are ready to back up the ePolicy Orchestrator 3.5 databases. It is important to back up the database should you need to continue using SQL Server 7 with Service Pack 3. Be sure to store the backup copy of the database files (for example, EPO_<SERVER>.BAK) in a safe and secure location.

- 1 Start SQL Server 7 Enterprise Manager.

- 2** In the console tree under **Microsoft SQL Servers | SQL Server Group**, select the SQL server where the ePolicy Orchestrator database resides. If the server doesn't appear in the console tree, you must register it.

To register a SQL server, right-click **SQL Server Group**, then select **New SQL Server Registration**. Specify the desired SQL server, authentication method, and SQL Server group.
- 3** In the console tree under the desired SQL server | **Databases**, right-click the desired ePolicy Orchestrator database (for example, EPO_<SERVER>), then select **All Tasks | Backup Database**. The **SQL Server Backup** dialog box appears.
- 4** On the **General** tab, verify that the name of the ePolicy Orchestrator database appears in **Database**.
- 5** Under **Backup**, select **Database - complete**.
- 6** Under **Destination**, click **Add** to open the **Select Backup Destination** dialog box.
- 7** Select **File name**, then type the desired path or click the browse button to select a directory.
- 8** Under **Overwrite**, select **Append to media**.
- 9** Click the **Options** tab, then select **Verify backup upon completion**.
- 10** Click **OK** to save the current entries and close the **SQL Server Backup** dialog box.

A .BAK file is created.

Installing SQL Server 2000

Now that you have successfully backed up the ePolicy Orchestrator 3.5 databases, you can install SQL Server 2000. Use the installation or upgrade procedure that is recommended by Microsoft. At press time, the SQL Server and Microsoft Developer Network (MSDN) home pages were located at:

SQL Server home page:

<http://www.microsoft.com/sql/default.asp>

MSDN home page:

<http://msdn.microsoft.com/default.asp>



You can move the ePolicy Orchestrator database to a different computer, but the name of the computer on which the ePolicy Orchestrator server resides cannot change. If you move the database, you will need to change the server configuration to use the new location. For information on this procedure, see [Configuring the ePolicy Orchestrator server on page 54](#).

Configuring the ePolicy Orchestrator server

If you moved the ePolicy Orchestrator database to a different computer, you need to change the server configuration to use the new location before you can connect to it from ePolicy Orchestrator.

- 1 Start the Server Configuration program (CFGNAIMS.EXE). The default location is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0
- 2 In the **Server Configuration** dialog box on the **SQL Server** tab, select the desired **SQL server name** and **Database name**.
- 3 Click **OK** to save the current entries.

Starting the ePolicy Orchestrator server service

Before you can begin using ePolicy Orchestrator, you need to restart the ePolicy Orchestrator server service (**McAfee ePolicy Orchestrator 3.5 Server**). Depending on the operating system that you are using, this procedure varies. For instructions, see the Microsoft product documentation.

B

Settings Conversions

McAfee AutoUpdate Architect 1.0 information conversion

Information in McAfee AutoUpdate Architect 1.0 is converted when it is migrated to ePolicy Orchestrator 3.5:

In McAfee AutoUpdate Architect, this...	Is converted to this...
Master repository.	Global distributed repository.
Distributed repositories.	Global distributed repositories.
Source repositories.	Source repositories.
Fallback repository.	Source repository.
Contents of the master repository.	The contents of the master repository are not migrated.
Proxy server settings.	These settings are not converted. You must define the proxy server settings for both the master repository and client computers.
Pull and replication tasks.	These tasks are not converted. You must schedule new Repository Pull and Repository Replication server tasks. You can still run pull and replication tasks immediately.



If there are repositories in McAfee AutoUpdate Architect and ePolicy Orchestrator with the same name, the ePolicy Orchestrator repository is used and the McAfee AutoUpdate Architect is not converted.

McAfee AutoUpdate 7.0 information conversion

If you are currently using ePolicy Orchestrator 2.5.1 to manage McAfee products that use AutoUpdate 7.0 (for example, McAfee VirusScan Enterprise 7.0), you can keep the **McAfee AutoUpdate 7.0** policies and tasks for use with the agent 2.5.1 and convert them to **ePolicy Orchestrator Agent** policies and tasks for use with the agent 3.5.



If you don't migrate the **McAfee AutoUpdate 7.0** policies and tasks, they are no longer enforced on client computers.

Regardless of whether you choose to migrate these policies and tasks during the installation, the **McAfee AutoUpdate 7.0** policy page is removed and cannot be added back to the **Repository** in version 3.5.

Although you cannot view or change the **McAfee AutoUpdate 7.0** policies and tasks after the installation, they continue to be enforced on the agent 2.5.1. Their settings remain in the ePolicy Orchestrator database and continue to be exchanged during agent-to-server communication. You can remove these settings from the database after you upgrade all agents to version 3.5, or when you no longer want to enforce these policies and tasks on the agent 2.5.1.

How AutoUpdate 7.0 information in ePolicy Orchestrator 2.5.1 is converted in version 3.5 is described below:

In version 2.5.1, this...	Is converted to this...
Repositories.	Hidden repositories. Although these repositories no longer appear, client computers using the agent 2.5 or 2.5.1 continue to retrieve updates from these repositories. These repositories are also converted to local distributed repositories. Client computers using the agent 3.1 retrieve updates from these repositories.
NAIFtp and NAIHttp default repositories.	Although these are converted to local distributed repositories, we recommend that you remove them after the installation as they are now used as the default fallback and source repositories, respectively.
Proxy server settings.	Proxy server settings are converted and applied to client computers. You must define the proxy server settings for the master repository separately.
McAfee AutoUpdate 7.0 — Update and Mirror client tasks.	Hidden McAfee AutoUpdate 7.0 — Update and Mirror client tasks. Although these tasks no longer appear, they continue to be enforced on the agent 2.5 and 2.5.1. These tasks are also converted to ePolicy Orchestrator agent — Update and Mirror tasks, which are enforced on the agent 3.1 only.
Policy and task inheritance.	Policy and task inheritance is preserved.

Index

A

- agent for NetWare
 - system requirements, 10
- agent for WebShield appliances
 - system requirements, 11
- 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, 35
 - calculating number of SQL licenses, 7
 - system requirements, 7
- database software
 - determining when to install, 13, 19, 32
 - upgrading to MDAC, 15, 20, 34
- distributed repository requirements, 8

E

- error messages
 - list of, 48

F

- first-time installation
 - calculating number of SQL licenses, 7
 - pre-installation checklist, 12, 19, 32
 - remote consoles, 28
 - server and console, 21

I

- installing the software
 - calculating number of SQL licenses, 7
 - pre-installation checklist, 12, 19, 32

K

- Korean reports, requirements, 8

L

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

M

- MDAC
 - upgrading, 15, 20, 34
- messages
 - list of, 48
- migrating to SQL Server 2000 from SQL Server 7, 51

O

- operating systems language support, 11

P

- pre-installation checklist, 12, 19, 32

R

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

S

- server and console
 - upgrade, 36
- server requirements, 5
- SQL licenses, calculating number of, 7
- starting the software, 16
- SuperAgent
 - system requirements, 10
- system requirements, 5

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

T

- troubleshooting
 - list of messages, 48

U

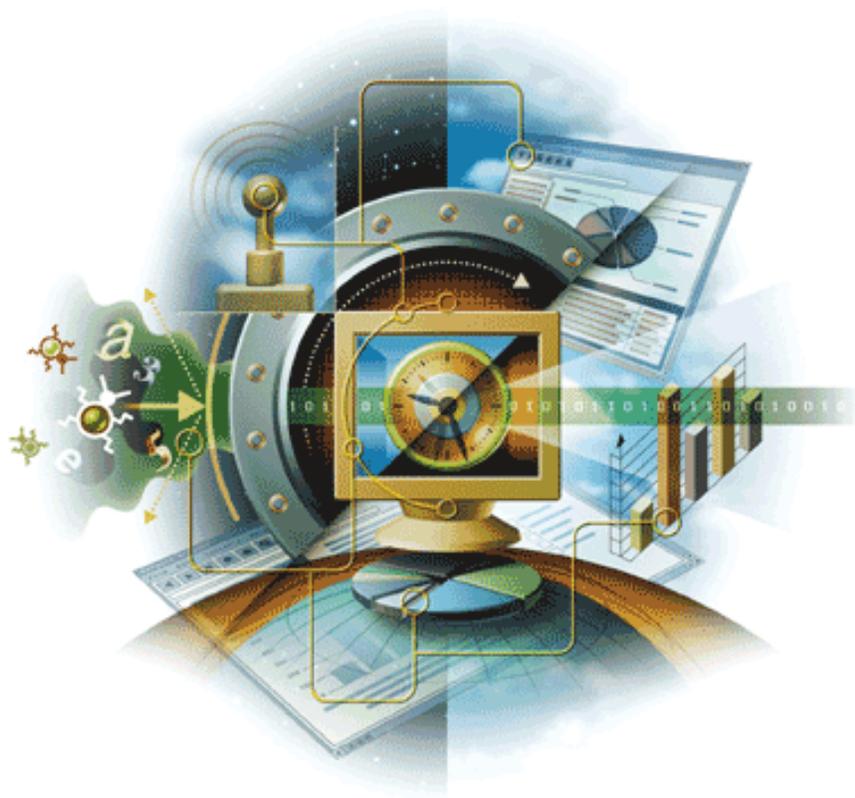
- update repository requirements, 8
- upgrade installation
 - backing up databases, 35
 - calculating number of SQL licenses, 7
 - pre-installation checklist, 12, 19, 32
 - remote consoles, 41
 - server and console, 36

W

- Windows 95 computers requirements, 8

ePolicy Orchestrator® 3.5

Easy steps to set up ePolicy Orchestrator and
try out new features in a test environment



McAfee®
System Protection

Industry-leading intrusion prevention solutions



COPYRIGHT

Copyright © 2004 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Entercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Viruscan, Virusscan (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. 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.

PATENT INFORMATION

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

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 provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. • Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. • Software written by Douglas W. Sauder. • Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. • Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. • FEAD™ Optimizer™ technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In™ Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In™ HTML Export, © 2001 Stellent Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1989. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems®, Inc. © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, © 1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, © 2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors. • Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>). • Software copyrighted by Kevin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. • Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, © 2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. • Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Contents

Introduction: Before You Begin	4
Step 1: Install the ePolicy Orchestrator server and console	8
Step 2: Create your Directory of managed computers	10
1. Add computers to your Directory	11
2. Organize computers into groups for servers and workstations	15
Step 3: Push agents to the clients in your Directory	16
1. Configure the agent policies before deploying	17
2. Initiate an agent installation to the computers in your site	18
Install agent manually on client computers	19
Step 4: Set up master and distributed repositories	20
1. Add VirusScan Enterprise to the master repository	21
2. Pull updates from McAfee source repository	22
3. Create a distributed repository	23
1. Create a shared folder on a computer to be a repository	24
2. Add the distributed repository to the ePolicy Orchestrator server	25
3. Replicate master repository data to distributed repository	26
4. Configure remote site to use the distributed repository	27
Step 5: Set VirusScan Enterprise 8.0i policies before deploying	28
Step 6: Deploy VirusScan Enterprise to clients	29
Step 7: Run a report to confirm your coverage	32
Step 8: Update DAT files with a client update task	33
Step 9: Schedule automatic repository synchronization	35
1. Schedule a pull task to update master repository daily	35
2. Schedule a replication task to update your distributed repository	36
3. Schedule a client update task to update DATs daily	37
Step 10: Test global updating with SuperAgents	38
1. Deploy a SuperAgent to each subnet	38
2. Enable global updating on ePolicy Orchestrator server	39
Step 11: Where to go from here?	40
Feature Evaluations	41
ePolicy Orchestrator Notification	41
Step 1: Configure agent policy to upload events immediately	41
Step 2: Configure Notifications	42
Step 3: Creating a rule for any VirusScan Enterprise event	44
Step 4: Providing a sample virus detection	46
Rogue System Detection	46
Step 1: Configure Rogue System Detection sensor policy	47
Step 2: Deploy the Rogue System Detection sensor	48
Step 3: Configure an automatic response	50
Step 4: Rogue detection and remediation	51

Introduction: Before You Begin

This evaluation guide demonstrates how you can install and deploy ePolicy Orchestrator in a test environment. It provides easy steps that gets you up and running quickly with a test deployment of ePolicy Orchestrator 3.5, and illustrates important features.

This guide is divided into two sections:

- Installation and Setup
- Maintaining and Monitoring your Environment

Install ePolicy Orchestrator and deploy VirusScan Enterprise in ten easy steps

The steps covered in this evaluation guide are:

- 1 *Install the ePolicy Orchestrator server and console.*
- 2 *Create your Directory of managed computers.*
- 3 *Push agents to the clients in your Directory.*
- 4 *Set up master and distributed repositories.*
- 5 *Set VirusScan Enterprise 8.0i policies before deploying.*
- 6 *Deploy VirusScan Enterprise to clients.*
- 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 in this guide

This evaluation guide describes how to deploy ePolicy Orchestrator 3.5 in a small lab environment consisting of one ePolicy Orchestrator server and a small number of client computers. The demonstrates the basic steps required to deploy ePolicy Orchestrator in this environment quickly and test its most important features.

What is not covered in this guide

This document does not cover everything that ePolicy Orchestrator can do, including many advanced features or installation scenarios typical in real-world deployments. While you can follow many of these basic steps for your live deployment, this guide may not cover everything you will need. For complete information on all aspects of the product, including advanced features, refer to the *ePolicy Orchestrator 3.5 Product Guide*.

What is and is not covered in this evaluation guide

What this guide covers	What is not covered	Comments
Single ePolicy Orchestrator server and console.	Multiple ePolicy Orchestrator servers and remote consoles.	In a small test environment, one server is enough.
MSDE database running on the same server as ePolicy Orchestrator.	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 to client computers	Manually installing the agent is also covered.
Simple network environment with NT Domain and Active Directory.	Unix, Linux, or Netware environments	This guide uses NT Domains and Active Directory to help illustrate key product features.

Set up your lab environment for testing ePolicy Orchestrator

Before you begin installing and testing ePolicy Orchestrator, you must first create a safe test network. Planning and testing a live deployment in your organization may take weeks or even months, especially if your organization is very large. However, you should be able to create a small test environment within several hours, or identify several existing computers on your network for testing within even less time.

At the very least, this environment should contain one server computer to host the ePolicy Orchestrator server, and one or more client computers, which can be either servers or workstations, to which you deploy agents and VirusScan Enterprise 8.0i. See the *ePolicy Orchestrator 3.5 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.

As you set up your test environment, ensure your network is correctly configured for ePolicy Orchestrator by considering:

- 1 Create a network user account with administrator privileges.** If you plan to use the ePolicy Orchestrator server to push agents to computers, the server must have administrator credentials. You can configure ePolicy Orchestrator to use these credentials when you install the server, or you can specify them when you push the agent. Either way, you will need an administrator user name and password to deploy agents from the ePolicy Orchestrator console.
- 2 Create trusted domain connections to any remote NT domains.** If you plan to test deploying agents to computers located outside the local NT domain where the ePolicy Orchestrator server resides, you must create a trusted connection between the domains. This connection is required to allow the server to deploy agents and install software on these remote clients. See your Microsoft Windows documentation for information on how to do this. Furthermore, you must have a user account with administrator rights in the remote domain for the ePolicy Orchestrator server to be able to deploy agents to those clients.

- 3 Ping client computers from the ePolicy Orchestrator server.** From the computer where you plan to install the ePolicy Orchestrator server, ping client computers to which you plan to deploy agents to test network connectivity. To do this from your server, open a command window by selecting **Start | Run** and typing `cmd` at the run prompt. Then type ping commands, using the syntax below. Test both computer name and IP address:

```
ping MyComputer  
  
ping 192.168.14.52
```

- 4 Confirm that client NT Admin\$ share folders are accessible from the server.** From the computer on which you plan to install your ePolicy Orchestrator server, test access to the default Admin\$ share folder on each client computer. The ePolicy Orchestrator server service requires access to this shared folder to install agents and other software, such as VirusScan Enterprise. This test also confirms your administrator credentials, because you cannot access remote Admin\$ shares without administrator rights. To access client Admin\$ shares from the ePolicy Orchestrator server, do the following:

- a Select **Start | Run**.
- b At the run prompt, type the path to the client Admin\$ share by specifying either computer name or IP address:

```
\\MyComputer\Admin$  
  
\\192.168.14.52\Admin$
```

If the computers 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.

- 5 Install Microsoft updates on any Windows 95, Windows 98, or Windows ME client computers.** If you include clients running Windows 95, Windows 98, or Windows ME in your test, download VCREDIST.EXE and DCOM 1.3 updates from the Microsoft web site and install them on these clients as required. ePolicy Orchestrator agents will not run on these clients without them. See the *ePolicy Orchestrator 3.5 Installation Guide* or the following links for information:

support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q259403&
www.microsoft.com/com/dcom/dcom95/dcom1_3.asp

- 6 Enable File and Print Sharing on Windows 95, Windows 98, or Windows ME client computers.** If you plan to deploy the agent to Windows 95, Windows 98, or Windows ME clients, you must first enable **File and Print Sharing** on those clients. This is only required if you plan to *push* agents to these clients. If you install the agent manually or through some other method, such as a logon script, this is not required. Once you have pushed the agent to these Windows 95, Windows 98, Windows ME clients, you can disable **File and Print Sharing** again and still manage agent policies on those clients with ePolicy Orchestrator.

About the lab environment used in this guide

The lab environment used in this guide consists of one NT domain and one Active Directory container, each containing several servers and several workstations.

Having multiple NT domains or Active Directory containers in your lab environment is not required to use this guide or test ePolicy Orchestrator.

Table 1 Computers in Domain1 (IP addresses 192.168.14.1-255)

Computer	Details
ePO Server	Windows 2000 Server SP 4 running SQL Server 2000 SP 3. This computer hosts the ePolicy Orchestrator server, console, database, and master software repository.
4 clients	Running Windows 2000 Professional.

Table 2 Computers in Domain2 (IP addresses 192.168.15.1-255)

Computer	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:

- **EPO350EML.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 computers 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 computer 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 3.5** from the list and click the **TRY** link.
- 3 Fill out the form and follow directions to download the EPO350EML.ZIP file.
- 4 Extract the contents of the EPO350EML.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 computer 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 computer you plan to use as your ePolicy Orchestrator server. In the examples used in this guide, we install the ePolicy Orchestrator server to the computer 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 **ePOTemp** folder where you extracted the **EPO350EML.ZIP**.
- 2 Click **Next** at the initial page of the **ePolicy Orchestrator 3.5.0 Setup** wizard.
- 3 If you are installing an evaluation version, click **OK** at the **Evaluation** page.
- 4 On the license agreement, select **I accept the terms in the license agreement** and click **OK**.
- 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 computer with a static IP address in your production environment, a DHCP-assigned IP address can be used for testing purposes.

- 7 On the **Set Server Password** dialog box, enter the password you would like to use for the ePolicy Orchestrator server. You cannot leave this blank.
- 8 On the **Server Service Account** dialog box, deselect **Use Local System Account**.
- 9 In the **Account Information** area, enter a domain, user name and password to be used by the ePolicy Orchestrator server service.
- 10 Click **Next** to save the account information and continue.

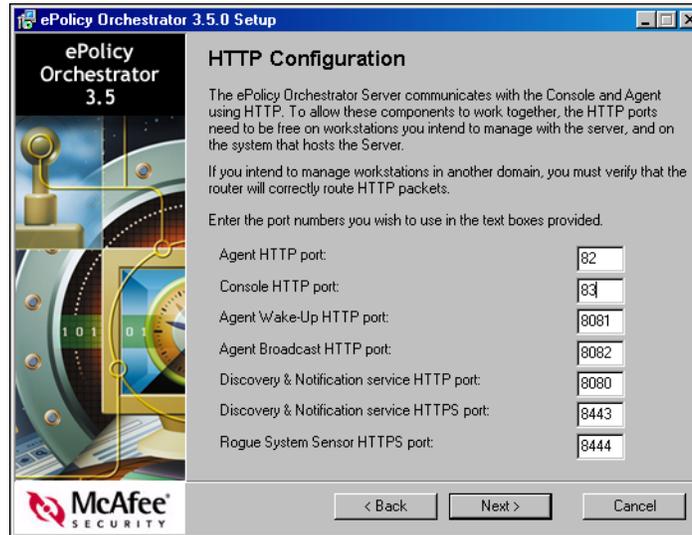


If the account you specified is not an administrator account, you will see a warning that you cannot use ePolicy Orchestrator to deploy agents. If you want the ePolicy Orchestrator server service to have rights so that you can deploy agents, click **OK** then **Back** and type a user account and password with administrator rights. Alternatively, you can use a non-administrator account for the ePolicy Orchestrator server service and still deploy agents by specifying administrator credentials at deployment time. Finally, you can choose not to deploy agents through ePolicy Orchestrator at all, but rather install the agent manually and use ePolicy Orchestrator only to manage policies. In this case you do not need administrator rights for your server service account.

- 11 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.
- 12 Click **Next**.
- 13 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.
- 14 Click **Next** to save the database account information.

- 15** On the HTTP Configuration dialog box, change the HTTP port for Agent communication to 82 and the HTTP port for Console communication to 83.

Figure 1 Change the HTTP ports used by agent and console if already being used



Some HTTP ports, and 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 this conflict.

- 16** 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 15](#), this time specifying unused HTTP ports.

- 17** 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.

- 18** 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 computer during the installation.

- 19** Click **OK** when prompted to reboot and be sure to log back in when the computer reboots to allow the installation to continue.

- 20** 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 computers 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 | Network Associates | ePolicy Orchestrator 3.5.0 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 `administrator`, then type the **Password** you set during the installation wizard, and 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.

Congratulations on a successful installation of your ePolicy Orchestrator server, console, and database!

STEP

2

Create your Directory of managed computers

The **Directory** is in the left-hand console tree of the ePolicy Orchestrator console. The **Directory** contains all the computers in your network that are managed by ePolicy Orchestrator. In other words, the **Directory** contains all the computers in your network running active ePolicy Orchestrator agents that are reporting to this server.

Before you start managing client anti-virus policies for computers on your network, you must add those computers to your ePolicy Orchestrator **Directory**. After installing the server, you initially have one computer in the **Directory**—the ePolicy Orchestrator server itself.

To organize your computers, you can group them into logical collections called *sites* and *groups*. You can create a tree hierarchy of sites and groups, much like you would create a hierarchy of folders in Windows Explorer. Grouping is useful because ePolicy Orchestrator allows you to define policies at the group level. You can group computers according to any criteria that makes sense for your organization.

This guide uses three common levels 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**, or parts of it, 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 computers 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 computers 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 computers to your Directory

The first step in creating your **Directory** is to add computers from your network. Try one of these three methods:

- *Option A: Automatically add entire existing NT domains to your Directory.* Very easy and fast. Very useful if you plan to deploy agents to every computer in that domain. Use this method if you organized your test client computers into domains in your lab network, as in the examples in this evaluation guide.
- *Option B: Automatically add entire Active Directory containers to your Directory.* Very easy and fast. Very 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 computers 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 computers in your test network.

Option A: Automatically add entire existing NT domains to your Directory

ePolicy Orchestrator allows you to import all computers in an NT domain into your **Directory** with just a few clicks. Use this feature if you organized your test client computers into domains in your lab network.

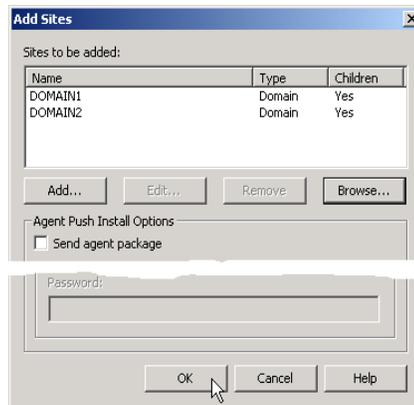
The examples in this guide use this method to create **Directory** sites from an NT domain on the test network, **Domain1**.

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 computers 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 policies.

Figure 2 Add Sites dialog box



After a few moments, the computers 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 computers 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 computers 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 computers 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 computer running the remote console, if you are using a remote console, can reach the Active Directory server.

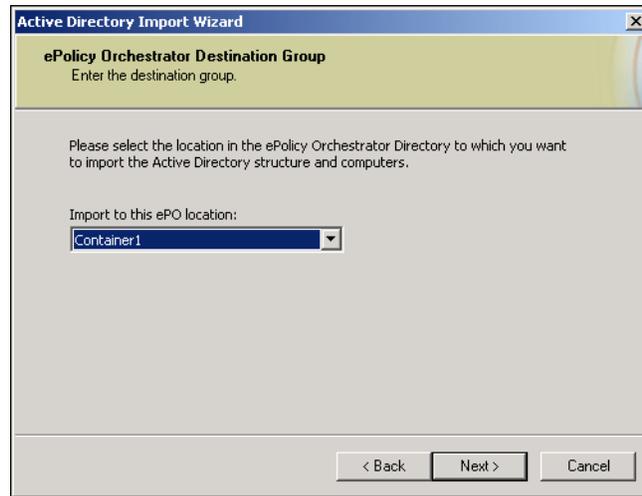
The **Active Directory Import** wizard is meant to be used as a tool to import Active Directory computers for the first time, while you create the entire **Directory**, or only a specific site of the **Directory**. You will use the **Active Directory Computer Discovery** task to regularly poll these Active Directory containers for any new computers.

