McAfee ePolicy Orchestrator 5.10.0 Installation Guide

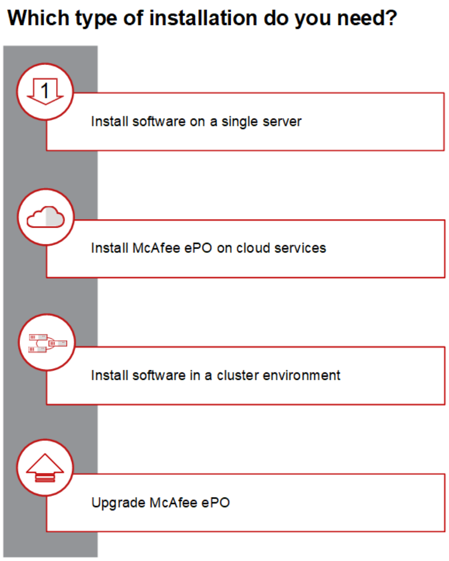
Contents

Installation overview

Which type of installation do you need?

Install McAfee ePO software as a single-server installation or as a cluster, cloud, or upgrade installation.

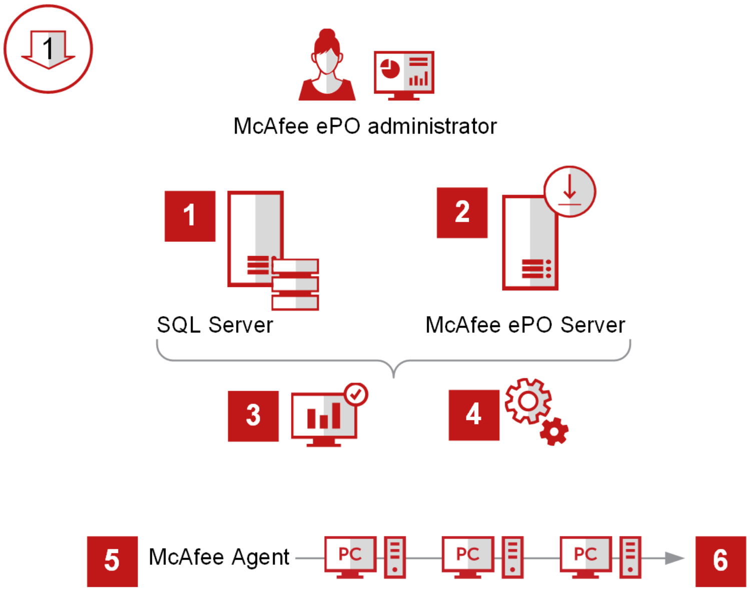
Each installation scenario includes a workflow and procedure. Planning your installation and reviewing system requirements are also part of the installation process.


Which type of installation do you need?
Install software on a single server
Install McAfee ePO on cloud services
Install software in a cluster environment
Upgrade McAfee ePO

Single server installation workflow

Before you can install McAfee ePO software for the first time, you must ensure your SQL Server software is configured for TCP/IP access and install a supported operating system on the McAfee ePO server.

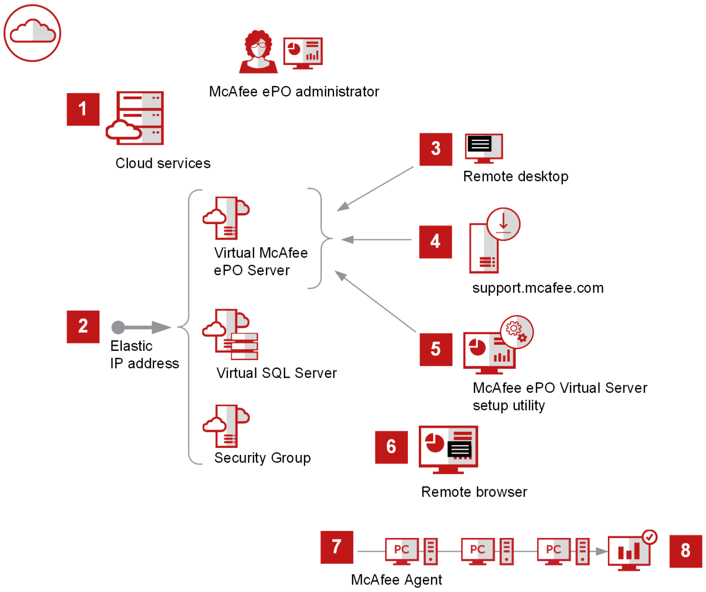
1. Ensure your SQL Server is configured for TCP/IP access.
2. Download and extract the McAfee ePO software from https://secure.mcafee.com/enterprise/en-gb/downloads/my-products.html or the McAfee download site using a grant number.
3. Verify the latest Microsoft updates are running on the SQL Server and the McAfee ePO server.
4. Run the setup utility on the McAfee ePO server to install McAfee ePO. As part of the installation process the McAfee ePO Pre-Installation Auditor checks for compliance issues.
5. Choose a deployment method to deploy McAfee Agent.
6. Confirm that systems are managed by ensuring that McAfee Agent can successfully connect to McAfee ePO.



