

McAfee ePolicy Orchestrator 4.0 Installation Guide

COPYRIGHT

Copyright © 2007 McAfee, Inc. All Rights Reserved.

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

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, MCAFFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT 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.

License Attributions

Refer to the product Release Notes.

Contents

Pre-Installation	5
System requirements.....	5
Server requirements.....	5
Database considerations.....	7
Distributed repositories.....	8
Agent and SuperAgent requirements.....	9
Requirements for agents in non-Windows environments.....	10
Operating systems language support.....	10
Supported products and components.....	10
First-Time Installation	12
Installing the server.....	12
Migrating to a licensed version.....	15
Tips for installing SQL Server.....	15
Upgrading to ePolicy Orchestrator 4.0	16
Unsupported products.....	16
Backing up ePolicy Orchestrator databases.....	17
Microsoft SQL Server.....	17
MSDE.....	17
Upgrading the server.....	17
Migrating to a licensed version.....	20
Post-Installation Tasks	21
Completing a first-time installation.....	21
Completing an upgrade.....	21
Migrating events from an earlier version.....	22
Checking in files manually.....	22
Configuring the software for a server with multiple NICs.....	23
Uninstalling the software.....	23
Troubleshooting	24
Common installation messages and their solutions.....	24
Default locations of troubleshooting log files.....	27

Installing in a cluster environment.....	29
Requirements.....	29
Setting up the ePolicy Orchestrator cluster.....	29
Installing ePolicy Orchestrator on each node.....	30
Creating the ePolicy Orchestrator group.....	30
Creating the data drive.....	30
Creating the IP address resource.....	31
Creating the Network Name resource.....	31
Creating the Generic Service resources.....	31
Testing the ePolicy Orchestrator cluster.....	32

Pre-Installation

Review these requirements and recommendations before installing ePolicy Orchestrator 4.0.

Contents

- ▶ [System requirements](#)
- ▶ [Supported products and components](#)

System requirements

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

- ▶ [Server requirements](#)
- ▶ [Database considerations](#)
- ▶ [Distributed repositories](#)
- ▶ [Agent and SuperAgent requirements](#)
- ▶ [Requirements for agents in non-Windows environments](#)
- ▶ [Operating systems language support](#)

Server requirements

Hardware and network requirements

- **Free disk space** — 1GB minimum (first-time installation); 1.5GB minimum (upgrade); 2GB recommended.
- **Memory** — 1GB available RAM; 2-4GB recommended.
- **Processor** — Intel Pentium III-class or higher; 1GHz or higher.
- **Monitor** — 1024x768, 256-color, VGA monitor.
- **NIC** — Network interface card; 100Mb or higher.
- **Dedicated server** — If managing more than 250 computers, McAfee recommends using a dedicated server.
- **File system** — NTFS (NT file system) partition recommended.
- **IP address** — McAfee recommends using static IP addresses for ePolicy Orchestrator servers.

Software requirements

- **Operating system**

- Windows 2000 Advanced Server with Service Pack 4 or later.
- Windows 2000 Server with Service Pack 4 or later.
- Windows Server 2003 Enterprise with Service Pack 1 or later.
- Windows Server 2003 Standard with Service Pack 1 or later.
- Windows Server 2003 Web with Service Pack 1 or later.
- Windows Server 2003 R2 Enterprise.
- Windows Server 2003 R2 Standard.
- **Browser**
 - Microsoft Internet Explorer 6.0 with Service Pack 1 or later.
 - Microsoft Internet Explorer 7.0.
 - If using a proxy, bypass the proxy server:
 - 1** In Internet Explorer, select **Internet Options** from the **Tools** menu.
 - 2** Select the **Connections** tab and click **LAN Settings**.
 - 3** Select **Use a proxy server for your LAN**, then select **Bypass proxy server** for local addresses.
 - 4** Click **OK** as needed to close Internet Options.
- **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.
- **Security software**
 - Install and/or update the anti-virus software on the ePolicy Orchestrator server and scan for viruses.

CAUTION: If running VirusScan Enterprise 8.5i on the system on which you are installing ePolicy Orchestrator, you must ensure the VSE Access Protection rules are disabled during the installation process, or the installation fails.
 - Install and/or update firewall software on the ePolicy Orchestrator server.
- **Ports**
 - McAfee recommends avoiding the use of Port 80 for HTTP communication via ePolicy Orchestrator because it is the primary port used by many web-based activities; it is a popular target for malicious exploitation; and it is likely to be disabled by the system administrator in response to a security violation or outbreak.

NOTE: Ensure that the ports you choose are not already in use on the ePolicy Orchestrator server computer.
 - Notify the network staff of the ports you intend to use for HTTP and HTTPS communication via ePolicy Orchestrator.

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

Supported virtual infrastructure software

- VMware ESX 3.0.x
- Microsoft Virtual Server 2005 R2

Database considerations

Using ePO with a database

A database must be installed before ePO can be installed.

- Any of the following databases, if previously installed, meets this requirement.
 - SQL Server 2005
 - MSDE 2000
 - SQL 2000
- If none of those databases was previously installed, the ePO installation wizard detects that no database is present and offers you the opportunity to install SQL Server 2005 Express.
- The following tables provide additional information about the database choices and other software requirements.

