Installation Guide

Revision B

McAfee ePolicy Orchestrator 5.9.0

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

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

Contents

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.

Italic	Title of a book, chapter, or topic; a new term; emphasis
Bold	Text that is emphasized
`Monospace`	Commands and other text that the user types; a code sample; a displayed message
Narrow Bold	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:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
	**Tip:** Best practice information
	**Caution:** Important 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

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

1 Installation requirements and recommendations

Your environment requires specific hardware and software to run McAfee® ePolicy Orchestrator® (McAfee® ePO™) software. Review these requirements and recommendations before installing your McAfee ePO software to make sure that your installation is successful.

Run a pre-installation audit to make sure that your environment meets the minimum requirements for a successful installation. For information about downloading and using the tool, see the *McAfee ePO Pre-Installation Auditor Release Notes*.

Contents

System 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, use 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.
Free disk space	20 GB — Recommended minimum.
IP address	Use static IP addresses for McAfee ePO. McAfee ePO supports both IPv4 and IPv6 networks.
Memory	8-GB available RAM recommended minimum.

Component	Requirements and recommendations
Network Interface Card (NIC)	100 MB or higher  If using a server with more than one IP address, McAfee ePO uses the first identified IP address. If you want to use more IP addresses for agent-server communication, create Agent Handler groups for each IP address.
Ports	• Don't use port 8443 for HTTPS communication. Although port 8443 is the default port, it is the primary port used by many web-based activities. This port is a frequent target for malicious exploitation, so 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 that you have the required and recommended software installed on your server system before installing McAfee ePO.

Software	Requirements and recommendations
Microsoft .NET Framework 3.5 or later	Required — This software is required for all versions of SQL Server and SQL Server Express.
Microsoft updates	Recommended — Make sure that 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.
Security software	Recommended. • Install and update the anti-virus software on the server and scan for viruses. • Install and update firewall software on the server.
Supported browser	Recommended — Although it is not a prerequisite for installation, McAfee ePO requires the use of a supported browser. For more information, see *Supported Internet browsers*.
Supported SQL Server	Required — A supported version of SQL Server or SQL Server Express is required to install McAfee ePO.

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 Server 2008 R2 Service Pack 1
- Windows Server 2012
- Windows Server 2012 Service Pack 1
- Windows Server 2012 R2
- Windows Server 2016

If you are using Windows Server 2012 or later, also install Microsoft update 2919355.

Operating systems for evaluation

You can use these operating systems to evaluate the McAfee ePO software, but support is not provided for these operating systems.

- Windows 7 (x64 only)
- Windows 8 and 8.1 (x64 only)
- Windows 10

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 tries to display text in English.

- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- Dutch
- English
- Finnish
- French (Standard)
- German (Standard)
- Italian
- Japanese
- Korean
- Norwegian
- Portuguese (Brazilian)
- 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 5.1
- VMware ESXi 5.5
- VMware ESXi 6
- 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.

McAfee ePO supports any edition of these Microsoft SQL Servers.

- Microsoft SQL Server 2008 Express
- Microsoft SQL Server 2008, with Service Pack 1 or later
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012 Express
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016

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 (these characters are 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

McAfee ePO software requires the use of one of these supported Internet browsers.

- Internet Explorer 11 or later
- Firefox 45 and later
- Chrome 51 and later
- Safari 10 and later (macOS only, Windows not supported)
- Microsoft Edge

TLS requirement

If you are using an older browser, make sure that you have TLS 1.1 or 1.2 enabled.

Using Internet Explorer enhanced security

If you're using Internet Explorer with enhanced security enabled, add the McAfee ePO server address to your Internet Explorer trusted sites list (formatted as `https://<servername>`). If you don't, Internet Explorer displays an error message when you try 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 Windows authentication 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 server-class operating systems:

- Windows Server 2008 R2 Service Pack 1
- Windows Server 2012
- Windows Server 2012 R2

If you are using Windows Server 2012 or later, also install Microsoft update 2919355.

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 for evaluations).
- Microsoft SQL authentication requires one of these credentials:
  - Windows authentication credentials — Domain credentials that have Database Owner (dbo) rights on the SQL server
  - SQL authentication credentials.
- A destination folder for McAfee ePO software installation (required for Custom and Cluster installations).

- A supported SQL Server.
- If you already have an SQL Server installed, you must provide these details (depending on your configuration) on the Database Information page:
  - 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.
  - 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 choose to configure their McAfee ePO server automatically. But manual configuration might be better for users with restrictions such as:
  - 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

McAfee ePO requires the use of a supported SQL Server. The installation scenario described in detail in this guide assumes that you have already installed a supported version of SQL Server or SQL Server Express.

In this scenario, you install the SQL Server manually and then the InstallShield wizard installs the McAfee ePO software. For more information about installing SQL Server, see your SQL Server software documentation.

Cluster installation requires that you manually install SQL Server on a system other than where you install McAfee ePO.

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 McAfee ePO software, specific SQL Server roles are required to install successfully.

If you use an existing SQL Server, or manually install a new SQL Server, provide credentials during the McAfee ePO 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 McAfee ePO 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 McAfee ePO 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 McAfee ePO 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, McAfee ePO downloads and installs all 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 McAfee ePO and is finished before you log on.

If the Automatic Product Configuration page appears when you initially log on to McAfee ePO, 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.

- Supported products — KB87142.
- Known issues — KB87673.

See also

Start and complete the InstallShield wizard on page 36

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. The **McAfee ePolicy Orchestrator - InstallShield Wizard** guides you through the installation process.

Contents

Set up your SQL Server and start the installation software

When you set up the McAfee ePO installation, you download the software and start the installation.

Before you begin

- Make sure that you have read, understood, and complied with the information in *Installation requirements and recommendations*. Also, verify that you are running a supported version of SQL Server or SQL Server Express.
- Update the system that hosts your McAfee ePO server with the latest Microsoft security updates, then turn off Windows updates during the installation process.

