Installation Guide

McAfee ePolicy Orchestrator 5.3.0 Software

COPYRIGHT

Copyright © 2014 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

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 ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **5**

About this guide 5

Audience 5

Conventions 5

Find product documentation 6

1 Installation requirements and recommendations **7**

Hardware requirements and recommendations 7

Software requirements and recommendations 8

Operating system requirements 9

Supported virtual infrastructure software 10

Supported SQL Servers 10

Supported Internet browsers 11

Agent Handler server requirements 11

Things to know before installation 12

About the SQL Server installation documented in this guide 13

About the SQL Server roles required for installation 13

Required SQL permissions for installing McAfee ePO 14

Supported SQL database user name and password formats 14

About HTTP port options 14

Automatic product configuration 15

Distributed repository requirements 16

Supported products and known issues 16

2 Installing McAfee ePO **17**

Initial installation options 17

Perform Express installation 18

Set up Express installation 18

Complete Express installation 19

Perform Custom installation 20

Set up Custom installation 21

Complete Custom installation 22

Perform cluster installation 24

Install on Windows Server 2008 25

Install on Windows Server 2012 28

Test the ePolicy Orchestrator cluster installation 31

Installing remote Agent Handlers 31

Install remote Agent Handlers 31

Complete a first-time installation 32

3 Restoring McAfee ePO **33**

Restore software installation options 33

Install ePolicy Orchestrator software on the restore server 34

Restore McAfee ePO software in a cluster environment 36

Restore remote Agent Handler connections 38

4 Upgrading McAfee ePO software 41
Upgrade overview . . . 42
Complete pre-upgrade tasks . . . 43
Make sure you can upgrade your McAfee ePO server . . . 43
Review products and known issues . . . 43
Back up McAfee ePO databases and directories . . . 44
Stop remote Agent Handlers services before upgrading . . . 44
Upgrade your McAfee ePO server . . . 44
Migrating from a 32-bit to a 64-bit platform . . . 46
32-bit Upgrade Compatibility Utility overview . . . 46
Connect your upgraded McAfee ePO server to an existing 32-bit SQL Server . . . 51
Upgrade your McAfee ePO cluster server . . . 52
Upgrade your remote Agent Handlers . . . 53

5 Uninstalling McAfee ePO software 55
Uninstall Express and Custom installations . . . 55
Uninstall cluster installations . . . 56

6 Troubleshooting and log file reference 57
Common installation messages and their causes and solutions . . . 58
Log files for troubleshooting . . . 59
Installer logs . . . 60
Server logs . . . 61
McAfee Agent logs . . . 63

Index 67

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.
- **Reviewers** — People who evaluate the product.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.

	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1 Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.

2 Enter a product name, select a version, then click **Search** to display a list of documents.

1

Installation requirements and recommendations

Your environment needs to include specific hardware and software to run McAfee ePO 5.3.0. Review these requirements and recommendations before installing your McAfee ePO software to make sure that your installation is successful.

Contents

- *Hardware requirements and recommendations*
- *Software requirements and recommendations*
- *Operating system requirements*
- *Supported virtual infrastructure software*
- *Supported SQL Servers*
- *Supported Internet browsers*
- *Agent Handler server requirements*
- *Things to know before installation*
- *Automatic product configuration*
- *Distributed repository requirements*
- *Supported products and known issues*

Hardware requirements and recommendations

Make sure that your environment conforms to these requirements and recommendations before installing McAfee ePO software.

Component	Requirements and recommendations
Dedicated server	If managing more than 250 systems, we recommend using a dedicated server.
Domain controllers	The server must have a trust relationship with the Domain Controller on the network. For instructions, see the Microsoft product documentation.
File system	NT file system (NTFS) partition recommended.
Free disk space	20 GB — Recommended minimum.
IP address	We recommend using static IP addresses for McAfee ePO servers. McAfee ePO supports both IPv4 and IPv6 networks.

Component	Requirements and recommendations
Memory	8 GB available RAM recommended minimum.
Network Interface Card (NIC)	100 MB or higher If using a server with more than one IP address, McAfee ePO software uses the first identified IP address. If you want to use more IP addresses for agent-server communication, we recommend creating more Agent Handler groups for each IP address. See *Manage Agent Handlers* in the *McAfee ePolicy Orchestrator Product Guide* or Help for details about setting up Agent Handler groups.
Ports	We recommend avoiding the use of port 8443 for HTTPS communication. Although port 8443 is the default port, it is also the primary port used by many web-based activities, it is a target for malicious exploitation, and system administrators are likely to disable the port in response to a security violation or outbreak. Make sure that the ports you choose are not already in use on the server system. Notify network staff of the ports you intend to use for HTTP and HTTPS communication. Installing the software on a Domain Controller is supported, but not recommended.
Processor	• 64-bit Intel Pentium D or higher • 2.66 GHz or higher

Software requirements and recommendations

Make sure you have the required and recommended software installed on your server system before installing ePolicy Orchestrator software.

Software	Requirements and recommendations
Microsoft .NET Framework 3.5 or later	Required — This software is required if you select an installation option that automatically installs the SQL Server Express 2008 software bundled with this ePolicy Orchestrator software. If this software is missing, the installer tries to install it. If the installer fails, you must exit the Setup and acquire and install the Microsoft .NET Framework manually before proceeding.
Microsoft updates	Recommended — Make sure your Microsoft software is running the latest updates. Turn off Windows updates before you begin installing or upgrading your software.
Microsoft Visual C++ 2005 SP1 Redistributable	Required — Installed automatically.
Microsoft Visual C++ 2008 Redistributable Package (x86)	Required — Installed automatically.
MSXML 6.0	Required — Installed automatically.

Software	Requirements and recommendations
Security software	Recommended. • Install and/or update the anti-virus software on the server and scan for viruses. • Install and/or update firewall software on the server.
Supported browser	Recommended — Although it is not a prerequisite for installation, ePolicy Orchestrator software requires the use of a supported browser. You should acquire and install a supported browser manually. For more information, see *Supported Internet browsers*.
Supported SQL Server	Required — If a supported version of SQL Server has not been previously installed, you can choose to install SQL Server 2008 Express automatically.

Operating system requirements

You can install McAfee ePO on any supported Microsoft Windows server-class operating system.

Supported server-class operating systems

The software requires one of these supported 64-bit server-class operating systems.

- Windows 2008 R2
- Windows Server 2008 SP2 (x64 only) or later
- Windows Server 2012
- Windows Server 2012 R2
- Windows 7 (x64 only), for evaluation only (message displays during install) — No Support (SLA)
- Windows 8 and 8.1 (x64), for evaluation only (message displays during install) — No Support (SLA)

Unsupported operating systems

You can evaluate the McAfee ePO software on the 64-bit versions of Windows 7, Windows 8, or Windows 8.1 operating systems.

Install this version of McAfee ePO on Windows 7, Windows 8, or Windows 8.1 for **evaluation purposes** only. McAfee support is not provided.

Operating system language

McAfee ePO software runs on any supported operating system regardless of the language of the operating system.

The McAfee ePO user interface has been translated into the languages in this list. When the software is installed on an operating system using a language that is not on this list, the interface attempts to display text in English.

- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- Dutch
- Japanese
- Korean
- Norwegian
- Portuguese (Brazilian)

- English
- Finnish
- French (Standard)
- German (Standard)
- Italian
- Portuguese (Iberian)
- Russian
- Spanish
- Swedish
- Turkish

Supported virtual infrastructure software

McAfee ePO software supports use of several types of virtual infrastructure software.

Supported virtual infrastructure software includes:

- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- XenServer 6
- XenServer 6.2

Supported SQL Servers

McAfee ePO software requires the use of a supported SQL Server.

The installation wizard detects whether a supported SQL Server is installed on the server system where you are installing your software. If no SQL Server is present, the wizard prompts you to install Microsoft SQL Server 2008 Express locally, or select an existing 32-bit or 64-bit SQL Server.

McAfee ePO supports any edition of these Microsoft SQL Servers.

- Microsoft SQL Server 2008, with Service Pack 1 or later
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014

Required SQL Server configuration settings

McAfee ePO software requires some specific SQL Server configuration settings. For information about working with these settings, see your SQL Server documentation.

Configuration	Details
Nested triggers	The **SQL Server Nested Triggers** option must be enabled.
Database collation	McAfee ePO software supports all Microsoft SQL Server collations using the following two SQL collation properties: • Case Insensitivity (CI) • Full ASCII character set support (this is included in all Unicode-based character sets)
Maintenance settings	We recommend making specific maintenance settings to McAfee ePO databases. For instructions, see the *McAfee ePolicy Orchestrator Product Guide* or Help.

Supported Internet browsers

ePolicy Orchestrator software requires the use of one of these supported Internet browsers.

- Internet Explorer 8.0 and later (Includes full support for Compatibility Mode)
- Firefox 10.0 and later
- Chrome 17 and later
- Safari 6.0 and later (Mac OS X, Windows not supported)

Using Internet Explorer enhanced security

If you're using Internet Explorer with enhanced security enabled, you must add the McAfee ePO server address to your Internet Explorer trusted sites list (formatted as `https://<servername>`). Failure to do so will display a You must have Javascript enabled to use this product error message when attempting to log on to the McAfee ePO server.

Agent Handler server requirements

You can install the McAfee ePO Agent Handler software on any supported Microsoft Windows server-class operating system.

The Agent Handler must authenticate domain credentials. If this is not possible, the account the Agent Handler uses to authenticate to the database must use SQL authentication. For more information about Windows and SQL authentication, see the Microsoft SQL Server documentation.

The Agent Handler software requires one of these 32-bit or 64-bit server-class operating systems:

- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2

Things to know before installation

Before you start the McAfee ePO installation, make sure that you have the information you need and the steps you must take.

Have this information available during the installation:

- McAfee Product License Key (not required to install an evaluation version of the software).
- Microsoft SQL authentication requires one of these credentials:
  - Windows authentication credentials — Credentials for a domain administrator user account
  - SQL authentication credentials — For more information about required SQL Server permissions, see *About the SQL Server roles required for installation*.
- A destination folder for McAfee ePO software installation (required for Custom and Cluster installations).
- A supported SQL Server.
- If you're using a new SQL Server installed manually or an existing SQL Server, you must provide these details (depending on your configuration) on the Database Information page:
  - The name of your SQL Server. This name should be formatted using the SQL Server name or the SQL Server name *with* instance name.
  - The dynamic port number used by your SQL Server.
- If you are restoring your McAfee ePO server, you must:
  - Have previously restored the SQL Server database using one of the Microsoft SQL restore processes. See the *McAfee ePolicy Orchestrator Product Guide* for details.
  - Know the Keystore encryption passphrase used with your Disaster Recovery Snapshot records. This passphrase is used to decrypt the sensitive information stored in the SQL Snapshot records.
- Decide if you want Initial Product Deployment to run automatically after installation. Most users will choose to configure their McAfee ePO server automatically. But manual configuration might be better for users with, for example, these restrictions:
  - No Internet access
  - Direct download restrictions to critical infrastructure
  - Phased deployment processes that require products be released incrementally into critical environments
  - Large organizations with specific requirements within their environment

  See *Automatic product configuration* for details.

About the SQL Server installation documented in this guide

ePolicy Orchestrator software requires the use of a supported SQL Server. The only installation scenario described in detail in this guide is a first-time installation of SQL Server 2008 Express.

In this scenario, the InstallShield wizard installs both the ePolicy Orchestrator software and the SQL Server software on the same system. If you want to install the SQL Server on a different server from the McAfee ePO server, install it manually. For more information on installing a different supported SQL Server, see the SQL Server software documentation.

Cluster installation requires you to use a manually installed a SQL Server on a system other than where you install your ePolicy Orchestrator software.

Other relevant SQL Server installations and upgrades

See the Microsoft documentation provided for information about these installation scenarios:

- Installing SQL Server 2008 or 2012
- Upgrading from SQL Server 2005 to SQL Server 2008 or 2012
- Upgrading from SQL Server 2005 Express to 2008 Express or 2012 Express

About the SQL Server roles required for installation

If you plan to use an existing SQL Server with your ePolicy Orchestrator software, specific SQL Server roles are required to install successfully.

If you select to use an existing SQL Server, or manually install a new SQL Server, provide credentials during the ePolicy Orchestrator installation process. These user account credentials, for either Windows or SQL authentication, must have been granted the server-role of dbcreator on the target SQL Server. This server-role is required for the Setup program to create and add the requisite core ePolicy Orchestrator database objects to the target SQL Server during installation.

By default, once the core database is created, this user account is granted the database-role of db_owner for the ePolicy Orchestrator database. After installation is complete, the dbcreator server-role can be revoked from this user account. Revoking the dbcreator server-role restricts the user account to only those permissions granted the db_owner database-role on the core database.

For more information about the specific standard SQL database roles required for your McAfee ePO server to operate once installed, see the product guide or Help. For a complete discussion of SQL Server roles and permissions, see the product documentation for the supported SQL Server you are using.

Required SQL permissions for installing McAfee ePO

Specific SQL Server roles are required if you plan to use an existing SQL Server or manually install a new SQL Server.