Database	Requirements	Note
SQL Server 2005	Dedicated server and network connection Local database server Licenses	Needed if managing more than 5,000 computers. If the database and ePO server are on the same system, McAfee recommends using a fixed memory size in Enterprise Manager that is approximately two-thirds of the total memory for SQL Server. For example, if the computer has 1GB of RAM, set 660MB as the fixed memory size for SQL Server. A license is required for each processor on the computer where SQL Server is installed. If the minimum number of SQL Server licenses is not available, you may have difficulty installing or starting the ePolicy Orchestrator software.
MSDE 2000	Service Pack 3	Ensure that the database is not installed on a backup domain controller (BDC).
SQL Server 2000	Service Pack 3	Ensure that the database is not installed on a backup domain controller (BDC).
SQL Server 2005 Express	NET Framework	You must acquire and install.

Software	Note
MSXML 6.0	You must acquire and install. <ol style="list-style-type: none"> 1 From the Internet Explorer Tools menu, select Windows Update. 2 Click Custom, then select Software. 3 Select MSXML6. 4 Select Review and install updates, then click Install Updates.
Internet Explorer 6 SP1 or later	You must acquire and install.
.NET Framework 2.0	You must acquire and install if using SQL Server 2005 Express.
MDAC 2.8	If not previously installed, the installation wizard installs automatically.
SQL Server 2005 Backward Compatibility	If not previously installed, the installation wizard installs automatically.

Software	Note
SQL Server 2005 Express	If no other database has been previously installed, this database can be installed automatically at user's selection.
Microsoft updates	Update the ePolicy Orchestrator server and the database server with the most current updates and patches.
MSI 3.1	The installation fails if using a version of MSI previous to MSI 3.1.

NOTE: Using ePolicy Orchestrator 4.0 with MSDE 7 or SQL 7 is not supported.

Database installation documented in this guide

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

Other relevant database installations and upgrades

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

- Installing SQL Server 2005.
- Upgrading from MSDE to SQL Server 2005.
- Upgrading from MSDE 2000 to SQL Server 2005.
- Upgrading from MSDE 2000 to SQL Server 2005 Express.
- **Maintenance settings** — McAfee recommends making specific maintenance settings to ePolicy Orchestrator databases. For instructions, see *Maintaining ePolicy Orchestrator databases* in the *ePO 4.0 Help*.
- **Remote database server** — Microsoft Data Access Components (MDAC) 2.8.

SQL Server

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

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

Distributed repositories

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

- **Possible hosts:**
 - HTTP-compliant 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.

Agent and SuperAgent requirements

Hardware and network requirements

- **Processor** — Intel Pentium-class, Celeron, or compatible processor; 166MHz processor or higher.
- **Free disk space (agent)** — 100MB.
- **Free disk space (products)** — Sufficient disk space on client computers for each McAfee product that you plan to deploy. For more information, see the corresponding product documentation.
- **Memory** — 20MB RAM.
- **Network environment** — Microsoft or Novell NetWare networks. NetWare networks require TCP\IP.
- **NIC** — Network interface card; 10Mb or higher.

Software requirements

- **Citrix** — These Citrix products are supported on operating systems that ePolicy Orchestrator supports:
 - Citrix Metaframe 1.8 for Windows.
 - Citrix Metaframe XP for Windows.
- **Cluster** — If using cluster services, Microsoft Cluster Server (MSCS) is supported. The following information is required during installation. It is advantageous to have this information available before starting the installation.
 - The ePO virtual server IP address.
 - The ePO virtual server name.
 - the ePO virtual server DNS name.
 - The location on DATA drive where you intend to place the ePO Cluster folder.
- **Operating system** — Agent versions 3.5.5 and 3.6 support 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 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 Vista (supported by ePO agent 3.6 only).

NOTE: The disk space requirement for the distributed repositories on agents that are designated as SuperAgents is equal to the disk space available for the master repository.

Requirements for agents in non-Windows environments

Non-Windows operating systems have agent support as follows:

Operating System	Support
• Linux Red Hat Enterprise	• ePO Agent 3.7
• Solaris 8, 9, 10	• ePO Agent 3.7
• Macintosh (before Leopard)	• Non-Windows agent 3.0.2
• Linux (for use with Linux Shield)	• Non-Windows agent 3.0.1
• Novell NetWare	• Non-Windows agent 2.1.1

Operating systems language support

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

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

Supported products and components

Supported products:

- McAfee VirusScan Enterprise 8.0i with McAfee AntiSpyware Enterprise 8.0
- McAfee VirusScan Enterprise 8.5i with McAfee AntiSpyware Enterprise 8.5
- McAfee ePO agent 3.5.5
- McAfee ePO agent 3.6
- McAfee ePO agent 3.7

- McAfee GroupShield for Lotus Domino 7.0
- McAfee GroupShield for Exchange 6.0.2, 6.0.3 (with SpamKiller)
- McAfee GroupShield for Exchange 7.0
- McAfee Host Intrusion Prevention 7.0
- McAfee Virex 7.7
- McAfee VirusScan for Mac 8.5, 8.6
- McAfee LinuxShield 1.3, 1.4, 1.5
- McAfee SiteAdvisor Enterprise 1.5
- Non-Windows Agent for Virex
- Non-Windows Agent for LinuxShield

First-Time Installation

This chapter provides instructions for installing ePolicy Orchestrator 4.0 in an environment where no previous version of ePolicy Orchestrator software has been installed.

CAUTION: If you are upgrading from a prior version of ePolicy Orchestrator or are migrating from evaluation versions, see the Upgrading to ePolicy Orchestrator 4.0 chapter.