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 3 Active Directory Import wizard



- 7 On the **ePolicy Orchestrator Destination Group** panel of the wizard you can select the **Directory** root or a site of the **Directory** to import the Active Directory computers.

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 will result 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 computers that have been imported. Verify in the ePolicy Orchestrator tree that these computers were imported.
- 12 Click **Finish**.

The Active Directory computers have been imported into the **Lost&Found** directory located under the site to which you imported them. If your Active Directory container included sub-containers, the **Lost&Found** directory retains the Active Directory hierarchy.

- 13 Click and drag the top of this structure from **Lost&Found**, to the site above it. (The site you selected in the wizard. For example **Container1**.)

Congratulations. You have imported your Active Directory computers 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 Computer Discovery** task. This task regularly polls administrator-specified Active Directory containers for any new computers. See the *ePolicy Orchestrator 3.5 Product Guide* for instructions. This task is beyond the scope of this guide.

Option C: Manually add individual computers to your Directory

When you deploy ePolicy Orchestrator in your production network, you probably want to populate the **Directory** automatically by importing your NT domains as shown in the previous section. However, for testing purposes in a small lab environment, you can also add sites and computers to your **Directory** manually. The first step, therefore, is to manually create a site. After that, you can manually add computers to it.

Create a new site in which to group the computers

- 1 Right-click the **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**.

Manually add new computers to your site

Now that you have created a site or sites, the next step is to manually add each new computer to your site. To do this:

- 1 In the **Directory**, right-click the site you added and select **New | Computer**.
- 2 In the **Add Computers** dialog box, add new computers either by clicking **Browse** to locate them in your NT Network Neighborhood, or by clicking **Add** and typing the computer's NetBIOS name.
- 3 Click **OK** once you have added the names of all the computers.

ePolicy Orchestrator adds the new computers to the **Directory** beneath the site.

2 Organize computers into groups for servers and workstations

Once you've created sites and added computers to your **Directory**, it is a good idea to organize them into groups. The groups you create depend on what makes sense in your network. You may want to group computers by functional area, such as Sales, Marketing, or Development. You may want to create groups for geographic units, such as office locations. Or you may want to group computers 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 3.5.0 actually allow you to set separate policies for servers and workstations without creating these groups. However, grouping computers by operating system is a conceptually simple way to illustrate how using **Directory** groups can make managing policies easier. Feel free to 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 computers 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.



Note that 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 computers.

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 computers 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**.

Add computers to the new groups you created

Once the new groups appear in the **Directory**, drag computers from that site into the appropriate group as you would drag files in Windows Explorer. You must drag computers in the **Directory** one at a time; you cannot select multiple computers. Alternatively, you can use the **Directory** search feature (right-click the **Directory** and select **Search**) to move multiple systems at one time.

While dragging computers into groups, ignore the **IP Integrity warning** message if you see it by clicking **OK**.

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 computers running both Windows 2000 and Windows 98. Due to limitations with older versions of Windows, we need to set different policies for computers 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 computers, either manually or by importing existing NT domains on your network. And you have separated the computers 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

Push agents to the clients in your Directory

Before you can do anything else to manage the client computers in your **Directory**, you must install an ePolicy Orchestrator agent to those client computers. The agent is a small application that resides on the client computer and periodically checks 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.** If you specified administrator credentials when you installed your ePolicy Orchestrator server service, you will automatically be able to deploy agents; otherwise, you will need to specify appropriate credentials when you deploy.
- **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 domain.
- **For Windows 95 and Windows 98 computers, 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 Installation Guide* for information on finding and installing these updates. You must install these updates to be able 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 computers, turn on File and Print Sharing.** Enable **File and Print Sharing** on each client to which you plan to push the agent. Note that this is only a requirement to *push* the agent from the ePolicy Orchestrator server, not to manage policies. Once you have deployed the agent to a Windows 95 or Windows 98 computer, you can disable file and print sharing.

From the **Directory** in the ePolicy Orchestrator console, you can install the agent to all computers in a site at once. To do this, send an agent install command at the site level. Because of the concept of *inheritance*, you can specify an agent installation at the parent site (or group) level and all children, whether groups or computers, inherit the command.

In our example **Directory** containing two sites you will initiate separate agent installations to each site. These two agent installation commands install the agent to all computers in these sites.

To deploy agents to a site:

- 1 [Configure the agent policies before deploying.](#)
- 2 [Initiate an agent installation to the computers in your site.](#)

Alternatively, if you do not plan to use ePolicy Orchestrator to push the agent, you can install the agent manually from the client computer. See [Install agent manually on client computers](#) on page 19.

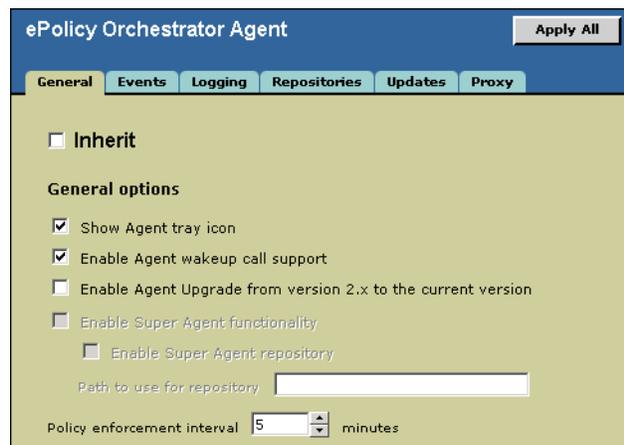
1 Configure the agent policies before deploying

You can deploy agents with the default policy settings. However, for testing purposes, you will modify the policy to allow the agent tray icon to display in the Windows system tray on the client computer. Not only will this expose you to setting agent policies, it also makes it easier to see when the agent has installed on your clients. When you make this policy change at the site level, it applies to all test computers that exist as children in this site. This allows you to change the policy configuration once then deploy it to all your computers in a site.

To change the agent policy so that the agent icon appears in the system tray after installation:

- 1 Select your site (*Domain1* in this example) by clicking it once in the **Directory** tree.
- 2 In the right-hand details pane, click the **Policies** tab and select **ePolicy Orchestrator Agent | Configuration**.
- 3 In the **ePolicy Orchestrator Agent** page, deselect **Inherit** to enable configuration options.

Figure 2-1 General tab



- 4 On the **General** tab, select **Show Agent tray icon** and click **Apply All** to save your change.

- 5 Repeat these steps to make the same agent policy change to other sites (**Container1** in this example).

Now your policies are set and your agents are ready to deploy. The next step is to begin an agent install.

2 Initiate an agent installation to the computers in your site

Use the **Install Agent** feature to have ePolicy Orchestrator push agents to your client computers. Push agents to all your test computers in a site at once by initiating the agent installation at your site level in the **Directory**.

To initiate an agent installation for all computers in a site:

- 1 Right-click the site in your **Directory** and select **Install Agent**.
- 2 Click **OK** on the **Install Agent** dialog box to accept all default settings and begin the agent installation.



If you installed the ePolicy Orchestrator server to use the local system account, you need to deselect **Use ePO server credentials** and specify a user account and password with domain administrator rights.

- 3 Repeat these steps for other sites in your **Directory**.

The agent installations begin immediately.

A word about deploying agents to computers running Windows 95, Windows 98, or Windows ME

When pushing agents to computers running Windows 95, Windows 98, or Windows ME you may not be able to tell that the agent has been successfully deployed until you log out of the client computer. This can include the agent icon not appearing in the system tray or the computer not showing up as managed in the ePolicy Orchestrator console **Directory**. If, after logging out and back into the Windows 95, Windows 98, or Windows ME clients, the agent still does not appear, try pushing it again. If that still does not work, you can install the agent manually from the client (see [Install agent manually on client computers on page 19](#)).

A word about deploying to computers outside the local NT domain

If the other site(s) contain computers 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 initiating the agent push, 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.

What can I do while I'm waiting for agents to install?

It may take up to ten minutes for all the agents to be installed on all computers in your sites, and for the **Directory** 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 computers 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 computers as managed until they call back to the server, usually within ten minutes. This is true even though the agent is installed and running on the clients.

You can also watch the installation from any of your client computers. 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 computer 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 for the first time.

Install agent manually on client computers

Rather than use ePolicy Orchestrator to push the agent, you may want to install it manually from the client. Some organizations may want to install software on clients manually and use ePolicy Orchestrator to manage policies only. Or, maybe you have many Windows 95 or Windows 98 clients and do not want to enable print and file sharing on them. In these cases, you can install the agent from 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\Network Associates\ePO\3.5.0\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 computer is added to the **Directory** as a managed computer. 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 computer is added to the **Lost&Found** folder. Once the computer 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 computer on which an agent has just been installed.

To manually force the initial agent callback:

- 1 From the client computer 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 back to the ePolicy Orchestrator server immediately.
- 5 From the ePolicy Orchestrator console on your server, refresh the **Directory** by clicking **F5**. The new client computer on which you have just installed the agent should now appear in your **Directory**.

STEP

4

Set up master and distributed repositories

Now you have agents installed on your clients, 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 anti-virus software installed on the client computers, 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 computers.

Software to be 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.

See the following sections for details on how to do this. The steps covered here are:

- 1 [Add VirusScan Enterprise to the master repository.](#)
- 2 [Pull updates from McAfee source repository.](#)
- 3 [Create a distributed repository.](#)

About using master and distributed repositories in your test network

ePolicy Orchestrator uses repositories to store the software that it deploys. This guide 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 DAT files, that you plan to deploy to clients. 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 can reside in other parts of your network, such as other network NT domains or other Active Directory containers. Computers 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 computer in the remote location. Computers in that location, **Container1** in our example, can update from the distributed repository instead of having to copy updates across the WAN.

Computers in the **Domain1** site receive updates and product deployments directly from the master repository, located on the ePolicy Orchestrator server (*ePOServer*). Computers located in the **Container1** site, however, receive them from a distributed repository located on a server.

The VirusScan Enterprise 8.0i NAP file

Policy pages, or NAP files, are used to configure client software from your ePolicy Orchestrator console. ePolicy Orchestrator 3.5 installs with several NAP files, including the VirusScan Enterprise 8.0 NAP.

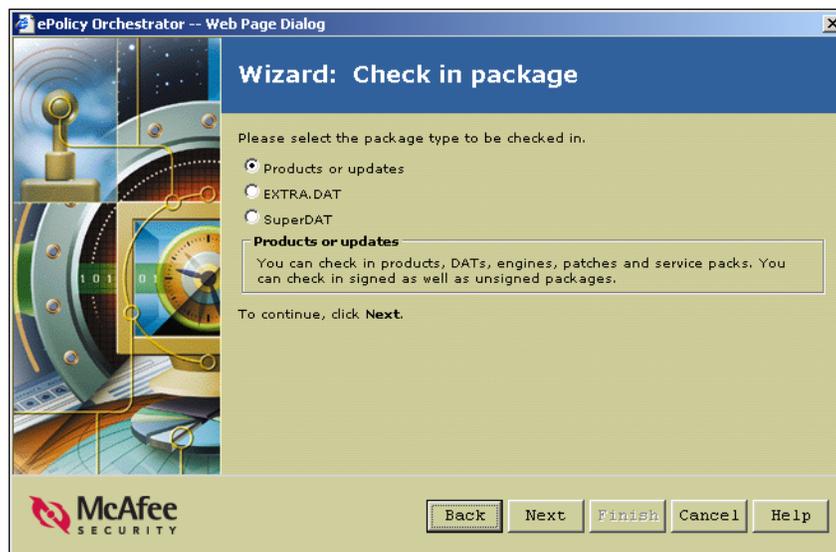
1 Add VirusScan Enterprise to the master repository

The VirusScan Enterprise 8.0i policy pages, or NAP file, allow you to manage VirusScan Enterprise 8.0i policies once it has been installed on client computers in your network. However, to be able to first use ePolicy Orchestrator to *push*, or deploy, VirusScan Enterprise 8.0i to those client computers, 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 7](#)).

To check in the VirusScan Enterprise package to your master repository:

- 1 From the ePolicy Orchestrator console, select **Repository** in the console tree.
- 2 Select **Check in Package** from the right-hand **Repository** details pane.
- 3 When the **Check in package** wizard opens, click **Next**.
- 4 On the second page of the wizard, select **Products or updates** and click **Next**.

Figure 4 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 in your VirusScan Enterprise temporary folder.
- 7 Click **Next** to continue.
- 8 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.

Check in the VirusScan 4.5.1 package if you have Windows 95, Windows 98, or Windows ME clients

VirusScan Enterprise 8.0i does not run on Windows 95, Windows 98, or Windows ME. If you have clients in your test network running these versions of Windows, as is the case in the examples in this guide, you must deploy VirusScan 4.5.1 to these systems. To be able 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, engine, and other updates. Initiate a repository 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.

Configure proxy settings through Internet Explorer or in ePolicy Orchestrator

Your ePolicy Orchestrator server must be able to access the Internet to pull updates from the McAfee source repository. All other computers on your network do not require Internet access—they pull updates either from your master repository or distributed repository on your network (which we will set up in the next step).

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 3.5 Product Guide* for information on how to do this.

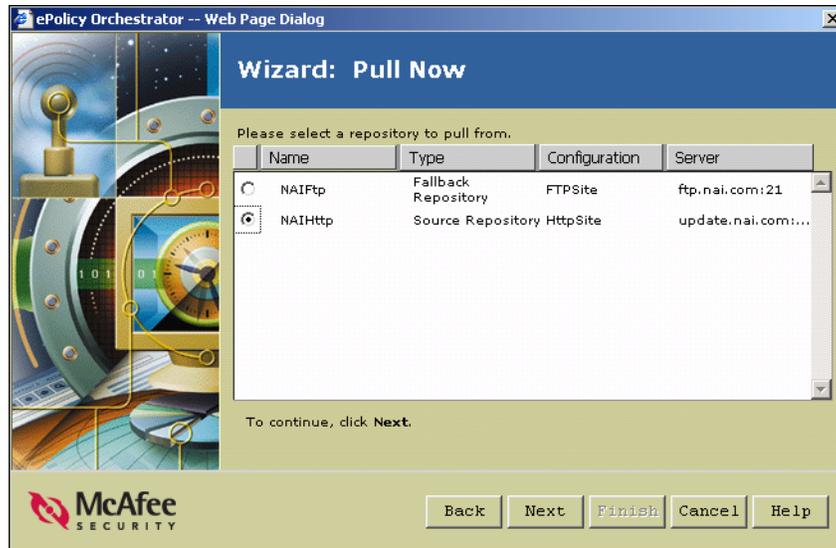
Initiate manual pull from the McAfee source repository

To manually pull updates from the source repository to your master repository:

- 1 From the console tree, click **Repository**.
- 2 Select **Pull Now** from the right-hand **Repository** details pane.

- 3 When the **Pull Now** wizard opens, click **Next** at the first wizard page.
- 4 On the next page, select **NAIHttp** and click **Next**. You can also select the default **NAIFtp**, but HTTP is often more reliable.

Figure 5 Pull Now wizard



- 5 If you are managing older products, such as VirusScan 4.5.1 for Windows 95 or 98 computers, be sure to select **Support legacy product update**.
- 6 Click **Finish** at the last page to accept all defaults on this page and begin the pull.
Wait several minutes while the pull task executes.
- 7 Click **Close** when the pull is complete.

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 computers located in the same domain as your ePolicy Orchestrator server, those computers in your **Domain1** site in the **Directory** in this example, get VirusScan Enterprise from the master repository.

But where do other computers get their software and updates? If these computers are located in different subnets or a WAN-connected location, it may be more efficient to create a distributed repository, or a copy of the master repository, that is more easily accessible to these computers.

3 Create a distributed repository

Now we need to create a distributed repository in **Container1** so that those computers can update from there. Your test network, with only a few clients and one ePolicy Orchestrator server, is small enough to not require an elaborate 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 computers 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 computers in the **Container1** site.

To do this:

- 1 *Create a shared folder on a computer to be a repository.*
- 2 *Add the distributed repository to the ePolicy Orchestrator server.*
- 3 *Replicate master repository data to distributed repository.*
- 4 *Configure remote site to use the distributed repository.*

1 Create a shared folder on a computer to be 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.

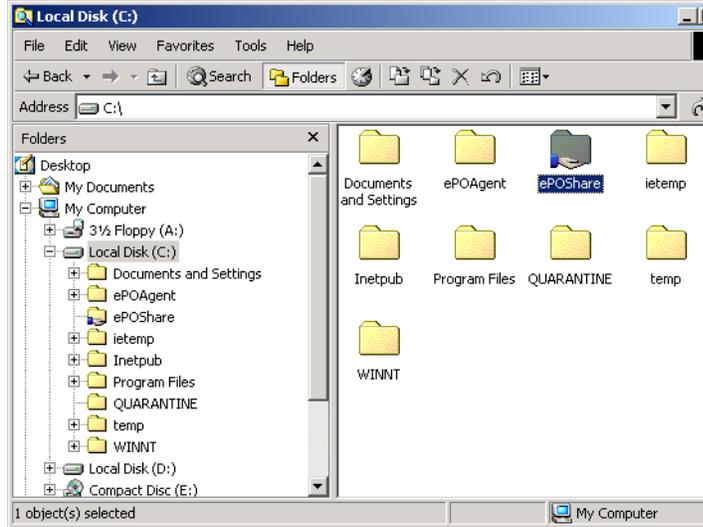
To create a shared folder for a UNC distributed repository:

- 1 From the computer on which you plan to host the distributed 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 computers 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 6 Microsoft Explorer



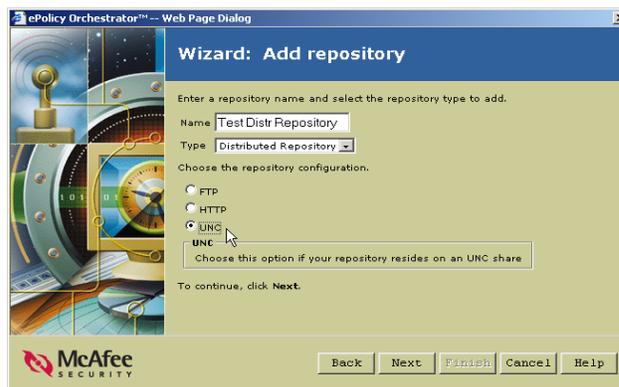
2 Add the distributed repository to the ePolicy Orchestrator server

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 into the **Name** field. Note this is how the distributed repository name appears in the repository list in the ePolicy Orchestrator console. It does not have to be the name of the share folder that actually hosts the repository.

Figure 7 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. The example in this guide would be: \\BU06\ePOShare where BU06 is the name of a computer in **Container1** and ePOShare is the name of the UNC shared folder.
- 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 computers 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 clients.

Figure 8 Verification dialog box



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, DAT files, engine files, or other product updates 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 [Initiate an agent installation to the computers in your site on page 18](#).
- 14 Click **Verify** to test that your ePolicy Orchestrator server can write to the shared folder on the remote computer. 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 computer to host a distributed repository, and added the repository location to your ePolicy Orchestrator database. Now the only thing 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 From the console tree, click **Repository**.

- 2 On the **Repository** page, click **Replicate now** to open the **Replicate Now** wizard.
- 3 Click **Next** at the first page of the wizard.
- 4 From the list of available distributed repositories, select the distributed repository you have created and 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. Wait a few minutes for replication to finish.
- 7 Click **Close** to close the wizard window.

If you browse to your ePOShare folder now, you can see that it now contains subfolders for agents and software.

4 Configure remote site to use the distributed repository

Since you have created a distributed repository, why not make sure it gets used? As stated earlier, 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 computers in one site in your **Directory** 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 in your **Directory** to use only the new distributed repository. In our example network used in this guide, this is the **Container1** site, which is where the Win2KServer computer 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 From the **Directory** in the console tree, select the site that you want to use the distributed repository.
- 2 In the right-hand policies pane, click the **Policies** tab.
- 3 Expand the **ePolicy Orchestrator Agent** and select **Configuration**.
- 4 Click the **Repositories** tab of the ePolicy Orchestrator Agent policy page.
- 5 Deselect **Inherit** to enable repository options.
- 6 Under **Repository selection**, select **User defined list**.
- 7 In the **Repository list**, deselect all repositories until only your distributed repository is selected.
- 8 Click **Apply All** at the top of the page to save all the changes.

Now, when the computers 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 computers 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 clients. 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 computer. To demonstrate how to do this, 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.

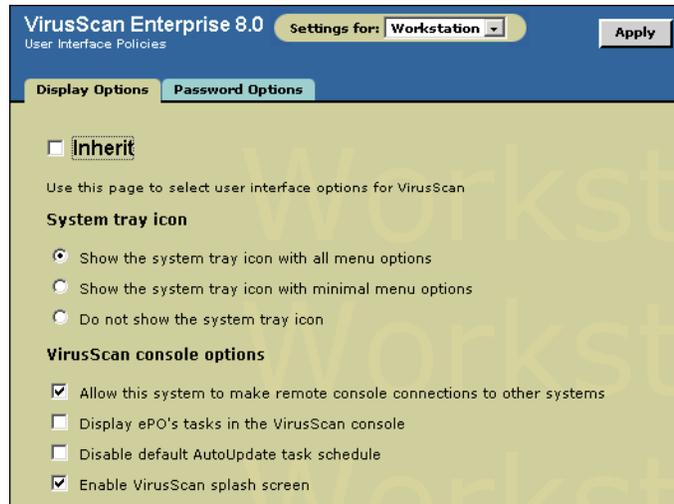
This could be a potentially useful implementation in your real network, where you may want to hide the system tray interface on your workstations to prevent end-users from easily changing policies or disabling features.

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 computers 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 From the console tree, click your *Workstations* group within a site.
- 2 In the details pane, click the **Policies** tab and select **VirusScan Enterprise 8.0i**.
- 3 Select the **User Interface Policies**.

Figure 9 User Interface Policies



- 4 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 computer and applies the right policy. However, for testing purposes, it can be useful to create server and workstation groups.

- 5 Deselect **Inherit** to enable user interface policy options.
- 6 Select **Show the system tray icon with minimal menu options**.
- 7 Click **Apply** to save the changes.
- 8 Repeat these steps for other *Workstations* groups in your **Directory**.

STEP

6

Deploy VirusScan Enterprise to clients

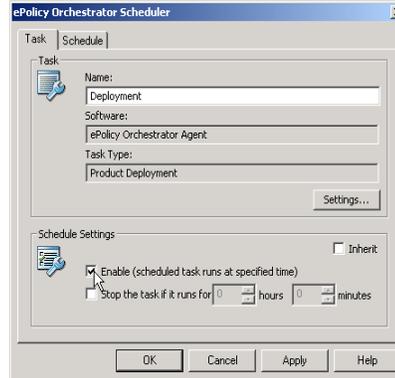
Now you have created master and distributed repositories, added the VirusScan Enterprise 8.0i PKGCATALOG.Z file to your master repository, and replicated this to a new distributed repository. Your computers are added to your **Directory** and they all have ePolicy Orchestrator agents installed on them. 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 clients in your test network.

Unlike deploying agents, which must be done at the site, group, or computer level, you can deploy VirusScan Enterprise from the **Directory** level to install it on all the computers 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 clients within those groups. Alternatively, you can deploy VirusScan Enterprise to sites, groups, or individual computers—you can use the steps in this section to deploy at any level in your **Directory**.

To deploy VirusScan Enterprise 8.0i to all computers in your Directory:

- 1 In the console tree, select **Directory**.
- 2 In the details pane, select the **Task** tab and then double-click the **Deployment** task in the task list.
- 3 Once the ePolicy Orchestrator Scheduler opens, click the **Task** tab and deselect **Inherit** under **Schedule Settings**.

Figure 10 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 computers 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 31](#).

Deploy VirusScan 4.5.1 to Windows 95, Windows 98, or Windows ME computers

If you have any Windows 95, 98, or ME computers in your test network, as this example does, you can repeat the steps in this section to deploy VirusScan 4.5.1 to these computers only. Make sure you have already checked the VirusScan 4.5.1 deployment package into the repository (see [Check in the VirusScan 4.5.1 package if you have Windows 95, Windows 98, or Windows ME clients on page 22](#)). Deploying VirusScan 4.5.1 to several computers is easiest if you have organized your Windows 95, Windows 98, or Windows ME computers into a group in your **Directory**, but you can also run the deployment task for individual computers too.

To deploy VirusScan 4.5.1:

- 1 In the console tree, select your group or computer in your **Directory**.
- 2 In the details pane, click the **Tasks** tab. Follow the steps in the previous section to configure the deployment as you would for VirusScan Enterprise 8.0i.
- 3 When you get to the **Deployment** settings page, set VirusScan 4.5.1 to **Install**.