Monitor the installation process. You might need to restart your system.

Task

1 Set up SQL Server and make sure that you can communicate with the database server.

   a Verify that the SQL Browser Service is running.

   b 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.

   c Decide if you want to run Automatic Product Configuration after installation.

   d Decide if you want to download the Product Compatibility List automatically from the McAfee website, or use an alternate list stored locally.

2 Enable TCP/IP protocol in the **SQL Server Configuration Manager**.

   a Start **SQL Server Configuration Manager**.

   b In the console pane, expand **SQL Server Network Configuration**.

   c In the details pane, right-click **TCP/IP** to open the **TCP/IP Properties** window.

d Select the **Protocol** tab, click **Enabled**, and select **Yes**.

e Click **Apply** and then **OK** to close the **Warning** dialog.

TCP/IP is enabled. You can now restart the service to make sure that your changes take effect.

f In the console pane, click **SQL Server Services**.

g In the details pane, right-click the SQL Server service and click **Restart**.

Your changes are now complete. Before continuing, make sure to capture the value for **TCP Dynamic Ports**.

h Right-click **TCP/IP** to open the **TCP/IP Properties** window.

i Select the **IP Addresses** tab.

j Under **IPAll**, make note of the value for **TCP Dynamic Ports**.

For example, `49657`. This information might be needed later in the installation.

You are now ready to begin the McAfee ePO installation.

3 Log on to the Windows Server computer to be used as the McAfee ePO server.

Use an account with local administrator permissions.

4 Locate the software you downloaded from the McAfee website and extract the files to a temporary location. Double-click **Setup.exe**.

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

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

The **McAfee ePolicy Orchestrator - InstallShield Wizard** starts.

5 Click **Next** to continue the installation.

The installation is set up and started. Now configure the database, communication ports, and license to complete the installation.

Configure your McAfee ePO installation in the InstallShield Wizard

Complete the installation by selecting and configuring your database, communication port, and license options.

Monitor the installation process when using the installation wizard. You might need to restart your system.

Task

1 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**.

2 In the Database Information step, specify information for your database, then click **Next**.

a Specify the **Database Server** and **Database Name**.

Database Server Select your server from the list. If it does not appear, enter the information based on whether you are using SQL Server or SQL Server Express:

- `ServerName\SQLSERVER`
- `ServerName\SQLEXPRESS`

Database Name This value populates automatically.

b Specify which type of **Database Server Credentials** to use.

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.

c If necessary, specify the value for the **SQL server TCP port**.

Use the value from the **TCP Dynamic Ports** field you wrote down when you enabled TCP/IP. This port is used to communicate between your McAfee ePO server and database server.

3 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 change 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**. To change your other port settings later, reinstall your McAfee ePO software.

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

a Type the user name and password you want to use for your primary administrator account.

b Type the keystore encryption password.

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

5 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 the application.

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

7 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.

8 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`).

Complete a first-time installation

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

To complete your initial configuration quickly, accept the default policies. If you need to customize your configuration, you can use the McAfee ePO 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.

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.

Install McAfee ePO software on the restore server

To re-create the McAfee ePO server, reinstall the McAfee ePO software on a server and link it to the restored SQL database.

Monitor the restore process. You might need to restart your system.

Task

1. When you select the existing SQL Server, gather this information and complete these steps before beginning your installation. These steps ensure that your McAfee ePO software can communicate with the database server:
   a. Verify that the SQL Browser Service is running.
   b. Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.
   c. 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.
   d. Confirm the SQL backup file that you copied from the primary server was restored using the Microsoft SQL process.
   e. Stop Remote Agent Handler services on all systems, before restoring the McAfee ePO software.
2. If you have remote Agent Handlers configured, log on to the systems where the Agent Handlers are installed, then open the Windows Services panel. Stop the **McAfee Event Parser** and **McAfee Apache** services.

   See your Microsoft software product documentation for more information about using the Windows Services panel.
3. Using an account with local administrator permissions, log on to the Windows Server computer used as the restore McAfee ePO server.
4. Downloaded from the McAfee website, extract the files to a temporary location, and double-click **Setup.exe**.

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

   The McAfee ePolicy Orchestrator - InstallShield Wizard is started.

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

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

7 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**.

8 In the **Database Information** step, select the Microsoft SQL Server name from the **Database Server** list. 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 McAfee ePO 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.

9 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.

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

11 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.

12 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 the application.

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

14 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.

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

This dialog box includes checkboxes to read the release notes and to start McAfee ePO.

16 If you restored McAfee ePO to a 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.

Create 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.

17 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. Start the **McAfee Event Parser** and **McAfee Apache** services.

Your McAfee ePO 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>`).

4 Upgrading McAfee ePO

Perform these tasks to upgrade McAfee ePO.

Read through the upgrade information completely to make sure that you understand the required steps.

If upgrading from your current version of McAfee ePO is not supported, upgrade to an interim version first.

Contents

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 upgrade your McAfee ePO, 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.

The Product Compatibility Check 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.

Upgrade checklist

This checklist includes all steps to upgrade one standalone McAfee ePO server.

Additional upgrade steps are required if you installed McAfee ePO in a cluster environment.