Be sure that you have read, understood, and complied with the requirements and recommendations in the Pre-Installation chapter.

Contents

- ▶ [Installing the server](#)
- ▶ [Migrating to a licensed version](#)
- ▶ [Tips for installing SQL Server](#)

Installing the server

McAfee recommends that you monitor the installation process. It may require you to restart the system.

Task

- 1** Log on to the desired system 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 is running. For instructions, see the Microsoft product documentation.
 - Verify TCP/IP is enabled in SQL Server. Launch **Server Network Utility** in SQL and verify **TCP/IP** is listed under **Enabled Protocols**
- 3** Run SETUP.EXE.
 - From the product CD: select the desired language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.0**.
 - From software downloaded from the McAfee website, go to the location containing the extracted files and double-click SETUP.EXE.

NOTE: If any prerequisite software is missing from the installation target computer, a list of those items appears. Click **Install**. The installation process for each software item not listed as **Optional** begins automatically. For optional items, a dialog box appears where you can allow installation or reject it.

- 4** Click **Install**. The installation process for each software item not listed as **Optional** begins automatically. For optional items, a dialog box appears where you can allow installation or reject it.

If you intend to use an existing instance of SQL Server 2005, MSDE 2000 or SQL 2000, you can reject the installation of SQL Server 2005 Express.

If you do not have a supported version of SQL or MSDE, take one of the following actions:

- Install a database.
- Install SQL Server 2005 Express on the same computer where ePolicy Orchestrator is to be installed.
- Install SQL Server 2005 Express on a remote computer before proceeding with the ePolicy Orchestrator installation. To do so, start the process on that computer. Accept the opportunity to install SQL Server 2005 Express. When it is installed, terminate the installation of ePolicy Orchestrator.

NOTE: If installing ePolicy Orchestrator with SQL 2005, the SQL Browser must be enabled or you cannot complete the installation wizard.

5 The **Welcome** window of the ePolicy Orchestrator Installation Wizard appears. Click **Next**.

6 In the **End User License Agreement** dialog box, select the appropriate license type and the location where you purchased the software. The license type must match the license you purchased. If you are unsure, contact the person who sold you the software.

7 Accept the agreement and click **OK** to continue. The **Choose Destination Location** dialog box appears.

8 Accept the default installation path or click **Browse** to select a different location. If the location does not yet exist, type the path of the intended location in the **Browse** dialog box, then click **Next**.

9 If installing on a cluster server, the **Set Database and Virtual Server Settings** dialog box appears. Otherwise the **Set Administrator Information** dialog box appears.

10 Type and verify the password for logging on to this ePolicy Orchestrator server. Click **Next**.

11 Use the **Set Database and Virtual Server Settings** dialog box if your environment employs Microsoft Cluster Server (MSCS) to provide a high availability system ensuring failover support.

CAUTION: If you are not installing ePolicy Orchestrator on a cluster server, the Set Database and Virtual Server Settings dialog box does not appear.

12 Click **Next**. Type and verify the password for logging on to this ePolicy Orchestrator server. Click **Next**.

13 In the **Set Database Information** dialog box, identify the type of account and authentication details that the ePolicy Orchestrator server will use to access the database.

a Use the drop-down list to select the desired server. If SQL Express was installed, the name of the database is: <computername>\EPOSERVER.

b Select the type of authentication (McAfee recommends using Windows authentication):

- **Windows authentication:** Specify the NetBIOS name of the **Domain** associated with the desired domain administrator user account. Then, provide and verify a password.

- **SQL authentication:** Provide the **User name** that the ePolicy Orchestrator software will use to access the database. Then provide a password. If the installer cannot identify the port used for communication to and from the server, you may be prompted to

provide that information. Otherwise, the SQL server TCP port field shows the port and is disabled

NOTE: If you are installing on a system with a local SQL 2005 database server, you must type the TCP port number on the **Set Database Information** page of the installation wizard.

14 Click **Next**.

15 Set the **HTTP Configuration**. Designate the port to be used by each function, then click **Next**.

Function	Port
Agent-to-Server communication port	Configurable. McAfee recommends using a port other than 80.
Agent Wake-Up communication port	Configurable.
Agent Broadcast communication port	Configurable port used to send SuperAgent wakeup calls.
Event Parser-to-Server communication port	Configurable.
Console-to-Application Server communication port	Configurable.
Sensor-to-Server communication port	Configurable port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL.
Security Threats communication port	Port 8801. Non-configurable port used by McAfee Avert to provide information on security threats and the required DAT and engine versions to protect against them.
SQL server TCP port	Port 1433. Non-configurable.

16 In the **Default Notification Email Address** dialog box, configure the recipient of ePolicy Orchestrator notification or leave the default. For a new recipient, complete these options:

- a** Provide default destination for messages.
- b** Select **Setup email server settings now**. If you choose **Setup email server settings later**, leave the default address.
- c** Type the Fully Qualified domain Name (FQDN) of the mail server and specify the **Port** to use for email.
- d** Select **This server requires authentication** if needed, then type the **User name** and **Password** required to access the server.
- e** Click **Next**.

For more information, see the Notifications chapter in the **ePolicy Orchestrator 4.0 Product Guide**.

17 In the **Set Windows Authentication** dialog box, specify the **WINS server** or **Domain** to be used with ePolicy Orchestrator, then click **Next**.

18 In the **Start Copying Files** dialog box, click **Install** to begin the installation.

- 19 In the **Installation Complete** dialog box, view the ReadMe file for the steps to start the software, then click **Finish** to complete the installation.