For new McAfee ePO installation...	Use these server roles
During installation	The user account credentials for either Windows or SQL authentication must have these **server roles** granted on the target SQL Server: • public • dbcreator The dbcreator server role is required for the setup program to create and add the requisite core McAfee ePO database objects to the target SQL Server during installation. This McAfee ePO SQL user account is granted the **database role** permission db_owner for the McAfee ePO database.
After the database is installed	The dbcreator server role can be removed from the McAfee ePO SQL user. Revoking the dbcreator server role restricts the user account to only those permissions granted to the db_owner database role on the McAfee ePO database.

For an upgrade or patch installation...	Use these roles
During installation	The user account credentials for either Windows or SQL authentication must have these **server roles** granted on the target SQL Server: • public • db_owner

Supported SQL database user name and password formats

Review these supported formats when creating McAfee ePO and SQL database user names and passwords.

All printable characters in the ISO8859-1 characters set are supported, with these exceptions.

Platform	Unsupported password and user name characters
SQL database	• Leading spaces, trailing spaces, or passwords that contain only spaces • Single quotes (') • Double quotes (") • Leading backslashes (\ ) • Colons in user names (:) • Semicolons in user names (;)

About HTTP port options

The ports used by ePolicy Orchestrator software are predefined, and populated by default. Most port designations can be changed only during the installation process.

Review this table for details about which port assignments you can modify.

Port	Default value	Can be changed during installation	Can be changed after installation
Agent-server communication port	80	X	
Agent-server communication secure port	443	X	
Agent wake-up communication port	8081	X	X
Agent broadcast communication port	8082	X	X
Console-to-application server communication port	8443	X	
Client-to-server authenticated communication port	8444	X	
SQL Server TCP port	1433	X	

Automatic product configuration

During an automatic configuration, your McAfee ePO server downloads and installs all the McAfee products entitled to you by your site license.

In most cases, during an automatic configuration, you never see the Automatic Product Configuration process run. It starts running as soon as you complete installing the ePolicy Orchestrator software and is usually finished before you log on.

If the Automatic Product Configuration page appears when you initially log on to ePolicy Orchestrator, an error occurred while downloading or installing your products. For example, if your Internet connection is interrupted. Make a note of the product that failed to install and click **Retry** to attempt the product installation again.

To stop the automatic product installation, click **Stop**. A confirmation dialog box asks you to confirm that you want to use Software Manager to install your products.

Once you click **OK** in the Stop Automatic Product Setup confirmation dialog box, you must use the Software Manager to install your products. Automatic Product Configuration is available only once during your initial configuration.

If a product continues to fail during Automatic Product Configuration, contact McAfee support. Or, click **OK** to exit the Automatic Product Configuration page and begin setting up the McAfee ePO server.

For future product installation status information, open the Software Manager: **Menu** | **Software** | **Software Manager**.

Distributed repository requirements

Distributed repositories are used throughout your environment to provide access to important content used by your McAfee ePO server. Your distributed repositories must conform to these minimum requirements.

Component	Requirements
Free disk space	400 MB minimum (800 MB recommended) on the drive where the repository is stored. The required space depends on the amount of data being served. The disk space requirement for the distributed repositories on systems where agents are designated as SuperAgents is equal to the disk space available for the master repository.
Memory	256 MB minimum.
Repository hosts	• HTTP-compliant servers on Microsoft Windows, or Linux operating systems. • Windows, Linux, or Open Enterprise FTP servers. • Windows, Linux, or UNIX Samba UNC shares. • Systems where a SuperAgent is installed.

Supported products and known issues

Review the products that McAfee ePO supports and known issues before completing your installation or upgrade.

Supported products and known issues KnowledgeBase articles

- McAfee ePO 5.3.0 Supported Products — KB82836 (https://kc.mcafee.com/corporate/index?page=content&id=KB82836)
- McAfee ePO 5.X installation and patch upgrade checklist for known issues — KB76739 (https://kc.mcafee.com/corporate/index?page=content&id=KB76739)

Product Compatibility Check

The Product Compatibility Check lists any products from your previous McAfee ePO version that are no longer supported with version 5.3.0 software. You can run the Product Compatibility Check two ways:

- As an option when you run the Upgrade Compatibility Utility.
- When you run `Setup.exe` to upgrade McAfee ePO to version 5.3.0.

See also

32-bit Upgrade Compatibility Utility overview on page 46
Upgrade your McAfee ePO server on page 44

2

Installing McAfee ePO

You can install the McAfee ePO software either as a first-time initial installation or as a recovery installation where your Microsoft SQL Server already includes an McAfee ePO configuration from a previous installation.

See *Restoring McAfee ePO* if this is a recovery installation where your Microsoft SQL Server already includes an McAfee ePO configuration from a previous installation.

Contents

- *Initial installation options*
- *Perform Express installation*
- *Perform Custom installation*
- *Perform cluster installation*
- *Installing remote Agent Handlers*
- *Complete a first-time installation*

Initial installation options

There are three initial installation options for ePolicy Orchestrator software. Each option walks you through the installation process using the ePolicy Orchestrator InstallShield wizard.

Use this table to determine which initial installation option is right for your environment.

Installation option	Details
Express	The most direct installation path. Use this option if you want to accept the McAfee default installation settings.
Custom	Customize your installation. Use this option when you want to specify the details of your software installation, including: • The destination folder where the software is installed (`C:\Program Files\McAfee\ePolicy Orchestrator\` by default). • The ports used. Installing SQL Server 2008 Express is optional. You can also specify a different supported SQL Server, if the SQL Server is installed before you begin the McAfee ePO software installation.
Cluster	Perform a cluster installation. Use this option when you want to install into a cluster environment. Before you begin installing the software: • Your Microsoft Cluster Server (MSCS) environment must be set up. • You must have a supported SQL Server installed in a location accessible to your cluster.

If you are upgrading from a prior version of McAfee ePO software or are migrating from an evaluation version, see *Upgrading McAfee ePO software*.

Perform Express installation

The Express installation installs your ePolicy Orchestrator software in the fewest possible steps by automatically accepting the default configuration.

The ePolicy Orchestrator Express installation is separated into two tasks.

Tasks

- *Set up Express installation* on page 18
  When you set up the ePolicy Orchestrator Express installation you download the software, choose the installation type, and start the installation.
- *Complete Express installation* on page 19
  Completing the ePolicy Orchestrator Express installation allows you to select and configure the database, the communication ports, and the license.

Set up Express installation

When you set up the ePolicy Orchestrator Express installation you download the software, choose the installation type, and start the installation.

Before you begin

- Make sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*.
- Update the system that hosts your McAfee ePO server with the latest Microsoft security updates, then turn off Windows updates during the installation process.

We recommend that you monitor the entire installation process. You might need to restart your system.

Task

1 Using an account with local administrator permissions, log on to the Windows server computer to be used as the McAfee ePO server.

2 From software downloaded from the McAfee website: extract files to a temporary location and double-click **Setup.exe**. The executable is located in the downloaded ePolicy Orchestrator installation file.

> If you attempt to run `Setup.exe` without first extracting the contents of the .zip file, the installation fails.

The **McAfee ePolicy Orchestrator - InstallShield Wizard** is launched.

3 Click one of these options:

- **Next** to continue with a normal ePolicy Orchestrator installation.
- **Restore ePO from an existing database Snapshot** and **Next** to continue with an ePolicy Orchestrator restore installation. The ePolicy Orchestrator Disaster Recovery Snapshot feature helps you quickly recover if the hardware hosting your McAfee ePO server fails. It saves your ePolicy Orchestrator configuration, extensions, keys, and more to Snapshot records in the ePolicy Orchestrator database.

> If this is a restore installation, some of the initial installation database selection dialog boxes do not appear during the installation.

4 In the **Setup Type** step, select Express, then click **Next**.

The ePolicy Orchestrator Express installation is setup and started. Now configure the database, communication ports, and license to complete the Express installation.

Complete Express installation

Completing the ePolicy Orchestrator Express installation allows you to select and configure the database, the communication ports, and the license.

Before you begin

You must have set up the ePolicy Orchestrator Express installation before you can complete the Express installation described in this task.

> Monitor the entire installation process when using the Custom installation process. You might need to restart your system.

Task

1 After you have completed the steps in *Set up Express installation*, in the **Choose Database Option** step, select **Microsoft SQL Express**, then click **Next**.

> If you use the Microsoft SQL Server Express database with ePolicy Orchestrator, **Disaster Recovery** is automatically disabled. McAfee does not recommend enabling **Disaster Recovery** with this database because of database memory limitations.

2 In the **Install additional software** step, any remaining prerequisites are listed. To install them, click **Next**.

> Microsoft .NET Framework 3.5 (or later) is required software when installing SQL Express; the installer tries to install it automatically. If the installer fails to install the Microsoft .NET Framework, exit the Setup and acquire and install it manually before proceeding.

3 In the **Database Information** step, specify your Windows authentication credentials, then click **Next**.

4 If any of the default port assignments are in conflict, resolve them by providing alternative ports in the **HTTP Port Information** step.

> If no conflicts exist, you cannot modify default port assignments. Select the **Custom** installation option if you need to modify port assignments

5 In the **Administrator Information** step, type this information, then click **Next**.

a Type the **Username** and **Password** you want to use for your primary administrator account.

b Depending on the installation, type the **Keystore encryption password**. If this is a:

- **Normal** or **initial installation** — Type a password used to encrypt Disaster Recovery Snapshot records.

  > Keep a record of this password. If you ever need to restore your ePolicy Orchestrator database, you need this password to decrypt the Disaster Recovery Snapshot records.

- **Restore installation** — Type the password to decrypt the Disaster Recovery Snapshot records. See the *McAfee ePolicy Orchestrator Product Guide* for details.

6 In the **Type License Key** step, type your license key, then click **Next**.

If you don't have a license key, you can select **Evaluation** to continue installing the software. The evaluation period is limited to 90 days. You can provide a license key after installation is complete from within the application. For more information, see the product guide or Help.

7 Accept the **McAfee End User License Agreement** and click **OK**.

8 From the Ready to install the Program dialog box, decide if you want to **Send anonymous usage information to McAfee**, then click **Install** to begin installing the software.

> Deselect the checkbox if you don't want McAfee to collect anonymous diagnostic and usage data.

9 When the installation is complete, click **Finish** to exit the InstallShield wizard.

Your ePolicy Orchestrator software is now installed. Double-click on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (`https://<servername>:<port>`).

Perform Custom installation

During **Custom** installation, you can modify the installation process at each step. You can specify destination folders and ports using this option.

The ePolicy Orchestrator **Custom** installation is separated into two tasks.

Tasks

- *Set up Custom installation* on page 21
  When you set up the ePolicy Orchestrator Custom installation, you download the software, choose the installation type, and start the installation.
- *Complete Custom installation* on page 22
  Completing the McAfee ePO Custom installation allows you to select and configure the database, the communication ports, and the license.

Set up Custom installation

When you set up the ePolicy Orchestrator Custom installation, you download the software, choose the installation type, and start the installation.

Before you begin

Make sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*.

If you use an existing SQL Server or manually install a new SQL Server, gather this information and complete these steps before beginning your installation. Make sure that your ePolicy Orchestrator software can communicate with the database server:

1. Verify that the SQL Browser Service is running.
2. Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
3. Update both the system that hosts your McAfee ePO server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.
4. Decide if you want to run Automatic Product Configuration after installation. See *Automatic Product Configuration* for details.
5. Decide if you want to download the Product Compatibility List automatically from the McAfee website, or use an alternate list stored locally. See *Product Compatibility Check* for details.

Monitor the entire installation process when using the **Custom** installation process. You might need to restart your system.

Task

1. Using an account with local administrator permissions, log on to the Windows server computer to be used as the McAfee ePO server.
2. Download the ePolicy Orchestrator software from the McAfee website, extract files to a temporary location, and find the `Setup.exe` file.

   The executable is located in the downloaded ePolicy Orchestrator installation file.

   If you attempt to run `Setup.exe` without first extracting the contents of the .zip file, the installation fails.

3. Run `Setup.exe` using any needed command-line options.
   a. To run or stop Automatic Product Configuration:
      - To *run* Automatic Product Configuration — Double-click **Setup.exe** and Automatic Product Configuration runs after the installation is complete.
      - To *stop* Automatic Product Configuration — Type `Setup.exe` and add the parameter `SKIPAUTOPRODINST=1` to stop Automatic Product Configuration from running:

        ```
        Setup.exe SKIPAUTOPRODINST=1
        ```

b To configure Product Compatibility List downloads:

- Disable automatic downloading of the Product Compatibility List from the McAfee website.

  ```
  setup.exe DISABLEPRODCOMPATUPDATE=1
  ```

- Specify an alternate Product Compatibility List file.

  ```
  setup.exe PRODCOMPATXML=<full_filename_including_path>
  ```

Multiple command-line options can be used together in a command string.

4 In the McAfee ePolicy Orchestrator InstallShield Wizard, click one of these options:

- **Next** — Continue with a normal ePolicy Orchestrator installation.
- **Restore ePO from an existing database Snapshot** and **Next** — Continue with an ePolicy Orchestrator restore installation.