Upgrade checklist
1. Plan for a successful upgrade
☐ Read the release notes.
☐ Review known issues, upgrade paths, and supported products.
☐ Gather required information.
☐ Run the Pre-Installation Auditor.  Verification steps with an asterisk (*) are performed for you by the Pre-Installation Auditor.
☐ Schedule the upgrade and inform users.
2. Prepare your environment
☐ Back up McAfee ePO databases and directories.
☐ Update registered server certificates.
☐ Make sure that your Windows Server has enough disk space.*
☐ Make sure that the Windows 8.3 naming convention is enabled.*
☐ Disable McAfee Agent installation tasks set to Run Immediately.
☐ Disable scheduled server tasks and Windows tasks.
☐ Disable third-party software.
3. Prepare your SQL database
☐ Update your Windows Server.
☐ Make sure that you use correct permissions.*
☐ Verify the SQL instance that McAfee ePO uses.*
☐ Make sure that Auto Close is set to False.*
☐ Make sure that Arithmetic Abort Enabled is set to True.*
☐ Make sure that the Compatibility level is set to 100 or higher.*
☐ Make sure that the correct database collation is set.*
☐ Make sure that the SQL browser service is running.*
☐ Make sure that IPv6 is enabled.
4. Perform the upgrade
☐ Download and extract the software.
☐ Stop automatic updates.
☐ Stop remote Agent Handlers.
☐ Stop McAfee ePO services.
☐ Start and complete the InstallShield wizard.

Upgrade checklist
☐ Upgrade remote Agent Handlers.
5. Restart processes and verify the upgrade
☐ Restart automatic updates.
☐ Migrate SHA-1 certificates to SHA-2 or higher.
☐ Verify the upgrade.

Plan for a successful upgrade

Perform these tasks to understand the upgrade process and the specific upgrade steps your environemnt requires.

Tasks

- *Read the release notes* on page 27
  The release notes describe important information about your McAfee ePO upgrade and we recommend that you read the whole document.
- *Review known issues, upgrade paths, and supported products* on page 28
  Before you upgrade your software, review known issues, and the latest information about supported upgrade paths and products.
- *Gather required information* on page 28
  Make sure that you have this information before you start the upgrade process.
- *Best practice: Run the Pre-Installation Auditor* on page 28
  Before you upgrade McAfee ePO, run the McAfee ePO Pre-Installation Auditor to reduce or prevent upgrade issues.
- *Schedule the upgrade and inform users* on page 29
  The amount of time required for the upgrade depends on your environment and the size of your database.

Read the release notes

The release notes describe important information about your McAfee ePO upgrade and we recommend that you read the whole document.

The McAfee ePO server release notes include information about these items:

- Upgrade paths
- New features
- Enhancements
- Resolved issues (patches only)

Review known issues, upgrade paths, and supported products

Before you upgrade your software, review known issues, and the latest information about supported upgrade paths and products.

Task

- View these KnowledgeBase articles:
  - Supported upgrade paths — KB86693

    If upgrading from your current version of McAfee ePO is not supported, upgrade to an interim version first.

  - Supported products — KB87142
  - List of McAfee ePO known issues — KB87673

Gather required information

Make sure that you have this information before you start the upgrade process.

- Grant number
- License key
- Database server and database name
- Database server credentials (either Windows credentials or SQL Server credentials)

  Windows Server authentication credentials
  - Domain
  - User name
  - Password

  SQL Server authentication credentials
  - User name
  - Password

- Primary administrator account credentials
  - User name
  - Password
- Keystore encryption password

Best practice: Run the Pre-Installation Auditor

Before you upgrade McAfee ePO, run the McAfee ePO Pre-Installation Auditor to reduce or prevent upgrade issues.

Running the McAfee ePO Pre-Installation Auditor automates many of the verification tasks included in the upgrade process.

The McAfee ePO Pre-Installation Auditor tool performs these checks:

- Confirms that your server meets the McAfee ePO and SQL Server hardware requirements.
- Confirms that you have the needed SQL Server access and permissions.
- Verifies that the services that must be stopped, can be, and that no third-party software can cause the services to start unexpectedly.
- Identifies the SQL Server browser status.
- Determines whether database encryption is enabled.

- Determines whether the SQL Server auto-close feature is enabled.
- Identifies the database recovery model.
- Checks for Microsoft Windows scheduled tasks and automatic updates.
- Determines whether Microsoft Windows 8.3 naming is enabled.
- Checks for pending file rename operations in this registry:
  HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations.
- Checks for OS permissions.
- Identifies the versions of McAfee ePO that the server OS and version support.
- Identifies the versions of McAfee ePO that the server OS and version support.
- Checks whether the database option for Arithmetic Abort is enabled.
- Checks the compatibility level of the SQL database.
- Checks whether the database index fragmentation is below the suggested limit.
- Checks whether the ePO version you plan to upgrade supports migration to SHA-2.
- Checks the database replication status.
- Checks the database query cursor threshold value.
- Verifies that no file handles are open in the McAfee ePO directory.
- Provides a list of running McAfee ePO server tasks and warns you to disable them.
- Estimates the required upgrade time.

Task

1. Download the McAfee ePO Pre-Installation Auditor from the McAfee ePO Downloads page: secure.mcafee.com/apps/downloads/my-products/login.aspx.
2. Double-click ePIP.exe to launch the auditor.
   For more information, see the *Pre-Installation Auditor Release Notes*.

Schedule the upgrade and inform users

The amount of time required for the upgrade depends on your environment and the size of your database.

Run the McAfee ePO Pre-Installation Auditor to get an estimate of how long your upgrade might take.

During the upgrade, your managed systems are still protected, but your security software updates are not performed.

- Notify your McAfee ePO administrators about the upcoming downtime.

Prepare your environment

Perform these tasks to avoid problems during the upgrade process.