You can also set VirusScan Enterprise 8.0i to **Ignore**, but this is not necessary. VirusScan Enterprise can detect that these computers are running an older version of Windows and will not install.
- 4 Complete the steps to configure the deployment. ePolicy Orchestrator deploys VirusScan 4.5.1 the next time the agents on these computers call back to the server.

Send an agent wakeup call to force agents to call back immediately

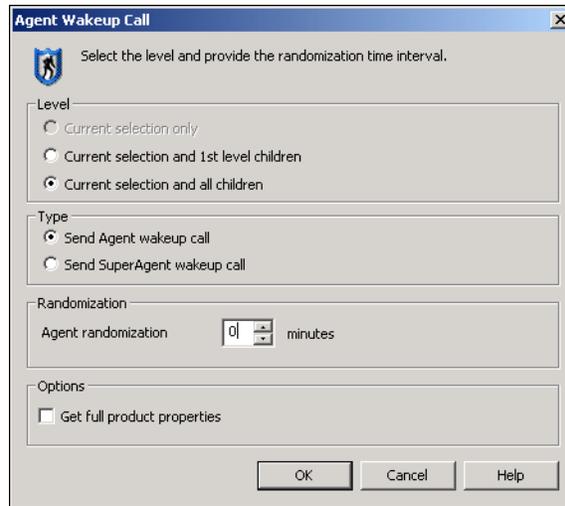
If you want, you can send the agents an immediate agent wakeup call. This forces the agents to check in immediately with the ePolicy Orchestrator server, rather than wait for the next regularly scheduled agent callback, which by default could be as long as 60 minutes. When the agents call back, they 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 computers in the **Domain1** site pull from the master repository and computers from **Container1** pull from the distributed repository we created.

You can send an agent wakeup call to any site, group, or individual computer in your **Directory**. Since we want to wake up all computers in the **Directory**, we'll initiate one wakeup call for each site, which inherit down to groups and computers 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 11 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.

You can check that it has successfully installed on clients in several ways. From the client computer, check that:

- 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/Network Associates` 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

Another way to confirm that your VirusScan Enterprise deployment was successful is to use one of the reports that comes with ePolicy Orchestrator. 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 From the left-pane 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 in to the database, type your MSDE `sa` 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. In our example, you can see that VirusScan Enterprise 8.0i and VirusScan 4.5.1 have installed on all of the computers in our test network.

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 to update DAT virus definition files. VirusScan Enterprise by default performs an update task immediately after installing. So, if you followed the steps in this evaluation guide to configure your repositories and pulled the latest DAT files to your master repository before deploying, VirusScan Enterprise will be 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 evaluation 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 clients 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 20](#).

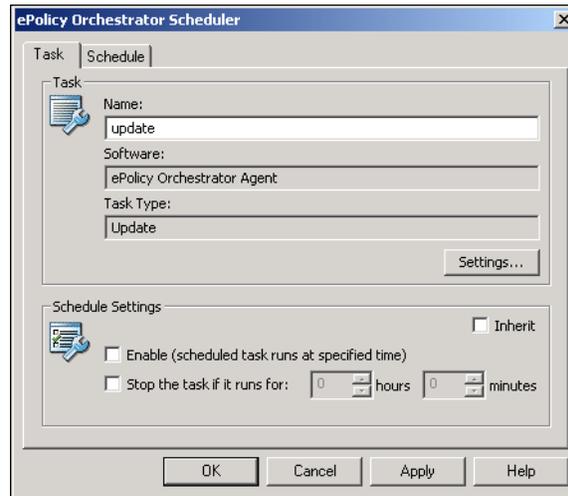
To create and run a client update task:

- 1 In the console tree, right-click the **Directory** and select **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 Press **F5** to refresh the console and make the new task appear in the list in 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 12 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 31.

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 computers after they updated. To do this:

- 1 From the console tree, select **Repository | Software Repositories | Master**. The details pane displays the list of packages currently checked in to the master repository.
- 2 Scroll to the bottom of the **Packages** list and locate the **Current DAT version**, which will be a 4-digit number like 4306.

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 ePolicy Orchestrator console, select any computer in your **Directory** that has recently been updated.
- 2 In the details pane, select the **Properties** tab.
- 3 In the **Properties** page, select **VirusScan Enterprise 8.0i | 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.

STEP

9

Schedule automatic repository synchronization

Well, you've certainly come a long way! 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 computers, 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 computers, and have created a small software repository that you can use to push updates and additional software to your client computers.

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 **Repository** page, select **Schedule pull tasks** to open the **Configure Server Tasks** page.
- 3 Select **Create task** to open the **Configure New Task** page.

Figure 13 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 Expand the **Advanced schedule options** and 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 computers on your network that get their updates from a distributed repository, such as the computers 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 out to your distributed repository. To do this, create an automatic replication task and schedule it to occur every day one hour after the scheduled pull task you already created.

To schedule an automatic replication task:

- 1** In the console tree, select **Repository**.
- 2** In the **Repository** page, 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 into the **Name** field, 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** Expand the **Advanced schedule options** and schedule the day and time for the task to run. Set the time for an hour after your scheduled pull task begins. This should give the pull task enough time to complete. Depending on your network and Internet connections, your pull task may require more or less time, so set your replication task start time accordingly.
- 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 33](#)). 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 is a new feature in ePolicy Orchestrator 3.5 that can automatically update all your client computers 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 can be very useful in a virus outbreak situation. Assume that McAfee's AVERT team has posted updated DATs in response to a newly-discovered virus in the wild. 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 DATs for all computers running active, communicating agents on your network within one hour.

Use SuperAgents to wake up all agents on 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 evaluation guide does not cover SuperAgent repositories, however. Refer to the *ePolicy Orchestrator 3.5 Product Guide* for information on SuperAgent repositories.

To enable global updating:

- 1 *Deploy a SuperAgent to each subnet.*
- 2 *Enable global updating on ePolicy Orchestrator server.*

1 Deploy a SuperAgent to each subnet

You can deploy a SuperAgent to any computer in your ePolicy Orchestrator **Directory**. You can also turn any regular ePolicy Orchestrator agent into a SuperAgent. Use the ePolicy Orchestrator Agent policy pages in the ePolicy Orchestrator console to do this. Since you only need one SuperAgent per network subnet, be sure to configure SuperAgents for individual computers in your **Directory**, and not for whole groups or sites as you did when deploying regular agents or VirusScan Enterprise.

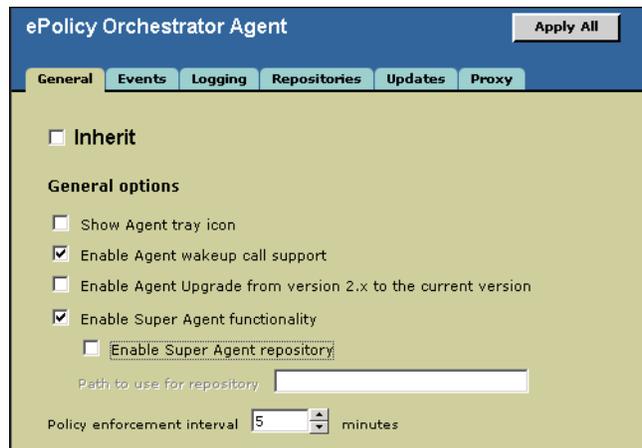
For example, in the sample test network used in this guide, we would deploy one SuperAgent to the Domain1 site.

You can deploy a SuperAgent to a computer that currently has no agent, or you can convert existing regular agents to SuperAgents. In our example, we can do this by changing the policies for an agent for one computer. To do this:

- 1 Select a specific computer in the **Directory**.

- 2 In the **Policies** tab, click **ePolicy Orchestrator Agent | Configuration** to display the agent policy page.
- 3 On the **General** tab, deselect **Inherit**.
- 4 Select **Enable SuperAgent functionality**.

Figure 14 General tab



You can also create a SuperAgent repository on the computer, but they are not required for global updating and are not covered in this guide. See the *ePolicy Orchestrator 3.5 Product Guide* for information on SuperAgent repositories.

- 5 Click **Apply All** to save the policy changes.
- 6 Right-click the computer in the **Directory** and select **Agent Wakeup Call**.
- 7 Set **Agent Randomization** to 0 and click **OK**.
- 8 Repeat these steps if you have computers in other network subnets.

Wait a few moments while the SuperAgent is created. Once enabled, the system tray icon on the computer hosting the SuperAgent looks slightly different.

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. SuperAgents are also critical for the new global updating feature.

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, any change to your master repository triggers 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 turn 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 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 computer 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 3.5.0. But there is also much more you can do with ePolicy Orchestrator and VirusScan Enterprise. Please refer to the *ePolicy Orchestrator 3.5 Product Guide*, the *VirusScan Enterprise 8.0i Product Guide*, and the *VirusScan Enterprise 8.0i Configuration Guide for ePolicy Orchestrator 3.5* for complete information on advanced product features. These and other helpful resources are available for download from the McAfee web site.

Feature Evaluations

This section of the *Evaluation Guide* demonstrates how you can configure and use two of the new features not covered in the previous section:

- [ePolicy Orchestrator Notification](#).
- [Rogue System Detection on page 46](#).

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 agent policy to upload events immediately](#).
- 2 [Configure Notifications](#).
- 3 [Creating a rule for any VirusScan Enterprise event](#).
- 4 [Providing a sample virus detection](#).

STEP

1

Configure agent policy to upload events immediately

Because the agent delivers the events to the ePolicy Orchestrator server from the managed systems, you need to configure the agent policy to deliver events immediately. Otherwise, the ePolicy Orchestrator server doesn't receive events until the agent-to-server communication interval (ASCI).

- 1 Click **Directory** in the console tree, then the **Policy** tab in the upper details pane.
- 2 Select **ePolicy Orchestrator Agent | Configuration** in the upper details pane.
- 3 Select the **Events** tab in the lower details pane, then deselect **Inherit**.

Figure 3-1 Events tab

ePolicy Orchestrator Agent Apply All

General Events Logging Repositories Updates Proxy

Inherit

Event forwarding

Enable immediate uploading of events

Report any events with severity value equal or greater than Major

Interval between immediate uploads 5 minutes

Maximum events per immediate upload 10

- 4 Select **Enable immediate uploading of events**, then click **Apply All**.

Now that you've configured the agents to upload events to the ePolicy Orchestrator server immediately, you are ready to configure ePolicy Orchestrator Notifications.

STEP**2****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 3-2 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"/> <input type="text" value="Seconds"/>
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"/>	

- 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.

- 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 evaluation guide. For more information, see the *ePolicy Orchestrator 3.5 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

3

Creating 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 *Chapter 9: ePolicy Orchestrator Notifications* in the *ePolicy Orchestrator 3.5 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 3-3 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: **Daily unknown category notification**
 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

Symantec NAV	Select All
System Compliance Profiler	Deselect All
ThreatScan	
Unknown Product	
Virex	
VirusScan	

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	

- 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 computers 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 3-4 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:

When the number of affected computers is at least:

or

When the number of events is at least:

Throttling: At most, send notification every:

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 in Step 2: [Configure Notifications on page 42](#) (for the **Administrator** contact) will be 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 computer, 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 3.5 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

4

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 computers. 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



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 computers that frequently log on and off the network, such as test servers, laptop computers, 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 computer 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 computer 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 computer has an active agent installed and is managed by ePolicy Orchestrator. If the new computer 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 pushing an ePolicy Orchestrator agent to the computer.

In this section of the *Evaluation Guide*, 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

1

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 Click **Directory** in the console tree, then select **Rogue System Sensor | Configuration** on the **Policy** tab of the details pane.

Figure 3-5 Rogue System Sensor | Configuration

The screenshot shows the configuration interface for the Rogue System Sensor. It has two tabs: 'General' and 'Binding and Reporting'. The 'Binding and Reporting' tab is active. At the top right, there is a red button labeled 'EPOLICY ORCHI'. Below the tabs, there is a checkbox for 'Inherit' which is unchecked. Under the 'General Options' section, there is a checked checkbox for 'Enable Rogue System Sensor'. Below this, there are three input fields: 'Server name or IP address' with the value 'JBAILEY-WK6', 'Sensor-to-server communication port' with the value '8444', and a 'Caution' note: 'Caution: Changing this value causes sensor communication to fail if the server configuration is not also changed. Please see the Rogue System Detection section of the Product Guide for details on changing the server port.' Under the 'Communication Intervals' section, there are three input fields: 'Minimum reporting interval for each detected host' with the value '120' seconds, 'Minimum sensor-to-server communication interval for primary sensors' with the value '5' seconds, and 'Minimum sensor-to-server communication interval for non-primary sensors' with the value '3600' seconds.

- 2 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.
- 3 Click **Apply All**.

STEP

2

Deploy the Rogue System Detection sensor

The sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect the computers, 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 3.5 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 Click **Rogue System Detection** in the console tree, then select the **Subnets** tab in the details pane to display the **Subnet List**.
- 2 Select the subnets to which you want to deploy sensors by clicking once in the checkbox for that subnet, then clicking **Deploy Sensors**.

Figure 3-6 Subnet List page

The screenshot shows the 'Subnet List' page in the ePolicy Orchestrator interface. The page has a navigation bar with tabs for 'Machines', 'Subnets', 'Events', 'Responses', and 'Configuration'. Below the navigation bar, there is a 'List' dropdown and a 'Back' button. The main content area is titled 'Subnet List' and includes a filter dropdown set to 'All', a 'Refresh (Paused)' button, a 'Configure Table' button, and a 'Custom Filter' button. A table displays the following data:

<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	

Below the table, there are links for 'Check All' and 'Uncheck All', and a status indicator '6 items in 1 page.'. At the bottom, there is a 'Checked subnets:' section with buttons for 'Deploy Sensors...' and 'Remove Subnet'.

- 3 When the **Sensor Deployment: Set Preferences** page appears, ensure **Let me select machines manually** is selected.
 - 4 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.
 - 5 Click **Next**, then select the checkbox next to the desired system to which you want to deploy a sensor, click **Mark for Deployment**, then **Close**.
 - 6 When the **Sensor Deployment: Review and Approve** page appears, click **Deploy Now**.
The **Action Progress** page of the **Events** tab displays, indicating the progress of each sensor deployment.
 - 7 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 Right-click the computer on which you installed the sensor in the **Directory** of the console tree, then select **Agent Wakeup Call**.
 - b Set **Agent randomization** to **0**, then click **OK**.
 - c Wait two minutes, then repeat.
 - 8 Once the **Action Status** is **Completed Successfully**, the sensor has called back to the server and is functioning.
 - 9 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

3

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 *Chapter 11: Rogue System Detection* in the *ePolicy Orchestrator 3.5 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 pushes 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 3-7 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 3-8 Add or Edit Automatic Response page

The screenshot shows the 'Add or Edit Automatic Response' page in the ePolicy Orchestrator interface. The page has a navigation bar with tabs for 'Machines', 'Subnets', 'Events', 'Responses', and 'Configuration'. The 'Responses' tab is active. The page title is 'Automatic Responses' and there is a 'Help' link. The main content area is titled 'Add or Edit Automatic Response' and includes a 'Back' button. The form contains the following fields:

- Name:** Push Agent
- Event:** Rogue Machine Detected (dropdown menu)
- Enabled:**
- Conditions:**
 - + Add Condition
 - Match All (AND) (selected)
 - Match Any (OR)

Property	Comparison	Value	Delete
Rogue Type	is	No Agent	✖

- 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

4

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 computer from an outside domain to the test domain you created earlier.

- 1 Add a computer 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** directory is a holding place for systems ePolicy Orchestrator has discovered, but doesn't know where to place within the **Directory**.

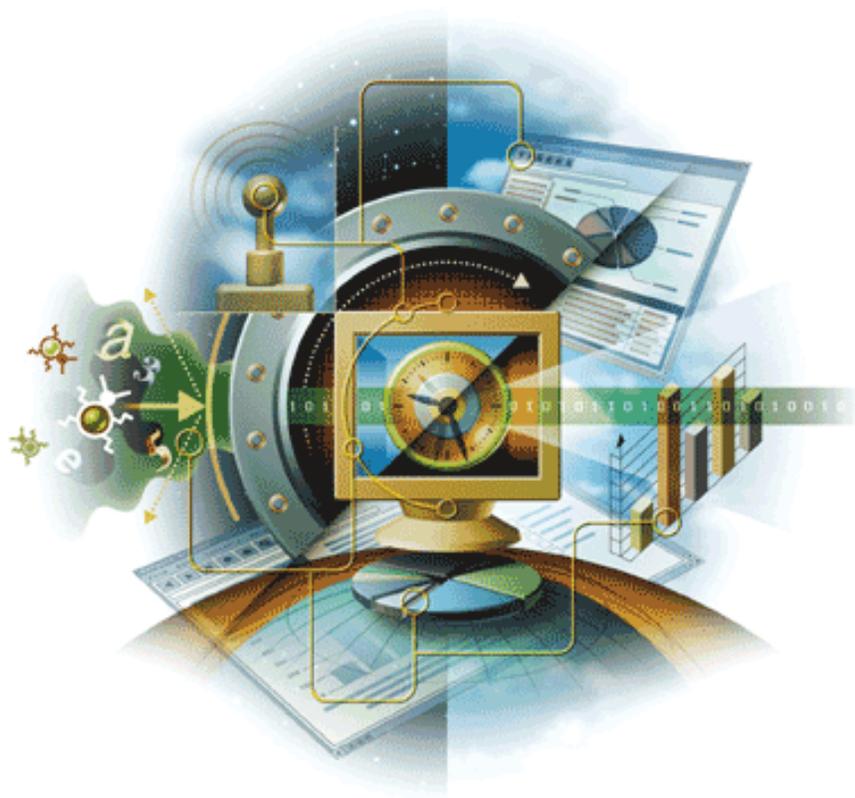
- 6 Click and drag the system to the desired site or group in your ePolicy Orchestrator **Directory**.

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**.

ePolicy Orchestrator®

Hardware sizing and network usage requirements data

version 3.5



McAfee®
System Protection

Industry-leading intrusion prevention solutions



COPYRIGHT

Copyright © 2004 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Entercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Viruscan, Virusscan (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. 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.

PATENT INFORMATION

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

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 provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. • Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. • Software written by Douglas W. Sauder. • Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. • Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. • FEAD™ Optimizer™ technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In™ Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In™ HTML Export, © 2001 Stellent Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1989. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems®, Inc. © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, © 1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, © 2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors. • Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>). • Software copyrighted by Kevin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. • Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, © 2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. • Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

1	ePolicy Orchestrator Hardware Sizing Recommendations	4
	Summary	4
	The test bed	5
	Recommendations	6
2	Bandwidth Usage	10
	Initial deployment	11
	Normal operations	18
	Outbreak situations	25

1

ePolicy Orchestrator Hardware Sizing Recommendations

What type of server do you require?

This section discusses the hardware size that McAfee recommends for the server-based components of your ePolicy Orchestrator 3.5 deployment. Use these recommendations as guidelines for buying server hardware.

- [Summary](#)
- [The test bed](#)
- [Recommendations](#)

Summary

McAfee, Inc. conducted extensive tests on three server-class systems with the goal of providing the ability for individuals to assess the hardware needed to support and manage environments of different sizes.



Although three server-class systems are profiled in this document, we are currently working to provide similar data regarding an eight-processor server.

The tests were performed to measure the number of agent communication transactions that could be processed over a period of time. Measurements were taken to determine the peak transaction rates for each server configuration.

Once these measurements were taken, the throughput the given server can sustain is known, providing data we can use to recommend a number range of systems the server can manage.

However, you must factor in your own outbreak response requirements when considering the hardware you should use to implement the ePolicy Orchestrator solution.

Outbreak response requirements

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

- **Response time** — The time period defined during which all systems must check into the ePolicy Orchestrator server. There are three factors that define the response time in ePolicy Orchestrator 3.5:
 - **ASCI** — You can configure the response time when setting the agent-to-server communication interval (ASCI). (This is configured on the **ePolicy Orchestrator Agent | Configuration** policy page.)
 - **Agent wakeup call** — The agent wakeup call is initiated manually, but you can determine the response time by setting this period of time as the **Agent randomization** interval. (This is configured on the **Agent Wakeup Call** dialog box that appears when you initiate the agent wakeup call.)
 - **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**. (This is configured on the **Settings** tab, available when you select the ePolicy Orchestrator server in the console tree.)



Although we are providing data regarding one to eight hour response times, our recommendations for each server is the three to six hour range.

- **Number of systems** — The number of managed systems required to check in within the response time.

The test bed

The tests were performed on three server-class systems:

- *Dual Processor 700 mhz*
- *Quad Processor 700 mhz*
- *Dual Processor 2.4 ghz*



Although three server-class systems are profiled in this document, we are currently working to provide similar data regarding an eight-processor server.

Dual Processor 700 MHz

The details of this server follow:

Component	Description
Processor	Dual 700 MHz
Random Access Memory (RAM)	2 GB
Hard Drive	RAID array 1
Network Access Card (NIC)	100 MB

Quad Processor 700 MHz

The details of this server follow:

Component	Description
Processor	Quad 700 MHz
Random Access Memory (RAM)	2 GB
Hard Drive	RAID array 1
Network Access Card (NIC)	100 MB

Dual Processor 2.4 GHz

The details of this server follow:

Component	Description
Processor	Dual 2.4 GHz — Hyperthread
Random Access Memory (RAM)	4 GB
Hard Drive	RAID array 5
Network Access Card (NIC)	100 MB

Database servers

In each test, a separate server was dedicated to host Microsoft SQL Server 2000. For each test, the server used was identical to the system used to host the ePolicy Orchestrator server.

Recommendations

For each server, we are providing a recommended limit for the number of client systems the server should be used to support, and a graph displaying the recommended response times (in hours) for the number of supported systems.



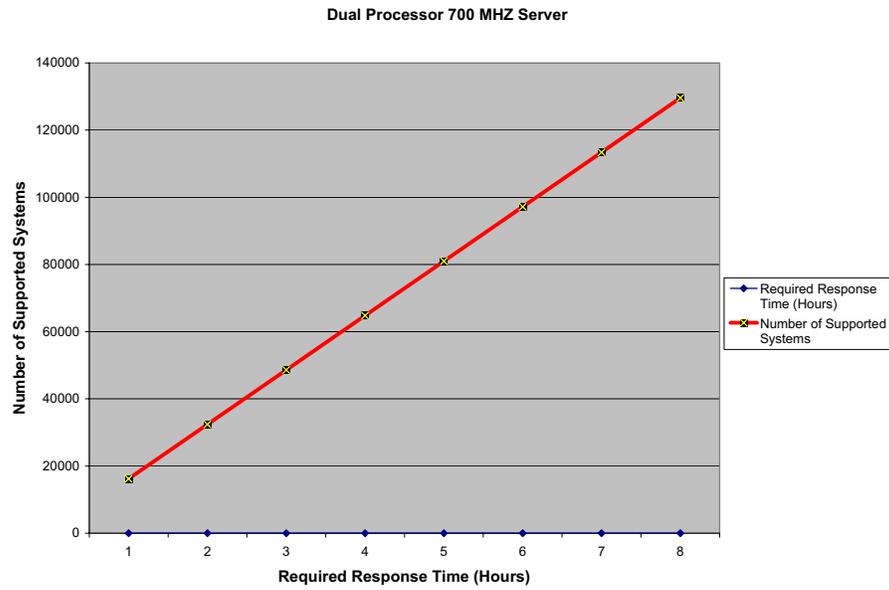
The recommendations provided are conservative, based on test results that were significantly higher, in order to accommodate for times of increased load.



Although we are providing data regarding a one to eight hour response requirements, our recommended response requirements for each server are three to six hours.

Dual Processor 700 MHz server

The following graph and table show the recommended response times for the number of supported systems.

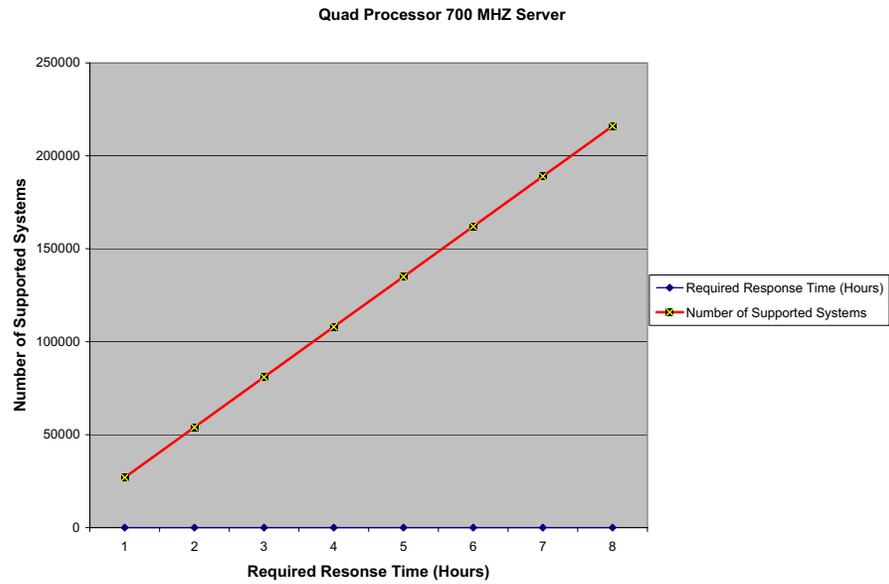


Required Response Time (Hours)	Number of Client Systems
1	16,200
2	32,400
3	48,600
4	64,800
5	81,000
6	97,200
7	113,400
8	129,600

We recommend that this system could be used to manage from 48,600 to 97,200 systems.