  The ePolicy Orchestrator **Disaster Recovery Snapshot** feature helps you quickly recover if the hardware hosting your McAfee ePO server fails. It saves your configuration, extensions, keys, and more to Snapshot records in the ePolicy Orchestrator database.

  If this is a restore installation, some of the initial installation database selection dialog boxes do not appear during the installation.

5 In the **Setup Type** step, select **Custom**, then click **Next**.

The ePolicy Orchestrator Custom installation begins. Now configure the database, communication ports, and license to complete the Custom installation.

Complete Custom installation

Completing the McAfee ePO Custom installation allows you to select and configure the database, the communication ports, and the license.

Before you begin

You must have setup the McAfee ePO Custom installation before you can complete the custom installation described in this task.

Monitor the entire installation process when using the **Custom** installation process. You might need to restart your system.

Task

1 After you have completed the steps in *Set up Custom installation*, in the **Choose Database Option** step, select one of these and click **Next**:

- **Microsoft SQL Express** — Automatically installs SQL Server 2008 Express to the default location defined by Microsoft (`C:\Program Files\Microsoft SQL Server`).

  If you use the Microsoft SQL Server Express database with McAfee ePO, Disaster Recovery is automatically disabled. We do not recommend enabling Disaster Recovery with this database because of database memory limitations.

- **Microsoft SQL Server** — To specify a previously installed SQL database server.

  McAfee ePO Disaster Recovery is automatically enabled when you specify a previously installed Microsoft SQL database server. See the *McAfee ePolicy Orchestrator Product Guide* for more information.

You cannot install SQL Server 2008 Express locally if the server system you are installing on meets any of these conditions:

- 16 or more named instances exist on the locally installed SQL Server.
- Any version of the locally installed SQL Server contains an instance with the name EPOSERVER.
- SQL Server 2008 Express is already installed locally.

2 In the **Install additional software** step, any remaining prerequisites are listed. To install them, click **Next**.

Microsoft .NET Framework 3.5 (or later) is required software when installing SQL Express; the installer tries to install it automatically. If the installer fails to install the Microsoft .NET Framework, exit the Setup and acquire and install it manually before proceeding.

3 In the **Destination Folder** step, click:

- **Next** — Install your McAfee ePO software in the default location (`C:\Program Files\McAfee\ePolicy Orchestrator\`).
- **Change** — Specify a custom destination location for your McAfee ePO software. When the **Change Current Destination Folder** window opens, browse to the destination and create folders if needed. When finished, click **OK**.

4 Specify which type of **Database Server Credentials** to use, then click **Next**.

Windows authentication	1 From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. 2 Type the **User name** and **Password**. If you are using a previously installed SQL Server, make sure that your user account has access.
SQL authentication	Type the **User name** and **Password** for your SQL Server. Make sure that credentials you provide represent an existing user on the SQL Server with appropriate rights. The **Domain** menu is grayed out when using SQL authentication.

You might need to type the **SQL server TCP port** to use for communication between your McAfee ePO server and database server (default ports for this communication are 1433 or 1434).

5 In the **HTTP Port Information** step, review the default port assignments. Click **Next** to verify that the ports are not already in use on this system.

You can modify some of these ports now. When your installation is complete, you can change only the **Agent wake-up communication port** and **Agent broadcast communication port**. If you need to change your other port settings later, reinstall your McAfee ePO software. For more information about changing port values, see *About HTTP port options*.

6 In the **Administrator Information** step, type this information then click **Next**.

a Type the **Username** and **Password** you want to use for your primary Administrator account.

b Depending on the installation, type the **Keystore encryption password**. If this is a:

- **Normal** or **initial installation** — Type a password used to encrypt Disaster Recovery Snapshot records.

Keep a record of this password. If you ever need to restore your McAfee ePO database, you need this password to decrypt the Disaster Recovery Snapshot records.

- **Restore installation** — Type the password to decrypt the Disaster Recovery Snapshot records. See the *McAfee ePolicy Orchestrator Product Guide* for details.

7 In the **Type License Key** step, type your license key, then click **Next**.

If you don't have a license key, you can select **Evaluation** to continue installing the software. The evaluation period is limited to 90 days. You can provide a license key after installation is complete from within the application. For more information, see the *McAfee ePolicy Orchestrator Product Guide* or Help.

8 Accept the **McAfee End User License Agreement** and click **OK**.

9 From the **Ready to install the Program** dialog box, decide if you want to **Send anonymous usage information to McAfee**, then click **Install** to begin installing the software.

Deselect the checkbox if you don't want McAfee to collect anonymous diagnostic and usage data.

10 When the installation is complete, click **Finish** to exit the InstallShield Wizard.

Your McAfee ePO software is now installed. Double-click on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (https://<servername>:<port>).

Perform cluster installation

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

Installing the software into your Microsoft Cluster Server environment requires you to take more steps beyond the steps needed to complete the Express and Custom installations. The installation process depends on the operating system you are installing on. Cluster installation is supported on Windows Server 2008 or 2012.

Successful installation depends on proper setup of the Microsoft Cluster Server software (MSCS). For more information on MSCS setup, see the Microsoft documentation.

Cluster.exe is a deprecated command on Windows Server 2012. Install the Failover Cluster Command Interface as an additional feature during cluster setup on Windows Server 2012.

Cluster installation terminology

This terminology is used in the cluster installation instructions.

Table 2-1 Cluster installation terminology

Term	Definition
Data drive	One of the two drives required by Microsoft Cluster Server and ePolicy Orchestrator software. The data drive is a remote drive that is accessible to all nodes in the cluster, and is the location where you install the ePolicy Orchestrator files.
ePO Virtual IP address resource	The IP address resource that you create as part of the ePolicy Orchestrator cluster installation. This virtual IP address represents the McAfee ePO cluster installation as a whole. References to this IP address point to the currently active node in your cluster.

Table 2-1 Cluster installation terminology *(continued)*

Term	Definition
ePO Virtual Network Name resource	The Network Name resource that you create as part of the ePolicy Orchestrator cluster installation. This virtual Network Name represents the McAfee ePO cluster installation as a whole. References to this Network Name point to the currently active node in your cluster.
Quorum drive	One of the two drives required by Microsoft Cluster Server software. The quorum drive is where the MSCS files are installed. Don't install any of the ePolicy Orchestrator files on this drive.

Cluster installation prerequisites

Before you begin your cluster installation, review this list of requirements and prerequisites, and make sure that each is in place or the information is available. These requirements apply to installations on both Windows Server 2008 and 20012.

- Microsoft Cluster Server is set up and running on a cluster of two or more servers.
- A quorum drive is present and configured according to Microsoft guidelines.
- A data drive is present and available to all nodes in the cluster.
- A supported remote SQL Server is configured.

  To confirm that the ePolicy Orchestrator software can communicate with this server during installation:

  - Verify that the SQL Browser Service is running.
  - Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
- You might need to provide these details during the installation process (depending on your configuration), on the Database Information page:
  - The name of your SQL Server. Depending on the configuration, format this name using the SQL Server name or the SQL Server name *with* instance name.
  - The dynamic port number, if any, used by your SQL Server. Specify the dynamic port number during the installation process, on the Database Information page.

Install on Windows Server 2008

Installing ePolicy Orchestrator software in a cluster environment that includes Windows Server 2008 systems requires that you complete each of these tasks in the order listed.

Before you begin

Update the systems that host your McAfee ePO server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.

Tasks

- *Create the ePolicy Orchestrator application group* on page 26
  The ePolicy Orchestrator application group is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.
- *Create the Client Access Point* on page 26
  The Client Access Point defines the ePolicy Orchestrator Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.
- *Add the data drive* on page 27
  The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.
- *Install McAfee ePO software on each node* on page 27
  Run the Cluster installation on each of the nodes. To make sure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.
- *Create the Generic Service resources* on page 27
  The Generic Service resources enable the cluster server to control the McAfee ePO server, by starting and stopping the ePolicy Orchestrator services.

Create the ePolicy Orchestrator application group

The ePolicy Orchestrator application group is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.

Task

1 Open the Failover Cluster Management tool on the active node by clicking **Start** | **Programs** | **Administrative Tools** | **Failover Cluster Manager**.

2 Right-click **Services and Applications** in the cluster management tree, then select **More Actions** | **Create Empty Service or Application**.

3 Right-click **New service or application** and **Rename** the Application Group to `ePO`.

Create the Client Access Point

The Client Access Point defines the ePolicy Orchestrator Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.

Task

1 Right-click the **ePO** group and select **Add a resource** | **Client Access Point.** The **Client Access Point Wizard** appears.

2 Type the **ePolicy Orchestrator Virtual Name** in the **Name** field and specify the **ePolicy Orchestrator Virtual IP address** in the **Address** field then click **Next**. The **Confirmation** page appears.

3 Click **Next** to allow the **Client Access Point** to be configured, then click **Finish** when the wizard is complete.

4 If the **Client Access Point** is offline, right-click the name and select **Bring this resource online**.

Add the data drive

The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.

Task

1 Right-click the **ePO Application Group** and select **Add Storage**.

2 In the **Add Storage** dialog box, select the data drive to be used for your ePolicy Orchestrator installation then click **OK**.

Install McAfee ePO software on each node

Run the Cluster installation on each of the nodes. To make sure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.

Task

1 Double-click `Setup.exe` in the installation folder.

2 Follow the wizard until you reach the Setup Type page, then select the **Cluster** option, then click **Next**.

3 In the Choose Destination Location page, specify the path for the shared data drive, then click **Next**.

Use this same path for each node.

4 On the first node in the Set Virtual Server Settings page, provide this identifying information for the McAfee ePO cluster:

- The McAfee ePO **Virtual Server IP address**
- The McAfee ePO **Virtual Cluster name**
- The McAfee ePO **Virtual Cluster FQDN**
- Create the McAfee ePO **Cluster Configuration Passphrase** and **Verify Cluster Configuration Passphrase**

On subsequent nodes, the Virtual Server IP address, Virtual Cluster name, and Virtual Cluster FQDN are automatically provided. You must add the Cluster Configuration Passphrase to each subsequent node.

5 Complete the installation on the first node.

6 For each node in your cluster, repeat this task.

Create the Generic Service resources

The Generic Service resources enable the cluster server to control the McAfee ePO server, by starting and stopping the ePolicy Orchestrator services.

Add three Generic Service resources for use with your clustered McAfee ePO server. Use this table and task to configure each resource. Create the resources in the order they are listed in the table.

Repeat this task for each generic service resource.

Resource	Properties: General tab	Properties: Dependencies tab
ePolicy Orchestrator 5.3.0 Application Server	No changes necessary.	Data drive
ePolicy Orchestrator 5.3.0 Server	Remove the **Startup parameters** and add a blank space. Apache will not start with any startup parameters specified, and an empty entry is not permitted. Therefore, a blank space is required.	ePolicy Orchestrator 5.3.0 Application Server
ePolicy Orchestrator Event Parser 5.3.0	No changes necessary.	ePolicy Orchestrator 5.3.0 Application Server

Task

1 In the Cluster Administrator, right-click **ePO Application Group** and select **Add a resource** | **Generic Service**.

2 On the Select Service Wizard, select a resource, then click **Next**.

3 On the Confirmation page, click **Next** to allow the service to be created. When the wizard is complete, click **Finish**.

4 Right-click the resource you've created and select **Properties**. In the **Properties** dialog box, set the properties specified in the Generic Service resource configurations table.

Install on Windows Server 2012

Installing ePolicy Orchestrator software in a cluster environment that includes Windows Server 2012 systems requires that you complete each of these tasks in the order listed.

Before you begin

Update the systems that host your McAfee ePO server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.

Tasks

- *Create the ePolicy Orchestrator application role* on page 29
  The ePolicy Orchestrator application role is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.
- *Create the Client Access Point* on page 29
  The Client Access Point defines the ePolicy Orchestrator Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.
- *Add the data drive* on page 29
  The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.
- *Install McAfee ePO software on each node* on page 29
  Run the Cluster installation on each of the nodes. To make sure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.
- *Create the Generic Service resources* on page 30
  The Generic Service resources enable the cluster server to control the McAfee ePO server, by starting and stopping the ePolicy Orchestrator services.

Create the ePolicy Orchestrator application role

The ePolicy Orchestrator application role is required to separate the ePolicy Orchestrator application from the Microsoft Cluster Services in your cluster environment.

Task

1 Open the Failover Cluster Manager: click **Server Manager** | **Tools** | **Failover Cluster Manager**.

2 Right-click **Roles** in the System Tree, then select **Create Empty Role**.

3 Click **OK**.

4 Right-click the empty role, then select **Properties**.

5 In the **New Role** dialog box, type a **Name** for the role. For example, `ePO`.

6 Click **OK**.

Create the Client Access Point

The Client Access Point defines the ePolicy Orchestrator Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.

Task

1 Right-click the **ePO** application role, then select **Add a resource** | **Client Access Point**. The **Client Access Point Wizard** appears.