Tasks

- *Back up McAfee ePO databases and directories* on page 30
  Before you upgrade your software, back up all McAfee ePO databases, as well as the McAfee ePO directory.
- *Update registered server certificates* on page 30
  Make sure that the certificates for any registered servers that McAfee ePO communicates with are supported by McAfee ePO.
- *Make sure that your Windows Server has enough disk space* on page 30
  Verify that the system temp drive and the McAfee ePO installation drive have sufficient disk space for the upgrade.
- *Make sure that the Windows 8.3 naming convention is enabled* on page 31
  Enable Windows 8.3 naming convention on the drive where McAfee ePO is installed.
- *Disable McAfee Agent installation tasks set to run immediately* on page 31
  Before you upgrade the McAfee Agent extension, disable any McAfee Agent installation tasks that are scheduled to Run Immediately.
- *Disable scheduled server tasks* on page 32
  Disable any tasks that might interfere with the upgrade (such as purge events, pull tasks, and replication tasks).
- *Disable third-party software* on page 32
  Disable any software that automatically restarts services on your McAfee ePO server.

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 backups are available in McAfee KnowledgeBase article KB66616.

Update registered server certificates

Make sure that the certificates for any registered servers that McAfee ePO communicates with are supported by McAfee ePO.

We recommend that you use certificates with RSA public key lengths of 2048 bits or greater for the registered servers that McAfee ePO connects to.

McAfee ePO might not be able to connect to registered servers that use less secure certificates, such as certificates with RSA public key lengths of only 1024 bits.

For more information, including additional supported public key algorithms and key lengths, see KnowledgeBase article, KB87731.

Make sure that your Windows Server has enough disk space

Verify that the system temp drive and the McAfee ePO installation drive have sufficient disk space for the upgrade.

- **System temp drive** — Requires 2 GB or more of free disk space
- **Installation drive** — Requires up to three times the size of the McAfee\ePolicy Orchestrator folder or 20 GB, whichever is greater.

For example, if the McAfee ePO server is installed on the same drive as the system temp folder and the McAfee ePO installation directory is 15 GB in size, the required available hard disk space is 47 GB (15 GB X 3 + 2 GB). If the McAfee ePO installation directory is 5 GB in size, the minimum size requirement means that the drive must have 22 GB (20 GB + 2 GB) of free space.

If you don't have enough space, purge log files and temporary files from the McAfee ePO Installation directory before upgrading:

Task

1 Stop the McAfee ePO services.

   a Press Windows+R, type **services.msc**, then click **OK**.

   b Right-click the following services and select **Stop**:

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

2 Delete the files in these folders:

   - **<McAfee ePO installation directory>\Server\Logs**
   - **<McAfee ePO installation directory>\DB\Logs**
   - **<McAfee ePO installation directory>\Apache2\Logs**
   - **<McAfee ePO installation directory>\Server\Temp**

3 Start the McAfee ePO services

   a Press Windows+R, type **services.msc**, then click **OK**.

   b Right-click the following services and select **Start**:

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

Make sure that the Windows 8.3 naming convention is enabled

Enable Windows 8.3 naming convention on the drive where McAfee ePO is installed.

For instructions to enable the 8.3 naming convention, see Solution 1 in KB51431.

Disable McAfee Agent installation tasks set to run immediately

Before you upgrade the McAfee Agent extension, disable any McAfee Agent installation tasks that are scheduled to Run Immediately.

When you check in a new McAfee Agentextension to McAfee ePO, previously executed tasks that are configured to run immediately are rerun at the next agent-server communication. This recurrence can cause products to be redeployed to managed systems.

To prevent this recurrence, before you upgrade the McAfee Agent extension or before the first ASC after the extension upgrade, disable any tasks that are configured to install the McAfee Agent and are scheduled to run immediately.

For more information, see KB74420.

Disable scheduled server tasks

Disable any tasks that might interfere with the upgrade (such as purge events, pull tasks, and replication tasks).

If you are using McAfee® Drive Encryption, disable all LDAP Sync tasks before initiating the upgrade of the McAfee ePO server. Make sure that there are no LDAP Sync tasks running. If any are running, wait for them to complete.

For more information, see KB84690.

Disable third-party software

Disable any software that automatically restarts services on your McAfee ePO server.

Disable monitoring software (such as Microsoft System Center Operations Manager) that might affect the McAfee ePO services starting and stopping during the upgrade.

Also, disable any third-party security software that could potentially introduce permissions issues.

Prepare your SQL database

To avoid upgrade problems and reduce upgrade times, perform these tasks on your SQL Server.

To quickly verify your SQL Server settings, run the Pre-Installation Auditor.

Tasks

- *Verify your SQL Server instance* on page 32
  Use one of these methods to determine the SQL Server instance that McAfee ePO uses.
- *Make sure that you use the correct SQL Server permissions* on page 33
  The account used to access the SQL Server requires these permissions.
- *Update your database server certificates* on page 33
  Use certificates with RSA public key lengths of 2048 bits or greater for the SQL Server that McAfee ePO connects to.
- *Verify SQL Server settings* on page 34
  To avoid potential upgrade problems, verify these SQL Server settings.

Verify your SQL Server instance

Use one of these methods to determine the SQL Server instance that McAfee ePO uses.

- Check the SQL Server service name: (SQL Server (SQLEXPRESS)) or (SQL Server (EPOSERVER)).
- In SQL Server Management Studio, run this query:

```
select @@servername
go
```

Make sure that you use the correct SQL Server permissions

The account used to access the SQL Server requires these permissions.

Task

1 Start the SQL Server Management Studio: Click **Start** | **Programs** | **Microsoft SQL Server** | **SQL Server Management Studio**.

2 Make sure that the default database is set to master.

   a Expand **Security** | **Logins**.

   b Right-click the account and select **Properties**.

   c Make sure that the default database is set to master.

   d Expand **User Mapping** and make sure that the account has dbo in the schema for the database.

3 Make sure that your account is the db_owner in the database security properties.

   a Expand **Databases** | **[your ePO database]** | **Security** | **Users**.

   b Right-click the **dbo** account and select **Properties**.

   c Ensure that the account has dbo in the **Default schema** for the database.

4 If you use an NT account to authenticate to the McAfee ePO database, make sure that the account has local administrator rights on the McAfee ePO server.