Quad Processor 700 MHZ

The following graph and table show the recommended response times for the number of supported systems.



Required Response Time (Hours)	Number of Client Systems
1	27,000
2	54,000
3	81,000
4	108,000
5	135,000
6	162,000
7	189,000
8	216,000

We recommend that this server could be used to manage from 81,000 to 162,000 systems.

Dual Processor 2.4 GHz

The following graph and table show the recommended response times for the number of supported systems.



Required Response Time (Hours)	Number of Client Systems
1	28,800
2	57,600
3	86,400
4	115,200
5	144,000
6	172,800
7	201,600
8	230,400



This dual-processor server performed better than the quad-processor server because the dual-processor server's processors are hyper-threaded.

We recommend that this server could be used to manage from 86,400 to 172,800 client systems.

2

Bandwidth Usage

Traffic generated by ePolicy Orchestrator 3.5

This section discusses how much network traffic is generated by ePolicy Orchestrator. It covers what you can expect during:

- *Initial deployment.*
- *Normal operations.*
- *Outbreak situations.*

This section also covers product tuning information to help you balance bandwidth resources with the needs of the product.

Use this information to help customize your deployment strategies and policy settings to maximize network efficiency in your ePolicy Orchestrator deployment.

Initial deployment

When you implement ePolicy Orchestrator in your environment, you are required to deploy agents and the security products you intend to use to manage and protect the systems on the network. You may also want to deploy other optional components such as the rogue system detection sensors into your environment as well.

This section covers bandwidth usage information for:

- [Agent deployment.](#)
- [Deploying VirusScan Enterprise and other products on page 13.](#)
- [Rogue Detection System sensor deployment on page 15.](#)
- [Initial repository replication on page 16](#)

Agent deployment

Deploying the agent from the ePolicy Orchestrator console during your initial ePolicy Orchestrator roll out generates an amount of network traffic over a short period of time that is large enough to require planning. The deployment is smaller than for deploying other products like VirusScan Enterprise or Desktop Firewall. But the agent must still be deployed to every computer in the network to be managed by ePolicy Orchestrator.

Table 2-1 Pushing the agent from the ePolicy Orchestrator console

Task / Action	Total KB	Server-to-client	Client-to-server	Description / Comments
Send agent install to client	1.64 MB	1.6 MB	44 KB	Includes the 1.6 MB agent installation package and network message overhead used to copy and run the agent installer.
Initial agent callback after install	146 KB	137 KB	8 KB	Agent calls into server for first time, sends all system properties and downloads all policies. The server populates the database with the computer properties information.

The agent deployment process is made up of two parts when considering bandwidth utilization:

- [Actual deployment on page 11.](#)
- [Initial agent-to-server communication on page 12.](#)

Actual deployment

The first, and most expensive, use of bandwidth occurs when the 1.6 MB agent deployment package is pushed to the client system and installed. You can push the agent deployment package from the ePolicy Orchestrator console to sites or groups in your **Directory** using the **Install Agent** command, a network login script, or a third-party software deployment tool. Regardless of the method you choose, you need to get the agent onto the client computer and that generates about 1.6 MB of traffic.

You must plan your agent deployment based 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 the clients you plan to manage.

Because of the variety of network environments and the types and numbers of factors that can limit available bandwidth between the organizational units of large companies, we do not have an easy mathematical equation that we can provide that would indicate how you should deploy the agent, we can say that you are probably going to want to deploy the agent in stages that won't push your network utilization over 80% at a given time or given segment of your resources. We do suggest that you deploy the agents out to individual **Directory** sites or groups, especially if you have more limiting factors on available bandwidth, such as bottlenecks between geographical locations.

Where the network is impacted

The agent deployment traffic is focused on the communication directly between the ePolicy Orchestrator server and the systems to which the agent is deployed.

Initial agent-to-server communication

After the agent installs and launches, the agent must call back into the server for the first time. When this occurs, the agent sends the server the computer properties, such as operating system, RAM memory, and IP address. It also downloads all the policy settings and client tasks that you have configured on the ePolicy Orchestrator console for that site or group (or individual computer).

The size of this initial agent callback is a combination of three factors:

- The number of .NAP files installed on the ePolicy Orchestrator server.
- The number of customizations to default policies in those .NAP files.
- The number of client tasks that you have created and configured.

With no additional .NAP files checked into the master repository, with no policy customizations, and with no client tasks configured, the initial agent ASCII generates about **146 KB** of traffic for each agent, or each managed system. Modifying .NAP files, policies, or tasks affects the total.

Where the network is impacted

Like with agent deployment, the traffic occurs between the ePolicy Orchestrator server and the systems to which the agent is deployed.

Ways to improve bandwidth utilization

To improve the bandwidth utilization caused by the initial agent-to-server communication, add and remove .NAP files to leave only the ones you need

If you check in additional .NAP files before deploying agents, the initial agent ASCII generated about **10 - 20 KB** more network traffic during the initial ASCII for each .NAP file, depending on the particular product.



Common McAfee product .NAP files not installed by default on the ePolicy Orchestrator 3.5 server are NetShield for NetWare, Desktop Firewall and GroupShield 6.0.

The agent filters which product policies it should download from the server based on the client operating system. The agent therefore downloads policies for all .NAP files of products that *could* be installed on the client operating system, even if those products aren't installed. 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. This is because usually agents are deployed first and .NAP files are downloaded before any client products are installed.

Therefore, remove any .NAP files you know you won't need from the console before deploying any agents. For example, if you are deploying VirusScan Enterprise 8.0i, to all servers and workstations on your network, you may not need VirusScan Enterprise 7.0 or 7.1, NetShield 4.5, or Norton Anti-Virus (all of which are older or alternate versions of 8.0i and are installed on the console by default). Removing unnecessary .NAP files saves about **10-20 KB** per .NAP file for each agent.

Configuring tasks and customizing policies adds to network traffic

You may want or need to customize agent or product policies in your deployment. For example, you might want to change the agent ASCII or show the agent icon in the system tray of the client computer. Or, you may want to create a custom list of exclusions for your VirusScan Enterprise On-Access scanner to improve system performance. Individual policy changes like this vary in how much network traffic they generate, but usually adds **1-2 KB** to the next ASCII for each policy change.

You should create and schedule some client tasks for each of your client systems, because none are created by default. For example, you should create at least one agent update task to update .DAT files and engines. Also, you should create regularly scheduled on-demand scans for VirusScan Enterprise that occur daily or at least weekly. You should create additional update tasks or scan tasks for other products that don't use the common management agent, such as NetShield for NetWare, or older versions of GroupShield. Ultimately, you will likely have 5-10 or more client tasks created, scheduled, and enabled. Each of these tasks that you create, or if you change a task configuration again in the future, adds **1-2 KB** to the next agent ASCII for each new or changed task.

Ways to improve impact to the network

Change the ASCII to a higher number, such as 4 or 6 hours. In very large networks, this can make a big difference in the total amount of network traffic generated in an hour.

Deploying VirusScan Enterprise and other products

During your initial ePolicy Orchestrator deployment, deploying VirusScan Enterprise 8.0i to client computers in your network is likely the single biggest impact in network traffic usage. Like the agent, anti-virus software must be installed on every workstation and server in your network you plan to manage.

However, unlike the agent deployment, you can use update repositories to deploy products. Using update repositories lessens the impact on your network utilization. From the server, you can deploy the package to update repositories strategically placed in your network. These update repositories contain identical contents to the master repository on the ePolicy Orchestrator server. Then client systems can pull the products and updates directly from a system much closer to them on the network, saving bandwidth resources.

We recommend creating and configuring update repositories before deploying anti-virus software to the client systems.

Table 2-2 Deploying VirusScan Enterprise to clients using ePolicy Orchestrator

Task / Action	Total bytes	Server-to-client	Client-to-server	Description / Comments
Push VirusScan Enterprise to client	9.8 MB	9.6 MB	221 KB	Use the deployment task to have the agent download and run the VirusScan Enterprise installation package. Create a custom deployment package with the latest .DAT files to avoid having to add a 4 MB .DAT file update.
Re-deploy VSE (such as at enforcement interval).	15	7	7	During the initial deployment, the installer is copied to the client "Documents and Settings" folder and launched from there. If VirusScan Enterprise is deleted for any reason, the agent can re-install it without having to download the 8 MB installer again. This 15 KB amount does not include the automatic .DAT file update that occurs after VirusScan Enterprise installs. This is either between 50-200 KB for each incremental *.UPD update, or 4 MB for a full a .DAT file update.

Where the network is impacted

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

- The master repository (on the ePolicy Orchestrator server) and each update repository.
- Each client system and its update repository.

Deploy a custom VirusScan Enterprise package that has the latest .DAT files

McAfee ships VirusScan Enterprise with the latest .DAT file available at release time. As new .DAT files are released once or more per week, the .DAT file shipped with VirusScan Enterprise will be out-of-date very quickly. Also, VirusScan Enterprise does an immediate and automatic .DAT file update after installing on the client. So, if you deploy VirusScan Enterprise using the .DAT file included in the default deployment package, plan on adding up to 4 MB of network overhead because each client needs to perform a full .DAT file update after installing. This increases the total network traffic generated by your VirusScan Enterprise deployment by 50%!

Instead, use McAfee Installation Designer (MID) to create a custom VirusScan Enterprise deployment package that includes the latest .DAT files and engine, and check this custom package into the master repository. Also, check the latest .DAT files and engine into the master repository, and replicate to your distributed repositories. After installing on the client, VirusScan Enterprise does an immediate update to the nearest repository. When VirusScan Enterprise installs, it installs using the latest .DAT files. Not only is the client fully protected against the latest threats immediately, but you won't clog up your network with an additional 4 MB .DAT file update for each client.

Ways to minimize impact

To improve the bandwidth utilization caused by deploying products to client systems, you can:

- Deploy the product to sections of your ePolicy Orchestrator **Directory**, rather than to every client on your network at once. Run the deployment task only one site or group at a time. You can either do this by running the deployment manually for each site or group, or schedule deployment separately at different times in the future.
- Use randomization intervals to spread the deployment to a particular site or group over a certain period, such as an hour.
- Schedule all deployment tasks to run at local time (which is already the default). This is helpful if you have office locations in different time zones, and can further help diffuse network usage over time.
- Use McAfee Installation Designer (MID) to create a custom VirusScan Enterprise deployment package that includes the latest .DAT files and engine. This can save up to 4MB because VirusScan Enterprise does not need to update .DAT files after being installed on the client.
- Use distributed repositories to localize network traffic as much as possible. Before running the deployment task, perform a **Replicate Now** server task to update all distributed repositories with the new deployment package. The deployment task generates traffic between the agent and the nearest repository only—the agent does not need to communicate with the ePolicy Orchestrator server. Updating from the closest distributed repository localizes network traffic between client and repository in the local parts of your network, often faster LAN links.

Deploying other point products

Deploying other point products to client machines generates network traffic proportional to the size of the deployment installation package, plus 30-40 KB of network overhead generated by the deployment task when it runs. All traffic is between the agent computer and the closest repository. The agent does not communicate with the ePolicy Orchestrator server when the deployment task runs.

You can make educated guesses about how much network traffic other product deployments generate by checking the size of the folder containing the product installation files. These would be located on your ePolicy Orchestrator server in the temporary folders that you extracted installation files after you downloaded them from McAfee. Be sure to consider all the contents of the installation folder including the setup file, the detection script, and readme, not just the PkgCatalog.z package file you check into the repository.

Rogue Detection System sensor deployment

Although you are only deploying a few sensors to each subnet, the initial sensor deployment generates about 3.8 MB of traffic between the server and each target system.

The sensor does not communicate with the ePolicy Orchestrator server directly, and does not receive any communications from it. All that the sensor does is “listen” passively for layer 2 broadcast traffic, capture and filter data on the computers that it detects on the local broadcast segment (subnet), and forward that detection data to the rogue system server that is running on the ePolicy Orchestrator console. Any policy information about the sensor is handled by the ePolicy Orchestrator agent, which is also installed on the client computer and communicates regularly with the server.

The sensor generates no network traffic as it detects other computers on the subnet. It is a passive listener only, and does not actively probe the network to find computers. The only time the sensor generates network traffic is when it periodically forwards recent detections to the server.

Table 2-3 Rogue system sensor network traffic

Task / Action	Total Bytes	Client to server	Server to client	Description / Comments
Deploy sensor to client	3.8 MB	96 KB	3.7 MB	Using the Subnet List interface to push a sensor to a client computer.

Deploying the rogue system sensor

Deploying the rogue system sensor to clients from the ePolicy Orchestrator console generates about 3.8 MB of network traffic. The sensor by default is deployed in a “disabled” state, and does not become enabled and begin communicating with the server until the first agent ASCII after the sensor starts, when the agent can retrieve the sensor policies from the server. So, depending on your ASCII settings and when you deploy the sensor during the ASCII period, the sensor may not startup for some time (up to an hour, if you use the default ASCII).



The first agent ASCII after you have deployed a sensor generates a few KB more traffic than other regular ASCIIs as the new sensor properties and policies are exchanged.

Where the network is impacted

The sensor deployment generates about 3.8 MB of traffic between the ePolicy Orchestrator server and each system to which you deploy the sensor (several per subnet).

Initial repository replication

The following measurements were taken replicating to a SuperAgent repository. The traffic generated should be more or less similar if you use other distributed repository types, such as UNC shares, HTTP or FTP servers.

Table 2-4 Replicating master repository to distributed repository

Task / Action	Total bytes	Server-to-client	Client-to-server	Description / Comments
Repository replication (initial / full)	27 MB	27 MB	160 KB	This includes all the default packages, plus VirusScan Enterprise 8.0i, a full .DAT file, and engine. If your repository contains more/less software, this amount varies.

Much bigger initial transfers but much fewer of them

Repository replication involves transferring more and larger packages compared with sending deployments and updates directly to individual servers or workstations. But, you'll have much fewer repositories to which to replicate, and using distributed repositories helps localize deployments to other clients.

Normal operations

Although not as large as the initial deployment of the agent, sensor, and products, there is significant bandwidth consumption 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 in order for your systems to be managed and secure.

The following topics are covered in this section:

- [Updating .dat files and engines.](#)
- [Policy Enforcement Interval on page 20.](#)
- [Agent-to-server communication interval \(ASCI\) on page 22.](#)
- [Rogue System Sensor on page 22.](#)
- [Update repository replication on page 24.](#)

Updating .DAT files and engines

Keeping .DAT files and engines up to date is probably the most critical thing you need to do to keep your anti-virus protection current. Updating engines and, especially, .DAT signatures, is a constant trade-off between protection and network performance. Update too infrequently, and your network becomes vulnerable to new viruses not detected by outdated .DAT files. Update too frequently, and you can generate considerable unnecessary network traffic for little or no added benefit.

.DAT file updates are released much more often than engines. McAfee does a full .DAT file release at least once a week, on Wednesday. If there are particularly virulent new viruses discovered in a week, McAfee may release full .DAT files several times a week. Current trends show that more and more viruses are appearing than ever before, and the rate is likely to continue increasing. Count on McAfee having to release updated .DAT files more and more frequently. Basically, expect that McAfee may have to release a new .DAT file on any given day of the week, at any hour.

Table 2-5 Use agent update tasks to update .DAT files and engines

Task / Action	Total Bytes	Server-to-client	Client-to-server	Description / Comments
Full .DAT file update	4.3 MB	4.2 MB	100 KB	Update full .DAT files (client .DAT files older than 15 versions). This involves downloading the 3.9MB .DAT file package, plus network overhead.
Incremental .DAT file increase (one version out-of-date... 43804381.updated is 45 KB)	~175 KB per update	167 KB	8 KB	Incremental updates vary in size between about 50 KB and 200 KB.

Table 2-5 Use agent update tasks to update .DAT files and engines

Task / Action	Total Bytes	Server-to -client	Client-to -server	Description / Comments
Update engine	2.1 MB	1.9 MB	100 KB	Engine package is 1.8 MB, plus ntwrk overhead.
Update task, .DAT files and engine only (no changes)	1.4 KB	673 bytes	732 bytes	Client already has most up-to-date .DAT files/engine, no updates to download.

About incremental vs full .DAT file updates

A full .DAT file update package is about 4 MB. If you had to update this full .DAT file at every .DAT file release, that would generate an incredible amount of network traffic, especially in very large networks. Luckily, each full .DAT file release includes separate incremental updates for updating to the new version from any of the previous 15 .DAT file releases.

Each of these incremental updates is a separate .UPD file that is saved in the repository along with the full SCAN.DAT file. These .UPD files vary in size from **50KB** to **200KB**, depending on how many new signatures are added for that release.

When running an update task, the agent compares the client .DAT file version 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. For example, if the client has the 4375.DAT files installed currently, and the latest .DAT files are version 4377, the client only updates the two incremental updates to make up the difference: 43754376.upd and 43764377.upd. If the currently installed .DAT files are older than 15 versions out-of-date, then the agent downloads the full 4 MB .DAT file. The agent makes this determination automatically—you don't need to configure it in the ePolicy Orchestrator console.

If you can, use global updating to automate on-demand updating

The best way to make sure updates occur automatically and only when you need them is to enable global updating and use the default selective updating settings to only allow .DAT file or engine packages to trigger it. This means that repository replication and client updates run only when necessary, i.e., rather than running at scheduled times whether there are new updates or not. Know that you must deploy a SuperAgent to every network broadcast segment for global updating to work.

Also, schedule very frequent repository **Pull** tasks—once an hour is not excessive—to ensure that new .DAT files or engines posted to the McAfee web site are added to the master repository as quickly as possible. Global updating occurs automatically, but only when updates are checked into the master repository on the ePolicy Orchestrator server. Most of the time, these pull tasks find nothing to download, generating minimal network traffic between the ePolicy Orchestrator server and the Internet and not triggering a global update.

Also, even if you use on global updating, you should still schedule a client update task as a backup. If a computer is offline when the global update occurs, that computer won't get the update until the next global update. If it's offline again, it will miss that global update, etc. Or, if the one SuperAgent computer in a network broadcast segment (subnet) is offline, all the other agents in that part of the network will miss the global update. As a backup, schedule a regular client update task for all agents too. You can schedule the task to run regularly, such as once a day, or at every time the computer logs into the network.

Schedule frequent client update tasks

When a scheduled client update task runs and there is nothing to update (the client already has the most recent .DAT file), the update task generates about 1.5 KB of traffic as it checks with the closest repository and determines the latest .DAT files or engines are already installed. Depending on your network, this traffic generated by extra scheduled updates may add a tolerable level of network “noise” if it means these frequently scheduled tasks make it more likely to retrieve updates quickly.

Ways to minimize the impact of policy enforcement traffic

- Use distributed repositories. During update tasks, the agent only communicates with a repository, not the ePolicy Orchestrator server. Updating from the closest distributed repository localizes network traffic between client and repository to the local parts of your network, often fast LAN links. This is much more efficient than updating over wider, slower links such as WAN or VPN.
- Use global updating and configure it to run only when new .DAT files or engines are checked into the master repository (as it is by default). This minimizes network traffic usage by only running repository replication and client updates when there is an actual new .DAT file or engine update available. If you do use global updating, and especially if your network is large, enable randomization to spread the network load out over time.
- If you use replication and client update tasks, as opposed to (or in addition to) global updating, experiment with how often you schedule your updates. Remember that each time you run an unnecessary update (i.e., when your .DAT files and engines are already up-to-date), the task generates a minimal 1.5 KB of network traffic between agent and server.
- Use selective updating to create a separate client update task for .DAT files and engines, and schedule it to run often. For example, create one task for .DAT files and schedule it to run often. Schedule separate tasks to update Desktop Firewall signatures, and other tasks to update.
- Ensure your .DAT files are up-to-date! Keeping .DAT files current ensures that, each time a .DAT file update is required, the client is always doing the minimal possible update. The more out-of-date your .DAT files are, the larger each update is.

Where the network is impacted

Updating generates traffic between:

- The master repository (on the ePolicy Orchestrator server) and each update repository.
- Each client system and its update repository.

Policy Enforcement Interval

The enforcement interval is how often the agent checks the client computer on which it is installed to make sure that the current policies configured on the ePolicy Orchestrator console are in effect. The agent uses the most recent policies that it downloaded from the ePolicy Orchestrator server at the last ASCI. By default, the agent enforces policies on the client every 5 minutes.

Most policy enforcement occurs locally on the client computer, and does not require contacting the ePolicy Orchestrator server. The exception is that if you have configured the default **Deployment** task to install client products, such as VirusScan Enterprise, Desktop Firewall, or System Compliance Profiler, at every enforcement interval. When the **Deployment** task is configured this way, the agent calls into the nearest distributed repository at each enforcement interval to confirm that the software versions installed on the client are match those in the repository.

Table 2-6 Policy enforcement interval

Task / Action	Total Bytes	Server-to-client	Client-to-server	Description / Comments
Policy enforcement, with deployment task enabled	1.4 KB	673 bytes	732 bytes	When deployment task is set to install for any deployment pkg, agent pings server at each enforcement interval to confirm currently installed versions are same as master repo, etc.
Policy enforcement, no deployment task install	0	0	0	When no deployments are set to install, the agent doesn't communicate with the server.

Note that the agent does not call into the ePolicy Orchestrator server during the enforcement interval. It calls into the nearest distributed repository only.

Re-installing products that have been removed

If a particular product is not installed but is supposed to be, for example if the end-user manually uninstalls VirusScan Enterprise, the agent reinstalls it on the client at the next policy enforcement interval. Note that when the agent re-installs the product, it does not need to download the installation files again from the repository. It only contacts the repository to download the SITESTAT.XML file to confirm the product versions. If the agent needs to re-install, it launches installation files that are already saved on the client computer during the initial product deployment. These files

Ways to minimize the impact of policy enforcement

- Make sure you are using distributed repositories wherever possible so that network traffic used during enforcement intervals and when running deployment tasks is localized in the faster parts of your network. Updating to a distributed repository in the local LAN is always much better than updating from the master repository on the ePolicy Orchestrator server.
- Change the enforcement interval to something larger than the default of five minutes, such as one hour.
- De-select the **Run this task at every policy enforcement** interval option on the Deployment task **Task Settings** page. If you do this, make sure you schedule the Deployment task to run at regular times, such as once a day. That way the task still makes sure the right products are installed at a regular interval.
- McAfee does *not* recommend setting the Deployment task actions for critical point products, especially VirusScan Enterprise, to **Ignore**. Ensuring that the right version of VirusScan Enterprise is installed and running on each client is one of the most important things that ePolicy Orchestrator does!

Agent-to-server communication interval (ASCI)

The agent ASCI is 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 for allowing communication between agent and server.

Table 2-7 Policy enforcement interval

Task / Action	Total Bytes	Server to client	Client to server	Description / Comments
ASCI	10 KB	4 KB	6 KB	The size of the ASCI depends on how many policies have changed since the previous ASCI, and how many products are installed on the client. This example is for a typical client computer with the agent, VirusScan Enterprise, and System Compliance Profiler installed. If you have more products deployed to a particular computer, the ASCI is likely to be larger.
Agent wakeup call with send full props	25 KB	22 KB	3 KB	The only way to force the agent to re-send all properties to the server is to send an agent wakeup call from the console and select the Get full product properties option. This example assumes also the three client products (agent, VSE, SCP) are installed on the client and use default policies. If more products are installed, the wakeup call is bigger.

Where the network is impacted

The ASCI traffic occurs between the ePolicy Orchestrator server and the systems to which the agent is deployed.

Ways to minimize the impact

It is important to configure the ASCI to occur frequently enough to ensure your agents get updates quickly enough, but not too frequently that your resources are impacted.

By default, the ASCI is set to 1 hour. In some very large networks where ePolicy Orchestrator manages tens of thousands of nodes, you may find you need to change the ASCI to something higher, like 4 or 6 hours or more, to keep network usage down.

Rogue System Sensor

The rogue system sensor generates traffic as it regularly generates and forwards detection messages to the Rogue System Detection server on the ePolicy Orchestrator server.

Table 2-8 Rogue system sensor network traffic

Task / Action	Total Bytes	Client to server	Server to client	Description / Comments
Sensor reports detected rogues	980 byte message overhead, plus 610 bytes per detected machine.	-	-	If the sensor uses default PSCI of 5 min, nearly all machines on subnet are reported as detected within first two reporting intervals after the sensor installs and starts up. The sensor re-sends detection events to the server at the configured reporting interval, as specified in the Minimum reporting interval for detected hosts setting (default is 1 hour).
Non-primary sensor communication interval (NPSCI)	~ 800 bytes	-	-	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 (PSCI)

You can configure how often the sensor sends detection events to the ePolicy Orchestrator server. This configurable interval is the The sensor communication interval for primary, or active, sensors is the primary sensor-to-server communication interval (PSCI, or “pesky”). The default is 5 minutes (300 seconds), but you can set it as low as 0 or higher, such as an hour.