2 Type the **ePolicy Orchestrator Virtual Name** in the **Name** field and specify the **ePolicy Orchestrator Virtual IP address** in the **Address** field, then click **Next**. The **Confirmation** page appears.

3 Click **Next** to apply the **Client Access Point** changes, then click **Finish** when the wizard is complete.

4 If the **Client Access Point** is offline, right-click the name and choose **Bring Online**.

Add the data drive

The data drive is the location where you install the ePolicy Orchestrator software. Use a remote drive that all nodes in your cluster can access.

Task

1 Right-click the **ePO** application role, then select **Add Storage**.

2 In the **Add Storage** dialog box, select the data drive to use for your ePolicy Orchestrator installation, then click **OK**.

Install McAfee ePO software on each node

Run the Cluster installation on each of the nodes. To make sure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.

Task

1 Double-click `Setup.exe` in the installation folder.

2 Follow the wizard until you reach the **Setup Type** page, select the **Cluster** option, then click **Next**.

3 On the **Choose Destination Location** page, specify the path for the shared data drive then click **Next**. If you specify a folder that does not exist, installation process creates a folder with that name in the designated location.

Use this same path for each node.

4 On the first node only of the **Set Virtual Server Settings** page, provide this identifying information for the McAfee ePO cluster:

- The McAfee ePO **Virtual Server IP address**
- The McAfee ePO **Virtual Cluster name**
- The McAfee ePO **Virtual Cluster FQDN**
- Create the McAfee ePO **Cluster Configuration Passphrase** and **Verify Cluster Configuration Passphrase**

> On subsequent nodes, the Virtual Server IP address, Virtual Cluster name, and Virtual Cluster FQDN are automatically provided. You must add the Cluster Configuration Passphrase to each subsequent node.

5 Complete the installation on the first node.

6 For each node in your cluster, repeat this task.

Create the Generic Service resources

The Generic Service resources enable the cluster server to control the McAfee ePO server, by starting and stopping the ePolicy Orchestrator services.

Add three Generic Service resources for use with your clustered McAfee ePO server. Use this table and task to configure each resource. Create the resources in the order they are listed in the table.

Resource	Properties: General tab	Properties: Dependencies tab
ePolicy Orchestrator 5.3.0 Application Server	No changes necessary.	ePolicy Orchestrator 5.3.0 Server
ePolicy Orchestrator 5.3.0 Server	Remove the **Startup parameters** and add a blank space. Apache will not start with any startup parameters specified, and an empty entry is not permitted. Therefore, a blank space is required.	No changes necessary
ePolicy Orchestrator Event Parser 5.3.0	No changes necessary.	ePolicy Orchestrator 5.3.0 Application Server

Task

1 For each Generic Service resource in the Cluster Administrator, right-click **ePO** application role, then select **Add Resource** | **Generic Service**.

2 On the New Resource Wizard, select a resource, then click **Next**.

3 On the Confirmation page, click **Next** to create the service. When the wizard is complete, click **Finish**.

4 Right-click the resource, then select **Properties**. In the **Properties** dialog box, set the properties specified in the Generic Service resource configurations table.

Test the ePolicy Orchestrator cluster installation

When the ePolicy Orchestrator cluster is set up and online, use this task to make sure that the software functions in a failover situation.

Task

1 Restart the system functioning as the active node. The passive node automatically becomes the active node.

The amount of time required for the passive node to become active depends on your unique environment.

2 Manually refresh your browser session. If failover is successful, you are redirected to the ePolicy Orchestrator log on page.

Installing remote Agent Handlers

Each McAfee ePO server contains a master Agent Handler. Installing more remote Agent Handlers can help manage an increased number of products and systems managed by a single, logical McAfee ePO server in situations where the CPU on the database server is not overloaded.

Remote Agent Handlers require the same high-speed network access to your database as the primary McAfee ePO server.

You can use more IP addresses for agent-server communication by creating an Agent Handler group, and adding the additional IP address to the virtual IP address input field. For more information, see *Manage Agent Handlers* in the product guide or Help.

Install remote Agent Handlers

You can install Agent Handlers throughout your environment to help manage agent-server communication and load balancing. You can install remote Agent Handlers at any time.

Before you begin

Update the system with the latest Microsoft security updates, then turn off Windows updates during the installation process.

Task

1 Open the folder where you extracted the contents of the ePolicy Orchestrator software installation package.

2 Copy the `Agent Handler` folder to the intended Agent Handler server system.

3 Double-click **Setup.exe** to launch the McAfee Agent Handler InstallShield wizard. After some installation activities take place in the background, the InstallShield wizard opens. Click **Next** to begin the installation process.

4 After accepting the terms in the license agreement, the **Destination Folder** step opens.

5 Accept the default destination, or click **Change** to select a different destination, then click **Next**.

The destination path must not contain double-byte characters. This is a limitation of the Apache web server. Using double-byte characters causes the installation to fail and the Apache web server service to fail on startup.

6 The **Server Information** step opens.

a Type the machine name of the McAfee ePO server with which the Agent Handler must communicate.

b Specify which port to use for Agent Handler-to-server communication. The default port is 8444, the same port used for **Client-to-server authenticated communication**.

Using the default port enables Agent Handler-to-server communication to be performed using only port 8444. You can optionally specify port 8443, the **Console-to-application server communication port**, but doing so requires that port 8444 continues to be available for Agent Handler communication.

c Type the **ePO Admin User** name and **ePO Admin Password** of a user with ePolicy Orchestrator Global Administrator rights, and click **Next**.

d In the **Database Information** page, specify these settings, then click **Next**:

- **Database Server** with instance name. For example, `DB-SERVER\SERVERNAME`.
- Authentication type.
- **Domain** name where the database server is hosted.
- **User name** and **Password**.
- **Database name** if not provided automatically.

7 Click **Install** to start the installation. When installation is complete, enable your remote Agent Handler from within the ePolicy Orchestrator interface. For more information on how to enable your Remote Agent Handler, see *Working with Agent Handlers* in the product guide or Help.

Complete a first-time installation

When you have completed the installation process, configure your McAfee ePO server.

You can use the ePolicy Orchestrator Guided Configuration to set up your server and managed environment. This configuration tool is an overlay to existing features and functionality intended to help you get your server up and running quickly. For more information, see *Using the Guided Configuration tool* in the *ePolicy Orchestrator Software Product Guide* or Help.

3

Restoring McAfee ePO

You can restore the McAfee ePO software as a recovery installation where your Microsoft SQL Server already includes an McAfee ePO configuration from a previous installation.

See *Installing McAfee ePolicy Orchestrator* if this is a first-time installation.

Contents

- *Restore software installation options*
- *Install ePolicy Orchestrator software on the restore server*
- *Restore McAfee ePO software in a cluster environment*
- *Restore remote Agent Handler connections*

Restore software installation options

There are three restore installation options for ePolicy Orchestrator software. Each option walks you through the restore installation process using the ePolicy Orchestrator InstallShield wizard.

Before you can run the ePolicy Orchestrator software restore, restore the SQL database backup file, that included the Disaster Recovery Snapshot records, to the restore SQL Server. See the Microsoft SQL Server documentation for details.

Use this table to determine which restore option is right for your environment.

Installation option	Details
Express	The most direct installation path. Use this option if you want to accept the McAfee default installation settings.
Custom	Customize your installation. Use this option when you want to specify the details of your software installation, including: • The destination folder where the software is installed (`C:\Program Files\McAfee\ePolicy Orchestrator\` by default). • The ports used. Installing SQL Server 2008 Express is optional. You can also specify a different supported SQL Server, if it is installed before you begin the McAfee ePO software installation.
Cluster	Perform a cluster installation. Use this option when you want to install into a cluster environment. Before you begin installing the software: • Your Microsoft Cluster Server (MSCS) environment must be set up. • You must have a supported SQL Server installed in a location accessible to your cluster.

If you are upgrading from a prior version of McAfee ePO software or are migrating from an evaluation version, see *Upgrading McAfee ePO software*.

Install ePolicy Orchestrator software on the restore server

To recreate the McAfee ePO server, reinstall the ePolicy Orchestrator software on a server and link it to the restored SQL database.

Before you begin

Make sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*.

When you select the existing SQL Server, gather this information and complete these steps before beginning your installation to make sure that your McAfee ePO software can communicate with the database server:

1. Verify that the SQL Browser Service is running.
2. Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
3. Update the system that hosts your McAfee ePO server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.
4. Confirm the SQL backup file you copied from the primary server was restored using the Microsoft SQL process.
5. Stop remote Agent Handler services on all systems, before restoring the ePolicy Orchestrator software.

Monitor the entire installation process when using the **Restore** installation process. You might need to restart your system.

Task

1 If you have remote Agent Handlers configured, log on to the systems where the Agent Handlers are installed, then open the Windows **Services** panel and stop the **McAfee Event Parser** and **McAfee Apache** services.

> See your Microsoft software product documentation for more information on using the Windows Services panel.

2 Using an account with local administrator permissions, log on to the Windows server computer used as the restore McAfee ePO server.

3 Downloaded from the McAfee website, extract the files to a temporary location, and double-click **Setup.exe**.

> Do not attempt to run `Setup.exe` without first extracting the contents of the .zip file.

The **McAfee ePolicy Orchestrator - InstallShield Wizard** is launched.

4 Click **Restore ePO from an existing database snapshot** and **Next** to begin the restore installation process.

5 In the **Install additional software** step, any remaining prerequisites are listed. To install them, click **Next**.

> Microsoft .NET Framework 3.5 (or later) is required software when installing SQL Express; the installer tries to install it automatically. If the installer fails to install the Microsoft .NET Framework, exit the Setup and acquire and install it manually before proceeding.

6 In the **Destination Folder** step, click:

- **Next** — Install your McAfee ePO software in the default location (`C:\Program Files\McAfee\ePolicy Orchestrator (x86)\`).
- **Change** — Specify a custom destination location for your McAfee ePO software. When the **Change Current Destination Folder** window opens, browse to the destination and create folders if needed. When finished, click **OK**.

7 In the **Database Information** step, select the Microsoft SQL Server name from the **Database Server** list and specify which type of **Database Server Credentials** to use, then click **Next**.

Windows authentication	1 From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. 2 Type the **User name** and **Password** of your restored SQL database.
SQL authentication	• Type the **User name** and **Password** for your SQL Server. Make sure that credentials you provide represent an existing user on the SQL Server with appropriate rights. The **Domain** menu is grayed out when using SQL authentication

> You might need to type the **SQL server TCP port** to use for communication between your McAfee ePO server and database server. The ePolicy Orchestrator installation tries to connect using the default ports, 1433 and 1434. If those ports fail, you are prompted to type an SQL Server TCP port.

8 In the **HTTP Port Information** step, review the default port assignments. Click **Next** to verify that the ports are not already in use on this system.

9 In the **Administrator Information** step, type the **Username** and **Password** you used for your previously existing server administrator account.

10 Type the **Keystore encryption passphrase** you saved during the initial installation of the previously existing McAfee ePO server, or changed in the Server Settings.

The Keystore encryption passphrase decrypts the sensitive files stored in the Disaster Recovery Snapshot.

11 In the **Type License Key** step, type your license key, then click **Next**.

If you don't have a license key, you can select **Evaluation** to continue installing the software. The evaluation period is limited to 90 days. You can provide a license key after installation is complete from within the application. For more information, see the *McAfee ePolicy Orchestrator Product Guide* or Help.

12 Accept the **McAfee End User License Agreement** and click **OK**.

13 From the **Ready to install the Program** dialog box, decide if you want to send anonymous usage information to McAfee, then click **Install** to begin installing the software.

Deselect the checkbox if you don't want McAfee to collect anonymous diagnostic and usage data.

14 When the installation is complete, click **Finish** to exit the InstallShield wizard.

This dialog box includes checkboxes to read the release notes and to launch ePolicy Orchestrator.

15 If you restored ePolicy Orchestrator to a McAfee ePO server with a different IP address or DNS name than your previously existing server, configure a way to allow your managed systems to connect to your new McAfee ePO server.

We recommend creating a CNAME record in DNS that points requests from the old IP address, DNS name, or NetBIOS name of the previously existing McAfee ePO server to the new information for the restore McAfee ePO server.

16 If you stopped the remote Agent Handlers in step 1, log on to the systems where the Agent Handlers are installed, then open the Windows **Services** panel and start the **McAfee Event Parser** and **McAfee Apache** services.

Your ePolicy Orchestrator software is now restored. If needed, double-click on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (`https://<server_name>:<port>`).

If you have remote Agent Handlers, see *Restore remote Agent Handler connections* to modify their settings to connect to the restored servers.

Restore McAfee ePO software in a cluster environment

To restore the McAfee ePO servers installed on server clusters with Microsoft Cluster Server (MSCS) software, reinstall the McAfee ePO software on all servers in the server cluster.

Before you begin

Make sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*.

When you select the existing SQL Server, gather this information and complete these steps before beginning your installation to make sure that your McAfee ePO software can communicate with the database server:

1 Verify that the SQL Browser Service is running.

2 Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.