Cloud services installation workflow

Set up a cloud services account and configure your virtual environment to run cloud services with McAfee ePO.

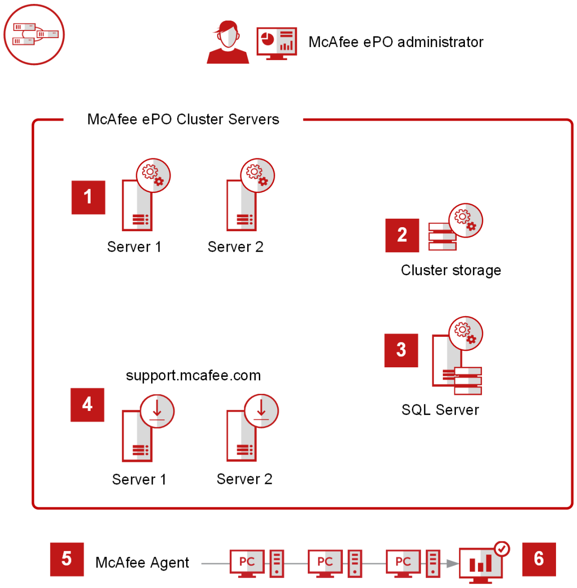
1. Set up a cloud services account and configure these items:
    - Virtual server to use as your McAfee ePO server
    - Virtual SQL Server
    - Security Group
2. Assign an elastic IP address to each virtual server.
3. From a management computer, use Remote Desktop to connect to the virtual McAfee ePO server.
4. From McAfee.com, copy the McAfee ePO software to the virtual McAfee ePO server.
5. From the McAfee ePO server, run the setup utility.
6. Using a remote browser, log on to McAfee ePO using `https://< elastic IP / DNS of virtual McAfee EPO server >:<port>`.
    - Update **McAfee ePO Server Public DNS** in **Server Settings** with elastic IP address or DNS of virtual McAfee ePO server.
    - Update Published DNS name or the IP address of Agent Handler (if any) with elastic IP address or DNS of virtual Agent Handler server.
    - Create a McAfee Agent deployment URL or extract the McAfee Agent deployment package.
7. Choose a deployment method to deploy McAfee Agent.
8. Confirm that systems are managed by ensuring that McAfee Agent can successfully connect to McAfee ePO.



Cluster installation workflow

McAfee ePO provides high availability for server clusters with Microsoft Cluster Server (MSCS) software.

1. Install Microsoft Cluster Server (MSCS) software on all your servers and configure these items:
   - Shared data drive
   - Quorum drive
   - Failover group
2. Configure shared storage.
3. Configure SQL Server and database settings.
4. Download and install McAfee ePO software on all servers.
5. Choose a deployment method to deploy McAfee Agent.
6. Confirm that systems are managed by ensuring that McAfee Agent can successfully connect to McAfee ePO.



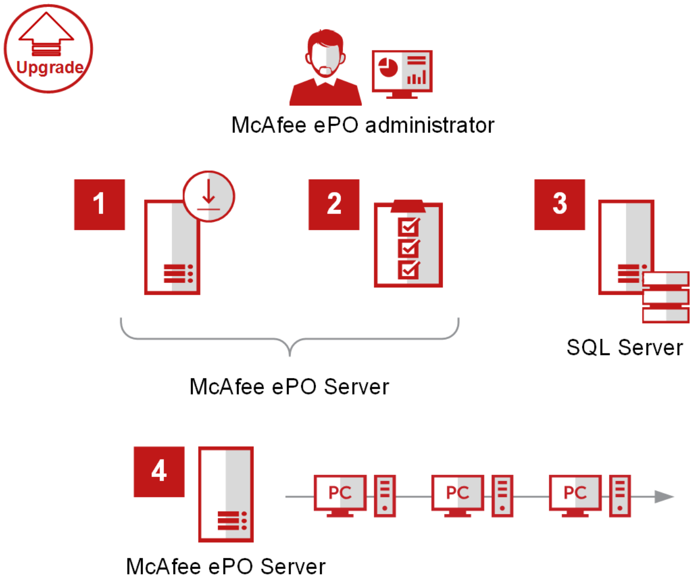
Upgrade installation workflow

Upgrade your existing McAfee ePO software to a new version.

1. Download and extract the software to your McAfee ePO server.
2. Prepare the McAfee ePO server environment.

   The McAfee ePO Pre-Installation Auditor runs, checking compliance with all requirements.

3. Configure SQL Server and database settings.
4. From the McAfee ePO server, run the setup utility.


Upgrade
McAfee ePO administrator
1
2
3
McAfee ePO Server
SQL Server
4
PC
PC
PC
McAfee ePO Server

Planning your installation

To use your McAfee ePO server effectively, create a comprehensive plan specific to your environment.

Considering the unique needs of your environment in advance can reduce the time it takes to get started.