   For detailed information about required SQL permissions, see KB75766.

Update your database server certificates

Use certificates with RSA public key lengths of 2048 bits or greater for the SQL Server that McAfee ePO connects to.

We recommend that you use certificates with RSA public key lengths of 2048 bits or greater for the SQL database that McAfee ePO connects to.

McAfee ePO might not be able to connect to SQL servers that use less secure certificates, such as certificates with RSA public key lengths of only 1024 bits.

Before upgrading, update the Windows Server where your SQL Server is installed with the latest Microsoft Service Packs and hotfixes. If you are using the default certificates, these updates help ensure that the SQL Server prioritizes more secure cipher suites and can communicate with McAfee ePO.

For more information, including additional supported public key algorithms and key lengths, see KnowledgeBase article, KB87731.

Verify SQL Server settings

To avoid potential upgrade problems, verify these SQL Server settings.

Task

1 Start the SQL Server Management Studio: Click **Start** | **Programs** | **Microsoft SQL Server** | **SQL Server Management Studio**.

2 Make sure that Auto Close is set to False.

   a Right-click the McAfee ePO database and select **Properties**.

   b Click **Options** and ensure Auto Close is set to False.

   If it is not, click **Auto Close**, select **False**, then click **OK**.

3 Make sure that **Arithmetic Abort** is set to True.

   a Right-click the McAfee ePO database and select **Properties**.

   b Click **Options** and make sure **Arithmetic Abort Enabled** is set to True.

   If it is not, click **Arithmetic Abort Enabled**, select **True**, then click **OK**.

4 Make sure that the **Compatibility Level** is set to 100.

   a Right-click the McAfee ePO database and select **Properties**.

   b Click **Options** and make sure that **Compatibility Level** is set to 100 instead of 80 or 90.

   If it is not, select **100** from the **Compatibility level** drop-down menu, then click **OK**.

5 Make sure that the correct database collation is set.

   McAfee ePO usesSQL_Latin1_General_CP1_CI_AS as the default collation for the database when an upgrade or fresh installation of McAfee ePO is performed.

   a In **Object Explorer**, expand **Databases**, and locate the McAfee ePO database.

   b Right-click the McAfee ePO database and select **Properties**.

   c Review the Collation field on the General page.

   For detailed information about supported collation types for McAfee ePO, see KB73717.

6 Make sure that the SQL browser service is running.

   a Press **Windows + R**, type `services.msc`, then click **OK**.

   b Locate the SQL Server Browser service and make sure that it is started and running.

   If the service is not started, right-click the SQL Server Browser service and select **Start**.

7 Make sure IPv6 is enabled.

   In a pure IPv6 environment, make sure that only IPv6 is enabled on the SQL Server that hosts the McAfee ePO database.

Perform the upgrade

Stop updates and services, and start the InstallShield wizard.

Tasks

- *Download and extract the software* on page 35
  Download the McAfee ePO software to your Windows Server.
- *Stop automatic updates* on page 35
  Disable Windows updates to ensure they do not interfere with your McAfee ePO installation or upgrade.
- *Stop remote Agent Handlers services before upgrading* on page 35
  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.
- *Stop McAfee ePO services* on page 36
  Perform these steps to make sure that the Apache Tomcat service stops.
- *Start and complete the InstallShield wizard* on page 36
  Use `Setup.exe` to upgrade your McAfee ePO server.
- *Upgrade your remote Agent Handlers* on page 38
  When you upgrade your McAfee ePO server software, upgrade any remote Agent Handlers installed throughout your environment. Agent Handlers must be upgraded separately.

Download and extract the software

Download the McAfee ePO software to your Windows Server.

Task

1 Use your Grant Number to log on to the My Products page: My Products.

2 Click the link for your product suite. On the Current Versions tab, click **McAfee ePolicy Orchestrator**.

3 On the Software Downloads tab, click the download link.

4 Extract the downloaded .zip file to a temporary location.

If you try to run Setup.exe before extracting the contents of the .zip file, the installation fails.

Stop automatic updates

Disable Windows updates to ensure they do not interfere with your McAfee ePO installation or upgrade.

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.

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 about using the Windows Services panel, see your Microsoft software product documentation.

See also

Upgrade your remote Agent Handlers on page 38

Stop McAfee ePO services

Perform these steps to make sure that the Apache Tomcat service stops.

If you don't perform these steps, the Apache Tomcat service can continue to run in some environments, causing problems during the upgrade.

Task

1 Press **Windows+R**, type `services.msc`, then click **OK**.

2 Stop these services:

- ePolicy Orchestrator Server Service
- ePolicy Orchestrator Event Parser Service

3 Restart the ePolicy Orchestrator Server Service.

Start and complete the InstallShield wizard

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

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, and find the `Setup.exe` file.

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

If you try to run `Setup.exe` before extracting the contents of the .zip file, the installation fails.

2 To start the McAfee ePO InstallShield wizard, right-click the **Setup.exe** file, and run it as an administrator.

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 this version of the software. These products are not migrated to the new McAfee ePO repository.

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

5 In the Database Information step, confirm that 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 want 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 license 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**.

Deselect **Send anonymous usage information to McAfee** 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**.

During the upgrade process, if your McAfee ePO database is large the process might take a long time and this message appears: Your McAfee ePO database has too many events. Your upgrade might take a long time.

For information about removing old events, see KB68961.

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>`)

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.

Task

1. Copy the `Agent Handler` folder, included in the McAfee ePO software installation package, to the target system.
2. Double-click **Setup.exe** to start 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 the McAfee ePO interface.

Restart updates and verify the upgrade

Restart automatic updates. Make sure your policies, tasks, product deployments, and repositories updated correctly and reflect your choices and customizations.