When the PSCI is 0, each event is forwarded immediately by itself. Note that, especially in large deployments, this can cause problems with having enough SSL connections on the ePolicy Orchestrator server. This is because each individual detection message requires an SSL socket connection, whether that message contains 1 event or 100.

If you use the default PSCI of 5 minutes, the sensor sends its first batch of machine detections on the local network subnet 5 minutes after that initial agent PSCI. The sensor sends additional detections at each 5-minute PSCI, until all machines in the subnet have been detected. In most networks with a normal amount of network activity, the sensor should detect all machines in the subnet within 10-15 minutes (within the first 2-3 PSCI, if you use the default).

Minimum reporting interval determines how often detections are resent for the same machine

Detection events are sent once for each machine, and then re-sent at the interval specified in the **Minimum reporting interval for detected host** setting. By default, this interval is 1 hour.

Multiple primary sensors multiplies the traffic generated

Note that the PSCI network traffic occurs for each primary sensor you have deployed, including if you have multiple primary sensors deployed in each subnet. McAfee actually recommends deploying at least two primary sensors to each subnet so you have some redundancy in rogue detections. If one primary sensor goes down for whatever reason, the other primary sensor is still sending detection messages back to

the server. Just be aware that all primary sensors in are forwarding detection event information to the server at all times (they don't switch off automatically). For example, if you have two primary sensors installed on a subnet, both will send detection messages to the server, which filters the data so you don't see duplicate information in the ePolicy Orchestrator console.

Non-primary sensor communication interval (NPSCI)

If you have deployed additional backup sensors to your subnets, these are non-primary sensors, and do not forward detection events to the server while they are in the non-primary, backup state. These backup sensors communicate periodically at a configurable interval (the default NPSCI is one hour) with the ePolicy Orchestrator server to see if they should continue "sleeping" in backup mode, or become primary sensors and begin forwarding detections to the server.

For most NPSCIs, the backup sensors are told to go back to sleep and continue in backup mode. Each of these NPSCIs generates about 800 bytes of traffic between sensor and server.

Where the network is impacted

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

Update repository replication

The following measurements were taken replicating to a SuperAgent repository. The traffic generated should be more or less similar if you use other distributed repository types, such as UNC shares, HTTP or FTP servers.

Table 2-9 Replicating master repository to distributed repository

Task / Action	Total bytes	Server-to-client	Client-to-server	Description / Comments
Repository replication (incremental) with one .DAT file	4.4 MB	4.2 MB	148 KB	1 new full .DAT file, no other changes. Updating repositories with .DAT files is the most frequent type of replication.
Repository replication (incremental) runs, no changes at all	80 KB	32 KB	48 KB	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 80KB in traffic is generated between the ePO server and each distributed repository.

Outbreak situations

During an outbreak, the most traffic is going to be generated by the outbreak itself. The traffic generated by your security products may also be greater. During such a situation, there may be a large number of event files travelling from the affected systems to the ePolicy Orchestrator server. During this time you must update your .DAT files as soon as possible to all client systems, while at the same time not overloading an already stressed network.

Event files

Event files allow the server to know what is happening on the managed systems. During an outbreak, this flow of event files is going to be greater from any affected system. There are many different types of event files of different products that are received by the ePolicy Orchestrator server. However, the sizes of these do not differ greatly. Some typical ones during an outbreak are represented in the table below.

Table 2-10 Replicating master repository to distributed repository

Task / Action	Total bytes	Server-to-client	Client-to-server	Description / Comments
Virus detected events	2 KB		2KB	
Buffer overflow	2 KB		2KB	

Although event files are quite small, during an outbreak they can have a significant impact on your network resources as well as to the ePolicy Orchestrator server.

Ways to improve network impact

Freeing up bandwidth during an outbreak allows ePolicy Orchestrator to distribute the updates more quickly that are critical to containing and remediating the outbreak. There are several configurations you can make to reduce the number of events that the agent forwards to the server, and ways to lesson the impact of a large number of events hitting the ePolicy Orchestrator server.

Ensure the agent only forwards critical events immediately

If you have the agent policy configured to upload events immediately to the server, then ensure that only events with a severity value equal or greater than Critical is selected.

- 1 Select **Directory** in the console tree.
- 2 Select the **Policies** tab in the upper details pane, then select **ePolicy Orchestrator Agent | Configuration**.
- 3 Select the **Events** tab, deselect **Inherit**, then select **Critical** from the **Report any events with severity value equal or greater than** drop-down list.
- 4 Click **Apply**.

Enable event filtering to identify the events that are forwarded immediately

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



If you have selected in the agent policy for the agent to send only **Critical** events immediately to the ePolicy Orchestrator, then you only need to worry about narrowing the set of critical events with the event filtering feature.

- 1 Log on to the ePolicy Orchestrator database from the console tree.
- 2 Select **Events** in the console tree under the name of the database.
- 3 Select the **Filtering** tab in the details pane.
- 4 Select **Send only the selected events to ePO**.
- 5 Ensure only the essential critical level events are selected, then click **Apply**.

Disable any unnecessary notification rules

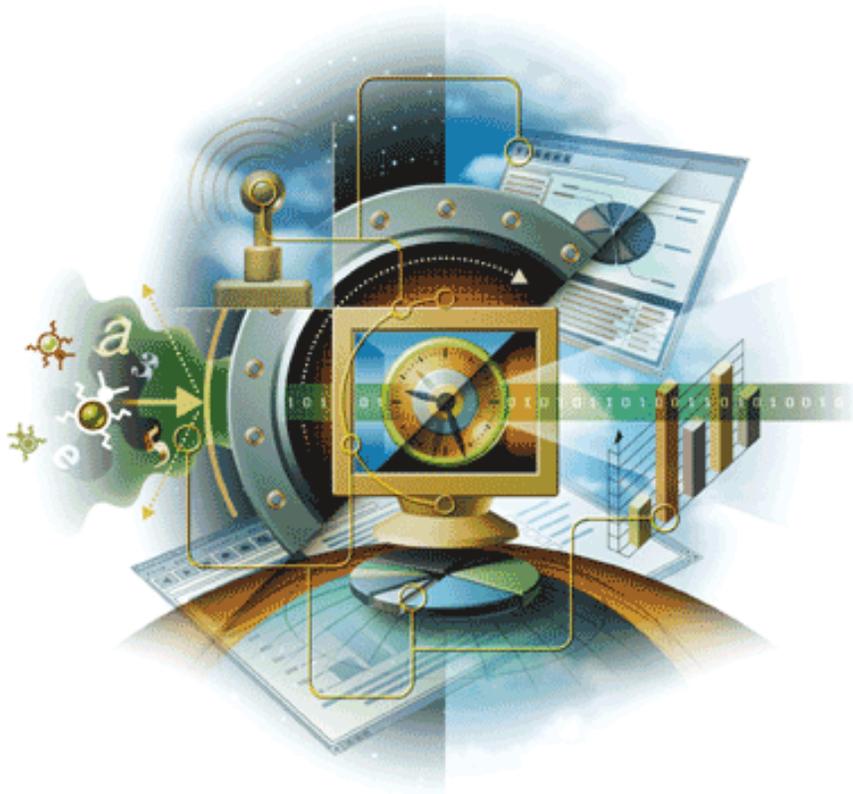
The ePolicy Orchestrator server processes events more slowly with each enabled notification rule. This can slow down the server if there are a large number of events coming into it. Therefore, during an outbreak, you should disable any unnecessary notification rules.

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 resource usage of updating, we recommend utilizing global updating and SuperAgents. Please see the *ePolicy Orchestrator 3.5 Product Guide* for more information.

ePolicy Orchestrator®

version 3.5



McAfee®
System Protection

Industry-leading intrusion prevention solutions



COPYRIGHT

Copyright © 2004 Networks Associates Technology, 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, ActiveSecurity (and in Katakana), ActiveShield, AntiVirus Anyware and design, Clean-Up, Design (Stylized E), Design (Stylized N), Entercept, Enterprise SecureCast, Enterprise SecureCast (and in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (and in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M and Design, McAfee, McAfee (and in Katakana), McAfee and Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (and in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Viruscan, Virusscan (And In Katakana), Webscan, Webshield, Webshield (And In Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. 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.

PATENT INFORMATION

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

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 provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- FEAD™ Optimizer™ technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1989.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems®, Inc. © 2003.
- Software copyrighted by Gisle Aas. © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, © 1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martijn Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, © 2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, © 2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Contents

1	Introduction	5
	Components of ePolicy Orchestrator	5
	Policy, properties, and events	8
	Policies	8
	Properties	8
	Events	8
	Tasks, services, and accounts	9
	Other times when credentials are needed	10
	Minimum requirements	10
2	Installing and Upgrading the Server	11
	Installing for the first time	11
	Pre-installation preparation	12
	Information to have during installation	12
	Upgrading from a previous version of ePolicy Orchestrator	14
	Preparation	16
	Information to have during the upgrade	16
	Upgrading issues	18
3	Organizing the Directory and Repositories	19
	ePolicy Orchestrator Directory: concepts and roles	19
	Roles	20
	Organizing the Directory	21
	Borders	22
	IP address filters and sorting	23
	Repositories	25
	Update repositories	26
	Distributed repositories	27
	SuperAgent repositories	27
	Update methods	28
	Global updating	28
	ePolicy Orchestrator agent update task	28
	Pull and replication tasks	29
4	Deploying the agent and products	30
	ePolicy Orchestrator agent	30
	About distributing the ePolicy Orchestrator agent	31
	Deploying the agent while creating the Directory	33
	Deploying the agent after creating the Directory	33
	Using login scripts to install the agent	33
	Manually installing the agent	34
	Including the agent on a standardized installation image	34
	Enabling the agent on unmanaged McAfee products	34
	Using third-party deployment tools to distribute the agent	35
	Advantages and disadvantages of agent distribution methods	35
	SuperAgents for communication with server	36
	About SuperAgent broadcast wakeup calls	36
	Deploying products with ePolicy Orchestrator	38
	Check in product deployment packages to the master repository	38

	Use the deployment task to install products on clients	40
5	Rogue System Detection	43
	About the rogue system sensor	44
	The Rogue System Detection server	45
	About status and rogue type	46
	Deploying Rogue System Detection sensors	47
	Deploying sensors automatically from the console	48
	Manually installing the sensor	49
	Remediating rogues systems	49
	Types actions	49
	Configure automatic responses for specific events	50
	Example of automatic response configuration	50
	Flag systems that don't need agents as Exceptions.	51
	Import and export exceptions from and to an XML file	52
6	ePolicy Orchestrator Notifications	53
	How it works	53
	Throttling and aggregation	54
	Notification rules and the Directory scenarios	55
	Planning	56
	Rules	57
	Configuring ePolicy Orchestrator Notifications.	57
	Default rules	57
	Creating rules	59
	Event forwarding	59
	Product and component list	61
	Viewing the history of Notifications	62
	Notification details	62
	Using custom filters	62
7	Outbreaks	64
	Things to do daily or weekly to stay prepared.	64
	Server and client tasks you should schedule to run regularly	64
	Are you prepared for an outbreak?	66
	Other methods to recognize an outbreak	66
	Network utilization key indicators	67
	E-mail utilization key indicators	67
	Virus detection events	67
	You think an outbreak is occurring.	68

1

Introduction

Getting to know ePolicy Orchestrator 3.5

ePolicy Orchestrator 3.5 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.

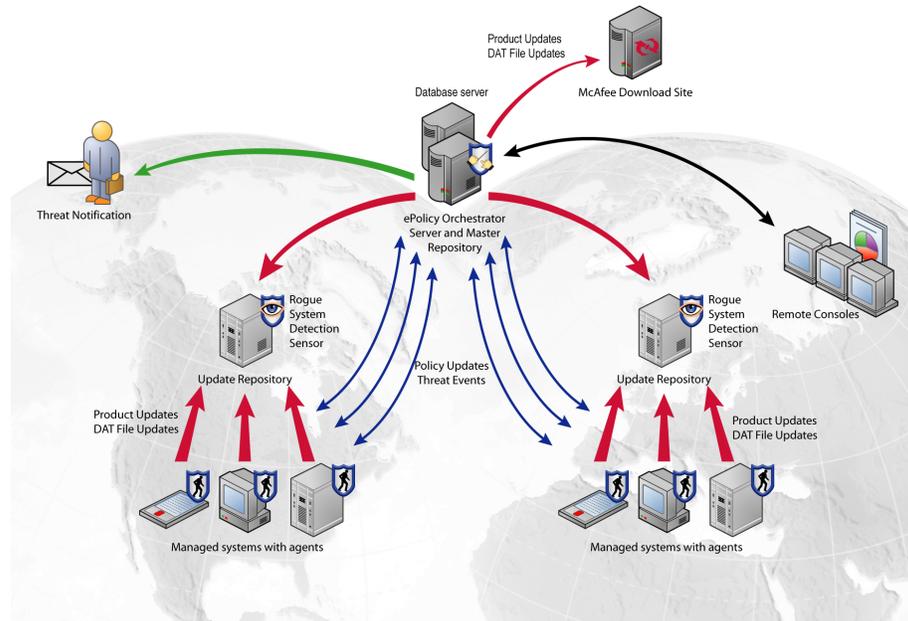
- *Components of ePolicy Orchestrator.*
- *Policy, properties, and events*
- *Tasks, services, and accounts*

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 computers), although it can be accessed from a local console as well.

For information on server sizing, see the *ePolicy Orchestrator 3.5 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 computer 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, the On-Demand Scanner. You can also 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 computer, the settings are returned to those set in the policy within five minutes.

Properties

Properties are collected from each system by the installed agent. These include:

- System information (computer 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 new 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 into the server	ePolicy Orchestrator server (NAIMSRV.EXE)	ePolicy Orchestrator server account.
Deploying agents	ePolicy Orchestrator server (NAIMSRV.EXE)	Server service account (specified during the installation wizard).
Upgrading agents	ePolicy Orchestrator server (NAIMSRV.EXE)	Local system account on client system.
Replicating UNC share distributed repositories	NAREPL32.EXE	Server service account.
Replicating FTP distributed repositories	NAREPL32.EXE	Specified account.
Replicating HTTP distributed repositories	NAREPL32.EXE	Specified 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 3.5.0 Discovery and Notification Services (TOMCAT.EXE)	Server service account.
Reporting (with an Authentication Type of ePO Authentication)	ePolicy Orchestrator server (NAIMSRV.EXE)	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)	ePolicy Orchestrator server (NAIMSRV.EXE)	SQL account.
Reporting (with an Authentication Type of NT Authentication)	ePolicy Orchestrator server (NAIMSRV.EXE)	NT account.
Reporting (with an Authentication Type of Currently logged on user)	ePolicy Orchestrator server (NAIMSRV.EXE)	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 3.5.0 Event Parser (EVENTPARSER.EXE)	Server service account.



If 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 other user credentials.

Table 1-1

Task	Credentials	Location stored
Logging on to Active Directory containers (set in Active Directory Import wizard)	Active Directory administrator credentials (for each container that is mapped to the ePolicy Orchestrator Directory). These credentials are stored to run as a task.	If the Active Directory Computer 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.
Pushing agents from the ePolicy Orchestrator console by manually specifying the user name and password.	Credentials with administrator rights to the desired computers.	Stored in the encrypted CONSOLE.INI file.

Minimum requirements

The following are minimum hardware and software requirements for the ePolicy Orchestrator 3.5 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 3.5 Hardware Sizing and Bandwidth Usage White Paper*.

Table 1-2 Hardware and Software Minimum Requirements

Hardware	Software and Network
250MB free disk space (first-time installation); 650MB (upgrade); 2GB recommended.	Windows 2000 Advanced Server with SP 2 or later, Windows 2000 Server with SP 2 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; 500MHZ or higher	Trust relationship with the primary domain controller (PDC).
1024x768, 256-color, VGA monitor	User must have administrator rights on the server.
100mb or higher NIC	
NTFS partition	
Static IP address recommended	

2

Installing and Upgrading the Server

Whether you are installing ePolicy Orchestrator 3.5 as a new installation or upgrading to it from prior versions you must understand the minimum system requirements, preparation tasks on your network, and what 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.



Specific complete instructions on installing ePolicy Orchestrator are located in the *ePolicy Orchestrator 3.5 Installation Guide* and the *ePolicy Orchestrator 3.5 Evaluation Guide*.

This section covers:

- [Pre-installation preparation.](#)
- [Information to have during installation.](#)

Pre-installation preparation

Before installing ePolicy Orchestrator 3.5 complete the following tasks:

- Determine what database you are going to use. ePolicy Orchestrator includes the Microsoft SQL Database Engine (MSDE) 2000 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 3.5 can record approximately 12 months of data for 10,000 client systems.

If the standard database does not meet your needs, then you can utilize a Microsoft SQL Server 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 computer and the ePolicy Orchestrator database server computer 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 and database server computers and scan for viruses.
- Install and/or update firewall software on the ePolicy Orchestrator server computer. (For example, Desktop Firewall 8.0.)
- 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.*
- *Server service account.*
- *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.

Server service account

During the installation wizard, you are asked to provide the domain and user credentials of the system that hosts the **McAfee ePolicy Orchestrator Server service**. This is the service account that pushes the agent to client systems.

Select the **Use Local System Account** checkbox if you don't plan to use the ePolicy Orchestrator server to push the agent. For example, if you plan to use products like Microsoft SMS or Novell Zenworks, or if you plan to use login scripts.

Database server

During the installation wizard, you are asked to select to install the MSDE 2000 database, or use an already installed database server on the local system (MSDE, MSDE 2000, or SQL Server).

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 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 HTTP 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 HTTP 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**.

- **Agent Wake-Up HTTP 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 HTTP port** — This is the port used to send SuperAgent wakeup calls. The default port is **8082**. This port can be changed after installation.

- **Discovery & Notification service HTTP 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.
- **Discovery & Notification service HTTPS 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.
- **Rogue System Sensor HTTPS 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 3.5, see the *ePolicy Orchestrator 3.5 Installation Guide*.

Upgrading from a previous version of ePolicy Orchestrator

You can upgrade or migrate to ePolicy Orchestrator 3.5 if you are currently using:

- ePolicy Orchestrator 2.5.1 or later.
- Protection Pilot 1.0.
- Evaluation versions of ePolicy Orchestrator 3.5.



You cannot upgrade from beta versions of the software.

This section provides information on:

- Preparation
- Information to have while upgrading
- Considerations for different scenarios

Preparation

Before installing ePolicy Orchestrator 3.5 complete the following tasks:

- Upgrade the database software if it does not meet the minimum requirements.
- Update both the ePolicy Orchestrator server computer and the ePolicy Orchestrator database server computer 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 computer and scan for viruses.
- Install and/or update firewall software on the server computer. (For example, Desktop Firewall 8.0.)
- 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:

- *Server service account.*
- *Ports you want to use.*
- *E-mail address for Notifications.*

Server service account

During the installation wizard, you are asked to provide the password for the user credentials of the system that hosts the **McAfee ePolicy Orchestrator Server service**. This is the service that pushes the agent to client systems.

The domain and user information from existing installation is auto-filled.

Don't use the local system account unless you do not intend to push agents from the ePolicy Orchestrator server.

Ports you want to use

As ePolicy Orchestrator runs, there is a considerable of 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. You cannot change some these assignments without uninstalling the software.

Make sure that the ports you assign are not already assigned to other products.

- **Agent HTTP port** — This is the port the agent uses to communicate with the server. The default port is **80**.



McAfee strongly recommends that you change this to another port due to potential conflicts in many environments. For example, to **82**

If you are upgrading from version 2.5.1 or 3.x, then you cannot change this setting from port you had designated in the prior version.

- **Console HTTP port** — This is the port the console uses to communicate with the server. The default port is **81**.



McAfee strongly recommends that you change this to another port due to potential conflicts in some environments. For example, to **83**.

If you are upgrading from version 2.5.1 or 3.x, then you cannot change this setting from port you had designated in the prior version.

- **Agent Wake-Up HTTP port** — This is the port to used to send agent wakeup calls. The default port is **8081**.



If you are upgrading from version 3.x, then you cannot change this setting from port you had designated in the prior version.

- **Agent Broadcast HTTP port** — This is the port used to send SuperAgent wakeup calls. The default port is **8082**.



If you are upgrading from version 3.x, then you cannot change this setting from port you had designated in the prior version.

- **Discovery & Notification service HTTP 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**.
- **Discovery & Notification service HTTPS 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**.
- **Rogue System Sensor HTTPS 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**.

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 3.5, see the *ePolicy Orchestrator 3.5 Installation Guide*.

Upgrading issues

When you upgrade from ePolicy Orchestrator 2.5.1 and the agent updater 3.0.0, the agent may not upgrade reliably.

If your agents are not upgrading to version 3.5 agents, and you're running VirusScan 7.0.0 on those systems, then you may need to physically go to these systems and perform the following:

- 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. (FRMINST.EXE is located in the Common Framework installation directory.)
- 3** Go back to the ePolicy Orchestrator server and push 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.*
- *Update methods.*

ePolicy Orchestrator Directory: concepts and roles

The **Directory** allows you to combine systems into groupings and sub-groupings. 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 computers. 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 network computers that you are managing with ePolicy Orchestrator. It is possible to add all the computers to be managed by ePolicy Orchestrator into one site in the **Directory**. However, this flat unorganized list makes setting specific policies for different computers very difficult. Therefore, organizing the computers 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 computers.

Groups

A group is a secondary grouping beneath a site. It can contain more groups (sub-groups) and individual computers, but a group cannot contain a site.

Lost&Found groups

Lost&Found groups store computer names whose locations could not be determined by the ePolicy Orchestrator server. The administrator must move the computers 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 **Lost&Found** site.

Inheritance

Inheritance is an important property of the ePolicy Orchestrator **Directory** that simplifies policy administration simpler. Inheritance allows lower-level nodes in the **Directory** hierarchy to inherit policies that have been set at higher levels. Policies set at the **Directory** are inherited by sites, site policies then are inherited by groups or individual systems within that site. Likewise, group policies are inherited by sub-groups or individual computers within that group.

Inheritance is enabled by default for all sites, groups and individual computers that you add to your **Directory**. This means you set policies and schedule client tasks in fewer places.

However, you can set custom policies for any site, group, or individual system, by breaking inheritance. Remember that groups and computers below will inherit those changed policies.



Let inheritance do the work for you. While you can set anti-virus and 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.

Roles

ePolicy Orchestrator users can have one of four different roles: global administrator, site administrator, global reviewer, or site reviewer. Once you've decided who should have access to ePolicy Orchestrator, you need to decide the level of access rights to assign to the specific user accounts.

Global administrators

Global administrators have read, write, and delete permissions and rights to all operations. When you install the ePolicy Orchestrator server and console, a global administrator account with user name `admin` is created (you set the password for this account during the installation wizard). You cannot delete this primary global user account, but you can create additional global administrator user accounts for others who need global administrative rights to all aspects of the ePolicy Orchestrator console.

From the ePolicy Orchestrator console, global administrators can deploy agents and security products, change agent or product policies, create and run client tasks for updating DAT files or perform on-demand scans for any node in any site in the **Directory**. In addition, global administrator user accounts are the only ones that can perform a variety of server-based functions. These are:

- Manage repository functions.
- Manage ePolicy Orchestrator server settings and tasks.

- Manage global-level **Directory** functions, such as creating or editing sites.

Site administrators

The site administrator has full read, write, and delete permissions and rights to all child nodes within the specific site.

Site administrators can neither view or modify other sites in the **Directory**.

Site administrators can run reports for their sites only.

You may only need to create site administrator accounts if different local administrators have local control over their parts of the network. For example, your organization may have remote offices in different cities or countries where the ePolicy Orchestrator server account does not have domain-administrative privileges, and these locations may have local IT or network administrators with rights to install and manage software on computers in that part of the network.

You can create site administrator accounts for these local administrators so they can log onto the server from their remote locations via a remote console.

Global reviewer

Global reviewers can view, but not edit, all settings in the console, including property, policy, and task settings for all nodes in the **Directory**.

Global reviewers cannot access the Notifications or Rogue System Detection features, but they can run reports.

Site reviewer

Site reviewers can only view settings for a single site in the **Directory**.

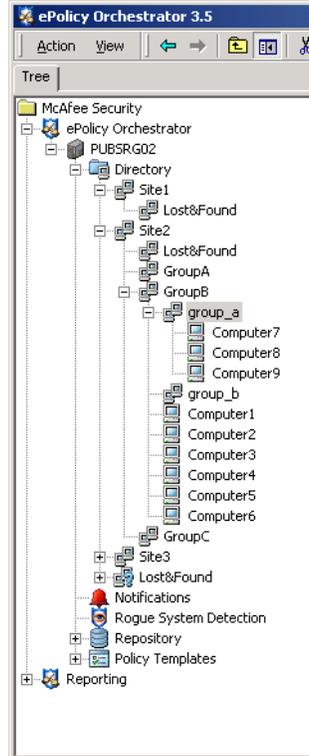
Site reviewers cannot access the Notifications or Rogue System Detection features, but they can run reports for their sites.