- How many systems do you manage?
- Are your systems located in one network or multiple geographic areas?
- Do you have specific security needs, such as a firewall?
- Do you use Network Address Translation (NAT) in an external network?
- Do you have bandwidth restrictions to remote network segments?
- Do you manage laptops that are connected to the Internet and outside the corporate network?
- Do you have multiple administrators with different permissions across different products, groups of systems, or different functions within the management console?

Considerations for scalability

You can scale your McAfee ePO infrastructure in multiple ways. Scaling is needed if the environment managed by McAfee ePO is growing beyond the capacity of the current McAfee ePO infrastructure.

To grow your McAfee ePO infrastructure, you can: Move the McAfee ePO SQL database to a larger and more powerful SQL Server, add more Agent Handlers, or increase CPU and memory to improve storage performance on the SQL Server.

With McAfee ePO software, you can scale your network vertically or horizontally.

- **Vertical scalability** — Adding and upgrading to bigger, faster hardware to manage larger and larger environments. Scaling vertically is accomplished by upgrading your server hardware, and installing McAfee ePO on multiple servers throughout your network, each with its own database.
- **Horizontal scalability** — Increasing the size of the environment that one McAfee ePO server can manage. Scaling horizontally is accomplished by installing additional Agent Handlers, all sharing a single database.

Make sure the McAfee ePO infrastructure is scaled to handle major peaks in outbreak situations.

Managed systems and servers

The number of systems your McAfee ePO server manages dictates the number and size of the servers needed. It also dictates the recommended server sizing needed to manage these systems.

Option	< 1,500 systems	1,500–10,000 systems	10,000–25,000 systems	25,000–75,000 systems	> 75,000 systems
Virtual McAfee ePO server	Yes	Yes	Yes	Yes	Yes

Option	< 1,500 systems	1,500–10,000 systems	10,000–25,000 systems	25,000–75,000 systems	> 75,000 systems
Virtual SQL database server	Yes	Yes	Yes	Conditional*	Conditional*
McAfee ePO server and SQL database on the same server	Conditional*	Conditional*	Conditional*	Conditional*	Not recommended
Add distributed repositories	Not required	Conditional*	Conditional*	Yes	Yes
Add Agent Handlers (virtual)	Not required	Conditional*	Conditional*	Yes	Yes

*For more information, see *Combining servers*.

Tip

We recommend one Agent Handler for every 50,000 systems.

There is no hard limit on the number of systems McAfee ePO can manage. The primary limitation is the SQL database performance, specifically disk performance (IOPS – I/Os per second). You can scale the SQL database, add distributed repositories, and add Agent Handlers to manage more systems as needed.

Important sizing considerations

- **Environment** — Estimates based on a McAfee ePO server running the Endpoint Security products.
- **Operating systems** — You must use a 64-bit operating system for the McAfee ePO server and SQL Server.
- **CPU cores** — Server class, minimum 2.2 GHz.
- **RAM** — Add 16 GB of RAM to SQL Server for every 25,000 nodes.
- **Storage capacity** — Estimated event retention period of 6 months.
- **Storage performance** — Storage estimated event retention period of 6 months.

Recommended hardware based on number of managed systems

Node count	McAfee ePO server		
	CPU cores	RAM (GB)	Storage (GB)
< 10,000	4	8	300
10,000–25,000	4	8–16	500
25,000–75,000	8	16–32	500
75,000–150,000	12	16–64	500
150,000 +	16	16–64	500

Node count	Agent Handler				
	Number of Agent Handlers	CPU cores	RAM (GB)	Storage (GB)	Notes
< 10,000	—	—	—	—	You can use a single server or multiple VMs.
10,000–25,000	0–1	4	8	150	
25,000–75,000	0–1	4	8	150	
75,000–150,000	1–3	4	8	150	
150,000 +	3+	4	8	150	

	SQL Server			
Node count	CPU cores	RAM (GB)	Storage (TB)	Performance (IOPS)
< 10,000	4	8–16	0.5–1.0	
10,000–25,000	4	8–16	0.5–1.5	
25,000–75,000	8	16–32	1.0–2.0	>10,000
75,000–150,000	16	32–128	2.0–3.0	>30,000
150,000 +	32+	128–256	3.0	>90,000

By default, IOPS is calculated with 4-KB sectors. Microsoft recommends that SQL storage solutions are allocated with a 64-KB sector size.

Baseline calculations

Your product configuration requires different resources than the baseline calculations we provide, which are estimates. Modify your baseline to meet the unique needs of your environment.

For calculation purposes, use 10,000 for *SystemsPerAddlCoreEPOServer* and 12,500 for *NumSystemsPerCoreAgentHandler*. We provide a table of calculations as a starting point, but be aware that your calculations depend on your environment. For example, for an environment with only 10,000 systems, the hardware requirements for a SQL Server using these calculations are high. For smaller or less complex environments, use the **Combining Servers** page for more accurate estimates.