NOTE: The installation procedure also installs the version of ePO agent that is appropriate to your operating system (version 3.6 or version 3.7).

Migrating to a licensed version

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

Task

- 1 To migrate any pre-release software to a licensed version, you must first uninstall the existing version of the software.
- 2 Log on to the desired computer using an account with local administrator permissions.
- 3 Start the setup program:
If you downloaded the software from the McAfee website, go to the location where you extracted all the files and double-click SETUP.EXE.

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

If installing the software from the product CD:

- a Insert the CD into the CD-ROM drive of the computer.
 - b In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 4.0**.
- 4 In the **ePolicy Orchestrator 4.0 Setup** wizard, click **Next** to begin the migration.

Tips for installing SQL Server

This guide does not provide complete instructions for installing SQL Server; refer to SQL Server documentation. The following tips are specific to the functioning of the ePO server.

In this dialog box...	Take this action...
Registration Information	<ul style="list-style-type: none">• Deselect Hide Advanced Configuration Options
Feature Selection	<ul style="list-style-type: none">• Database Services Entire feature will be installed on local hard drive Installing other components is optional.
Instance Name	<ul style="list-style-type: none">• Named instance. (Ensure that EPOSERVER appears in the text box.)
Service Account	<ul style="list-style-type: none">• Use the built-in System account
Authentication Mode	<ul style="list-style-type: none">• Mixed Mode Authentication• Set the SA Logon password
User Instances (SQL Express)	<ul style="list-style-type: none">• Deselect Enable User Instances

NOTE: If you are installing SQL Server 2005 Express, you may be prompted to install SQL Server 2005 Backward Compatibility. You must install it.

Upgrading to ePolicy Orchestrator 4.0

Contents

- ▶ [Unsupported products](#)
- ▶ [Backing up ePolicy Orchestrator databases](#)
- ▶ [Upgrading the server](#)
- ▶ [Migrating to a licensed version](#)

Unsupported products

The following products are no longer supported in version 4.0 and are not migrated.

AntiSpyware Enterprise 8.5 Standalone	Outbreak Manager 4.6	Virex 8.0
Desktop Firewall 8.0, 8.5	PortalShield 1.0	VirusScan 4.x
Dr. Ahn V3 Pro 2002 Deluxe	Quarantine Manager	VirusScan Enterprise 7.x
Entercept 5.x	NetShield 4.6.2 for NetWare	VirusScan for Net App 7.1
ePO Agent 3.0.2, 3.5.0	Secure Content Management 4.0,4.2 for e series and 3000 appliances	WebShield 3.0 for e series and 3000 appliances
GroupShield Domino 5.2.1, 5.3	Secure Content Management 4.5	WebShield 3.0 for e series and 3000 appliances
GroupShield Domino 5.3	System Compliance Profiler 1.1, 1.2	WebShield 5.0 SMTP
Host Intrusion Prevention 6.0.x	McAfee Policy Enforcer 1.1, 2.0, 2.5	

Removing unused consoles

Earlier versions of ePolicy Orchestrator provided the option of installing remote consoles . If remote consoles are present, use Windows Add/Remove programs feature to remove them.

Backing up ePolicy Orchestrator databases

Before you upgrade to version 4.0, back up all ePolicy Orchestrator databases:

- ▶ [Microsoft SQL Server](#)
- ▶ [MSDE](#)

Microsoft SQL Server

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

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 servers using this utility. This tool cannot change the database location.

Task

- 1** Stop the **McAfee ePolicy Orchestrator 3.6.1 Server** service and ensure that the SQL Server service is running.
- 2** Double-click DBBAK.EXE.
 - If you are upgrading from version 3.6.1, the default location is:
C:\PROGRAM FILES\NETWORK ASSOCIATES\EPO\3.6.1
 - If you are upgrading from ProtectionPilot 1.5 (after it has been upgraded to ePolicy Orchestrator 3.6.1) the default location is:
C:\PROGRAM FILES\NETWORK ASSOCIATES\PROTECTION PILOT\EPO\3.6.1
- 3** Type the **Database Server Name**.
- 4** Select **NT Authentication** or **SQL Account**.
If you select **SQL Account**, type a user **Name** and **Password** for this database.
- 5** Type the **Backup File path**, then click **Backup**.
- 6** Click **OK** when the backup process is done.
- 7** Start the **McAfee ePolicy Orchestrator 3.6.1 Server** service and ensure that the SQL service is running.

Upgrading the server

McAfee recommends that you monitor the upgrade process. It may require you to restart the system.

This task upgrades the ePolicy Orchestrator server from ePolicy Orchestrator version 3.6.1 and ProtectionPilot version 1.5, after it has been upgraded to ePolicy Orchestrator 3.6.1. This upgrade also installs the agent on the server system. The default location of the agent on ePolicy Orchestrator ePolicy Orchestrator 3.6.1 or higher and ProtectionPilot 1.5 or higher is:

C:\PROGRAM FILES\MCAFFEE\EPOLICYORCHESTRATOR

NOTE: The installation process may require you to restart the system.

Task

- 1 Log on to the desired computer using an 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 is running. For instructions, see the Microsoft product documentation.
- 3 Run SETUP.EXE.
 - From the product CD, select the desired language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.0**.
 - From software downloaded from the McAfee website, go to the location containing the extracted files and double-click SETUP.EXE.