Task

1. Enable Windows updates to ensure that your servers receive the latest updates and patches.
2. Make sure that your policies, tasks, product deployments, and repositories are accurate and reflect your choices and customizations.
3. To verify McAfee ePO is operating correctly, run a query or server task.
4. To verify connectivity, perform a McAfee Agent wake-up call with one or more managed systems.
5. Make sure that your registered servers are communicating with McAfee ePO.

Migrate SHA-1 certificates to SHA-2 or higher

To remediate vulnerabilities in your McAfee ePO environment, migrate your existing certificates to more secure algorithm certificates or regenerate them.

The SHA-1 algorithm has reached end-of-life (EOL). Many organizations are deprecating TLS/SSL certificates signed by the SHA-1 algorithm. If you continue to use SHA-1 certificates, browsers such as Google Chrome or Microsoft Internet Explorer will flag the McAfee ePO console as an unsecure HTTPS site.

If you have upgraded McAfee ePO from an older version, migrate McAfee ePO certificates to the latest hash algorithm. A fresh installation of McAfee ePO installs the latest hash algorithm certificates.

The **Certificate Manager** allows you to:

- Migrate certificates that are signed by older signing algorithm to the new algorithm such as SHA-1 to SHA-256.
- Regenerate your certificates when your existing certificates are compromised due to vulnerabilities in your environment.
- Migrate or regenerate certificates for managed products that are derived from McAfee ePO root CA.

This task replaces certificates that are used for all these McAfee ePO operations:

- Agent-server communication
- Authenticating to browsers
- Certificate-based user authentication

Read these instructions carefully before proceeding with the steps. If you activate the new certificates before they are populated on the systems in your network, those systems won't be able to connect to your McAfee ePO server until the agents on those systems are re-installed.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Log on as an administrator, then click **Menu** | **Configuration** | **Certificate Manager**.

The Certificate Manager page provides information about the installed Root Certificate, Agent Handler certificates, server certificates, and other certificates that are derived from McAfee ePO root Certificate Authority (CA).

2 Click **Regenerate Certificate**, then click **OK** to confirm the certificate generation.

The McAfee ePO root CA and other certificates that are derived from the root CA are regenerated and stored in a temporary location on the server. The time required to complete the regeneration process depends on the number of Agent Handlers and extensions that derive certificates from McAfee ePO root CA.

3 After the certificates regenerate, wait for sufficient saturation of the new certificates throughout your environment.

As agents communicate to the McAfee ePO server, they are given the new certificate. The percentage of agents that have received the newly-generated certificates is provided in the **Certificate Manager** under **Product: Agent Handler** | **Status**.

This distribution percentage is based on the number of agent-server communications that have occurred since the certificates were regenerated. Unmanaged inactive systems will affect this percentage.

Make sure that the distribution percentage is as close to 100% as possible before you continue. Otherwise, any pending systems will not receive the newly generated certificates and will be unable to communicate with the McAfee ePO after the certificates are activated. You can stay in this state for as long as is necessary to achieve sufficient saturation.

4 Once you've achieved a distribution percentage close to 100%, click **Activate Certificates** to carry out all future operations using the new certificates.

A backup of the original certificates is created, and a message appears.

5 Click **OK**. You must re-install any agents that still use the old certificates to restore agent-to-server communication.

6 Once activation of certificates is complete, perform these steps.
   a Stop the Agent Handler services (including the Remote Agent Handler services).
   b Restart the McAfee ePO services.
   c Start the Agent Handler services.
7 Monitor your environment and make sure that your agents are successfully communicating.
   You can cancel the migration at this point to roll back the certificate and restore agent-to-server communication; however, this is not possible after you have completed the next step.
8 Click **Finish Migration** to complete the certificate migration.
   The certificate backup taken during activation is deleted.

For any issues during the migration, click **Cancel Migration** to revert to the previous certificates. If you cancel the migration, stop the Agent Handler services, restart the McAfee ePO service, and start the Agent Handler service again.

You can start the certificate migration again after fixing any issues.

Upgrade your McAfee ePO cluster server

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

Before you begin

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

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 change 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.

5 After completing installation on each node, create the new Generic Service resources. Configuration for these resources depends on your operating system.

See also

Perform cluster installation on page 57

5 Uninstalling McAfee ePO

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.

Uninstall McAfee ePO

Uninstalling the McAfee ePO software requires specific consideration of your database.

Task

1 Close all database management software.

2 On the system where your McAfee ePO 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 complete the uninstall process without removing the database.

6 Managing Agent Handlers

After installing or restoring McAfee ePO, you can install or restore the master Agent Handler for your server.

Contents

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 one, 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.

To use more IP addresses for agent-server communication, create an Agent Handler group, and add the additional IP address to the virtual IP address input field.

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 McAfee ePO software installation package.
2. Copy the `Agent Handler` folder to the intended Agent Handler server system.
3. Double-click **Setup.exe** to start 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. The path characters are 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 system 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 remains available for Agent Handler communication.

c Type the **ePO Admin User** name and **ePO Admin Password** of a user with McAfee ePO 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 the McAfee ePO interface.

Restore remote Agent Handler connections

After you restored your McAfee ePO server and SQL database, you must change 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

1 On the Agent Handler server, find the `Agent Handler` folder you extracted from the McAfee ePO software installation package.

2 Double-click `Setup.exe` to start the McAfee Agent Handler InstallShield wizard. After some installation activities take place in the background, the InstallShield wizard opens. Click **Next** to begin the change 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 system 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 remains available for Agent Handler communication.

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

   d Click **Next** to use the **ePO Admin** credentials to access the database as well; make sure that 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 the ePolicy Orchestrator interface.