Component	Calculation	100,000 systems with 6-month retention period and average 10 events/day per system
Estimating cores for McAfee ePO server	NumEpoCores = 4 + (NumSystems/ SystemsPerAddlCoreEPOServer)	4 + (100,000 /10,000) = 14 McAfee ePO processor cores
Estimating RAM for McAfee ePO server	NumEpoCores * 4	14 * 4 = 56 GB RAM

Component	Calculation	100,000 systems with 6-month retention period and average 10 events/day per system
Estimating cores for Agent Handlers (every 4 = new Agent Handler)	NumAgentHandlerCores = (NumSystems-50,000)/ NumSystemsPerCoreAgentHandler	(100,000–50,000) / 12,500 = 4 Agent Handler cores (1 Agent Handler)
Estimating SQL cores	(NumEpoCores + NumAgentHandlerCores) * 2	(14 + 4) * 2 = 36 SQL cores
Estimating SQL RAM	8 GB * NumSQLCores	8 * 36 = 288 GB RAM
Estimating SQL storage	(NumSystems * AveSizeOfAgentProperties) + (NumSystems * EventsPerDay * AveSizeOfEvent * NumDaysToRetain)	(100,000 * 100,000) + (100,000 * 10 * 3,000 * 180) = 550,000,000,000 bytes = 550-GB storage
Estimating network bandwidth to SQL	(NumSystems * EstimatedAveBytesPerASC * Asc/Hr * ASCtoSQLExpansionFactor * SystemOnHoursPerDay) + (NumSystems * EventsPerDayPerSystem * AveSizeOfEvent * EventtoSQLExpansionFactor) / (HoursPerDay * MinutesPerHour * SecondsPerMinute)	(100,000 * 23,000 * 1 * 2.5 * 10) + (100,000 * 10 * 3,000 * 1.1) / (24 * 60 * 60) = 703,704 bytes/sec

Note

We have not included a generic calculation for IOPS (input/output operations per second) because of the number of variables in a McAfee ePO environment. Each environment is unique, and includes variables such as administrator query use, SQL index fragmentation, and scheduled reports.

Default numbers for estimating network bandwidth to SQL

Variable	Type	Default
NumSystems		100,000
EstimatedAveBytesPerASC	Bytes	23,000

Variable	Type	Default
ASC/Hr	Count (6 hr ASC would be .166)	1
SystemsPerAddlCoreEPOServer		10,000
NumSystemsPerCoreAgentHandler		12,500
ASCtoSQLExpansionFactor		2.5
SystemOnHoursPerDay		10
EventsPerDayPerSystem		10
AveSizeOfEvent	Bytes	3,000
EventtoSQLExpansionFactor		1.1
HoursPerDay	H/D	24
MinutesPerHour	M/H	60
SecondsPerMinute	S/M	60
BytesPerBlock	B/B	4,000

Sizing distributed repositories

Sizing for distributed repositories depends on the network architecture of the environment.

Distributed repository sizing recommendations:

- Server class hardware or equivalent VM, 2–4 CPU
- Gigabit or greater network interface
- 100-GB disk free space
- Up to 5,000 systems with high latency connections
- Up to 20,000 systems with low latency connections

Tip

When configuring updates, randomize update times across endpoints. Peer-to-peer enabled agents can increase distributed repository system capability by 10–100X, enabling endpoints to share repository files within the network segment.

Example 1: Endpoints concentrated in a single low-latency data center

Fewer than 5,000 endpoints, updating can be done directly from the McAfee ePO server or Agent Handlers. After the first 5,000 endpoints, start adding a distributed repository for every 20,000 systems.

Actual endpoint count per repository is a factor of client update speed versus concurrent repository connections versus network interface usage.

Tip

Peer-to-peer updating significantly reduces network usage and concurrent connections experienced by the distributed repository, allowing more endpoints per repository.

Example 2: Endpoints concentrated in high-latency data centers

With geographically distant data centers, to reduce WAN bandwidth, place distributed repositories in each zone where high concentrations of endpoints exist. Use the same calculation of one repository for every 20,000 systems.

Example 3: Endpoints concentrated in branch offices with fewer than 1,000 endpoints

Peer-to-peer updating is highly effective in this environment. With peer-to-peer enabled, choose a single SuperAgent distributed repository or no repository at all (preferred). If a local distributed repository is not available, only the initial catalog downloads and peer-to-peer traffic cross the WAN to download from a remote distributed repository."

For information about creating and using SuperAgent repositories, see the product guide for McAfee ePO.

Example 4: Home office or endpoints directly connected to the Internet

For small endpoint counts, updating can occur using an Agent Handler in a DMZ. For environments where more than 5,000 systems connect to the DMZ, add distributed repositories. These systems typically use connections that are geographically distant. The total concurrent connection load on the distributed repositories is high so the scale factor is lower.

Start with 5,000 systems per distributed repository. Peer-to-peer updating is ineffective because the endpoint's subnet likely has few endpoints (if any) to share content with.

Sizing DXL Brokers

DXL Brokers route messages between clients connected to the DXL messaging fabric. Connect brokers to allow for redundancy, scalability, and communication across different geographical locations.