NOTE: If any prerequisite software is missing from the installation target computer, a list of those items appears. Click **Install**. The installation process for each software item not listed as **Optional** begins automatically. For optional items, a dialog box appears where you can allow installation or reject it.

NOTE: You must install the SQL 2005 Backwards Compatibility package before upgrading an ePolicy Orchestrator installation if you are using a remote database server or a local SQL 2005 server that does not already have it installed.

- 4 After completing prerequisite installations, the **Welcome** window of the ePolicy Orchestrator Installation wizard appears. Click **Next** to review the license.
- 5 In the **End User License Agreement** dialog box, select the appropriate license type and the location where 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.
- 6 Accept the agreement and click **OK** to continue. A warning message notifies you which products are no longer supported with this version of the software. These products are not migrated to the ePolicy Orchestrator 4.0 **Repository** when you click **Next**.
- 7 In the **Choose Destination Location** dialog box, accept the default installation path or click **Browse** to select a different location, then click **Next**.
- 8 If installing on a cluster server, the **Set Database and Virtual Server Settings** dialog box appears. Otherwise the **Set Administrator Information** dialog box appears.
- 9 In the **Set Administrator Information** dialog box, type and verify the password for logging on to this ePolicy Orchestrator server for the first time, then click **Next**. For security reasons, ePolicy Orchestrator does not allow accounts with blank passwords.
- 10 In the **Set Database Information** dialog box, identify the type of account and authentication details that the ePolicy Orchestrator server will use to access the database. Indicate whether ePolicy Orchestrator will use a Windows NT user account or a SQL Server user account. McAfee recommends using Windows NT authentication.

NOTE: The name of the database server that was set during the original installation cannot be changed here.

- If you select **Windows authentication**, specify the NetBIOS name of the **Domain** associated with the desired domain administrator user account. Then, provide and verify a password.

- If you select SQL authentication, provide the **User name** that ePolicy Orchestrator will use. Then provide a password. If the installer cannot identify the port used for communication to and from the server, you may be prompted to provide that information. Otherwise, the SQL server TCP port field shows the port and is disabled.

When upgrading an installation using NT authentication, the **Set Database Information** panel of the wizard appends the domain name to the **User name** field and auto-populates the port field with 1433. For the installation to succeed, you must progress past this page. Remove the domain from the user name field and click **Next**. You will receive a port error. Dismiss this error and manually retype the port number 1433 and click **Next**.

- For security reasons, ePolicy Orchestrator does not accept accounts with blank passwords.

NOTE: If you are installing on a system with a local SQL 2005 database server, you must manually enter the TCP port number on the **Set Database Information** page of the installation wizard.

- 11 Click **Next** to display the **HTTP Configuration** dialog box. The values that were set during the original installation cannot be changed here.

Function	Port
Agent-to-Server communication port	Configurable. McAfee recommends using a port other than 80.
Agent Wake-Up communication port	Configurable.
Agent Broadcast communication port	Configurable port used to send SuperAgent wake up calls.
Event Parser-to-Server communication port	Configurable.
Console-to-Application Server communication port	Configurable.
Sensor-to-Server communication port	Configurable port used by the Rogue System Detection sensor to report host-detected messages to the Rogue System Detection server using SSL.
Security Threats communication port	Port 8801. Non-configurable port Used by McAfee Avert to provide information on security threats and the required DAT and engine versions to protect against them
SQL server TCP port	Port 1433. Non-configurable.

- 12 Click **Next**. In the **Default Notification Email Address** dialog box, type the email address for the recipient of messages from ePolicy Orchestrator Notifications, or keep the default address. Changing the address is not required at this time. For more information, see the Notifications chapter in the ePolicy Orchestrator 4.0 Product Guide.

- a Provide the default destination for messages.
- b Setting email server settings can be postponed until some time following installation by selecting **Setup email server settings later** and leaving the default example address untouched. However, the required information can be provided during installation.

Selecting **Setup email server settings now** enables the remaining fields in the dialog box:

- **Email server FQDN:** Type the Fully Qualified Domain Name of the mail server and specify the **Port** to use for email.
- If appropriate, select **This server requires authentication**. Then type the **User name** and **Password** required to access the server. Click **Next**.

- 13** In the **Set Windows Authentication** dialog box, specify the **WINS server** or **Domain** to be used with ePolicy Orchestrator. Click **Next**.
- 14** In the **Start Copying Files** dialog box, click **Install** to begin the installation.
- 15** In the **Installation Complete** dialog box, click **Finish** to complete the installation.

Migrating to a licensed version

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

Task

- 1** To migrate any pre-release software to a licensed version, you must first uninstall the existing version of the software.
- 2** Log on to the desired computer using an account with local administrator permissions.
- 3** Start the setup program:
If you downloaded the software from the McAfee website, go to the location where you extracted all the files and double-click SETUP.EXE.

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

If installing the software from the product CD:

- a** Insert the CD into the CD-ROM drive of the computer.
 - b** In the ePolicy Orchestrator autorun window, select the desired language, then select **Install ePolicy Orchestrator 4.0**.
- 4** In the **ePolicy Orchestrator 4.0 Setup** wizard, click **Next** to begin the migration.
 - 5** A message appears indicating that the migration was completed successfully.

Post-Installation Tasks

After completing the Setup wizard, follow the appropriate procedures to configure the software.