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

7 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 the *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

McAfee ePO provides feedback during installation that might require additional action. Review this table for more information about 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 McAfee ePO software has been installed on this computer. You can only upgrade from a supported version of McAfee ePO server.	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 trying to install the software is using an unsupported version of the browser.	Install a supported Internet browser before continuing.
Another instance of the ePolicy Orchestrator installer is already running.	The McAfee ePO setup program is already running. You can't run more than one instance of the installer at a time.	Allow the first instance of the installer to finish, or stop the first instance and restart your installation.

Message	Cause	Solution
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 trying 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 whole 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 trying 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 software requires that your computer is running Windows Server 2008, or Windows Server 2012.	The computer where you are trying to install the software is using a non-supported version of the operating system.	Use a supported server-class operating system.
Enter a value in the "Agent Broadcast communication" field.	The **Agent Broadcast communication port** box is blank.	Specify the port number (default is 8082) that the McAfee ePO server uses to send 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 McAfee Agent wake-up calls.
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 trying to install the software is using a non-supported version of the operating system.	Use a supported server-class operating system.
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.

Message	Cause	Solution
This system is not currently configured with a static IP address, which is recommended for the McAfee ePO server.	The computer where you are trying 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 McAfee ePO 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 OrchestratorMcAfee ePO 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
AH590-Install-MSI.log	Agent Handler installation	%temp%\McAfeeLogs	This file logs all Agent Handler installation details including: • Installer actions • Installation failures
AH590-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 about: • 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.
EPO590-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
EPO590-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
EPO590-Install-MSI.log	Installation	%temp%\McAfeeLogs	The primary McAfee ePO installation log. Contains installation details such as installer actions and installation failures.

File name	Log type	Location	Description
`<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.
`MFS590-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.
`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.

File name	Log type	Location	Description
`Replication _<serverName> .log`	Server	`[InstallDir]\DB \Logs`	The McAfee ePO server replication log file. This file is generated only when all these criteria 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 Server (Apache) service. Enable this file for the minimum time to capture the required information, because the resulting files grow rapidly.

* In cluster environments, the log file is 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
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.

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.

A Cluster installations

In addition to the standard installation process, you can install McAfee ePO into a Microsoft Cluster Server (MSCS) environment.

Contents

Perform cluster installation

McAfee ePO 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 additional steps. 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 about MSCS setup, see the Microsoft documentation.

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

Cluster installation terminology

This terminology is used in the cluster installation instructions.

Term	Definition
Data drive	One of the two drives required by Microsoft Cluster Server and McAfee ePO. The data drive is a remote drive that is accessible to all nodes in the cluster, and is the location where you install the McAfee ePO files.
ePO Virtual IP address resource	The IP address resource that you create as part of the McAfee ePO 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.
ePO Virtual Network Name resource	The Network Name resource that you create as part of the McAfee ePO 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 McAfee ePO 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 2012.

- 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 McAfee ePO 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 McAfee ePO 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. Turn off Windows updates during the installation process.

Tasks

- *Create the ePolicy Orchestrator application group* on page 59
  The ePolicy Orchestrator application group is required to separate the McAfee ePO application from the Microsoft Cluster Services in your cluster environment.
- *Create the Client Access Point* on page 59
  The Client Access Point defines the McAfee ePO Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.
- *Add the data drive* on page 59
  The data drive is the location where you install the McAfee ePO software. Use a remote drive that all nodes in your cluster can access.
- *Install McAfee ePO software on each node* on page 59
  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 60
  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 McAfee ePO 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 McAfee ePO 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 McAfee ePO 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 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 **Cluster**, 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. 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 Application Server	No changes necessary.	Data drive
ePolicy Orchestrator Server	Remove the **Startup parameters** and add a blank space.  Apache Http Server does not start with any startup parameters specified, and an empty entry is not permitted. Therefore, a blank space is required to start Apache Http Server.	ePolicy Orchestrator Application Server
ePolicy Orchestrator Event Parser	No changes necessary.	ePolicy Orchestrator 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 have 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 McAfee ePO 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 61
  The McAfee ePO 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 61
  The Client Access Point defines the McAfee ePO Virtual IP address and Virtual Network names so your cluster nodes can communicate with your McAfee ePO server.
- *Add the data drive* on page 62
  The data drive is the location where you install the McAfee ePO. Use a remote drive that all nodes in your cluster can access.
- *Install McAfee ePO software on each node* on page 62
  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 62
  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 McAfee ePO 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 McAfee ePO 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 McAfee ePO. 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 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 **Cluster**, 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. 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 Application Server	No changes necessary.	ePolicy Orchestrator Server
ePolicy Orchestrator Server	Remove the **Startup parameters** and add a blank space. Apache Http Server does 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	No changes necessary.	ePolicy Orchestrator Application Server

Task

1. For each Generic Service resource in the Cluster Administrator, right-click the **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 McAfee ePO cluster installation

When the McAfee ePO 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 McAfee ePO logon page.

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.

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.

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

For details about product features, usage, and best practices, click **?** or **Help**.

Task

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

   a Verify that the SQL Browser Service is running.

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

   c 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.

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

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

2 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 about using the Windows Services panel.

3 Perform the Cluster installation.

4 Create the McAfee ePO application group or role.

5 Create the Client Access Point.

6 Add the data drive.

7 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**.

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

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

   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 **Cluster**, 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.

8 Enable the cluster server Generic Service resources.

9 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.

10 Make sure that the software functions in a failover situation.

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

Uninstall McAfee ePO from a cluster

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.

B Using McAfee ePO in FIPS mode

McAfee ePO provides an operating mode with a higher level of security for environments that require it. This mode (FIPS mode) follows security guidelines detailed in section 140 of the Federal Information Processing Standard (FIPS).

Contents

FIPS basics

The United States Government developed the Federal Information Processing Standards (FIPS) to define procedures, architecture, algorithms, and other techniques used in computer systems.

FIPS 140-2 is a government standard for encryption and cryptographic modules where each individual encryption component in the overall solution requires an independent certification.