We recommend a maximum of 50,000 clients per DXL Broker. Size brokers so that if a broker is down, other regional brokers have sufficient capacity to take the load.

For information about redundancy and sizing DXL Brokers, see the DXL Architecture Guide here: https://community.mcafee.com/t5/Documents/DXL-Architecture-Guide/ta-p/550280.

The use cases for DXL Brokers are similar to the McAfee ePO distributed repositories.

Standalone broker requirements

	Linux	Windows
Recommended requirements		
Processor (CPU cores)	4 cores	4 cores
Memory	8 GB	12 GB
Disk space	25 GB	20 GB
Minimum requirements		
Processor (CPU cores)	2 cores	2 cores
Memory	4 GB	8 GB
Disk space	20 GB	20 GB

Combining servers

Depending on the size of the environment, combining certain services reduces the total number of management servers required for the McAfee ePO environment.

Depending on the size of your environment, running multiple services on the same physical server require increased CPU, RAM, disk, and network resources.

Use this table as a starting point. Your calculations will depend on your environment.

Total node count	Services being added	Size
< 10,000	McAfee ePO + DXL Broker	6 cores, 16-GB RAM, 350-GB disk

Total node count	Services being added	Size
< 10,000	McAfee ePO + DXL Broker + SQL	10 cores, 24-GB RAM, 1.5-TB disk
10,000–25,000	McAfee ePO + DXL Broker	Not recommended
10,000–25,000	Agent Handler + DXL Broker	8 cores, 16-GB RAM, 200-GB disk
25,000–75,000	McAfee ePO + DXL Broker	Not recommended
25,000–75,000	Agent Handler + DXL Broker	8 cores, 16-GB RAM, 200-GB disk
75,000–150,000	Agent Handler + DXL Broker	8 cores, 16-GB RAM, 200-GB disk
150,000 +	Agent Handler + DXL Broker	8 cores, 16-GB RAM, 200-GB disk
Other	SuperAgent + DXL Broker < 10,000 systems per server	8 cores, 16-GB RAM, 120-GB disk

- When sharing SQL resources with another service, you must configure SQL Server to only use the resources it would be allocated if run as a separate server. Otherwise, the SQL Server will consume all available system memory and CPU capacity for itself.
- For large environments with 75,000 or more systems, don't share resources on the McAfee ePO server to maximize the performance of the McAfee ePO console.
- Combining DXL and repository resources, such as a SuperAgent, lowers the total number of systems that can be served by the shared resource. Each service requires many network connections.

Factors that affect McAfee ePO performance

It's important to know which factors affect the performance of your server and the attached SQL database.

For example, a single McAfee ePO server and database can manage up to 200,000 client systems with only the Endpoint Security product installed. But as you add more software products and clients, that same server hardware can no longer provide the performance you expect.

Consider these factors as your managed network grows and your security needs change.

- **McAfee ePO server hardware**
- **SQL Server** — This server is the main engine within the McAfee ePO infrastructure and affects the performance of the McAfee ePO server, queries, dashboards, and McAfee ePO console.

- **Number of software products installed** — Each software product you install adds processing load on the McAfee ePO server and the SQL database.
- **Number of managed clients and their Agent Handlers** — These numbers are proportional to the McAfee ePO server and database performance. Each **Agent Handler** places these fixed loads on the database server:
  - Heartbeat updates (every minute)
  - Work queue checks (every 10 seconds)
  - Pool of database connections held open to the database (two connections per CPU to the Event Parser service and four connections per CPU to the Apache service)

Internet protocols in a managed environment

McAfee ePO software is compatible with Internet Protocol versions: IPv4 and IPv6.

The McAfee ePO server work in three different modes:

- **Only IPv4** — Supports only IPv4 address format
- **Only IPv6** — Supports only IPv6 address format
- **Mixed mode** — Supports IPv4 and IPv6 address formats

The mode in which your McAfee ePO server works depends on your network configuration. For example, if your network is configured to use only IPv4 addresses, your server works in Only IPv4 mode. Similarly, if your network is configured to use IPv4 and IPv6 addresses, your server works in Mixed mode.

Until IPv6 is installed and enabled, your McAfee ePO server listens only to IPv4 addresses. When IPv6 is enabled, it works in the mode in which it is configured.

When the McAfee ePO server communicates with an Agent Handler on IPv6, address-related properties such as IP address, subnet address, and subnet mask are reported in IPv6 format. When transmitted between client and McAfee ePO server, or when displayed in the user interface or log file, IPv6-related properties are displayed in the expanded form and are enclosed in brackets.

For example, `3FFE:85B:1F1F::A9:1234` is displayed as:

```
[3FFE:085B:1F1F:0000:0000:0000:00A9:1234]
```

When setting an IPv6 address for FTP or HTTP sources, no changes to the address are needed. But, when setting a Literal IPv6 address for a UNC source, you must use the Microsoft Literal IPv6 format. See Microsoft documentation for more information.