Contents

- ▶ [Completing a first-time installation](#)
- ▶ [Completing an upgrade](#)
- ▶ [Migrating events from an earlier version](#)
- ▶ [Checking in files manually](#)
- ▶ [Configuring the software for a server with multiple NICs](#)
- ▶ [Uninstalling the software](#)

Completing a first-time installation

The tasks needed to complete the first-time installation are listed here. Information about performing these actions can be found in the ePolicy Orchestrator 4.0 Product Guide.

Tasks

- 1 Plan your ePolicy Orchestrator System Tree and updating scheme.
- 2 Create the ePolicy Orchestrator System Tree .
- 3 Distribute the McAfee agent to the systems you want to manage with ePolicy Orchestrator.
- 4 Create the updating repositories.
- 5 Check in to the repositories the products ePolicy Orchestrator is to manage, and configure their policy settings.
- 6 Deploy products to the managed computers.
- 7 Configure the advanced features of ePolicy Orchestrator.

Completing an upgrade

The version and product you are upgrading determines which tasks you must perform to complete your installation of ePolicy Orchestrator 4.0.

Tasks

- 1 Migrate events from the previous version of ePolicy Orchestrator. See [Migrating Events from an earlier version](#), below.
- 2 Plan and implement any ePolicy Orchestrator System Tree (formerly Directory) and repository changes.

- 3 Upgrade the agents on your network to version 3.6, if desired.
- 4 Check in and deploy new products you want to manage.
For details, see the *ePolicy Orchestrator 4.0 Product Guide*.

Migrating events from an earlier version

Events recorded in earlier versions of ePolicy Orchestrator can be migrated to version 4.0.

Task

- 1 From the ePolicy Orchestrator console, select **Automation**.
- 2 On the **Server Tasks** tab, click **New Task**.
- 3 On the **Description** tab, type a name for the task and any notes you want; select **Enabled**, then click **Next**.
- 4 On the **Actions** tab, select **Event Migration** from the drop-down list. A list of **DTS** (Data Transformation Services) packages appears. Deselect any package that you do not want to migrate, then Click **Next**.
- 5 Click **Next** to schedule the migration. To implement the continuous migrating of events until conclusion:
 - a Select **Daily**.
 - b Specify a **Start date** and make the **End date** the same.
 - c Select a time of day.
 - d Click **Next**.
- 6 Review your settings, then click **Save**.

Checking in files manually

These are the files that you must check in to the master repository after you install or upgrade the software. For more information, see the *ePolicy Orchestrator 4.0 Product Guide*.

- **Custom packages** — Only custom packages created with McAfee Installation Designer 7.0 can be checked in to the master repository.
- **Product extensions**— If the extension for a product was not added to the repository during the installation, you must manually add it as a .ZIP file.
- **Product plug-in files** — Any product plug-in (.dll) files that were not checked in as part of the installation must be checked in to the master repository manually as .ZIP files.
- **Products** — Check in to the repository the software you intend to deploy.
 - If you are installing the software for the first time, you must check in all products that you want to deploy via ePolicy Orchestrator.
 - If you are upgrading the software, any supported products that were not already present must be checked into the master repository manually as .ZIP files.
- **Product updates** — You must check in all product updates that you want to deploy via ePolicy Orchestrator.

Configuring the software for a server with multiple NICs

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

Task

- 1 Open the SEVER.INI file. The default location is:
C:\PROGRAM FILES\MCAFFEE\EPOLICYORCHESTRATOR\4.0.0\DB
- 2 Add the following line at the end of the [server] section of the file:
ServerIPAddress=XXX.XXX.XXX.XXX
where XXX.XXX.XXX.XXX is the IP address of the NIC to which you want ePolicy Orchestrator bound.
- 3 Save and close the SERVER.INI file.
- 4 Restart all of the ePolicy Orchestrator services.

NOTE: The server IP address is used by the master repository and for agent-server communication. If this address is not provided, the IP address of the first NIC in the binding order is used.

Uninstalling the software

If you need to uninstall this software, use this procedure. If you used the ePolicy Orchestrator Setup program to install MSDE, you can remove it at the same time.

Task

- 1 Close all database management software, such as SQL Enterprise Manager.
- 2 Use **Add/Remove Programs** in the **Control Panel** to remove the software. For instructions, see the Windows Help file.
- 3 To remove the existing MSDE database, select **Remove MSDE**.
- 4 Click **Remove**.

Troubleshooting

The most common messages that appear during an installation and their solutions are listed in this chapter.

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

- Verify that you have met the minimum installation requirements.
- Review the *ePolicy Orchestrator 4.0 Release Notes* (ReadMe.html) for any known installation issues.
- Verify that the user account you used to log on to the computer on which you are installing the software has full administrator permissions to that computer.
- Collect the exact text of all messages, and be sure to take note of any message codes that appear.
- Gather the installation log files.