Organizing the Directory

The **Directory** allows you to combine nodes into sites and groups. Combining computers with similar properties or requirements allows you to manage policies in one place, at the site or group level, rather than having to set policies for individual computers.

In many respects, sites and groups are very similar. Both can contain sublevels of groups as well as individual computers. You can create both sites or groups manually, or create them automatically by browsing or importing lists of computers directly from your NT Network Neighborhood or Active Directory.

Figure 3-1 Directory organization



In some respects, sites are different. You can use sites to define administrative roles by creating site administrator and site reviewer user accounts in ePolicy Orchestrator that are specific to a site. Site administrators can only work within that site and do not have access to other parts of the **Directory**.

Sites also contain **Lost&Found** groups. These are temporary containers for computers that ePolicy Orchestrator cannot place automatically in other sites or groups in your **Directory**.

Only ePolicy Orchestrator global administrators can create sites. Site administrators can make groups within the site over which they have administrator rights.

You can manually drag and drop groups and individual computers to different locations in the **Directory**. You cannot, however, “promote” a group to a site in this way.

Borders

How you implement ePolicy Orchestrator and organize the systems you wish to manage with ePolicy Orchestrator **Directory** depends significantly on the borders that exist in your network. Borders influence how you set up your **Directory** differently than how you set up your network topology.

We recommend that you evaluate 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 is, the easier it is to create and use the ePolicy Orchestrator **Directory**.
- **Geographical** — If your organization has sites in multiple locations, even on multiple continents, then this must be taken into consideration when building your **Directory**. Bandwidth and administrative roles must be considered when your organization has multiple locations.
- **Political** — Many large networks have divisions created 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 which parts 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 ePolicy Orchestrator **Directory** by functionality if different groups of users require different policies.

Because every network is different and requires different policies — and possibly even different management — we recommend that you plan your **Directory** before beginning implementing the software.

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. These organizational groupings can be useful ways to organize computers for setting policies through ePolicy Orchestrator. For this reason, ePolicy Orchestrator allows you to set IP address filters to sites and groups in the **Directory**. ePolicy Orchestrator provides tools, such as IP sorting and IP integrity check tasks that can automatically place computers in the correct site or group according to IP address. This can be a very powerful tool for automatically populating your **Directory**.

This feature is useful if you do not plan to deploy agents to managed systems on your network from ePolicy Orchestrator. If you use another network software tool, such as Microsoft SMS, or if you deploy the agent using login scripts, the agent is installed on the client 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 discovered system is added to the appropriate location. Otherwise, it is added to the **Lost&Found** group and you will have to move it manually to the appropriate group. Especially in a large network, using IP filters to automatically place the discovered system in the right location can save considerable time.

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.



Automatic IP address sorting does not apply to systems you add to the **Directory** using the new **Active Directory Discovery** task in ePolicy Orchestrator 3.5.

Apply IP filters at each level of the Directory

If you use IP filtering, you should set the IP filtering properties at each level of the Directory properly. 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.
- The 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 which 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 to make sure your IP filter hierarchy is valid. The check alerts you if it finds any conflicts or overlaps between IP filters for different sites or groups.

ePolicy Orchestrator uses IP filtering

These guidelines apply only the first time that the agent communicates with the ePolicy Orchestrator server. After the initial contact, the agent updates the location to which it has been assigned. When an agent contacts the server for the first time, the server searches for the appropriate site whose IP mask or range matches the IP address.

The automated ability to place systems in the Directory is the result of a complex algorithm that uses both IP filters you create and domain information for the NT domain where 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.

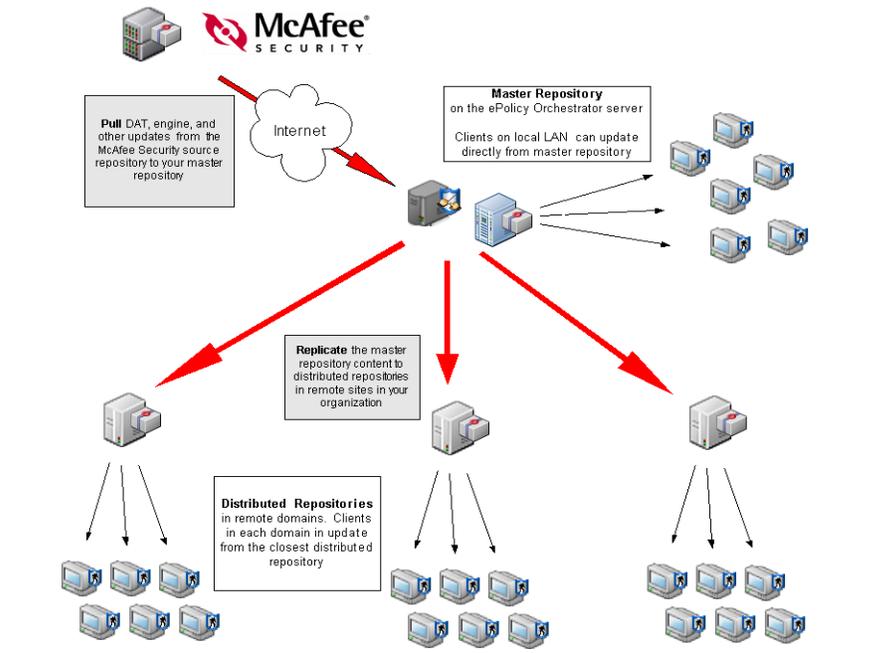
The ePolicy Orchestrator server uses the following search algorithm to place new computers in the Directory:

- 1 Site IP filter** — If a site with a matching IP filter is found, the computer is placed in that site. ePolicy Orchestrator tries the following, in order, to place the computer:
 - a** In a group named the same as the NT domain to which the computer belongs.
 - b** In a group with a matching IP filter.
 - c** If no group match is found for IP address or domain name, the system is placed in the site's **Lost&Found** group.
- 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 computer belongs. If such a site is found, the server searches for a group with a matching IP filter and places the computer there. If no group is found, the computer is placed in the site's **Lost&Found**.
- 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 computer to the global **Lost&Found**.

Repositories

Before implementing the ePolicy Orchestrator software, you should decide the type of update repositories to use, and how they should be organized.

Figure 3-2 Update repositories



Here are some basic terms you'll need to understand:

Source repository

The source repository (usually the McAfee download site) contains the latest DAT and engine files, and product updates issued by McAfee, Inc.

Master repository

The master repository maintains a copy of the source repository, and any other packages that have been checked in manually, to distribute to the update repositories in your environment. The master repository goes to the source repository on a scheduled or on-demand basis to retrieve the latest updates.

The master repository is a part of the ePolicy Orchestrator server.

Update repository

Update repositories can be distributed repositories (HTTP, FTP, or UNC share) or SuperAgent repositories. These contain copies of the contents of the master repository. These repositories are updated on a scheduled or on-demand basis. Client systems can be configured to retrieve updates from the update repositories on a scheduled or on-demand basis.

Global updating

Global updating is a method of automatic product updating. Whenever a new update is checked into the master repository, it is automatically replicated to the update repositories from which client systems are updated. For this type of updating, you must have a SuperAgent on each subnet.

Selective updating

Selective updating is a new feature to ePolicy Orchestrator 3.5. You can use selective updating with both global updating, and update tasks. 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 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 3.5 provides different types of update repositories and several methods for implementing them:

- [Update repositories](#)
- [Update methods](#)

Update repositories

Update repositories are copies of your master repository and contain all the DAT file, engine, and product update packages that are saved in your master repository. As you update your master repository, ePolicy Orchestrator replicates the updates to the repositories. You can configure client systems in remote sites to access the update repository closest to their location. This can save a significant amount of bandwidth — the update files are retrieved only once per remote location, rather than once for each computer at that location.

How do repositories save bandwidth?

Using repositories allows you to balance network load when you have a large LAN with thousands of clients. During an outbreak situation, you may want to have all your clients update at the same time. Having several distributed repositories allows you to balance network load, rather than having them all update from one server.

In a large organization over multiple geographic locations, using update repositories helps limit network traffic in the low-bandwidth sections of your network. For example, you want a remote office with 100 computers to retrieve full weekly DAT files. The office is located in another country and has limited available bandwidth. If you create a distributed repository in the remote network and configure those clients to update from it, you only copy the DAT file package (about 3MB) once across the WAN to the distributed repository. Then, all the clients retrieve their DAT files from this update repository.

Which computers in my network should I use as update repositories?

You do not need to use a dedicated computer for the update repository. Ideally, the computer should be a server and be large enough to have many client computers connect to it for updates. Servers are recommended over workstations because they are more likely to be running all the time. If you do not have a server computer that you can use for this purpose, choose a computer that you feel is up and running as continuously as possible.

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 agents point to 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.

- [Distributed repositories.](#)
- [SuperAgent repositories.](#)

Distributed repositories

Distributed repositories can be created as FTP or HTTP servers, or UNC shares. These repositories can be created by a wizard accessed on the **Reposities** page in the ePolicy Orchestrator console.

SuperAgent repositories

In addition to using SuperAgents to send broadcast wakeup calls to other agents during a global update, you can also use SuperAgents as repositories for updating client systems.

SuperAgent repositories have several advantages over other types of distributed repositories, making them easier to create and configure:

- You don't need to manually create folder locations on the host computer before adding the repository to the repository list. Instead you enable the SuperAgent repository feature from the agent policies for a specific computer, and ePolicy Orchestrator creates the required share folder.
- SuperAgent repositories don't require replication or updating credentials. Once the SuperAgent is installed and enabled on the computer, ePolicy Orchestrator can replicate repository contents to that SuperAgent, and other agents can update from it. ePolicy Orchestrator uses a proprietary network protocol to replicate updates to SuperAgent distributed repositories.
- SuperAgent repositories are required for global updating.

When SuperAgents are used for broadcast wakeup calls, only one can be used per network broadcast segment. (In most networks this is synonymous with a network subnet.) However, it is not necessary that a SuperAgent repository be located in the same broadcast segment for a client computer to update from it. A client computer only needs to be able to “see” the computer that hosts the SuperAgent repository on the network.



Computers hosting SuperAgent repositories may need to be more powerful than those hosting SuperAgents used for broadcast wakeup calls. If you plan to use SuperAgent repositories, make sure the computer you create them on is powerful enough to allow however many client computers you have to update from it, potentially simultaneously in an outbreak situation.

SuperAgents and SuperAgent repositories can be created on the **General** tab of the ePolicy Orchestrator Agent policy pages.

Update methods

ePolicy Orchestrator 3.5 offers several updating methods. Some can be used with any type of update repository, and some of these can be used with other methods.

Global updating

Global updating is an automated method of updating. When updates are checked into the master repository, they are automatically replicated.

To use global updating:

- 1 Select the ePolicy Orchestrator server in the console tree.
- 2 Select the Settings tab in the details pane.
- 3 Select **Yes** next to **Enable global updating**.

To use global updating, you need a SuperAgent repository on each subnet you want to take part in global updating.

Global updating also allows you to use selective updating to pick and choose which updates you want to be replicated during a global update.



McAfee, Inc. recommends using global updates for DAT file and engine updates only in order to save bandwidth. You can make these selections on the **Settings** tab below the selection to **Enable global updating**.

ePolicy Orchestrator agent update task

By scheduling an ePolicy Orchestrator update task, you can schedule DAT file, engine, and specific product updates for any node in the **Directory**. Remember that all nodes below the selected node will receive the updates as long as inheritance is not broken.

To schedule an update task:

- 1 Select the **Directory** or the desired site, group, or system in the console tree.
- 2 Click the **Tasks** tab in the upper details pane.
- 3 Right-click in the details pane and select **Schedule Task**. The **Schedule Task** dialog box appears.

- 4 Type a **New Task Name**.
- 5 Select **ePolicy Orchestrator Agent | Update**, then click **OK**. This dialog disappears.
- 6 Double-click the task name when it appears on the **Tasks** tab.
- 7 Click **Settings** on the **Task** tab of the **ePolicy Orchestrator Scheduler** dialog box.
- 8 Deselect **Inherit**, scroll down, and select the components you wish to update with this task, then click **OK**.
- 9 Click the **Schedule** tab of the **ePolicy Orchestrator Scheduler** dialog box.
- 10 Schedule the task as needed.

Pull and replication tasks

From the Repository page (accessed by clicking Repository in the console tree), you can schedule or manually initiate pull and replication tasks.

A pull task initiates the master repository to go to the source repository and retrieve any new updates.

A replication task causes the master repository to replicate its contents to the update 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. These include:

- [ePolicy Orchestrator agent.](#)
- [SuperAgents for communication with server](#)
- [Deploying products with ePolicy Orchestrator.](#)

ePolicy Orchestrator agent

The agent is the distributed component of ePolicy Orchestrator that is installed on each client system that you want to manage in your network. The agent collects and sends information between the ePolicy Orchestrator server, repositories, and the managed systems. The way you configure the agent and its policy settings determines how it functions and facilitates communication and updating in your environment.

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. This section covers:

- [About distributing the ePolicy Orchestrator agent.](#)
- [Deploying the agent while creating the Directory.](#)
- [Deploying the agent after creating the Directory.](#)
- [Using login scripts to install the agent.](#)
- [Manually installing the agent.](#)
- [Including the agent on a standardized installation image.](#)
- [Enabling the agent on unmanaged McAfee products.](#)
- [Using third-party deployment tools to distribute the agent.](#)

About distributing the ePolicy Orchestrator agent

Know and consider the following details about the agent before deployment:

Install operating system updates on any Windows 95, Windows 98, or Windows ME systems

Make sure your network computers running these operating systems are able to be managed by ePolicy Orchestrator. By default, these operating systems do not allow it. To enable them 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.

In addition, if you plan to use ePolicy Orchestrator to deploy the agent to client systems running these operating systems, you must also enable file and print sharing.

See the *ePolicy Orchestrator 3.5 Product Guide* for more details.

Agent installation directory

The location of the agent installation directory differs depending on where the agent is located — on client systems or the ePolicy Orchestrator server.

- If the agent was installed as part of another product installation, pushed from the ePolicy Orchestrator console to client computers, or as an upgrade from version 2.5.1, it is installed by default into the `<SYSTEM_DRIVE>\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK` folder.
- If the agent was installed on the ePolicy Orchestrator server system during the product installation, it is located in the `COMMON FRAMEWORK` folder in the ePolicy Orchestrator software installation directory.



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 client computers, you must check the desired agent language packages into the master repository, then replicate them to distributed repositories the same as other product update packages.

Each agent language package includes only those files needed to display the user interface for that language.

After the initial agent-to-server communication:

- 1 The agent retrieves language packages from repositories based on the client system's locale setting during the update.
- 2 If the in-use locale corresponds to an available language package, the agent retrieves the new package and applies it. In this way, the agent retrieves only language packages for the locales being used on each client computer.
- 3 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 client computers 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
- Swedish

Create a custom deployment package to deploy the agent without ePolicy Orchestrator

If you are using another deployment method, such as login scripts or third-party deployment software, you may need to embed administrator user credentials in a custom agent deployment package using the **Agent Installation Package Creation** wizard. Because users might not have local administrator permissions, you can embed the appropriate set of credentials as part of the FRAMEPKG.EXE agent installation package by creating a custom installation package. The user account you embed is used to install the agent.

You can also create a custom deployment package with embedded user credentials if you deploy the agent via ePolicy Orchestrator.

For instructions on creating a custom deployment package, see the *ePolicy Orchestrator 3.5 Product Guide*.

About the FRAMEPKG.EXE agent installation package

The FRAMEPKG.EXE file is created when you install the ePolicy Orchestrator server. It is a customized installation package for agents that will report to your server, and it contains the server name, IP address, ASCII port number, and other information that allows the agent to communicate with the server. By default, the agent installation package is located in the following folder on your ePolicy Orchestrator server:

```
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.5.0\DB\SOFTWARE\CURRENT\  
ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE
```

This is the same installation package that the ePolicy Orchestrator server uses to install the agent if you were to push the agent through the console. However, you can run the installation package from the client computer, just as you install any client software.

The default agent installation package contains no user credentials embedded. When executed on the client, it uses the user account of the currently logged-on user.

Deploying the agent while creating the Directory

If you have not yet created the **Directory**, you can send the agent installation package to computers at the same time that you are add sites, groups, and computers to the **Directory**. For instructions, see the *ePolicy Orchestrator 3.5 Product Guide*.

Deploying the agent after creating the Directory

You can deploy the agent installation package (FRAMEPKG.EXE) from the ePolicy Orchestrator console to selected sites, groups, or computers in the **Directory**.

Once logged on to the ePolicy Orchestrator server, right-click the desired site, group, or system in the **Directory**, select **Send Agent Install**, and complete the options in the **Install Agent** dialog box.

For complete instructions, see the *ePolicy Orchestrator 3.5 Product Guide*.

Using login scripts to install the agent

Using network login scripts is a reliable method to make sure that every computer logging into your network is running an ePolicy Orchestrator agent. You can write a login script to call a batch file that tests whether the agent is installed on systems attempting to log on to the network. If no agent is present, the batch file can install the agent before allowing the computer to log on. Within ten minutes of being installed, the agent calls into the ePolicy Orchestrator server for updated policies, and the computer is added to the **Directory**.

You can also use network login scripts to test the agent version and, if the agent is older than version 2.5.1, install the new 3.5 agent.



If you deploy the agent with login scripts, McAfee recommends that you first manually create some sites and groups in your **Directory** that use either network domain names or IP filters. When agents call into the server for the first time, they can populate these sites and groups automatically. If you don't do this, they are added to the **Lost&Found** group and you must move them manually later. Creating a **Directory** structure that uses some automated sorting method *before* deploying agents via logon script can save you significant time later. See the *ePolicy Orchestrator 3.5 Product Guide* for more information.

How you write the login script to install the agent can vary greatly, depending on what exactly you want the script to do. Consult your operating system documentation for more details on writing login scripts. Generally, to set up agent deployment via network login scripts:

- 1 Create a custom agent installation package if necessary.
- 2 Copy the agent installation package to a central folder to which all users have permissions.
- 3 Create a batch file, which tests new computers for an agent and either installs the new agent if one is not present or updates the agent if it is an older version.
- 4 Save the batch file to your primary domain controller (PDC) so that it runs from the PDC every time a computer logs on to the network.
- 5 Update your network login scripts to call the batch file.

Manually installing the agent

A simple way to install the agent is to run the installer (FRAMEPKG.EXE) from the managed system.

You can install the agent at client systems, or you can distribute the installer to users in your organization and have them run the installer themselves. After the agent installs, it calls back to the server, and ePolicy Orchestrator adds the new computer to the **Directory**, if it doesn't already exist in the tree.

Including the agent on a standardized installation image

If your organization uses standard installation images for new workstations and servers, you can include the ePolicy Orchestrator agent on your images. You can install the ePolicy Orchestrator agent on computers used to create common images for your environment. The first time the user logs on to a computer using an image that includes the agent, the computer 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.

Enabling the agent on unmanaged McAfee products

Before you decided to buy ePolicy Orchestrator, you may have already been using McAfee products in your network. Some of the more recent McAfee products that use the AutoUpdate 7.x, such as VirusScan Enterprise, install with the ePolicy Orchestrator agent in a disabled state. When you want to start managing these products with ePolicy Orchestrator, you can enable the agent that is already on the client computer.

Enabling the agent in this way, rather than re-deploying the 1.5MB agent installation package to each client computer, can save network bandwidth. This is especially true if you have many computers like this and plan to bring them all under ePolicy Orchestrator management.

You must copy the SITELIST.XML repository list file from the ePolicy Orchestrator server to the client computer. The repository list contains network address information for the ePolicy Orchestrator server that the client agent needs in order to call into the server for the first time.

To enable the agent on products that already have a disabled agent installed:

- 1 Export the repository list (SITELIST.XML) from the ePolicy Orchestrator server and copy it to a temporary folder on the client computer (such as C:\TEMP). For instructions, see the *ePolicy Orchestrator 3.5 Product Guide*.
- 2 Run this command on the client system:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

where /SITEINFO equals the location of the repository list (SITELIST.XML) you exported.

Reference the SITELIST.XML file in the temporary folder. By default, FRMINST.EXE is located in the following folder on the client computer:

C:\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK



Some products may have an older version of the agent. When you enable these older agents, they are *not* automatically upgraded to the latest agent version from the ePolicy Orchestrator server. To do this, you should also enable and run the default deployment task to install the new agent on the client system. See the *ePolicy Orchestrator 3.5 Product Guide* for complete instructions.

Using third-party deployment tools to distribute the agent

You may already use other network deployment tools in your organization for deploying software. You can use many of these tools, such as Microsoft Systems Management Server (SMS), IBM Tivoli, or Novell ZENworks, to deploy the ePolicy Orchestrator agent. Configure your deployment tool of choice to distribute the FRAMEPKG.EXE agent installation package located on your ePolicy Orchestrator server.

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.
Pushing agent from console	This is an efficient method for deploying the agent.	If you selected Use Local System Account in the Server Service Account dialog box when you installed the ePolicy Orchestrator server, you cannot use the ePolicy Orchestrator server credentials to deploy the agent. If you want to embed user credentials into the agent installation package, 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 a great method for an environment where systems log on to the network frequently. You do the work once, and the agent is deployed automatically.	Systems that don't log on to the network frequently, may not be running the most up-to-date agent.
Installing manually	This is an effective 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.

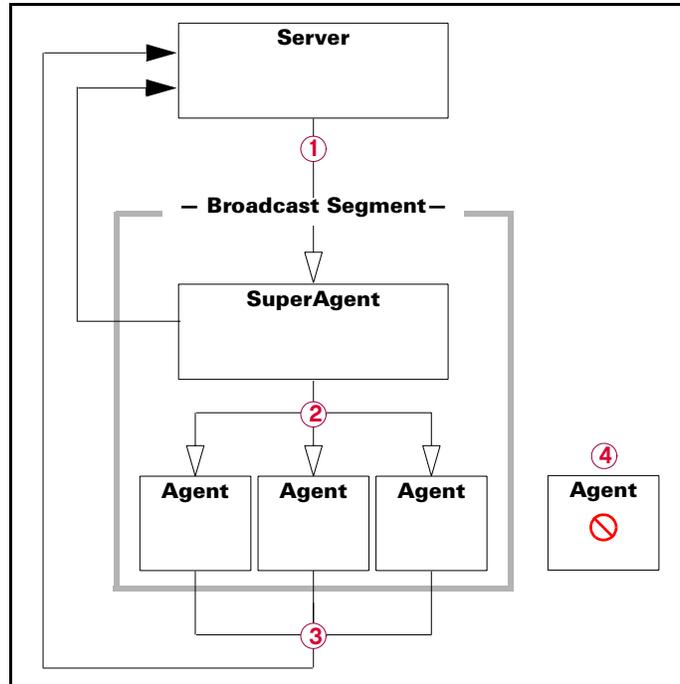
Method	Advantages	Disadvantages
Including the agent on an image	Installing the agent as part of an image prevents the bandwidth impact that other forms of deployment can incur. This method also reduces the overhead by integrating the task into another one that must occur.	If you do not use images consistently, 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.

SuperAgents for communication with server

If you plan to use regular agent wakeup calls in your network, consider deploying SuperAgents to distribute the agent wakeup call and minimize network traffic. Depending on your network environment, you might find SuperAgent wakeup calls to be a more efficient way to prompt wakeup agents.

About SuperAgent broadcast wakeup calls

A SuperAgent is an agent that can send broadcast wakeup calls to other ePolicy Orchestrator agents located on the same network broadcast segment. Instead of having the ePolicy Orchestrator server send agent wakeup calls to every agent, it can send them only to a few SuperAgents. This helps reduce network traffic by sending fewer agent wakeups from the ePolicy Orchestrator server. This can be especially beneficial in large networks where ePolicy Orchestrator may manage agents in remote sites across by lower-speed WAN or VPN connections. Send out wakeup calls to a few SuperAgents that then wake up the other agents in the local LAN.

Figure 4-1 Communication using SuperAgents

- 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 will not be prompted to communicate with the server.

When you send a SuperAgent wakeup call to a selected site or group in your *Directory*, the server sends a wakeup call to all SuperAgents deployed in those groups. Then each SuperAgent sends an agent wakeup call to all agents in the same broadcast segment as the SuperAgent. Then the agents call into the ePolicy Orchestrator server for updates.



You must know how physical broadcast segments and logical subnets are organized in your network to be able to deploy the right number of SuperAgents to the right locations. Any agents that do not have a SuperAgent in the local broadcast segment do not receive the broadcast wakeup call.

Usually a broadcast segment is the same as a network subnet, since most network routers block UDP broadcast traffic between subnets by default. However, you may have configured your routers to allow UDP broadcast traffic between certain subnets. In this case you only need to deploy one SuperAgent for all these UDP-connected subnets. Conversely, you may have one subnet separated into several broadcast segments. In this case, you need to install a SuperAgent in each broadcast segment within the subnet.