Note

> TLS 1.0 is disabled by default for communication to external servers, such as SQL Server. For more information about TLS support, see KB90222. This version of McAfee ePO requires enabling TLS 1.2 support on your browser.

Things to know before installation

To make sure that you have the necessary information before installing McAfee ePO, review the checklist.

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	
Destination folder for McAfee ePO software installation (required for **Custom** and **Cluster** installations)	
Installed SQL Server — 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 intend to restore the McAfee ePO server from a database snapshot, you must: • Have previously restored the McAfee ePO SQL database using one of the Microsoft SQL restore processes • Know the server recovery passphrase used with your **Disaster Recovery Snapshot** records. This passphrase is used to decrypt the sensitive information stored in the SQL Snapshot records	

System requirements

System requirements and recommendations

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

Run the Pre-Installation Auditor to make sure that your environment meets the minimum requirements for a successful installation. For information about downloading and using the Pre-Installation Auditor, see the tool's release notes.

Component	Requirements and recommendations
Dedicated server	If managing fewer than 250 systems, McAfee ePO can be installed on a pre-existing server, such as a file server. If managing more than 250 systems, use a dedicated server for McAfee ePO.
Domain controllers	(Recommended) The server must have a trust relationship with the Domain Controller on the network. For instructions, see the Microsoft product documentation. **Note:** Installing the software on a Domain Controller is supported, but not recommended.
File system	NT file system (NTFS) partition.
Free disk space	20 GB — Minimum.
IP address	Use static IP addresses for McAfee ePO. Static IP addresses are recommended for McAfee ePO and Agent Handlers. McAfee ePO supports IPv4 and IPv6 networks.
Memory	8-GB available RAM minimum.
Network Interface Card (NIC)	100 megabit minimum.

Component	Requirements and recommendations
	Tip: If using a server with more than one IP address, McAfee ePO uses the first identified IP address. To use more IP addresses for agent-server communication, create Agent Handler groups for each IP address. For more information, see KB56281.
Ports	• 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 McAfee ePO and McAfee Agent communication.
Processor	• 64-bit Intel compatible • (Recommended) 4 cores minimum

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 updates	Recommended — Make sure that your Microsoft Windows and Microsoft applications are running the latest updates. **Important:** Turn off Windows updates before you begin installing or upgrading your software.
Microsoft Visual C++ 2010 Redistributable Package (x64 and x86)	Required — Installed automatically.
Microsoft Visual C++ 2015 Redistributable Package (x64 and x86)	Required — Installed automatically.

Software	Requirements and recommendations
MSXML 3.0 and 6.0	Required — Installed automatically.
Security software	Recommended. • Install and update the anti-virus software on the server and scan for viruses prior to any installation. • 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.
Supported SQL Server	Required — A supported version of SQL Server or SQL Server Express is required to install McAfee ePO.
SQL Server 2012 (or later) Native Client	Required — Installed automatically.

Operating system requirements

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

Supported server-class operating systems

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

- Windows Server 2012
- Windows Server 2012 Service Pack 1
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Important

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 (x64 only)

Operating system language

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

The McAfee ePO 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.

- English
- Italian
- English (United Kingdom)
- Chinese (Simplified)
- Chinese (Traditional)
- French
- German
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish
- 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 2016
- Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2008 R2
- VMware ESXi 6
- VMware ESXi 5.5
- VMware ESXi 5.1
- XenServer 6.2
- XenServer 6

For information about the latest supported platforms, environments, and operating systems for McAfee ePO, see KB51569.

Supported SQL Servers

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

McAfee ePO supports any edition of these Microsoft SQL Server versions.

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

Note

McAfee ePO also supports Amazon RDS for SQL Server which allows you to deploy SQL Server in the cloud. https://aws.amazon.com/rds/sqlserver/

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) To view the supported Microsoft SQL Server collation types, see KB73717.
Maintenance settings	We recommend making specific maintenance settings to McAfee ePO databases. For instructions, see the product guide for McAfee ePO.

Disable Backup Retention Period in Amazon Relational Database Service for SQL Server

If you are using Amazon Relational Database Service (RDS) to manage your SQL Server instance in the cloud, make sure to disable database backups during McAfee ePO installation.

Before you begin

Complete this task before beginning a new installation of McAfee ePO.

For more information about working with backups, see the Amazon Relational Database Service (RDS) User Guide: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html.

Task

1. Sign into the AWS Management Console and open the RDS console.
   https://console.aws.amazon.com/rds/
2. In the navigation pane, select **Databases**, and select the DB instance that you want to modify.
3. Select **Modify**.
   The **Modify DB Instance** page appears.
4. For **Backup Retention Period**, select **0 days**.
5. Select **Continue**.
6. Select **Apply Immediately**.
7. On the confirmation page, select **Modify DB Instance**.

Results

You are now ready to install McAfee ePO. After installation, you can return to the RDS console and configure the Backup Retention Period as needed.