Federal Information Processing Standard 140-2 specifies requirements for hardware and software products that implement cryptographic functionality. FIPS 140-2 is applicable to "all Federal agencies that use cryptographic-based security systems to protect sensitive [but unclassified] information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104–106." The "-2" in FIPS 140-2 denotes the revision of the standard.

The full FIPS text is available online from the National Institute of Standards and Technology (NIST).

FIPS 140-2 cryptographic modules and certification

McAfee leverages these RSA cryptographic modules to meet the requirements for FIPS-compliance.

Table B-1 Validated FIPS 140-2 cryptographic modules used by McAfee ePO

Cryptographic Module	Certificate number	Link
RSA BSAFE Crypto-C Micro Edition (Crypto-C ME) 4.0.1	2056	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2056
RSA BSAFE Crypto-J JSAFE and JCE (JCM) 6.2.1	2057	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057
OpenSSL FIPS Object Module 2.0.8 This module is used only for TLS communication between McAfee ePO and the McAfee Agent.	1747	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747

McAfee ePO operating modes

Depending on your environment and installation choices, McAfee ePO operates in FIPS mode or Mixed mode.

The mode that a McAfee ePO server runs in is determined during installation or upgrade and can't be changed.

FIPS mode

A McAfee ePO server runs in FIPS mode after a clean installation with FIPS mode enabled.

In FIPS mode, McAfee ePO:

- Places extra constraints on the types of security methods allowed
- Performs additional tests on startup
- Allows connections only from a FIPS-compliant version of the McAfee Agent

Reasons to use McAfee ePO in FIPS mode

Your organization might need to use McAfee ePO in FIPS mode if you fall into one of these categories:

- You are a US Government organization required to operate FIPS 140-2 compliant cryptographic models per FISMA or other Federal, State, or local regulations.
- Your organization requires the use of standardized and independently evaluated cryptographic modules per Company policy.

Reasons to not install McAfee ePO in FIPS mode

Don't use McAfee ePO in FIPS mode if you fall into one of these categories:

- You integrate with legacy systems or products that do not support McAfee ePO in FIPS mode.
- Your organizational polices allow you to choose which products or cryptographic modules to operate in FIPS mode. For example, an organization might elect not to operate McAfee ePO in FIPS mode, and only operate McAfee® Drive Encryption on mobile computers in FIPS mode.

Mixed mode

This mode is a standard McAfee ePO installation not running in FIPS mode.

In Mixed mode, McAfee ePO does not follow the constraints and tests described for FIPS mode, and is not compliant with FIPS levels of security.

Your managed systems are still secure, but the certificates and Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are different.

The cryptographic boundary

FIPS compliance requires a physical or logical separation between the interfaces by which critical security parameters enter and leave the cryptographic module and all other interfaces. McAfee ePO creates this separation by creating a *boundary* around the cryptographic module. An approved set of interfaces is used to access the modules inside the boundary. No other mechanism to access these modules is allowed or provided when in FIPS mode.

Modules in the boundary perform these processes:

- FIPS-validated security methods performing cryptography, hashing, and related services running in McAfee ePO
- Startup and verification testing required by FIPS
- Extension and executable signature verification
- TLS connection management
- Cryptographic API wrapping

Some older versions of McAfee products use non-FIPS-compliant ways to access McAfee ePO cryptography and hashing services. Because these products violate the cryptographic boundary, they cannot be used in FIPS mode. Check new versions of McAfee products for further information about FIPS compliance as they are released.

Installing McAfee ePO in FIPS mode

FIPS mode installation requires that you run the `Setup.exe` installer from the command line, adding a command-line option.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. In a command window, change directories to the folder that include the McAfee ePO installer.
2. Invoke the installer with the command `setup.exe ENABLEFIPSMODE=1`.
3. Continue with the installation.

Do not change the default setting for the agent-server secure communication (ASSC) port. Leave it set as enabled on port 443. In FIPS mode, the agents communicate with the McAfee ePO server using this ASSC secure port.

Upgrade from an earlier FIPS-compliant McAfee ePO server

FIPS mode upgrades require you to run the `Setup.exe` installer from the command line, adding a command-line option.

Before you begin

If your existing McAfee ePO server isn't running in FIPS mode, perform a complete reinstallation to change to FIPS mode.

When you install McAfee ePO in FIPS mode, you can't restore a McAfee ePO database from a previous non-FIPS McAfee ePO server.

Task

1. In a command window, change directories to the folder with the new McAfee ePO installer.
2. Invoke the installer with the command `setup.exe ENABLEFIPSMODE=1`.
3. Continue with the upgrade.

Restoring McAfee ePO server in FIPS mode

You can restore a McAfee ePO server in FIPS mode only if the server was previously running in FIPS mode.

You can't restore a McAfee ePO server that wasn't in FIPS mode as a FIPS mode McAfee ePO server. The McAfee ePO software and database must be reinstalled as a new instance of McAfee ePO.

The complete McAfee ePO reinstallation is required because all existing signed and encrypted content was signed with non-FIPS mode keys. Also, the database contains content encrypted with non-FIPS mode keys and can't be decrypted with the FIPS mode keys.

Verify that your McAfee ePO server is in FIPS mode

View the `server.ini` file to make sure that your McAfee ePO server is running in FIPS mode.

Task

1. Use a text editor to open the `server.ini` file.

   The `server.ini` file is located in your McAfee ePO installation directory: `<epoinstalldirectory>\DB\server.ini`.

2. Look for the FipsMode value.

   This value indicates the server operating mode:

   - FipsMode=0 — The server is in Mixed (normal) mode. To put your server in FIPS mode, repeat the installation or upgrade process.
   - FipsMode=1 — The server is in FIPS mode.

Index

K

L

M

N

O

P

Q

R

S

T

U

V

W