3 Update both the system that hosts your McAfee ePO server and your SQL Server with the latest Microsoft security updates, then turn off Windows updates during the installation process.

4 Confirm the SQL backup file you copied from the primary server was restored using the Microsoft SQL process.

5 Stop remote Agent Handler services on all systems, before restoring the McAfee ePO software.

Monitor the entire installation process when using the **Restore** installation process. You might need to restart your system.

Restoring the McAfee ePO software in a Microsoft Cluster Server environment is similar to installing the software initially. The only new instructions are in step 6 of this task.

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

Task

1 If you have remote Agent Handlers configured, log on to the systems where the Agent Handlers are installed, then open the Windows **Services** panel and stop the **McAfee Event Parser** and **McAfee Apache** services.

See your Microsoft software product documentation for more information on using the Windows Services panel.

2 Perform the Cluster installation. See *Perform Cluster installation* for an overview of the cluster software installation process.

3 Create the McAfee ePO application group or role. See *Create the ePolicy Orchestrator application group* or *Create the ePolicy Orchestrator application role* for the tasks needed to separate the McAfee ePO application from the Microsoft Cluster Services in your cluster environment.

4 Create the Client Access Point. See *Create the Client Access Point* for the tasks to define an McAfee ePO Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.

5 Add the data drive. See *Add the data drive* for the tasks to set the data drive location where you install the McAfee ePO software.

6 Restore the McAfee ePO software on each node using these steps.

> Run the Cluster installation on each of the nodes. To make sure that each node has exclusive access to the quorum and data drives during installation, shut down all other nodes in the cluster.

a Using an account with local administrator permissions, log on to the Windows server computer used as the restore McAfee ePO server.

b Run the Setup program from the software downloaded from the McAfee ePO website, extract the files to a temporary location, and double-click **Setup.exe**.

> Do not attempt to run `Setup.exe` without first extracting the .zip file.

The **McAfee ePolicy Orchestrator - InstallShield Wizard** is launched.

c Click **Restore ePO from an existing database snapshot** and **Next** to begin the restore installation process.

d Follow the wizard until you reach the **Setup Type** page, select the **Cluster** option, then click **Next**.

e In the **Choose Destination Location** page, specify the path for the shared data drive, then click **Next**.

Use this same path for each node.

f On the first node only in the **Set Virtual Server Settings** page, provide this identifying information for the McAfee ePO cluster:

- The McAfee ePO Virtual Server IP address
- The McAfee ePO Virtual Cluster name
- The McAfee ePO Virtual Cluster FQDN

> This information is automatically provided on subsequent nodes.

g Complete the installation on the first node.

h Repeat this task for each node in your cluster.

7 Enable the cluster server Generic Service resources. See *Create the Generic Service resources* to control the McAfee ePO server, by starting and stopping the McAfee ePO services.

8 If you stopped the remote Agent Handlers in step 1, log on to the systems where the Agent Handlers are installed, then open the Windows **Services** panel and start the **McAfee Event Parser** and **McAfee Apache** services.

9 Make sure that the software functions in a failover situation. See *Test the ePolicy Orchestrator cluster installation* for details.

After completing these steps, your McAfee ePO software is restored on all servers in the server cluster.

Restore remote Agent Handler connections

After you restored your McAfee ePO server and SQL database you must modify the remote Agent Handler settings to connect to the restored servers.

Before you begin

Update the system with the latest Microsoft security updates, then turn off Windows updates during the installation process.

Task

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

1 On the Agent Handler server system find the `Agent Handler` folder you extracted from the ePolicy Orchestrator software installation package.

2 Double-click `Setup.exe` to launch the McAfee Agent Handler InstallShield wizard. After some installation activities take place in the background, the InstallShield wizard opens. Click **Next** to begin the modify process.

3 From the Program Maintenance dialog box, click **Modify** to change which program features are installed.

The **Server Information** step opens.

4 Configure these settings:

a Type the restored machine name of the McAfee ePO server with which the Agent Handler must communicate.

b Specify which port to use for Agent Handler-to-server communication. The default port is 8444, the same port used for **Client-to-server authenticated communication**.

Using the default port enables Agent Handler-to-server communication to be performed using only port 8444. You can optionally specify port 8443, the **Console-to-application server communication port**, but doing so requires that port 8444 continues to be available for Agent Handler communication.

c Type the **ePO Admin User** name and **ePO Admin Password** of a user with ePolicy Orchestrator global administrator rights.

d Click **Next** to use the **ePO Admin** credentials to access the database as well; make sure they are assigned the appropriate SQL Server role and permissions.

The **Database Information** step opens.

5 Configure the new credentials to access the restored database then click **Next**:

- **Database Server** with instance name. For example, `DB-SERVER\SERVERNAME`.
- Authentication type.
- **Domain** name where the restored database server is hosted.
- **User name** and **Password**.
- **Database name** if not provided automatically.

6 Click **Install** to start the changes to the installation. When installation is complete, enable your remote Agent Handler from within the ePolicy Orchestrator interface. For more information on how to enable your Remote Agent Handler, see *Working with Agent Handlers* in the product guide or Help.

Your remote Agent Handlers can now communicate with the restored McAfee ePO server and SQL database.

4

Upgrading McAfee ePO software

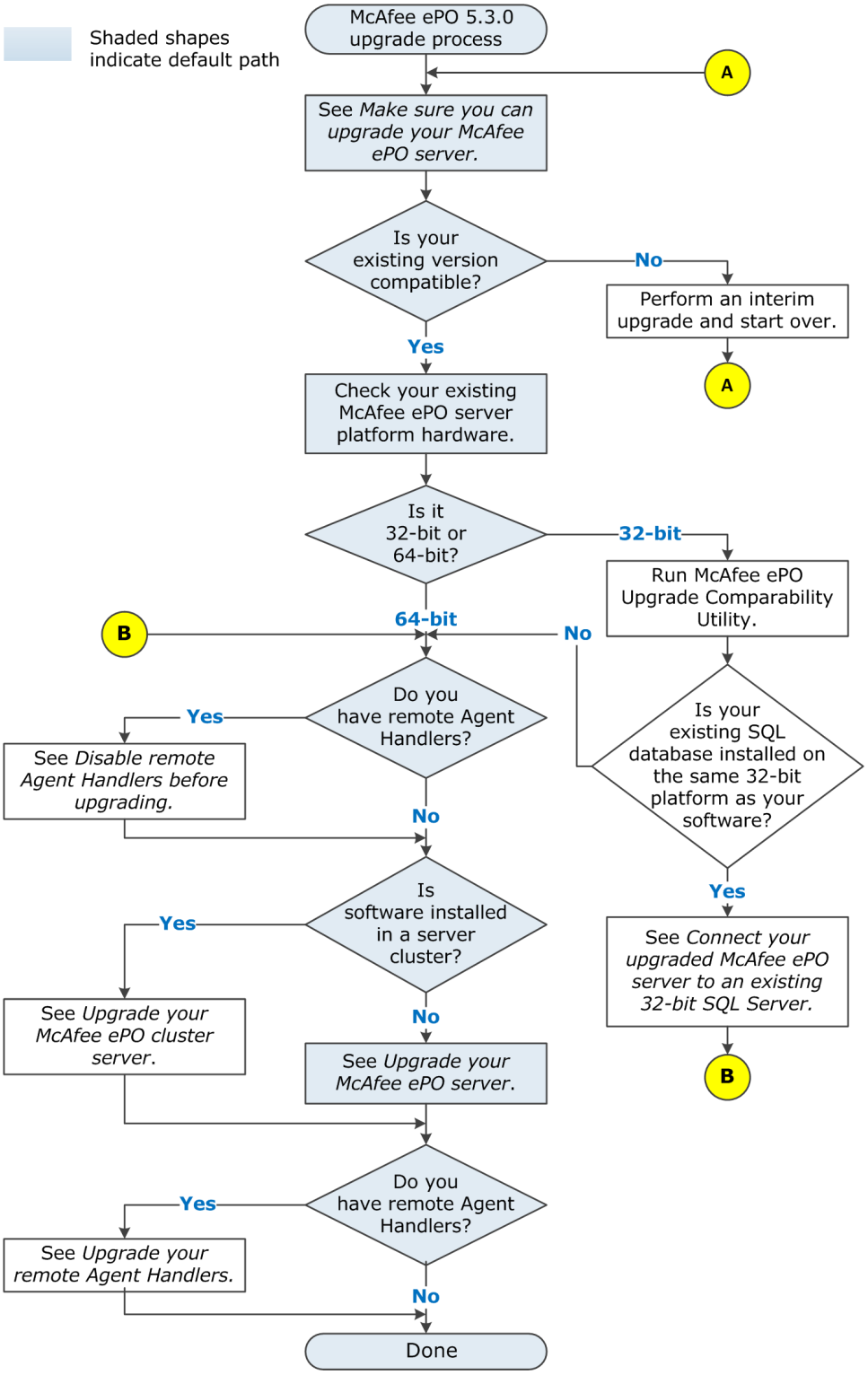
You can upgrade specific McAfee ePO versions to version 5.3.0. See *Make sure you can upgrade your McAfee ePO server* for upgrade versions.

Contents

- *Upgrade overview*
- *Complete pre-upgrade tasks*
- *Upgrade your McAfee ePO server*
- *Migrating from a 32-bit to a 64-bit platform*
- *Upgrade your McAfee ePO cluster server*
- *Upgrade your remote Agent Handlers*

Upgrade overview

The process of upgrading your McAfee ePO server to version 5.3.0 depends on your current environment. Factors include whether you are upgrading a McAfee ePO 32-bit or 64-bit server, using Agent Handlers, or installing McAfee ePO in a cluster environment.



Read through the upgrade information completely to make sure that you understand the upgrade tasks required for your McAfee ePO server.

See also

Migrating from a 32-bit to a 64-bit platform on page 46
Upgrade your McAfee ePO server on page 44
Upgrade your McAfee ePO cluster server on page 52
Upgrade your remote Agent Handlers on page 53

Complete pre-upgrade tasks

Complete these tasks before you upgrade your McAfee ePO server.

Tasks

- *Make sure you can upgrade your McAfee ePO server* on page 43
  Before upgrading the software on your existing McAfee ePO server, make sure that you can upgrade your existing server to McAfee ePO version 5.3.0.
- *Review products and known issues* on page 43
  Before you install or upgrade your software, review information about supported products and known issues.
- *Back up McAfee ePO databases and directories* on page 44
  Before you upgrade your software, back up all McAfee ePO databases, as well as the McAfee ePO directory.
- *Stop remote Agent Handlers services before upgrading* on page 44
  If you use remote Agent Handlers in your environment, you must stop two McAfee services on each remote Agent Handler server to successfully complete your upgrade.

Make sure you can upgrade your McAfee ePO server

Before upgrading the software on your existing McAfee ePO server, make sure that you can upgrade your existing server to McAfee ePO version 5.3.0.

If your existing McAfee ePO software is installed on a 32-bit platform, you must run the Upgrade Compatibility Utility to migrate the 32-bit configuration to a 64-bit configuration.

You can upgrade these versions to McAfee ePO 5.3.0.

Table 4-1 Minimum McAfee ePO upgrade versions

McAfee ePO version	Server platform	
	32-bit	64-bit
4.6.8	X	X
5.1.0		X
5.1.1		X

You cannot upgrade McAfee ePO version 5.0.0 or 5.0.1 directly to version 5.3. You must install one of these versions first.

Review products and known issues

Before you install or upgrade your software, review information about supported products and known issues.

Task

View the supported products and known issues KnowledgeBase articles.

- View these KnowledgeBase articles:
  - McAfee ePO 5.1.0 Supported Products — KB79169 (`https://kc.mcafee.com/corporate/index?page=content&id=KB79169`)
  - McAfee ePO 5.X installation and patch upgrade checklist for known issues — KB76739 (`https://kc.mcafee.com/corporate/index?page=content&id=KB76739`)

Back up McAfee ePO databases and directories

Before you upgrade your software, back up all McAfee ePO databases, as well as the McAfee ePO directory.

Details on performing these tasks are available in McAfee KnowledgeBase article KB66616 (`https://kc.mcafee.com/corporate/index?page=content&id=KB66616`)

Stop remote Agent Handlers services before upgrading

If you use remote Agent Handlers in your environment, you must stop two McAfee services on each remote Agent Handler server to successfully complete your upgrade.

After your remote Agent Handlers event parser and server services are stopped, you can upgrade your McAfee ePO server. Once the upgrade is complete, upgrade your Agent Handlers software. See *Installing remote Agent Handlers* for details.

Task

1. Log on to the system where the Agent Handler is installed.
2. From Windows **Control Panel**, click **Administrative Tools** | **Services**.
3. In the **Services** list, scroll down and stop these two services.
   - McAfee ePolicy Orchestrator <version> Event Parser — Event Parser service
   - McAfee ePolicy Orchestrator <version> Server — Apache service

   For more information on using the Windows Services panel, see your Microsoft software product documentation.

See also

Upgrade your remote Agent Handlers on page 53

Upgrade your McAfee ePO server

Use `Setup.exe` to upgrade your McAfee ePO server to version 5.3.0.