Contents

- ▶ [Common installation messages and their solutions](#)
- ▶ [Default locations of troubleshooting log files](#)

Common installation messages and their solutions

If this message appears...	Then...
You are attempting to upgrade from a product version that is not supported. For a complete list of upgrade requirements, see the ePolicy Orchestrator Installation Guide.	No version of ePolicy Orchestrator has been installed on this computer. You can only upgrade from ePolicy Orchestrator 3.6.0 or later.
Internet Explorer 6 or later needs to be installed for this installation to continue.	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 ePolicy Orchestrator software.
Another instance of the McAfee ePolicy Orchestrator installer is already running	The ePolicy Orchestrator 4.0 Setup program is already running. You cannot run more than one instance of Setup at a time.
For security reasons McAfee does not allow blank passwords. Please enter a valid password to continue.	The Password box is blank. Specify the password of the user account that you want to use.
McAfee recommends that you set the video display to 1024x768 or higher resolution.	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

If this message appears...	Then...
	the monitor resolution, see the Windows Help File. To open this file, click the Start button, then select Help .
McAfee recommends that you install the software on a computer with at least 512 MB of RAM.	The computer on which you are attempting to install the software does not meet the minimum memory requirement.
McAfee ePolicy Orchestrator 4.0 requires that your computer is running Windows 2000, Windows Server 2003, or Windows Longhorn.	The computer on which you are attempting to install the software is using a non-supported version of the operating system.
Enter a value in the "Agent Broadcast communication" field.	The Agent Broadcast communication 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.
Enter a value in the "Agent-to-Server communication" field.	The Agent-to-Server communication port box is blank. Specify the port number that the agent will use to communicate with the server.
Enter a value in the "Agent Wake-Up communication" port.	The Agent Wake-Up communication port box is blank. Specify the port number (default is 8081) that the ePolicy Orchestrator server will use to send agent wakeup calls.
McAfee ePolicy Orchestrator must be installed in a folder. Enter a Destination Folder to continue.	The Destination Folder is blank or the root of a drive. Click Browse to select a location. The default location is: C:\PROGRAM FILES\MCAFFEE\EPO
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.
The License file is missing is missing or corrupt. Contact support for assistance.	Setup is unable to read the license information required to install the software. Contact McAfee Customer Service.
The operating system or service pack 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 passwords you entered do not match. Enter a valid password to continue.	The value you typed in Password and Confirm Password do not match. Specify the password of the user account that you want to use.
The McAfee ePolicy Orchestrator license has expired.	Your license to use the software has expired. Go to the beta feedback page on the McAfee website, where you can supply your comments about the beta 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. McAfee recommends using static IP addresses for ePolicy Orchestrator servers to improve performance and reduce bandwidth usage.
account credentials	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 provided the account credentials and database server name correctly, then try again. If this message continues to appear, see the ePolicy Orchestrator installation Guide for more information.	<p>A connection could not be made to the corresponding ePolicy Orchestrator database server.</p> <ol style="list-style-type: none"> 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.

If this message appears...	Then...
Unable to connect using the information you provided. Verify that you entered the correct information and try again.	The user account that you specified could not be accessed. <ol style="list-style-type: none"><li data-bbox="841 281 1372 338">1 Verify that the Domain, User Name, and Password you provided are typed correctly.<li data-bbox="841 359 1372 415">2 Verify that the user account you used to log on to this computer has access to this domain.

Default locations of troubleshooting log files

Log File Name	Log Type	File Location	Description
EPO400-DBINIT.log	Install	%temp%\Nailogs	Main DB log file for the ePolicy Orchestrator 4.0.0 installer. Contains any output captured by NaiLog.Dll during installation.
EPO400-TRACE.LOG	Install	%temp%\Nailogs	Main log file for the ePolicy Orchestrator 4.0.0 installer.
licensing.log	Install	%temp%\Nailogs	Used by the Common License Application (CLA). Created by NaiLite.Dll during the EULA and other License API calls.
MSXML6Inst.Log	Install	%temp%\Nailogs	MSI log file created when ePolicy Orchestrator installs MSXML 6.0.
MSXML6PatchInst.Log	Install	%temp%\Nailogs	MSI log file created when ePolicy Orchestrator installs the MSXML 6.0 Patch.
[ExtensionFileName].cmd	Temporary	%temp%\Nailogs\OutputFiles	File created by ePolicy Orchestrator installer, containing the command (sent to Remote-Client) to check-in extensions.
ePO##.tmp	Temporary	%temp%\Nailogs\OutputFiles	File created by the ePolicy Orchestrator installer, containing the command (sent to Remote-Client) to check in Plugin, Point Products, and Agent packages.
core-install.log	Install	[InstallDir]\Installer\core	Log file created when the ePolicy Orchestrator installer calls the Orion ANT installer.
epo-install.log	Install	[InstallDir]\Installer\ePO	Log file created when the ePolicy Orchestrator installer calls the Mercury ANT installer.
EpoApSvr.log	Primary	[InstallDir]\DB\LogS	Application Server log file. Present only after initial service startup. Output = RManJNI, DalPolicy, SiteMgr, and SiteMgrWrap.
eventparser.log	Primary	[InstallDir]\DB\LogS	Event Parser log file. Present only after initial service startup. Output = EventParser.
server.log	Primary	[InstallDir]\DB\LogS	ePolicy Orchestrator Server agent handler and other C++ code log file. Present only after initial service startup. Output =

Log File Name	Log Type	File Location	Description
			EPOServer, and Mod_EPO.
errorlog.####-##-##-##_##_##_	Apache	[InstallDir]\Apache2\logs	Apache2 log file for the Apache service. Present only after initial service startup.
jakarta_service_#####.log	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup.
localhost_access_log.####-##-##.txt	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup.
orion.log	Primary	[InstallDir]\Server\logs	Log4J log file used by the Orion Platform and, by default, all loaded extensions. Present only after initial service startup Output = Orion, Orion extensions, and Mercury extensions.
stderr.log	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup The file contains any Standard Error output captured by the Tomcat service.