Configure TCP/IP access to the SQL Server

McAfee ePO can only communicate with SQL using a TCP/IP connection. Before installing McAfee ePO, verify that the SQL Server that will host the McAfee ePO database has TCP/IP enabled.

Note

Make note of the port that SQL is using.

Task

1. To configure TCP/IP protocol for the SQL Server:
   a. Start **SQL Server Configuration Manager**.
   b. In the console pane, expand **SQL Server Network Configuration**, and select the Protocols item for your SQL instance. For example, if you are using the default MSSQLSERVER instance, select **Protocols for MSSQLSERVER**.
   c. In the details pane, locate the entry for **TCP/IP** and check the **Status** column. If it's set to **Enabled**, go to step 2 to determine the port being used.
   d. If TCP/IP is set to **Disabled**, double-click **TCP/IP** to open the **TCP/IP Properties** window.
   e. Select the **Protocol** tab, click **Enabled**, and select **Yes**.
   f. 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.
   g. In the console pane, click **SQL Server Services**.

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

2. To determine the port being used by SQL:
   a. If needed, start **SQL Server Configuration Manager**, expand **SQL Server Network Configuration**, and select the Protocols item for your SQL instance.
   b. Double-click **TCP/IP** to open the **TCP/IP Properties** window.
   c. Select the **IP Addresses** tab.

      Make sure **Enabled** is set to **Yes** for each active IP address.
   d. Under **IPAll**, make note of the value for **TCP Dynamic Ports**.

      If there is a value specified, for example `57482`, your SQL Server is using dynamic ports. Make a note of the value because this information might be needed later in the installation.

      Note

      > If you are using dynamic ports, the SQL Browser service must be running on the SQL Server. If the value for **TCP Dynamic Ports** is blank, then your SQL Server is using a static port and the value for this port will be shown in the **TCP Port** field.

3. If you are using dynamic ports, make a note of the SQL instance name that will host the McAfee ePO database. If you are using the default instance for SQL, the instance name is MSSQLSERVER.

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 1.2 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 can authenticate to the McAfee ePO SQL database using 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 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

ⓘ **Important**

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

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 Setup program installs the McAfee ePO software. For more information about installing SQL Server, see your SQL Server software documentation.

ⓘ **Important**

If McAfee ePO is installed in a cluster environment, the SQL Server must be separate from McAfee ePO: it must not be installed on the same cluster as McAfee ePO.

Other relevant SQL Server installations and upgrades

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

- Installing SQL Server 2012, 2014, 2016, or 2017
- Upgrading from SQL Server 2005 or 2008 to supported SQL Server versions
- Upgrading from SQL Server 2005 Express or 2008 Express to supported SQL Server versions

Required SQL permissions

Specific SQL Server roles are required for the account used by McAfee ePO.

For new McAfee ePO installation...	Use these server roles
During installation	The user account credentials for Windows or SQL authentication must have these **server roles** granted on the target SQL Server:

For new McAfee ePO installation...	Use these server roles
	• public • dbcreator **Note:** The dbcreator server role is required for the setup program to create and add the 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 created	The dbcreator server role can be removed from the McAfee ePO SQL user. **Note:** 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 account credentials for Windows or SQL authentication must have these **server roles** granted on the target SQL Server: • public • dbcreator

Supported SQL database user name and password formats

Review the 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

Platform	Unsupported password and user name characters
	• Single quotes (') • Double quotes (") • Leading backslashes (\ ) • Colons in user names (:) • Semicolons in user names (;)

For more information about supported McAfee ePO user name and password formats, see KB66286.

Port options

The ports used by McAfee ePO are predefined, and populated by default.

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 installation

During an automatic installation, McAfee ePO downloads and installs all McAfee products entitled to you by your McAfee ePO license key.

⚠ **Caution**

Using **Automatic Product Installation** downloads all available products in the Software Catalog.

Usually, during an automatic installation, you will not see the **Automatic Product Installation** process run. It starts running when you complete installing McAfee ePO and is finished before you log on.

If the **Automatic Product Installation** 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 try 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 Catalog** to install your products.

ⓘ **Important**

Once you click **OK** in the **Stop Automatic Product Setup** confirmation dialog box, you must use the **Software Catalog** to install your products, or manually install them in the Main Repository. **Automatic Product Installation** is available only once during your initial installation.

If a product continues to fail during **Automatic Product Installation**, contact Technical Support, or click **OK** to exit the **Automatic Product Installation** page and begin setting up the McAfee ePO server.

For future product installation status information, open the **Software Catalog**: **Menu** → **Software** → **Software Catalog**.

Distributed repository requirements

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

Component	Requirements
Free disk space	1 GB minimum (4 GB recommended) on the drive where the repository is stored. The required space depends on the size of the software packages being replicated from the **Main Repository**. **Note:** 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 **Main Repository**.

Component	Requirements
Memory	512 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 — KB90383
- Known issues — KB90382

Installing McAfee ePO 5.10.0 on a single server

You can install McAfee ePO 5.10.0 on Windows operating systems. This topic describes the high-level steps of installing ePO on a single server.