Before you begin

Update the system that hosts your McAfee ePO server with the latest Microsoft security updates, then turn off Windows updates during the installation process.

If your existing McAfee ePO server is installed on a 32-bit platform, you must run the McAfee ePO 32-bit Upgrade Compatibility Utility. See *Migrating from a 32-bit to a 64-bit platform*.

We recommend that you monitor the upgrade process. You might need to restart your system.

The default location of McAfee ePO software is:

```
C:\Program Files (x86)\McAfee\ePolicy Orchestrator
```

Task

1 Log on to the system using an account with local administrator permissions, download the McAfee ePO 5.3.0 software from the McAfee website, extract files to a temporary location, and find the `Setup.exe` file.

   The executable is located in the downloaded McAfee ePO installation file.

   If you attempt to run `Setup.exe` without first extracting the contents of the .zip file, the installation fails.

2 To launch the McAfee ePolicy Orchestrator InstallShield Wizard, double-click the **Setup.exe** file.

3 In the Welcome dialog box of the installation wizard, click **Next**.

   A warning message might appear listing products from your previous version of McAfee ePO that are no longer supported with the 5.3.0 version of the software. These products are not migrated to the McAfee ePO 5.3.0 repository.

4 The Install additional software step lists any remaining prerequisites. To install them, click **Next**.

5 In the Database Information step, confirm the automatically selected **Database Server** and **Database Name** are correct. If not, select the correct information from the lists.

6 Specify which type of **Database Server Credentials** to use, then click **Next**.

Database Server Credentials	Description
Windows authentication	1 From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. 2 Type the **User name** and **Password**. If you are using a previously installed SQL Server, make sure that your user account has access.
SQL authentication	Type the **User name** and **Password** for your SQL Server. Make sure that credentials you provide represent an existing user on the SQL Server with appropriate rights. The **Domain** menu is grayed out when using SQL authentication.

7 In the Administrator Information step:

   a For the **Username**, replace the default admin and type your primary Administrator account user name.

   b For the **Password**, type your primary Administrator account password.

   c For the **Keystore encryption password**, type a password to encrypt Disaster Recovery Snapshot records.

   Keep a record of this password. If you ever need to restore your McAfee ePO database, you need this password to decrypt the Disaster Recovery Snapshot records.

8 In the **Type License Key** step, click **Next**.

   Your existing licence key is automatically populated in the field.

9 Accept the **McAfee End User License Agreement** and click **OK**.

10 In the Ready to install the Program dialog box, decide if you want to **Send anonymous usage information to McAfee**, then click **Install** to begin installing the software.

   Deselect the checkbox if you don't want McAfee to collect anonymous diagnostic and usage data.

11 In the Installing McAfee ePolicy Orchestrator dialog box, the **Status** area shows the progress of the upgrade. When the upgrade is complete, click **Next**.

12 In the InstallShield Wizard Completed dialog box, click **Finish** to complete the installation.

   If you want, click **Yes, I want to start McAfee ePolicy Orchestrator now.**

Your McAfee ePO software is now updated. Double-click on your desktop to start using your McAfee ePO server, or browse to the server from a remote web console (`https://<servername>:<port>`)

Migrating from a 32-bit to a 64-bit platform

If your existing McAfee ePO server is installed on a 32-bit server platform, run the Upgrade Compatibility Utility before upgrading to McAfee ePO version 5.3.0.

Before proceeding with the migration, confirm that McAfee ePO is installed on a 32-bit server platform. If not, see *Upgrade your McAfee ePO server*.

32-bit Upgrade Compatibility Utility overview

If you are upgrading your 32-bit McAfee ePO server to a 64-bit McAfee ePO 5.3.0 platform, run this utility to convert your existing configuration to the upgrade server and run the **Product Compatibility Check**.

For minimum McAfee ePO upgrade versions, see *Complete pre-upgrade tasks*.

This figure shows the interface of the **Upgrade Compatibility Utility**.

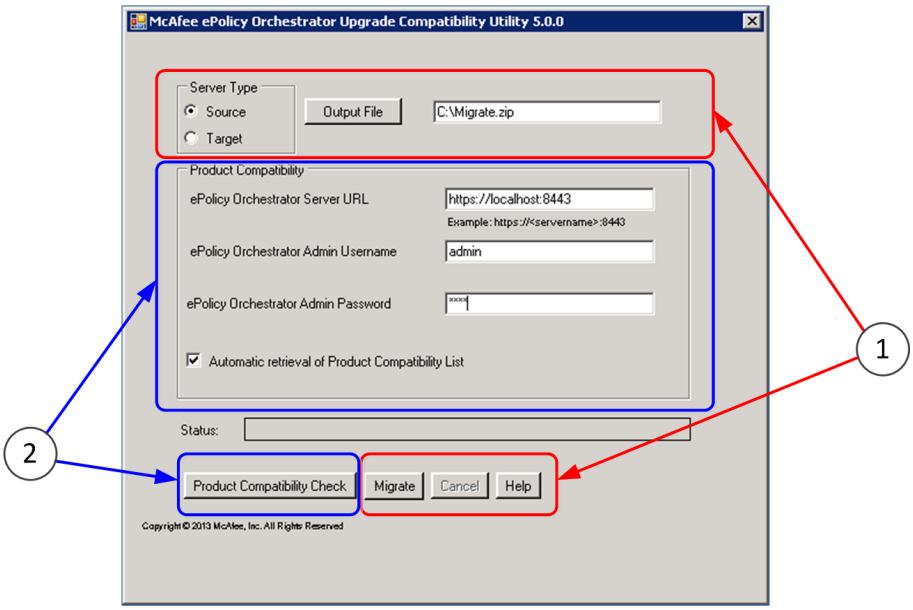


Figure 4-1 Upgrade Compatibility Utility user interface

1 Converts your 32-bit McAfee ePO software configuration to your new 64-bit version 5.3.0 platform.

This utility does not move the existing McAfee ePO SQL database to a new database server. See the Microsoft documentation to move your database.

2 Runs a **Product Compatibility Check** that determines if any of your installed version McAfee ePO software extensions are *not* compatible with your new upgrade version of McAfee ePO.

Product Compatibility Check

An initial Product Compatibility List is included in the McAfee ePO software package that you downloaded from the McAfee website.

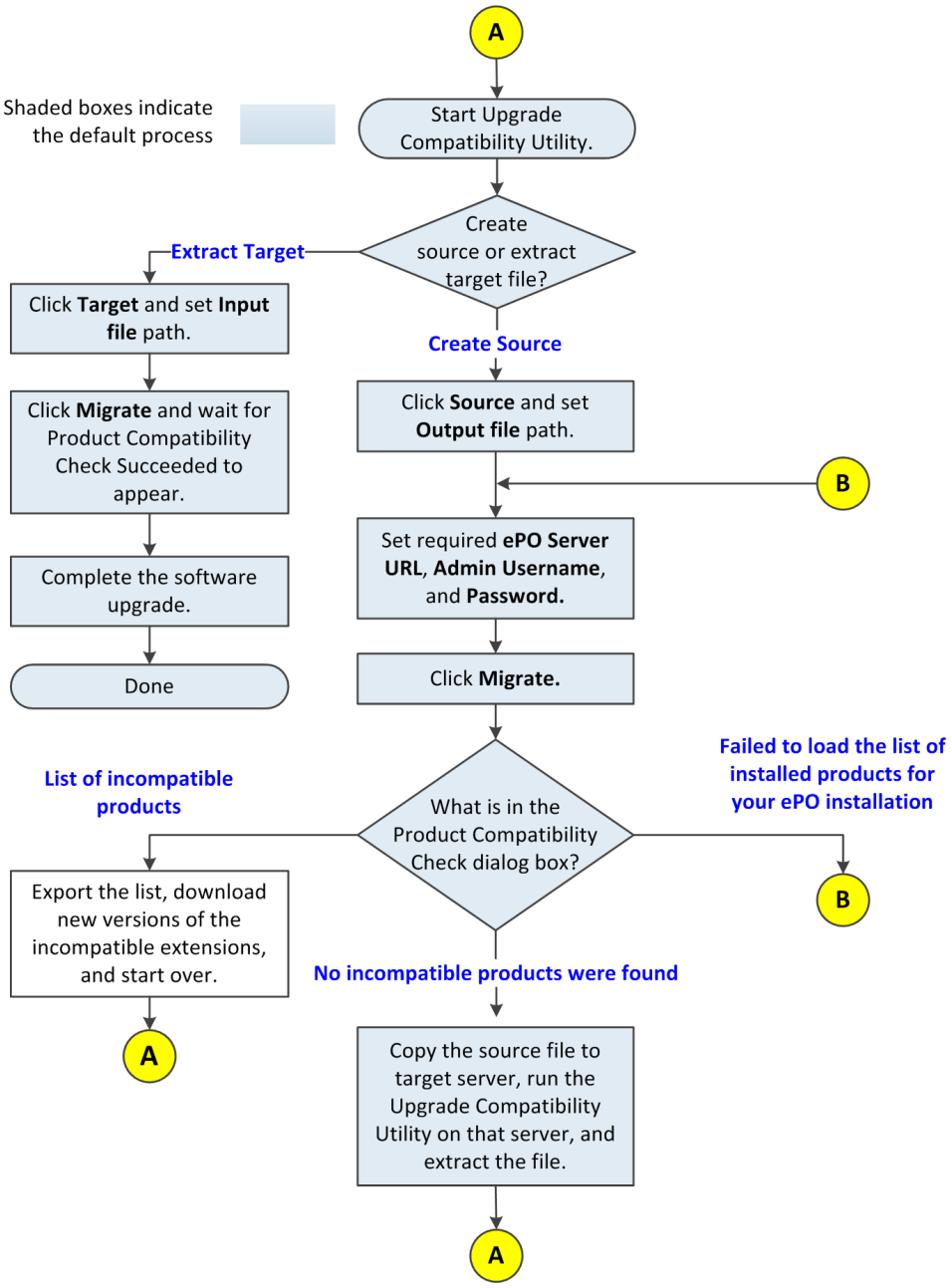
When you run the **Product Compatibility Check**, it retrieves the most current list of compatible extensions from a trusted McAfee source over the Internet. If the Internet source is unavailable, or if the downloaded list can't be verified, McAfee ePO uses the latest version available.

If you have the **Product Compatibility List** enabled, the McAfee ePO server updates this list, in the background, once a day.

When you run the **Product Compatibility Check**, it either confirms that the current product extensions are compatible with the new version of McAfee ePO, or creates a list of blocked or disabled extensions.

- **Blocked** extensions prevent the McAfee ePO software upgrade.
- **Disabled** extensions do not block the upgrade, but the extension is not initialized until a known replacement extension is installed.

This flowchart describes the steps needed to convert the 32-bit McAfee ePO configuration to a 64-bit platform and complete the upgrade compatibility process.



See also

Upgrade overview on page 42

Run the Upgrade Compatibility Utility

Run the Upgrade Compatibility Utility to convert your existing 32-bit McAfee ePO version 4.x configuration to a new 64-bit version 5.3.0 configuration file.

Before you begin

1 Back up your McAfee ePO database.

2 Extract the McAfee ePO 5.3.0 installation software and find the `UpgradeCompatibility` folder, which contains the `UpgradeCompatibility.exe` file.

3 Microsoft .NET Framework 3.5 or later is required to use the Upgrade Compatibility Utility. See the Microsoft Download Center to download and install this software.

An error appears if this software framework is not installed and you try to run the utility.

The utility also runs a Product Compatibility Check to determine if existing product extensions can interfere with a successful migration from version 4.x to 5.3.0.

This utility is specifically designed to convert your 32-bit McAfee ePO version 4.x configuration to a 64-bit platform version 5.3.0 configuration.

Task

1 Find and run the McAfee ePolicy Orchestrator Upgrade Compatibility Utility.

a Download the McAfee ePO 5.3.0 software from the McAfee website.

The software is in the downloaded McAfee ePO installation file.

b Extract the files to a temporary location, find the `UpgradeCompatibility` folder, and double-click **UpgradeCompatibility.exe**.

The **ePolicy Orchestrator Upgrade Compatibility Utility** appears.

2 Create the version 4.x source output file.

a Under **Server Type**, click **Source**.

b Click **Output File**, browse to where you want to store the McAfee ePO data file, and add a name with the extension `.zip`. By default the file is stored as `C:\Migrate.zip`.

c To remotely log on to your existing McAfee ePO server, type the information at these prompts:

- **ePolicy Orchestrator Server URL**
- **ePolicy Orchestrator Admin Username**
- **ePolicy Orchestrator Admin Password**

d Choose which Product Compatibility List file to use:

- Select **Automatic retrieval of Product Compatibility List** — The Product Compatibility Check automatically retrieves the most current list from a trusted McAfee source over the Internet. If the Internet source is unavailable, or if the list can't be verified, the check uses the list downloaded with the latest version of the McAfee ePO software.
- Deselect **Automatic retrieval of Product Compatibility List** — The Product Compatibility Check uses the manually downloaded Product Compatibility List.