Installing in a cluster environment

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

Contents

- ▶ [Requirements](#)
- ▶ [Setting up the ePolicy Orchestrator cluster](#)
- ▶ [Testing the ePolicy Orchestrator cluster](#)

Requirements

Before Running ePolicy Orchestrator as a clustered application, ensure that:

- Microsoft Cluster Server (MSCS) is set up and running on a cluster of two or more servers.
- Two separate drives are configured for clustering - a Quorum drive and a Data drive.
- Remote database server is configured for one of these ePolicy Orchestrator databases:
 - SQL Server 2000 with Service Pack 3.
 - SQL Server 2005.
- The following information is available during installation.
 - The ePolicy Orchestrator virtual server IP address.
 - The ePolicy Orchestrator virtual server name.
 - The ePolicy Orchestrator virtual server DNS name.
 - The location on the Data drive where you intend to place the ePolicy Orchestrator Cluster folder.

Setting up the ePolicy Orchestrator cluster

Once the requirements are met, use these tasks to set up the node of the cluster.

Tasks

- ▶ [Installing ePolicy Orchestrator on each node](#)
- ▶ [Creating the ePolicy Orchestrator group](#)
- ▶ [Creating the data drive](#)
- ▶ [Creating the IP address resource](#)
- ▶ [Creating the Network Name resource](#)

► [Creating the Generic Service resources](#)

Installing ePolicy Orchestrator on each node

Run the ePolicy Orchestrator setup on each of the nodes. McAfee strongly recommends that, during installation, only one node at a time be powered on.

Task

- 1 Double-click SETUP.EXE in the installation folder. The default location is:
<Drive>\Program Files\McAfee\ePolicy Orchestrator
- 2 Follow the wizard until you reach the **Set Database and Virtual Server Settings** page.
- 3 Select **Enable Microsoft Cluster Server Support**.
- 4 Click **Browse** and navigate to the location on the Data drive where you intend to place the ePO Cluster folder. If you type a path and specify a folder that does not exist, the installer creates the folder in the designated location.
- 5 Provide the following identifying information for the ePO cluster:
 - The ePO virtual server IP address.
 - The ePO virtual server name.
 - The ePO virtual server DNS name.
 - The location on the Data drive where you intend to place the ePO Cluster folder.
- 6 Complete the installation of ePolicy Orchestrator on the first node as described in the First-Time Installation chapter.
- 7 Repeat this task for the second node.

Creating the ePolicy Orchestrator group

Task

- 1 Open the Cluster Administrator on the active node:
Start | Program Files | Administrative Tools | Cluster Administrator
- 2 Right-click **Groups** in the System Tree, then select **New | Group**. The **New Group** dialog box appears.
- 3 Type the **Name** and **Description** of the group, then click **Next**.
- 4 In the **Preferred Owners** dialog box, identify the owners of the group. Select the desired node under **Available Nodes**, then click **Add**. Repeat until all owners are added, then click **Next**.
- 5 Click **Finish**.

Creating the data drive

Task

- 1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The **New Resource** dialog box appears.
- 2 Type the **Name** and **Description** of the resource. For example, Data Drive.

- 3 Select **Physical Disk** from the **Resource type** drop-down list.
- 4 Ensure that **ePO** is the selected group, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.
- 6 In the **Dependencies** dialog box, click **Next**.
- 7 In the **Disk** pull-down, select the disk and click **Finish**.

Creating the IP address resource

Task

- 1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The **New Resource** dialog box appears.
- 2 Type the **Name** and **Description** of the resource. For example, IP Address.
- 3 Select **IP Address** from the **Resource type** drop-down list.
- 4 Ensure that **ePO** is the selected group, then click **Next**.
- 5 In the **Possible Owners** dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.
- 6 No information is required in the **Dependencies** dialog box. Click **Next**.
- 7 Type the virtual IP address and subnet mask for the ePO group, then click **Finish**.

Creating the Network Name resource

Task

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

Creating the Generic Service resources

Task

- 1 Add Generic Service resources in the following order:
 - a McAfee ePolicy Orchestrator 4.0.0 Server
 - b McAfee ePolicy Orchestrator 4.0.0 Application Server (Dependency on Server)
 - c McAfee ePolicy Orchestrator 4.0.0 Event Parser (Dependency on Application Server)
- 2 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The **New Resource** dialog box appears.

- 3 Type the **Name** and **Description** of the resource. For example, ePO 4.0 Server.
- 4 Select **Generic Service** from the **Resource type** drop-down list.
- 5 Ensure **ePO** is the selected group, then click **Next**.
- 6 In the **Possible Owners** dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.
- 7 In the **Dependencies** dialog box, type the dependency specific to each service.

Service	Dependency
ePolicy Orchestrator 4.0.0 Application Server	ePolicy Orchestrator 4.0.0 Server
ePolicy Orchestrator 4.0.0 Event Parser	ePolicy Orchestrator 4.0.0 Application Server

- 8 For each service, type the **Service Name**, leave the **Start Parameters** field blank, then click **Finish**.

Service	Service Name
Server	MCAFEEAPACHESRV
Application Server	MCAFEETOMCATSRV
Event Parser	MCAFEEventPARSERSRV

Testing the ePolicy Orchestrator cluster

When the ePolicy Orchestrator cluster is set up, test its functionality by bringing the ePO group online. To do so:

Task

- 1 Select the **ePO** group, and select **Bring online**.
- 2 Right-click any of the resources for the ePO group, then select **Initiate Failure**. A series of messages report the progress of the failure of the resource and its restoration.