SuperAgent wakeup call uses ICMP ping

Similar to the regular agent wakeup call, the SuperAgent wakeup call is a McAfee proprietary SPIPE message over HTTP sent from the ePolicy Orchestrator server. Many network routers block such traffic between subnets by default. If your network is configured this way, using SuperAgent wakeup calls will not be able to wake up any computers located outside the local subnet where the ePolicy Orchestrator server is installed. Therefore, do not use agent or SuperAgent wakeup calls. Instead, use the regular agent ASCII.

SuperAgent repositories not the same as SuperAgents

SuperAgents can also be configured to function as a distributed repository for updates. This is separate SuperAgent functionality and is not related to the SuperAgent broadcast wakeup call. See [SuperAgent repositories on page 27](#).

Change any agent into a SuperAgent by selecting **Enable SuperAgent functionality** on the **General** tab of the ePolicy Orchestrator Agent policy pages.

Deploying products with ePolicy Orchestrator

You can use ePolicy Orchestrator to deploy security programs to systems in your network. To do this, you must first check in a package catalog (PKG.CATALOG.Z) file for each product you want to deploy with ePolicy Orchestrator. This file contains the installation files for the product which are compressed in a secure format that ePolicy Orchestrator uses to push to managed systems and install.

Using ePolicy Orchestrator to deploy products to clients is a two-step process:

- 1 [Check in product deployment packages to the master repository.](#)
- 2 [Use the deployment task to install products on clients.](#)

You only need to perform these steps if you plan to use ePolicy Orchestrator to deploy these products to your managed clients.



In addition to checking in the product deployment packages, you also must check in the NAP files to manage the products. This does not need to be done at the same time.

Check in product deployment packages to the master repository

Product deployment packages exist as a package catalog (PKG.CATALOG.Z) file. Every product that is released by McAfee, Inc. and is deployable through ePolicy Orchestrator includes a PKG.CATALOG.Z file. Usually, the package catalog file is located in the same folder as the other product installation files, either on the product CD or in the product installation .ZIP file, available on the McAfee product download site.

You must manually check in any product package (PKG.CATALOG.Z) file to the master repository that you plan to deploy through ePolicy Orchestrator except those for the ePolicy Orchestrator agent or System Compliance Profiler, which are installed with the ePolicy Orchestrator server.

Package signing and security

All packages created and distributed by McAfee are signed with a key pair using the Digital Signature Algorithm (DSA) verification system, and are encrypted using 168-bit 3-DES 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 PKGCATALOG.Z files signed by ePolicy Orchestrator or McAfee. This protects your network from receiving updates from unsigned or untrusted sources.

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.

Checking in PKGCATALOG.Z product packages to the master repository:

To check in a product deployment package:



You must be a global administrator to check in product deployment packages.

- 1 Locate the folder that contains the PKGCATALOG.Z file you want to check in; copy the entire contents of the folder to a temporary folder on your ePolicy Orchestrator server. Usually, the package catalog file is located in the same folder as the other product installation files, either on the product CD or in the product installation .ZIP file available on the McAfee product download site.



You must copy *all* the files in the PKGCATALOG.Z folder, not just the PKGCATALOG.Z file itself, or the package check-in will fail.

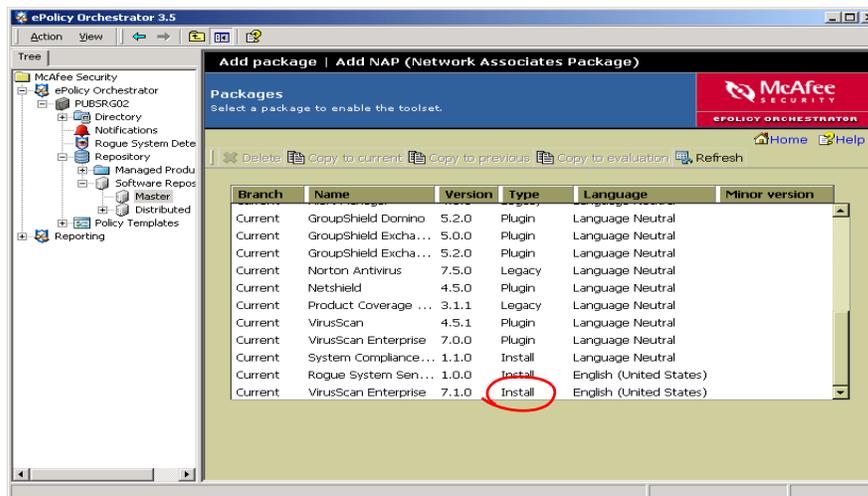
- 2 From the ePolicy Orchestrator console **Directory**, select **Repository**.
- 3 In the details pane under **AutoUpdate Tasks**, click **Check in package** to launch the **Check-in package** wizard.
- 4 Click **Next** to open the **Package Type** dialog box, and select **Products or updates** for the package type and click **Next**.
- 5 Browse to and locate the PKGCATALOG.Z file that you saved in a temporary folder in [Step 1](#).
- 6 Click **Next** to view the package check-in summary information.
- 7 Click **Finish** to begin checking in the package. Wait a few minutes while the package checks in.
- 8 Click **Close** after the package check-in completes.

Confirming which product packages are in your master repository

After you check in the PKGCATALOG.Z, confirm that the correct package and version was added to your master repository:

- 1 In the **Directory** of the ePolicy Orchestrator console, navigate to **Repository | Software Repositories | Master**.

Figure 4-2 Packages page



- 2 In the details pane, scroll through the list until you find the product name and version for the product package you added.

Replicate packages checked into master repository to update repositories

If you are using update repositories in your network, be sure to perform replicate the contents of the master repository to any update repositories.

When you run the ePolicy Orchestrator deployment task to distribute a product to client systems, those systems that receive updates from an update repository also get the product package from that repository rather than the master repository.

Use the deployment task to install products on clients

Once you have checked in the PKGCATALOG.Z file, you can use the deployment task to install the product on systems in your **Directory**. The deployment task is a unique client task created automatically when ePolicy Orchestrator installs. You can use this deployment task to install almost any product that is deployable through ePolicy Orchestrator.



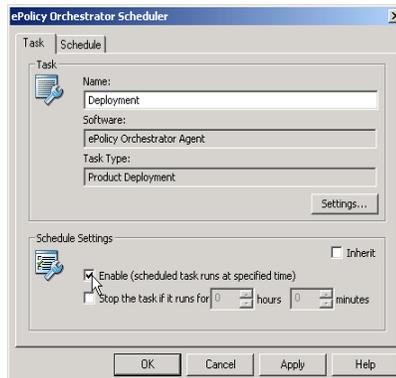
Do not delete the default deployment task. Once deleted, it is difficult to recreate.

To deploy products using the product deployment task:

- 1 In the **Directory** of the ePolicy Orchestrator console, select the site, group, or individual computer in your **Directory** to which you want to deploy the product.
- 2 In the details pane, select the **Task** tab and then double-click the **Deployment** task in the task list.

- Once the ePolicy Orchestrator Scheduler opens, click the **Task** tab and deselect **Inherit** under **Schedule Settings**.

Figure 4-3 ePolicy Orchestrator Scheduler dialog box

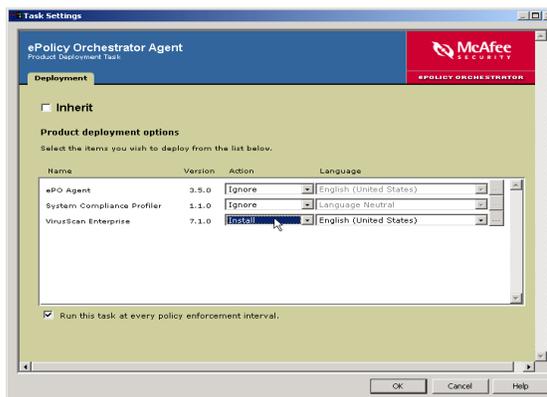


- Under **Schedule Settings**, select **Enable (scheduled task runs at specified time)**. The task will not run unless you enable it here.
- Click **Settings**, then deselect **Inherit** to enable product deployment options on the **Deployment** page.

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 package file.

- Set the **Action** for the product you want to deploy to **Install**.

Figure 4-4 Task Settings dialog box



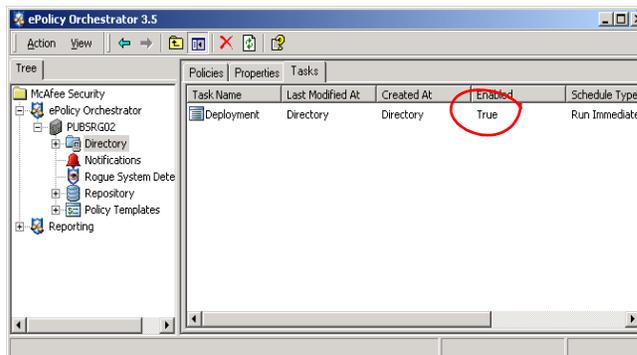
- To specify command-line installation options, click **...** and type the command-line options in the **Command line** text field. See your product documentation for information on command-line options.
- Click **OK** to save the product deployment options and return to the ePolicy Orchestrator Scheduler dialog box.
- On the ePolicy Orchestrator Scheduler dialog box, click the **Schedule** tab and deselect **Inherit** to enable scheduling options.

10 To run the task once from the **Schedule Task** drop-down list, select **Run Immediately**.

11 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**.

Figure 4-5 The VirusScan deployment task is configured and enabled



Once configured, the deployment will occur the next time the agents call back to the ePolicy Orchestrator server for updated instructions. You can also initiate an agent wake-up call to have the deployment occur immediately.

How many systems should I deploy to at one time?

You can run the product deployment task at any site, group, or individual computer in your **Directory**. This could mean deploying to tens of thousands of clients all at once. In addition to potentially overwhelming the ePolicy Orchestrator server or your network, deploying to too many computers can make troubleshooting problems overly complicated.

Instead, for workstation deployments, plan a phased roll-out to install products to groups of computers 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 installs.

Deploy server products to individual computers

If you chose to deploy server-based McAfee products, such as GroupShield for e-mail servers or WebShield SMTP for gateway servers, you will probably want to deploy them to specific systems in your **Directory**, rather than groups or sites. Typically, there is a small number of such servers in a site.

5

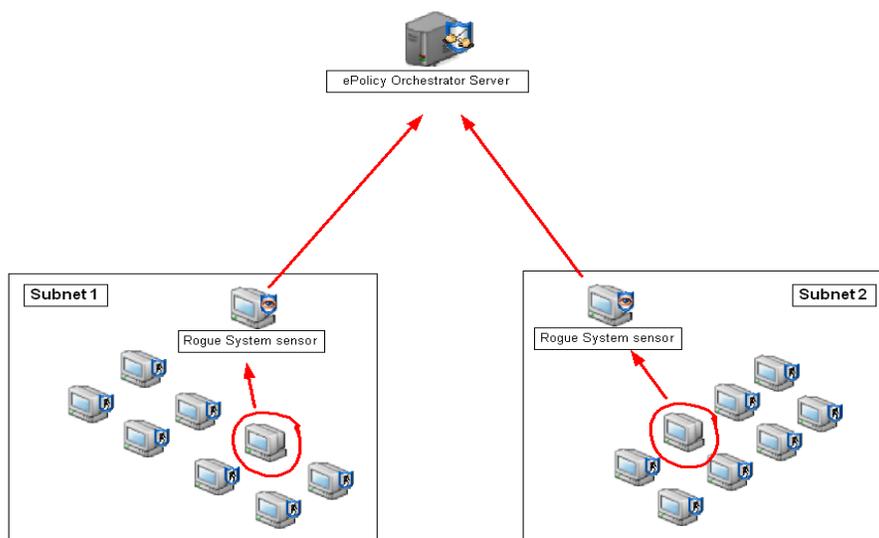
Rogue System Detection

A *rogue system* is any system on your network that is not currently managed by an ePolicy Orchestrator agent (but should be).

In any managed network, there are inevitably a small number of computers that do not have an ePolicy Orchestrator agent installed. These can be systems that frequently log on and off the network, such as test servers, laptop computers brought from home, or wireless devices. Also, users can uninstall or disable agents on their own computers. These unprotected systems are a weakness of any anti-virus and security strategy because they can serve as entry points through which viruses and other potentially harmful programs gain access to your network.

The Rogue System Detection system helps you monitor *all* the systems on your network—not only those that ePolicy Orchestrator manages already, but these rogue systems as well. 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 passively to network broadcast messages and detects when a new computer has connects to the network.

Figure 5-1 Rogue system sensors reporting computers without agents



When the sensor detects a new system on the network, it sends a message to the Rogue System Detection server. That server then checks with the ePolicy Orchestrator server to determine whether the newly-identified computer has an active agent installed and is managed by ePolicy Orchestrator. If the new computer 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 pushing an ePolicy Orchestrator agent to that computer.



The Rogue System Detection server is on the ePolicy Orchestrator server. No additional installation is necessary.

Topics covered in this section

- [About the rogue system sensor](#)
- [The Rogue System Detection server](#)
- [About status and rogue type](#)

About the rogue system sensor

The sensor is the distributed portion of the Rogue System Detection architecture. It detects computers and other devices connected to your network. The sensor gathers information about the devices it detects and forwards the information to the Rogue System Detection server.

The sensor is a small Win32 native executable application that runs unobtrusively on server and workstation computers. To use the feature, you must deploy at least one sensor to each broadcast segment, usually the same as a network subnet, in your network.

Sensor installation requirements

The sensor installs and runs on any computer running a Windows NT-based operating system, such as Windows NT, Windows 2000, Windows XP, and Windows 2003. The sensor does not run on earlier versions of Windows or on non-Windows operating systems.

Additional installation recommendations are as follows:

- File system — NTFS recommended.
- Memory — 128 MB RAM.
- Processor — 166 MHz processor or higher.
- An Ethernet interface that supports 802.3, Ethernet II, or 802.11 protocols.

The sensor interfacing with your network

To detect systems on the network, the sensor utilizes WinPCap, an open source packet capture library. Using WinPCap, the Rogue System Detection sensor captures network layer-two broadcast packets sent by computers connected to the same network broadcast segment. The sensor listens for and parses Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and IP traffic. The sensor “listens” passively to the broadcast traffic of all devices on that part of the network, but does not actively probe the network for connected systems and devices.

The sensor does not use promiscuous mode.

Intelligent filtering of network traffic

The Rogue System Detection sensor implements intelligent filtering of network traffic to ignore “chatter” 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 those devices that are part of the local network.

To optimize performance and minimize network traffic, the sensor limits its communication to the server by relaying only new system detections, and ignoring any re-detected systems for a configurable period of time.

The sensor further filters on systems it has already detected by:

- Always reporting any system the first time it is detected on the network.
- Adding the MAC address of every detected system to the packet filter so that it will not be re-detected.
- Implementing 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 re-reported to the server.

Gathering data on detected systems and communicating to the server

Once the sensor detects a system located on the local network, it gathers as much information about that system as it can from the network packet. The information gathered includes DNS name, operating system version, and NetBIOS information such as domain membership, NetBIOS name, and the list of currently logged-on users. All of this information is subject to standard limitations, as documented in the Microsoft management API.

The sensor sends the information about the detected system in an XML message via secure HTTPS to the Rogue System Detection server, which then queries the ePolicy Orchestrator database to determine whether the computer is a rogue system.



To save bandwidth, you can configure how often the sensors send detection messages to the server. The sensor can send every detection event to the server immediately or it can cache detection events for a given time period, such as one hour, then send a single message containing all the events from that period.

The sensor makes no determination about system rogue status. It simply reports detected systems to the Rogue System Detection server.

The Rogue System Detection server

The Rogue System Detection server consists of a number of servlets running within the Apache Tomcat web server (TOMCAT.EXE). These servlets and the Tomcat web server are installed and started when you install the ePolicy Orchestrator server. They collect detection messages sent by the sensors deployed on your network, and maintain tables in the ePolicy Orchestrator database for detection information.



The Rogue System Detection server is a separate process from the ePolicy Orchestrator server service, and runs regardless of whether the ePolicy Orchestrator server is running.

When a sensor detects a new system on the network and informs the server, the server queries the ePolicy Orchestrator database to determine whether the system is listed. If it is, that system is managed and has an active ePolicy Orchestrator agent running. If it is not listed in the ePolicy Orchestrator database, that system does not have an active ePolicy Orchestrator agent installed and could be a rogue system.

About status and rogue type

Every system detected by sensors is listed in the **Machine List** with a **Status** and, if the status is **Rogue**, a **Rogue Type**. These classifications are useful for grouping computers in the **Machine List** table, and identifying criteria for triggering automated responses.

Machine status

Every system detected by a rogue system sensor has one of four different statuses:

Status	Description
Managed	A system with an active agent installed and running.
Rogue	A system without an agent.
Exception	A system flagged as an exception, such as a network router, switch, or printer, that you know does not require an agent.
Inactive	A computer 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 most likely computers that have been shut down or disconnected from the network.

Rogue types

Systems identified as having a **Rogue** or **Inactive** machine status must also have a **Rogue Type**. These are systems not listed in the database, but may not be true rogues. Classifying rogues by type gives you greater flexibility and control in your network.

Rogue Type	Description
No Agent	The detected computer has no agent installed.
Grace Period	Using the grace period allows you to create a time buffer to avoid false positive rogue detections. The grace period is disabled by default, so all systems that are detected by sensors and are not listed in the database are immediately classified as Rogue (No Agent) . You might consider enabling the grace period if you have configured automatic responses that are triggered by a rogue detection event. For example, if you install agents with a login script, the initial agent call to the server may take up to 10 minutes. In this situation, the sensor would likely detect the computer, classify it as Rogue (No Agent) even though the computer has an agent, and take any automatic responses you have configured.
Inactive Agent	The computer has an agent installed, but the agent has not called into the ePolicy Orchestrator server for a configurable number of days.

Rogue Type	Description
Alien Agent	<p>The computer has an agent installed, but the agent does not report into your ePolicy Orchestrator server. This can occur if you use multiple ePolicy Orchestrator servers to manage different parts of your network. Laptop users who travel and log into your network could have an alien agent. This rogue type is distinct and you probably would not want to take action on these computers. But since they are not managed by your server, you don't want them to be classified as Managed.</p> <p>To reduce false positive rogue detections, you can configure automated responses to avoid acting on systems with alien agents.</p>
Managed	The computer has not been detected by a sensor in a while, but when last detected it had an agent.

Deploying Rogue System Detection sensors

To ensure that your Rogue System Detection coverage is complete, you must install at least one sensor in each network broadcast segment in your network. Typically, a network broadcast segment is the same as a network subnet. You can install more than one sensor in a subnet — the Rogue System Detection server filters duplicate detection messages. Note, however, that having multiple active sensors in each subnet results in duplicate messages sent from each sensor to the server.

Primary and inactive sensors

The **Subnet List** 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. You can deploy sensors to computers from this location also.

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**. While maintaining as many as five or ten primary sensors in a subnet should not cause problems, McAfee recommends not maintaining more primary sensors in a subnet than is necessary to guarantee that the subnet is covered. The more primary sensors you have, the more network traffic Rogue System Detection generates.

Any additional sensors you deploy are backups that sleep until told to become active by the Rogue System Detection server. These are the **Inactive Sensors**. At regular intervals, the Rogue System Detection server changes primary sensors so that it is not dependant on any one sensor for too long. If the primary sensor is disabled or stops responding, the ePolicy Orchestrator server automatically makes a different sensor on that subnet the primary sensor.

Recommended locations to install sensors?

The system on which the sensor is installed should be a computer that is 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 subnet, deploy several sensors to several workstations to maximize the chance that any one of them will be turned on and connected to the network at any time.

Consider sensor policies before deploying

Before you deploy sensors, you should configure the sensor-to-server parameters to suit your network needs. These are most likely the same for all sensors that communicate to your Rogue System Detection server so, you can configure sensor policies at the highest levels of the **Directory** and let the systems below inherit them.

What happens when the sensor-hosting computer changes subnets?

Occasionally, you may need to move the computer hosting a sensor from one subnet to another. The sensor is designed to correctly recognize when its subnet location has changed and report this change to the Rogue System Detection server. If the computer running the sensor changes subnets, this is reflected immediately in the **Subnets** list in the Rogue System Detection server interface.

If you deploy a sensor to a computer that changes subnets, such as a laptop, make sure you deploy another sensor to cover that subnet.

Deploying sensors automatically from the console

Installing sensors one by one throughout your network can take considerable time, especially if you are rolling out Rogue System Detection for the first time and need to deploy many sensors to all subnets in your organization. Deploying sensors from the ePolicy Orchestrator console can save significant time.

When deploying sensors from the console, you can either manually pick specific computers to host the sensors, or you can let ePolicy Orchestrator pick computers automatically from the those on the subnet.

For complete instructions, see the *ePolicy Orchestrator 3.5 Product Guide*.

About selection criteria

If you allow Rogue System Detection to pick systems automatically on the subnet, you can specify criteria for choosing those systems. For example, you can deploy three sensors and specify the **Server OS** and **Most Memory** criteria. Rogue System Detection then selects the three computers running server operating systems that have the most memory and deploys a sensor to each.

You can specify any or all of the criteria listed here when configuring automatic sensor deployment:

Criteria	Description
Most Recent ePO Agent Communication	The more recent the agent communication, the more likely it is to be connected to the network and currently active.
Server OS	Servers are more likely than workstations to remain on and connected to the network at all times.
Hostname	<p>If you use naming conventions when creating the DNS names for computers, you can have Rogue System Detection select sensor hosts by a text string you use in the DNS name. For example, if you add an "SRV" prefix to all your server computers, you could have Rogue System Detection deploy to a computer with "SRV" in its DNS name.</p> <p>If you add Hostname to the Selected criteria list, type the text string that appears in your server DNS name in the Hostname text box.</p>

Criteria	Description
Most Memory	Although the sensor is not a memory-intensive application, the more memory available the better.
Fastest CPU	Although the sensor is not CPU-intensive, the faster the CPU the better.

For instructions, see the *ePolicy Orchestrator 3.5 Product Guide*.

Manually installing the sensor

If you do not wish to deploy your rogue system sensors automatically from the ePolicy Orchestrator console, you can perform the installation manually. To do so, you must be at the computer where the sensor is to be installed and have administrative privileges on that computer.

You can install the sensor using either the `SETUP.EXE` installation wizard or via the command line.

For specific instructions, see the *ePolicy Orchestrator 3.5 Product Guide*.

Remediating rogues systems

Once rogue systems have been detected, they can be remediated automatically or manually.

To remediate rogue systems automatically, you can configure automatic responses for Rogue System Detection to take on these systems (and the conditions that must be met before Rogue System Detection acts on the systems).

You can perform actions manually on one or more systems listed in the **Machine List**. For example, you may want to push an agent to a new rogue system, or flag computers for later follow-up action.

Types actions

The following table lists the actions you can take on selected systems in the **Machine List**.

Action	Description
Add to ePO tree	Adds a computer node to a Rogue System site beneath the Directory . You can then drag the computer into the appropriate site or group.
Mark for Action	Flags the detected computer as Mark for Action in the Machine List so you can take the appropriate action at a later time.
Mark as Exception	Flags selected computers as Exception systems in the Machine List to identify systems that don't require an agent.
Push ePO Agent	Have the ePolicy Orchestrator server push an agent to the selected computer.

Action	Description
Query ePO agent	Queries the newly-detected system to determine if there is an ePolicy Orchestrator agent installed that is managed by another ePolicy Orchestrator server. This query is required if you want to be able to use the Alien Agent rogue type in your Machine List . Systems managed by a different ePolicy Orchestrator server will appear as rogues in your environment. Using this action allows you to identify these systems.
Remove Host	Hides the detected system from the Rogue System Detection Machine List but does not delete it from the database.
Send E-Mail	Generally, only for automatic responses. Sends a user-configured e-mail to desired recipients when rogues are detected.
Send ePO Server Event	Forwards <i>Rogue System Detection</i> and <i>Subnet Uncovered</i> events to the Notification server. This is required if you plan to use the new Notification feature in ePolicy Orchestrator 3.5 to automatically send e-mail alerts for rogue detection events.
Unmark for Action	Deselects computers that you have already flagged for follow up using Mark for Action .
Unmark as Exception	Deselects computers that you have already flagged as Exceptions using the Mark as Exception action.

Configure automatic responses for specific events

You can configure automatic responses in the Rogue System Detection interface so that ePolicy Orchestrator responds automatically to the rogue system detection events. There are two 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.** There is a subnet in your network that does not have a rogue system sensor installed.

Automatic responses can be alerts, like sending an e-mail to a network administrator notifying him or her of the new detection. They can also be server actions, such as automatically adding newly-detected computers to the **Directory** or deploying an ePolicy Orchestrator agent to a newly detected rogue system. The automatic responses will occur within one minute of the event being triggered.

Example of automatic response configuration

To demonstrate how easy it is to configure an automatic response, here's an example of a response that pushes 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 Click **Add Automatic Response** to display the **Add or Edit Automatic Response** page.
- 3 Type a name for the response. For example, **Push Agent**.