Click ProductCompatibilityList.xml to manually download the file.

e Click **Migrate** or **Product Compatibility Check**. One of these appears in the **ePO Product Compatibility Check** dialog box:

- **No incompatible products were found** — Continue to step 3.
  The compression process can take several minutes on an enterprise McAfee ePO server.
- **A list of incompatible products** — Use this list of blocked and disabled extensions. Use this list to replace the blocked extension with compatible versions, then retry the Product Compatibility Check.
  If an extension is disabled, it does not block the upgrade, but the extension isn't initialized after the McAfee ePO upgrade until a known replacement extension is installed.
- **Failed to load the list of installed products for your ePO installation** — This indicates the Product Compatibility List file is not available, or the information that you typed to access the source McAfee ePO server was incorrect. Return to step 2c and try again.

If you interrupt the migration file creation process, start the process over again to create a new file.

Status displays the file creation status and **Migration Completed** appears when the process is complete.

3 On the upgrade server:

a Download the McAfee ePO 5.3.0 software from the McAfee website.

The software is in the downloaded McAfee ePO installation file.

You can also copy the McAfee ePO 5.3.0 software from the existing McAfee ePO 4.x server where you downloaded it.

b Extract the files to a temporary location, find the folder `UpgradeCompatibility`, and double-click **UpgradeCompatibility.exe**.

c Copy the McAfee ePO data file that you created to the upgrade server.

If you have McAfee® VirusScan® Enterprise installed on the upgrade server, disable the On-Access Scan before you migrate your version 4.x files to your 5.3.0 server.

d Under **Server Type**, click **Target**.

e Click **Input File** and browse to where you copied the source configuration file. By default the file is stored as `C:\Migrate.zip`.

f Click **Migrate** to extract and convert McAfee ePO configuration files to 5.3.0 configuration files.

Status displays the file extraction status and **Migration Completed** appears when the process is done. The extraction process can take several minutes on an enterprise McAfee ePO server.

If you interrupt the migration file extraction process, restart the upgrade McAfee ePO 5.3.0 server and start the migration process over again to extract the file.

4 Run the upgrade described in *Upgrade your McAfee ePO server*.

All your existing McAfee ePO 4.x server configuration files are copied to your McAfee ePO 5.3.0 server. You are now ready to run the ePolicy Orchestrator software upgrade.

If your McAfee ePO upgrade fails and you have migrated and run the upgrade to McAfee ePO 5.3.0, revert to the backup database on your version 4.x server.

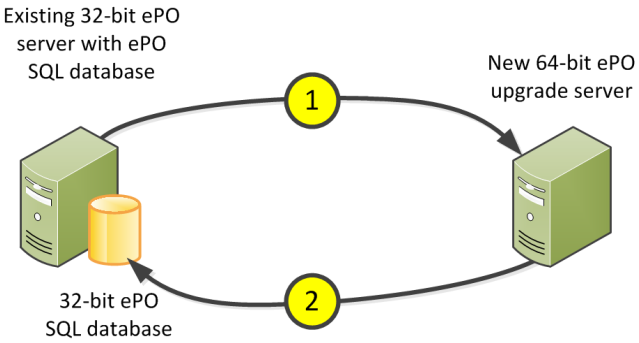
See also

Upgrade your McAfee ePO server on page 44

Connect your upgraded McAfee ePO server to an existing 32-bit SQL Server

When you upgrade your existing 32-bit McAfee ePO server to a 64-bit McAfee ePO 5.3.0 platform, you can connect back to the previous 32-bit McAfee ePO SQL database. The existing database connection information is included in the Migrate.zip that file you created using the Upgrade Compatibility Utility.

This example shows the two major steps needed to use the existing 32-bit McAfee ePO database.



To reuse an existing 32-bit McAfee ePO database:

1 Use the Upgrade Compatibility Utility to convert an existing 32-bit McAfee ePO server configuration to the new 64-bit server configuration and start a McAfee ePO custom installation. See *32-bit Upgrade Compatibility Utility overview* for details.

2 During the upgrade, the existing 32-bit McAfee ePO SQL database is configured by default.

We recommend confirming that your upgraded McAfee ePO server is working correctly, then delete the existing 32-bit McAfee ePO software from the existing server. Make sure **Also remove the McAfee ePO database** is *not* selected during the uninstallation process or you will delete the database used by the McAfee ePO upgrade.

Make sure that two instances of McAfee ePO never try to connect to the same SQL database.

Restarting your existing McAfee ePO server if your upgrade fails

When you run the Upgrade Compatibility Utility on your existing server, it changes these three instances of McAfee ePO services' Startup Type to **Disabled**.

- McAfee ePolicy Orchestrator 5.3.x Application Server services
- McAfee ePolicy Orchestrator 5.3.x Event Parser service
- McAfee ePolicy Orchestrator 5.3.x Server

If the upgrade process fails and you need to restart your existing McAfee ePO server, change the **Startup Type** to **Automatic** and restart the existing server.

To change the service **Startup Type**, use the Services snap-in for Windows Server. To start the snap-in, click **Start** and type `services.msc`.

See also

Upgrade overview on page 42

Upgrade your McAfee ePO cluster server

Upgrading your McAfee ePO software in a cluster environment requires special consideration.

Before you begin

To upgrade to McAfee ePO version 5.3.0, your current environment must be supported for upgrading.

You can't use the McAfee ePO 32-bit Upgrade Compatibility Utility when upgrading to version 5.3.0 in a cluster server environment.

Task

1. Depending on your Windows Server, from the active node, open the **ePO group** in your Windows cluster management tool.
   - For Windows Server 2008 — Start Administrative Tools, then click **Failover Cluster Manager**.
   - For Windows Server 2012 — Start Server Manager, then on the **Tools** menu, click **Failover Cluster Manager**.
2. Take each of these Generic Service resources offline, then delete them:
   - ePolicy Orchestrator Server
   - ePolicy Orchestrator Application Server
   - ePolicy Orchestrator Event Parser

   Do not modify these resources, which are required for a successfully upgrade:
   - Data drive
   - McAfee ePO virtual IP address
   - McAfee ePO virtual Network Name
3. Open the Services Control Manager and start each of these services:
   - ePolicy Orchestrator Server
   - ePolicy Orchestrator Application Server
   - ePolicy Orchestrator Event Parser

   Repeat this step on each node before you begin installing your new software.
4. Install your new McAfee ePO software on each node.

   For detailed installation steps, see *Install ePolicy Orchestrator software on each node* under *Perform Cluster installation*.
5. After completing installation on each node, create the new Generic Service resources for version 5.3.0 of the software. Configuration for these resources depends on your operating system. For operating system-specific configuration details, see *Create the Generic Service resources* under *Perform Cluster installation*.

See also

Perform cluster installation on page 24

Upgrade your remote Agent Handlers

When you upgrade your McAfee ePO server software, upgrade any remote Agent Handlers installed throughout your environment. Agent Handlers must be upgraded separately.

Remote Agent Handlers installed with previous versions of your software are not compatible with this new version, and are not upgraded automatically.

The upgrade process is a streamlined version of the procedure used for first-time installation of a remote Agent Handler. See *Install remote Agent Handlers* under *Installing McAfee ePO* for details.

Task

1. Copy the `Agent Handler` folder, included in the ePolicy Orchestrator software installation package, to the target system.
2. Double-click **Setup.exe** to launch the McAfee ePO Agent Handler InstallShield wizard.
3. Click **Next** to begin the upgrade process.
4. Accept the license agreement, then click **OK**.
5. Click **Install** to begin the installation.
6. The InstallShield wizard completes the installation without any additional input. When the wizard is complete, click **Finish**.
7. When the upgrade is complete, enable your remote Agent Handler from within the ePolicy Orchestrator interface.

   For information on enabling your Remote Agent Handler, see *Work with Agent Handlers* in the product guide or Help.

See also

Upgrade overview on page 42

5

Uninstalling McAfee ePO software

You might need to uninstall the McAfee ePO software if, for example, you are reinstalling it on another server. Use these topics to complete the uninstall process.

If you intend to reinstall McAfee ePO software later, and want to manage agents deployed by the current installation, back up your agent-server communication keys. You cannot restore these keys later.

Contents

- *Uninstall Express and Custom installations*
- *Uninstall cluster installations*

Uninstall Express and Custom installations

Uninstalling the ePolicy Orchestrator software for Express and Custom installations requires specific consideration of your database.

If you used the Setup program to install SQL 2008 Express, you can remove the database added to that SQL Server when you remove the ePolicy Orchestrator software.

Task

1 Close all database management software.

2 On the system where your ePolicy Orchestrator server is installed, open the Windows **Control Panel**, then click **Programs and Features** | **McAfee ePolicy Orchestrator** | **Uninstall/Change**.

3 The **Remove McAfee ePolicy Orchestrator** dialog box opens. Select whether to **Also remove the ePolicy Orchestrator database**, then click **Remove**.

Supply credentials to grant sufficient permissions to remove the database. If the provided credentials are not sufficient, you can select to complete the uninstall process without removing the database. For more information about SQL Server permissions, see *Maintaining your ePolicy Orchestrator databases* in the product guide or Help.

Uninstall cluster installations

Uninstalling McAfee ePO from a cluster environment requires that you take specific steps, depending on which server-class operating system you are running.

Task

1. To set all McAfee ePO services to offline, open the Windows Cluster Administrator/Management tool, then click **Start** | **Programs** | **Administrative Tools** | **Failover Cluster Manager**.
2. In the McAfee ePO application group, right-click each of the McAfee ePO resources and select **Delete**.
3. To uninstall the software, click **Programs and Features** | **McAfee ePolicy Orchestrator** | **Uninstall/Change**.
4. Repeat this task on each node in your cluster.

6

Troubleshooting and log file reference

The most common messages that appear while installing McAfee ePO during an installation and their solutions are listed here. Use this information to troubleshoot problems with your installation.

If you are unable to resolve an issue using the information in this table, contact McAfee Technical Support after you have taken these steps:

1 Verify that you have met the minimum installation requirements.

2 Review McAfee ePolicy Orchestrator Release Notes (`Readme.html`) and click the link to the McAfee KnowledgeBase article to see any known installation issues.

3 Verify that the account you used to log on to the computer where you are installing the software has full administrator permissions to that computer.

4 Collect the exact text of all messages, and make sure to write down any message codes that appear.

5 Gather the installation log files.

Contents

- *Common installation messages and their causes and solutions*
- *Log files for troubleshooting*

Common installation messages and their causes and solutions

ePolicy Orchestrator software provides feedback during installation that might require additional action. Review this table for more information on actions required if these messages appear.

Message	Cause	Solution
You are attempting to upgrade from a product version that is not supported.	No version of ePolicy Orchestrator software has been installed on this computer. You can only upgrade from a supported version of McAfee ePO server. *Make sure you can upgrade your McAfee ePO server* listed under *Complete pre-upgrade tasks*.	See *Installing McAfee ePO* in this guide and select an appropriate installation option.
Internet Explorer 8.0 or later, or Firefox 10 must be installed for this installation to continue.	The computer where you are attempting to install the software is using an unsupported version of the browser.	Install a supported Internet browser before continuing. For more information, see *Supported Internet browsers*.
Another instance of the ePolicy Orchestrator installer is already running.	The ePolicy Orchestrator 5.3 Setup program is already running. You can't run more than one instance of Setup at a time.	Allow the first instance of the installer to complete, or stop the first instance and restart your installation.
For security reasons, McAfee does not allow blank passwords. Please type a valid password to continue.	The **Password** box is blank.	Specify the password of the user account that you want to use.
We recommend that you set the video display resolution to 1024x768 or higher.	The computer where 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 screen after you start the software. For instructions on changing the monitor resolution, see the Windows Help file (click **Start**, then select **Help**).
We recommend that you install the software on a computer with at least 8 GB of RAM.	The computer where you are attempting to install the software does not meet the minimum memory requirement.	Add more memory to your system or select a different system for installation that has at least 8 GB of RAM.
ePolicy Orchestrator 5.3.0 software requires that your computer is running Windows Server 2008, or Windows Server 2012.	The computer where you are attempting to install the software is using a non-supported version of the operating system.	See *Supported server-class operating systems*.
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 McAfee ePO server uses to send agent wake-up 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 uses 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 McAfee ePO server uses to send agent wake-up calls.

Message	Cause	Solution
ePolicy Orchestrator must be installed in a folder. Enter a Destination Folder to continue.	The **Destination Folder** box is blank or shows the root of a drive.	Click **Browse** to select a location. The default location is: `C\Program Files\McAfee\ePolicy Orchestrator`.
Enter a value in the "User Name" field.	The **User name** box is blank.	Specify the user name of the account that you want to use.
The License file is missing or corrupt. Contact support for assistance.	Setup is unable to read the license information required to install the software.	Contact McAfee technical support.
The operating system or Service Pack you are using is not currently supported.	The computer where you are attempting to install the software is using a non-supported version of the operating system.	See *Supported server-class operating systems*.
The passwords you typed do not match. Type a valid password to continue.	The value you typed in **Password** and **Confirm Password** do not match.	Specify the password of the account that you want to use.
The ePolicy Orchestrator license has expired.	Your license to use the software has expired.	Contact your administrator or designated McAfee representative.
This system is not currently configured with a static IP address, which is recommended for the McAfee ePO server.	The computer where you are attempting to install the software does not use a static IP address. We recommend using static IP addresses for McAfee ePO servers to improve performance and reduce bandwidth use.	Specify a static IP address for use with your McAfee ePO server.
Unable to make a connection to the database server. Verify that you provided the account credentials and database server name correctly, then try again.	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.
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.	1 Verify that the **Domain**, **User Name**, and **Password** you provided are typed correctly. 2 Verify that the account you used to log on to this computer has access to this domain.