- Under **Conditions**, click **Add Condition**, then select **Rogue Type** from the **Property** list.

Figure 5-2 Add or Edit Automatic Response page

The screenshot shows the 'Add or Edit Automatic Response' page. The 'Name' field contains 'Push Agent'. The 'Event' dropdown is set to 'Rogue Machine Detected'. The 'Enabled' checkbox is checked. Under the 'Conditions' section, there is a table with the following data:

Property	Comparison	Value	Delete
Rogue Type	is	No Agent	X

- Select **is** for the **Comparison**, and **No Agent** for the **Value**.
- Under **Actions**, change the default **Send E-mail** action to **Push ePO Agent** as the **Method**, and accept the default **Parameters**.
- Click **OK**.
- 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**.

Flag systems that don't need agents as Exceptions

Some of the systems that the Rogue System sensors detect, such as network switches, routers, or printers, do not require agents and therefore are not rogues. You can flag these systems as **Exceptions** to indicate they are not managed by ePolicy Orchestrator but are also not rogues. You can then easily sort or filter the **Machine List** to hide these **Exception** systems the focus stays on finding and remediating real rogues.

You can also configure rules for automatic responses to classify certain computers as exceptions. You can set an exception for a system with a state of either **Rogue** or **Inactive**. Systems in a **Managed** state already have an ePolicy Orchestrator agent installed and therefore are not exceptions.

To flag a specific computer or computers as an exception:

- On the **Machine List**, click the checkbox for one or more systems.
- From the **Checked machines** drop-down list, select **Mark as Exception** and click **Run**.
- Refresh the **Machine List** to see that the state for the selected system has been changed to **Exception**.

You can unflag systems that have already been flagged as exceptions by checking them and clicking **Unflag as Exception**.

See the *ePolicy Orchestrator 3.5 Product Guide* for more information.

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 3.5 Product Guide*.

6

ePolicy Orchestrator Notifications Alerting you to compliance and threat events

The ePolicy Orchestrator Notification feature can alert you to events that occur on the managed computers in your environment or on the ePolicy Orchestrator server itself. You can configure rules in ePolicy Orchestrator to send e-mail, SMS, text pager messages, or SNMP traps when specific events are received and processed by the ePolicy Orchestrator server. The feature is highly configurable to specify event categories that generate a notification message and the frequencies with which notifications are sent are highly configurable.

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 programs (PUPs) 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 computer infecting the rest of your environment.
- **Outbreak situations.** For example, 1,000 virus-detected events are received within five minutes.
- **Compliance events from McAfee System Compliance Profiler.** For example, computers are found that are not up-to-date 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-line applications and launch registered executables when the specified conditions are met.

How it works

When events occur on computers 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 computers and each parent above it) are applied to the events. If the conditions of any such rule are met, a notification message is sent per the rule's configurations.

This design allows you to configure similar (or very different) rules at the various levels of the console tree that may differ according to:

- **Thresholds used to send a notification message.** For example, a site administrator may want to be notified if viruses are detected on 100 computers within 10 minutes on the site, but a global administrator may not want to be notified unless viruses are detected on 1,000 computers within the same amount of time within the entire environment.
- **Recipients for the notification message.** For example, you may want only the individual site administrator to receive a notification message if a specified number of virus detection events occur within his or her site. You may also want every site administrator to receive a notification message if a specified number of virus detection events occur within the whole **Directory**.

This section includes:

- [Throttling and aggregation on page 54.](#)
- [Notification rules and the Directory scenarios on page 55.](#)
- [Rules on page 57.](#)

Throttling and aggregation

You can configure *when* notification messages are sent by setting thresholds based on *aggregation* and *throttling*. These are configured while you create (or edit) rules with the **Create or Edit Rule** wizard.

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 both when the ePolicy Orchestrator server receives 100 virus detection events from different systems within an hour *and* whenever it has received 1,000 virus detection events altogether from any system within the same time period.

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, you may be receiving tens of thousands of events during an hour, which creates thousands of notification messages based on such a rule. ePolicy Orchestrator Notification 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.

Notification rules and the Directory scenarios

To show how Notifications functions with the **Directory**, two scenarios are used.

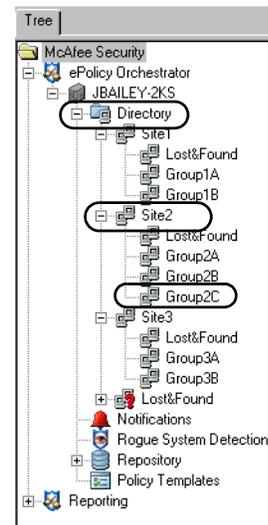
For both scenarios, we can assume that each group, site, and the **Directory** of the console tree has a similar rule configured. These rules are each configured to send a notification message when 100 virus infection events have been received from any product within 60 minutes.

Scenario one

For this scenario, 100 virus infections are detected in **Group2C** within 60 minutes on a certain day.

Conditions of these rules configured at **Group2C**, **Site2**, and the **Directory** are met, sending notification messages per the rules' configurations.

Figure 6-1 Console tree

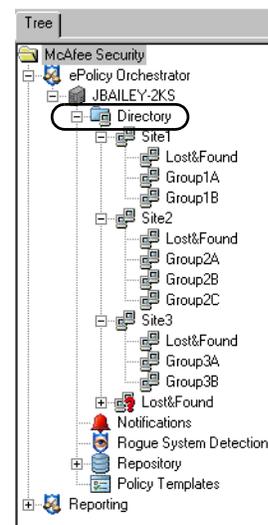


Scenario two

For this scenario, 50 virus infections are detected in **Group2C** and 50 virus infections are detected in **Group3B** within 60 minutes on a certain day.

The **Directory** is the only node whose rule can be applied to all 100 events, so only this rule of the **Directory** sends notification messages based on these 100 events.

Figure 6-2 Console tree



Planning

Before creating rules that send notifications, it can save you time to plan:

- 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 2 about a failed replication task in site 1, but you may want all site administrators to know that an infected file was discovered in site 1.
- The type and level 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-line applications 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.

This section covers:

- [Configuring ePolicy Orchestrator Notifications.](#)
- [Default rules.](#)
- [Creating rules.](#)

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 3.5 Product Guide*.

Default rules

Default rules allow you to use the feature immediately. These rules will send notification messages to the e-mail address you specify in the installation wizard.



Before using the default rules, you must configure Notifications to use your e-mail server and ensure the Administrator e-mail address is correct.

The default rules also provide the basic types of rules McAfee recommends. These default rules can be modified to meet your needs and the needs of your environment.

Descriptions of each of the default rules follow:

Daily unknown product notification

This rule sends a notification message when an event is received from any unknown product. This rule sends a notification message a maximum of once a day.

Daily unknown category notification

This rule sends a notification message when an event of an unknown category is received from any product. This rule sends a notification message a maximum of once a day.

Virus detected and not removed

This rule sends a notification message:

- When **Virus Detected and Not Removed** events are received from any product.
- When the number of events exceeds 1,000 within an hour.
- A maximum of once every two hours.
- With the source computer IP address, actual threat names, and actual product information, if available.

Virus detected heuristics and not removed

This rule sends a notification message:

- When **Virus Detected (Heuristic) and Not Removed** events are received from any product.
- When the number of events exceeds 1,000 within an hour.
- A maximum of once every two hours.
- With the source computer IP address, actual threat names, and actual product information, if available.

Repository update or replication Failed

This rule sends a notification message when any **Repository Update Failure** or **Repository Replication Failure** events are received.

Non-compliant computer detected

This rule applies to an ePolicy Orchestrator server task (**Compliance Check**) that actually contains four rules that check for compliance on: **DAT file version**, **Engine version**, **Agent version**, and **VirusScan version**. This rule can only send one event for each of these four rules each time the task runs. A **Non-compliant Computer Detected** event represents a collection of all computers found for a given rule.

This rule sends a notification message:

- When a **Non-compliant Computer Detected** event is received.
- Once for each rule of the server task.

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 3.5 Product Guide*.

Event forwarding

The ePolicy Orchestrator server receives events from the ePolicy Orchestrator agent. You must configure its policy pages to forward events either immediately to the ePolicy Orchestrator server, or during at agent-to-server communication intervals.

If you want all events sent to the ePolicy Orchestrator server immediately so that they can be processed by ePolicy Orchestrator Notification 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 that are designated by the issuing product as high priority. Other events are only sent at the agent-to-server communication intervals.

Along with being able to determine when events are forwarded to the server, you can select which events are forwarded.



If you choose not to select which events are forwarded, all events are forwarded. This is the default setting.

Configuring the agent to forward events immediately

Although not a requirement, McAfee recommends configuring the agent to send events immediately to the server if you plan to use the Notifications feature.

To set the ePolicy Orchestrator agent policy:

- 1 Select the **Directory**, or the desired site, group, or computer, then select the **Policies** tab in the upper details pane.
- 2 Select **ePolicy Orchestrator Agent | Configuration** in the upper details pane.
- 3 In the lower details pane, select the **Events** tab.
- 4 Deselect **Inherit**.

Figure 6-3 Events tab

- 5 Select **Enable immediate uploading of events** to enable the agent to forward events to the server immediately, then specify:
 - The lowest severity of events you want to send to the server in **Upload events of priority <SEVERITY> and above**. (For example, if you select **Minor**, then all events with a severity of Minor or greater are forwarded to the server.)
 - The event forwarding interval in **Interval between immediate uploads**. The amount of time you select here determines the highest frequency that events are forwarded. (For example, if you select **5 minutes**, the agent forwards events to the server every five minutes, at most.)
 - The maximum number of events to send at a time in **Maximum events per immediate upload**. (If the number of events exceeds this limit, the remaining events are sent during the next event forwarding interval.)
- 6 Click **Apply All** to save these settings. Changes take effect during the next agent-to-server communication.

Determining which events are forwarded

By selecting which events are forwarded, you can ensure that only events that concern you are sent to the ePolicy Orchestrator server. This gives greater control over the resource usage of ePolicy Orchestrator.

If you want to select which events are forwarded:

- 1 Select the desired ePolicy Orchestrator database server under **Reporting** in the console tree, and log on to 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**.

Product and component list

You can configure rules to generate notification messages for specific event categories for specific products and components. Here is a list of products and components for which you can configure rules, and a list of all possible event categories.

Products and Components Possible Event Categories

Dr. Ahn	Access Protection rule violation detected and blocked
Desktop Firewall	Access Protection rule violation detected and NOT blocked
Entercept	Banned content or file detected and NOT removed
ePO Server	Banned content or file detected and removed
ePO Agent	Computer placed in quarantine mode
GroupShield Domino	E-mail content filtered or blocked
GroupShield Exchange	Encrypted/corrupted file detected and removed
System Compliance Profiler	Firewall rule triggered
Symantec NAV	Virus detected (heuristic) and NOT removed
NetShield	Virus detected (heuristic) and removed
NetShield for NetWare	Unwanted program detected (heuristic) and NOT removed
PortalShield	Unwanted program detected (heuristic) and removed
Stinger	Intrusion detected
ThreatScan	System Compliance Profiler rule violation
Unknown product	Non-compliant computer detected
Virex	Normal operation
VirusScan	On-access scan disabled
VirusScan PDA	Policy enforcement failed
WebShield	Repository update or replication failed
LinuxShield	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
	Virus detected and removed

Viewing the history of Notifications

This feature also 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, as well as by time and site in the **Directory**.
- **Notification list** — The **Notification List** page allows you to view a list of all notifications sent. This list can be sorted by the data in any column by clicking the column title.

Getting there

To get to these pages:

- 1 Select **Notifications** under the **Directory** in the console tree.
- 2 Select the **Log** tab, then click **Summary** or **List**.

Notification details

By clicking any notification from the **Notification List** page, you can drill down to its details. These can include:

- | | |
|----------------------------------|---------------------------------|
| ■ Time notification sent | ■ Notification rule name |
| ■ Rule priority | ■ Rule site |
| ■ First event time | ■ Rule defined at |
| ■ Actual number of events | ■ Actual products |
| ■ Number of computers | ■ Selected products |
| ■ Affected computer IP addresses | ■ Actual categories |
| ■ Affected computer names | ■ Selected categories |
| ■ Source computers | ■ Actual threat or rule names |
| ■ Notification status | ■ Selected threat or rule names |
| ■ Notification type | ■ Message subject |
| ■ Event IDs | ■ Event descriptions |
| ■ Affected objects | ■ 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.

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.

ePolicy Orchestrator can help reduce the costs of managing an outbreak.

What's in this section

You can use ePolicy Orchestrator 3.5 to help be prepared for, then manage virus outbreaks when they occur:

- [Things to do daily or weekly to stay prepared](#)
- [Are you prepared for an outbreak?](#)
- [Other methods to recognize an outbreak](#)
- [You think an outbreak is occurring](#)

Things to do daily or weekly to stay prepared

You can use features of ePolicy Orchestrator 3.5 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 and client tasks to run scans and keep client software current with the latest updates. It will take you some time initially to configure and schedule these tasks, but then 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.

Server task	Description
Daily DAT & engine pull task	Performs a repository pull for updated weekly DAT or engine files from the default source repository on the McAfee FTP site. The task is scheduled to run 4 times every day, starting at 1 am. Repeat task is selected to repeat the task every 6 hours, so it occurs 4 times a day.
Daily incremental repository replication	Replicates only changes to the master repository to all distributed repositories. It is scheduled to mirror the pull task by running 4 times a day, one hour after each repository pull (first one runs at 2 am).
Weekly full repository replication	Runs once each week 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	Scans the Directory for computers with agents that have not communicated with the server and places them in an "InactiveAgents" group.

Schedule client update and scan tasks to keep clients protected

To keep anti-virus and security software on client computers up-to-date, make sure you have the right client tasks created and scheduled for the appropriate parts of your **Directory**.

Client task	Task type	Description
Daily engine and DAT client update task	ePolicy Orchestrator agent Update	Updates DAT files every day for products using the common updater, such as VirusScan Enterprise. Also updates anti-virus engines. McAfee releases new engines once every 2-3 months. However, consolidating these updates means fewer tasks to manage. The task is scheduled to run 4 times every day, starting at 3 am, one hour after your replication server task. Repeat task is selected to repeat the task every 6 hours, so it occurs 4 times a day. In the Task Settings , select only DAT, EXTRA.DAT, and Engine only. You will update these the most often.
Weekly agent patch and service pack update	ePolicy Orchestrator agent Update	Updates the agent and security products like VirusScan Enterprise or Desktop Firewall with patches and service packs. Run the task once per week. In the Task Settings , select all the Service Pack and Patch types. You will update these the most often.
Daily VirusScan 8.0i update	VirusScan for Windows AutoUpdate	Updates DAT files daily for Windows 95, Windows 98, and Windows ME clients using VirusScan Enterprise. Schedule it to run several times a day.
Daily VirusScan 8.0i On-Demand Scan	VirusScan for Windows On-Demand Scan	Runs a daily on-demand scan for VirusScan Enterprise.
Daily update task for Novell NetWare servers	NetShield for NetWare 4.6 On-Demand Scan	Updates NetShield for NetWare on Novell NetWare servers.

Are you prepared for an outbreak?

- Know your network, what creates traffic, and how much traffic is usually created.
- The ePolicy Orchestrator software is fully installed and implemented.
- An anti-virus software product is installed and configured on your computers. For example, McAfee VirusScan Enterprise 8.0i.
- Your anti-virus software is up-to-date with the latest 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 ePolicy Orchestrator 3.5 reports to determine coverage. For more information and instructions, see the *ePolicy Orchestrator 3.5 Report and Template Reference*.
- 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 computers 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 computers are compliant to the latest Microsoft patches and service packs.
- You have configured ePolicy Orchestrator Notification to send a message to you or others when specified events (such as a virus detection) are received and processed by the ePolicy Orchestrator server.
- The Rogue System Detection feature is implemented to recognize and deploy agents to rogue computers and devices coming on to your network.
- You are performing regular, scheduled updates of products through ePolicy Orchestrator.
- You have enabled the agent wakeup call and tested the agent's communication with the computers 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 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. Computers 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 increases 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:

- 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.
- ePolicy Orchestrator Notifications alerts 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.

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 information on viruses and threats.
- 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 computer.

- 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 are not running a McAfee anti-virus product or do not have the ePolicy Orchestrator agent deployed to each computer, you must manually scan the system or computer using the command-line scanner.

Troubleshooting ePolicy Orchestrator 3.5 Using Log Files

This document describes how to troubleshoot ePolicy Orchestrator 3.5 using log files, and provides the following information:

- The name and location of each log file.
- The types of issues recorded in each log file and when to analyze them.
- The format of the debug logs.
- How to control the level of logging in the debug and other log files.
- How to set the maximum size of the debug log files.
- How the debug log 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 3.5 log file.

Log file name	Location
AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG	<AGENT DATA PATH>\DB
EPOAUDIT.LOG	<INSTALLATION DRIVE>\EPOAUDIT
CLEANUP_<COMPUTER>.LOG, CLEANUP_<COMPUTER>_BACKUP.LOG	<WINDOWS DIRECTORY>\NAI LOGS
CONSOLE.LOG, CONSOLE_BACKUP.LOG	<INSTALLATION PATH>
DBINIT.LOG	<WINDOWS DIRECTORY>\NAI LOGS
EVENTPARSER.LOG, EVENTPARSER_BACKUP.LOG	<INSTALLATION PATH>
FRMINST_<COMPUTER>.LOG, FRMINST_<COMPUTER>_BACKUP.LOG	<WINDOWS DIRECTORY>\NAI LOGS
LICENSING.LOG	<WINDOWS DIRECTORY>\NAI LOGS
LOCAL_HOST.<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>
ROGUE.LOG	<INSTALLATION PATH>\TOMCAT\LOGS
SERVER.LOG, SERVER_BACKUP.LOG	<INSTALLATION PATH>
SITEMGR.LOG, SITEMGR_BACKUP.LOG	<INSTALLATION PATH>
TRACE.LOG	<WINDOWS DIRECTORY>\NAI LOGS

<AGENT DATA PATH>

The default location of the agent data files is:

<DOCUMENTS AND SETTINGS>\ALL USERS\APPLICATION DATA\NETWORK ASSOCIATES\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. For more information, see *Agent installation directory* in the *ePolicy Orchestrator 3.5 Product Guide* or *Help*.

<AGENT INSTALLATION PATH>\DATA

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

HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TV\SHARED COMPONENTS\FRAMEWORK\DATA PATH

<WINDOWS DIRECTORY>

The location of the Windows program files; for example, WINNT.

<INSTALLATION PATH>

The default location of the ePolicy Orchestrator 3.5 server and console software is:

C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3

If you upgraded the software from 2.0, 2.5, or 2.5.1, the default location is:

C:\PROGRAM FILES\MCAFFEE\EPO\2.0

When to analyze each log file

This table identifies the type of issues recorded in each ePolicy Orchestrator 3.5 log file to help you determine when to analyze each log file.

If issues with...	See these log files...
Agent (general issues)	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.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
Console setup	TRACE.LOG
Events, Event Update	EVENTPARSER.LOG, EVENTPARSER_BACKUP.LOG
Licensing	LICENSING.LOG
Notifications	NOTIFICATIONS.LOG, LOCALHOST_LOG.TXT
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
Product Property Update	EVENTPARSER.LOG, EVENTPARSER_BACKUP.LOG
Pull now	CONSOLE.LOG, CONSOLE_BACKUP.LOG
Replicate now	CONSOLE.LOG, CONSOLE_BACKUP.LOG REPLICATION.LOG
Repository Pull server tasks	SITEMGR.LOG, SITEMGR_BACKUP.LOG

If issues with...	See these log files...
Repository Replication server tasks	SITEMGR.LOG, SITEMGR_BACKUP.LOG REPLICATION.LOG
Rogue system detection	ROGUE.LOG, LOCALHOST_LOG.TXT
Script engine, script messages	MCSCRIPT.LOG
Server (general issues)	SERVER.LOG, SERVER_BACKUP.LOG
Server installation	DBINIT.LOG TRACE.LOG
Server setup	TRACE.LOG
Updating	AGENT_<COMPUTER>.LOG, AGENT_<COMPUTER>_BACKUP.LOG

Debug logs

Except where noted, the following 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
- SITEMGR.LOG

What are debug logs?

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

What are 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. Each column is described below.

```

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   UsrSpcCont       Enforcing policies
20021231113407      i   Agent            Agent finished Enforcing policies
20021231113407      i   Agent            Next policy enforcement in 5 minutes
    
```

Figure 1-1. Example of the AGENT_<COMPUTER>.LOG file

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 is shown using the 24-hour clock.

Column 2 — Message type

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

Table 1-1. Message types and logging level

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.”

How do you control 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 listed in [Table 1-1](#).
- 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 quite a bit of output, including every SQL query that is done, 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.

How do turn 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.

How do you control 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, 2 = 2MB, etc.
- The default size is 1MB.
- For information on what happens when the maximum size is reached, see [What are the “_backup” debug logs? on page 5.](#)

When does a change in logging level take effect?

For this log file...	Change in logging level takes effect...
AGENT_<COMPUTER>.LOG	Once per minute
CLEANUP.LOG	Always level 7, 1MB
CONSOLE.LOG	On startup
DBINIT.LOG	On startup
EVENTPARSER.LOG	Once per minute
FRMINST.LOG	Always level 7, 1MB
PRDMGR_<COMPUTER>.LOG	Once per minute
SERVER.LOG	Once per minute
SITEMGR.LOG	Once per minute

How does the agent debug log relate to 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 3.5 Product Guide* or *Help*. (There is a known issue where the instructions for viewing agent activity log files remotely don't match the user interface.)

How do the debug logs relate to AVIView?

- AVIView shows the same information as the debug log files.
- AVIView gives you the ability to view all of the log files merged together.
- AVIView has an additional “system” column inserted between the log level and the component. In this example AVIView line, the system is “Srv”:

```
20030102182201 I Srv EPOServer Processing Console Request...
```

The system can be one of:

- ◆ **Cns** — Console
- ◆ **Fsv** — Framework Service
- ◆ **Pmg** — Product Manager
- ◆ **Srv** — Server and Event Parser
- ◆ **Ins** — Framework Installer

- Here is an example AVIView log with comments:

- ◆ The console (Cns) sends a message via HTTP to tell the server to schedule a task:

```
20030102182154    i    Cns    InetMgr    Downloading a file from HTTP
server, HTTP return code:
HTTP/1.0 200 OK
20030102182154    i    Cns    InetMgr
20030102182154    i    Cns    InetMgr    HTTP Session closed
```

- ◆ Then in the framework (Fsv), the scheduler starts the task:

```
20030102182200    i    Fsv    Scheduler  (332)Scheduler: Invoking task
[123]...
20030102182200    I    Fsv    Scheduler  (3780)>>--RunTask
20030102182200    I    Pmg    Management Running task
SoftwareID:EPOSERV_3000,
TaskID:{9B0CEB87-693C-43E2-BA5E
-630BA4135E5A}
```

- ◆ The server plug-in starts enforcing the task:

```
20030102182200    I    Pmg    EPOSRVSP  EnforceTaskW
20030102182200    I    Pmg    EPOSRVSP  cookie = 0xe4f4c0
```

- ◆ The scheduler finishes starting the task:

```
20030102182200    I    Fsv    Scheduler  (3780)<<--RunTask
20030102182200    I    Fsv    Scheduler  (332)123 - Last run time is Thu
Jan 02 18:22:00 2003
20030102182200    I    Fsv    Scheduler  (Local)
20030102182200    I    Fsv    Scheduler  (332)NTTR(Local) Fri Jan 03
18:22:00 2003
20030102182200    I    Fsv    Scheduler  (332)NTTR( UTC ) Fri Jan 03
18:22:00 2003
20030102182200    I    Fsv    Scheduler  (332)End of invoking the task
```

- ◆ The task (domain synchronization as it turns out) starts running on the server (Srv):

```
20030102182200    I    Srv    DOMSYNCH  Start
20030102182200    I    Srv    DOMSYNCH
credential=EPO;EPO\administrator;k5rwsEfem/1nY6QN0sVexH9psAU8z0HbZ20kDTrF
XsR/abAFPM9B3Q==
```

- ◆ The server plug-in checks the status of the task:

```
20030102182200    I   Pmg   EPOSRVSP   GetTaskStatus 0x1150f70
20030102182200    i   Fsv   Scheduler  (328)The task 123 is still
running
20030102182201    I   Pmg   EPOSRVSP   GetTaskStatus 0x1150f70
```

- ◆ The server tries to push the agent, but it fails – this is the source of the problem!

```
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!
```

How do the debug logs relate to the VirusScan Enterprise 8.0 UPDATELOG.TXT file?

- The McAfee VirusScan Enterprise 8.0 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 8.0 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 were available on the following MSDE web site. You can also use the ERRLOOK.EXE utility to determine the cause of these error codes. This utility is distributed with Microsoft Visual Studio.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp

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, a literal description of the issue is provided, which gives you more detailed information about the cause of the issue:

Logon failure: unknown user name or bad password.