Log files for troubleshooting

ePolicy Orchestrator provides log files that contain important information when troubleshooting.

These log files are separated into three categories:

- **Installer logs** — Include details about installation path, user credentials, database used, and communication ports configured.
- **Server logs** — Include details about server functionality, client event history, and administrator services.
- **Agent logs** — Include details about agent installation, wake-up calls, updating, and policy enforcement.

Installer logs

Installer log files list details about the McAfee ePO installation process.

These logs provide information about:

- Actions taken by specific components
- Administrator services used by the server
- Success and failure of critical processes

File name	Log type	Location	Description
`AH530-Install-MSI.log`	Agent Handler installation	`%temp%\McAfeeLogs`	This file logs all Agent Handler installation details including: • Installer actions • Installation failures
`AH530-ahetupdll.log`	Temporary	`%temp%` (on the Agent Handler server)	Logs Agent Handler back-end events.
`core-install.log`	Temporary	`%temp%\McAfeeLogs\ePO500-Troubleshoot\MFS`	Generated when the McAfee ePO installer calls the MFS ANT installer. Provides information on: • Creation of server database tables • Installation of server components This file is deleted if the installation succeeds.
`epo-install.log`	Installation	`%temp%\McAfeeLogs\ePO500-Troubleshoot\Mercury Framework`	Created when the McAfee ePO installer calls the ANT installer.
`EPO530-Checkin-Failure.log`	Installation	`%temp%\McAfeeLogs`	Generated when McAfee ePO installer fails to check in any of these package types: • Extensions • Plug-ins • Deployment packages • Agent packages

File name	Log type	Location	Description
EPO530-CommonSetup.log	Installation	%temp%\McAfeeLogs	Contains McAfee ePO installer details such as: • Custom Action logging • SQL, DTS (Microsoft Data Transformation Services), and service-related calls • Registering and unregistering DLLs • Files and folders selected for deletion at restart
EPO530-Install-MSI.log	Installation	%temp%\McAfeeLogs	The primary McAfee ePO installation log. Contains installation details such as installer actions and installation failures.
<ExtensionFileName>.cmd	Temporary	%temp%\McAfeeLogs\ePO500-troubleshoot\OutputFiles	Created by the McAfee ePO installer. Contains the command (sent to Remote-Client) to check in extensions. If the installation succeeds, these files are deleted.
MFS530-CommonSetup.log	Installation	%temp%\McAfeeLogs	Contains core functionality installer details.

Server logs

Server log files contain details about server functionality and various administrator services used by McAfee ePO.

File name	Log type	Location	Description
EpoApSvr_<serverName>.log	Primary	[InstallDir]\DB\Logs	Application Server log file with details about repository actions such as: • Pull tasks • Checking in deployment packages to the repository • Deleting deployment packages from the repository This file is not present until after initial service startup.
Errorlog.<CURRENT_DATETIME>	Apache	[InstallDir]\Apache2\logs	Contains Apache service details. This file is not present until after the Apache service is started for the first time.
Eventparser_<serverName>.log	Primary	[InstallDir]\DB\Logs	Contains McAfee ePO event parser services details, such as product event parsing success or failure.

File name	Log type	Location	Description
`Jakarta_service_<DATE>_<serverName>.log`	Tomcat	`[InstallDir]\Server\logs` *	Contains McAfee ePO Application Server service details. This file is not present until after the initial Tomcat service startup.
`Localhost_access_log.<DATE>.txt`	Tomcat	`[InstallDir]\Server\logs` *	Records all McAfee ePO server requests received from client systems. This file is not present until after the initial Tomcat service startup.
`Orion_<serverName>.log`	Primary	`[InstallDir]\Server\logs` *	Contains platform details and all extensions loaded by default. This file is not present until after the McAfee ePO Application Server service is started for the first time.
`Replication_<serverName>.log`	Server	`[InstallDir]\DB\Logs`	The McAfee ePO server replication log file. This file is generated only when all these are true: • There are distributed repositories. • A replication task has been configured. • A replication task has run.
`Server_<serverName>.log`	Primary	`[InstallDir]\DB\Logs`	Contains details related to these McAfee ePO server services: • Agent-server communications • McAfee ePO Server Agent Handler This file is not present until after initial service startup.
`Stderr_<serverName>.log`	Tomcat	`[InstallDir]\Server\logs` *	Contains any Standard Error output captured by the Tomcat service. This file is not present until after the initial Tomcat service startup.
`<AgentGuid>_<Timestamp>_Server_manifest.xml`	Policy	`[InstallDir]\DB\DEBUG`	Contains details about policy updating issues. To enable this file: 1 Browse to this registry key: `HKEY_LOCAL_MACHINE\Software\Network Associates\ePolicy Orchestrator\` 2 Create this DWORD with value 1: `SaveAgentPolicy` 3 Restart the McAfee ePolicy Orchestrator 5.3.0 Server (Apache) service. We recommend that you enable this file for the minimum time needed to capture the required information, because the resulting files grow rapidly.

* In cluster environments, the log file is located at `[InstallDir]\Bin\Server\logs`.

McAfee Agent logs

McAfee Agent log files contain actions triggered or taken by the McAfee Agent.

File names in this list reflect McAfee Agent version 5.0.0

McAfee Agent 5.0.0 file name	Log type	Location	Description
`masvc_<hostname>.log`	Server	`[Agent DATA Path]\logs`	Generated when `masvc.exe` is used. The file contains information related to: • Property collection • Agent server communication • Policy enforcement • Update sessions • Scheduling of tasks
`macmnsvc_<hostname>.log`	McAfee Agent	`[Agent DATA Path]\logs`	Generated when `macmnsvc.exe` is used. The file contains information related to: • Peer-to-Peer server • SuperAgent • Wake-up • RelayServer
`macompatsvc_<hostname>.log`	McAfee Agent	`[Agent DATA Path]\logs`	Generated when `macompatsvc.exe` is used. The file contains information related to the compatibility of managed products with McAfee Agent services.
`masvc_<hostname>_backup_<backupcountnumber>.log`	McAfee Agent	`[Agent DATA Path]\logs`	Generated as backup files for agent services.
`marepomirror.log`	Server		Generated when `marepomirror.exe` is used. The file contains information related to mirroring of the repository.
`FrmInst_<hostname>.log`	McAfee Agent	`%temp%\McAfeeLogs`	Generated when `FrmInst.exe` is used to install the McAfee Agent. This file contains: • Informational messages • Progress messages • Failure messages if installation fails

McAfee Agent 5.0.0 file name	Log type	Location	Description
mcScript.log	McAfee Agent Debug	[Agent DATA Path]\logs	Contains the results of script commands used during agent deployment and updating. To enable the DEBUG mode for this log, set this DWORD value on the client's registry key: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2 Delete this key when you finish troubleshooting.
MFEAgent.msi.<system time stamp>.log	McAfee Agent	%temp%\McAfeeLogs	Contains details about the MSI installation of the agent.
UpdaterUI_<system>.log	McAfee Agent	%temp%\McAfeeLogs	Contains details about the updates to managed products on the client system.

File names in this list reflect McAfee Agent version 4.8.0

McAfee Agent 4.8.0 file name	Log type	Location	Description
Agent_<system>.log	Agent	[Agent DATA Path]\DB	Generated on client systems when the server deploys an agent to them. This file contains details related to: • Agent-server communication • Policy enforcement • Other agent tasks
FrmInst_<system>.log	Agent	%temp%\McAfeeLogs	Generated when FrmInst.exe is used to install the McAfee Agent. This file contains: • Informational messages • Progress messages • Failure messages if installation fails
MCScript.log	Agent Debug	[Agent DATA Path]\DB	Contains the results of script commands used during agent deployment and updating. To enable the DEBUG mode for this log, set this DWORD value on the client's registry key: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2 Delete this key when you finish troubleshooting.
MfeAgent.MSI.<DATE>.log	Agent	%temp%\McAfeeLogs	Contains details about the MSI installation of the agent.
PrdMgr_<SYSTEM>.log	Agent	[Agent DATA Path]\DB	Contains details about agent communications with other McAfee products.
UpdaterUI_<system>.log	Agent	%temp%\McAfeeLogs	Contains details about the updates to managed products on the client system.

McAfee Agent error logs

When the McAfee Agent traps errors, they are reported in McAfee Agent error logs. These error logs are created at `%temp%\McAfeeLogs`. McAfee Agent error logs are named for their primary log counterpart. For example, when errors occur while performing client tasks, the `MCScript_Error.log` file is created. Error logs contain only details about errors.

Index

32-bit to 64-bit platform conversion utility 44, 49, 51
64-bit server-class operating systems supported
    ePolicy Orchestrator 9

A

about this guide 5
Agent Handlers
    authenticate domain credentials 11
    installation 31
    operating systems 11
    restore connections 38
    stop services 44
    upgrading 53
application group in a cluster installation 26
Automatic Product Configuration
    disable command line parameter 21
    overview 15

B

backup databases and directories 44
browsers supported 11

C

Chrome browser 11
Client Access Point configuration in a cluster installation 26, 29
cluster installation
    restore 36
    Windows Server 2008 25
    Windows Server 2012 28
cluster servers
    installation 24
    restore 36
    terminology 24
    testing 31
    uninstalling 56
    upgrading 52
communication ports, *See* ports
conventions and icons used in this guide 5

D

data drive configuration in a cluster installation 27, 29
database collation 10
database servers
    communication port 14
    support for 10
    upgrade from 32-bit version 4.x to 64-bit version 5.3.0 49
Disaster Recovery Snapshot
    keystore encryption passphrase 12, 21, 22
    used during Express installation 18, 19
    used during software restore 34
    used during software upgrade 44
distributed repositories, requirements 16
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

E

ePolicy Orchestrator software 34
error messages, causes of 58

F

Firefox 11

G

Generic Service resources in a cluster installation 27, 30

I

installation
    Agent Handlers 31
    cluster 25, 28
    completing 32
    custom completion 22
    custom setup 21
    express 18
    options 17, 33
    preparing for 12
    preparing for, cluster servers 24
    required SQL Server roles 13
    servers 17, 33
Internet browsers supported 11
Internet Explorer 11
    Enhanced Security 11

K

keystore encryption passphrase 12, 21, 22

L

languages supported 9

M

McAfee ePO software
- default file location 44
- minimum upgrade versions 43
- remote web console access 19, 44

McAfee ServicePortal, accessing 6
Microsoft SQL Servers 10

N

nested triggers 10

O

operating systems supported
- Agent Handler servers 11
- McAfee ePO servers 9

P

passwords
- supported formats 14

permissions
- SQL 14

ports
- changing 14
- default values 14

Product Compatibility Check
- command line options 21
- supported products 16, 43
- Upgrade Compatibility Utility 46
- using Upgrade Compatibility Utility 49

Q

quorum and data drive configuration in a cluster installation 27, 29

R

requirements
- distributed repositories 16
- hardware 7
- operating systems 9
- software 8
- SQL Server roles 13

restore
- cluster installation 36
- ePolicy Orchestrator software 34
- remote Agent Handler connections to servers 38

restore process 34

S

Safari browser 11
servers
- installation 17, 33
- SQL permissions 14
- uninstalling 55
- upgrading 44
- virtual infrastructure 10

ServicePortal, finding product documentation 6
Snapshot 34
SQL Servers
- backup file 34
- backup file in cluster 36
- configuration requirements 10
- installation 13
- installation requirements 13
- roles 13
- support for 10
- upgrade scenarios 13

support for
- Agent Handler operating systems 11
- Internet browsers 11
- operating systems 9
- SQL Servers 10
- virtual servers 10

supported products 16, 43

T

technical support, finding product information 6
troubleshooting, error messages 58

U

uninstalling
- cluster servers 56
- servers 55

Upgrade Compatibility Utility 49
- overview 46
- Product Compatibility check 46
- to reuse an exist 32-bit database 51

upgrading
- Agent Handler 53
- cluster servers 52
- prepare your environment and minimum McAfee ePO version 43
- prerequisites 44
- process flowchart 42
- restarting existing server if needed 51
- servers 44
- stop Agent Handlers services before 44
- Upgrade Compatibility Utility 46

V

virtual servers supported 10

W

Windows Server 2008
cluster installation 25
support for Agent Handlers 11
Windows Server 2012
cluster installation 28
Windows Server 2012 *(continued)*
support for Agent Handlers 11
support for ePolicy Orchestrator 9