1. Download McAfee ePO installation packages. For more information about the latest build details, see McAfee ePO 5.10.0 Release Notes.
2. Review the minimum supported version of server components and prepare your Windows server ready to install ePO (KB51569).
3. Configure TCP/IP access to the SQL Server.
4. Run the Pre-Installation Auditor (PIA) tool to validate that your server meets the minimum requirements. For more information about how to install and run the PIA tool, see the Pre-Installation Auditor (PIA) 3.1.0 Release Notes.
5. Things to know before installation.
6. Run the setup utility on server to install ePO.
7. Set up your McAfee ePO environment.

Download McAfee ePO 5.10.0 installation packages

To install McAfee ePO 5.10.0, you must download the installation packages from the McAfee Product Downloads site using a valid grant number.

Task

1. Go to McAfee Product Downloads.
2. Enter the grant number and email address associated with the product, then click **Submit**.
   The **My Products** page displays information about your licensed products.
3. In the **Find Products** section under **Filters**, select **Management Solutions** for the **Category**.
   A table displays your licensed ePolicy Orchestrator products.
4. Navigate through the table to locate and select McAfee ePolicy Orchestrator.
   A table displays all product files that are available to download.
5. In the **Available Downloads** section, under **Filters**, select **Type** as **Installation**.
   The table displays information about each downloadable installation package, including the release date, file size, and notes.
6. Select the **Install - ePolicy Orchestrator Version 5.10.0** package.
7. Move the downloaded installation packages to a location where you plan to install ePO, then extract the compressed folder.

Results

The installation packages are ready to run.

Things to know before installation

To make sure that you have the necessary information before installing McAfee ePO, review the checklist.

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	
Destination folder for McAfee ePO software installation (required for **Custom** and **Cluster** installations)	
Installed SQL Server — 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 intend to restore the McAfee ePO server from a database snapshot, you must: • Have previously restored the McAfee ePO SQL database using one of the Microsoft SQL restore processes • Know the server recovery passphrase used with your **Disaster Recovery Snapshot** records. This passphrase is used to decrypt the sensitive information stored in the SQL Snapshot records	

Install McAfee ePO extension file on a single server

Installing McAfee ePO for the first time requires downloading and starting the installation.

Task

1. Log on to the Windows Server system to be used as the McAfee ePO server.
   Use an account with local administrator permissions.
2. Locate the software you downloaded from the McAfee website and extract the files to a temporary location. Right-click **Setup.exe** and select **Run as Administrator**.
   The executable is available in the downloaded McAfee ePO installation folder.

   Caution

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

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

3. Click **Next** to continue installation.

   Monitor the installation process for a notification to restart your system.

4. To select the destination folder, click:

   - **Next** to install your McAfee ePO software in the default location (C:\Program Files (x86)\McAfee\ePolicy Orchestrator\).
   - **Change** to 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 as needed, then click **OK**.

5. The installer discovers active SQL Servers and displays the servers in a drop-down list. Select a SQL server.

   If the installer doesn't discover any SQL server, Click **No** and specify the SQL server details manually.

6. In the **Database Information**, specify information of your database, then click **Next**.

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

Database Server	If the installer discovers active SQL Servers, select your server from the drop-down list. If the installer doesn't discover any SQL server, you can specify the SQL server details manually. If you are using dynamic SQL ports, enter the name of the SQL Server and the name of the SQL instance separated by a backslash. For example, if your SQL Server is called **SQLServer** and you are using the default instance name of **MSSQLSERVER**, enter `SQLServer\MSSQLSERVER`.
Database Name	This value is auto-populated with the name of the database. You can enter a more suitable name.

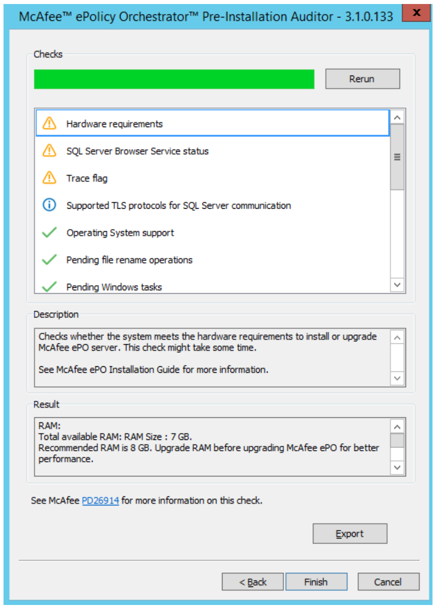
   b. Specify which type of **Database Server Credentials** to use.

Windows authentication	Select a domain of the user account from the drop-down list to access the SQL Server. If the required domain is not listed, type the domain name, user name, and password.
SQL authentication	Type the user name and password for your SQL Server. Make sure that credentials you provide are active and have appropriate administrator rights. **Note:** The **Domain** menu is grayed out once you select the **SQL authentication**.

   c. Click **Next**.

The installer connects to the SQL Server using the credentials. If the installer can't automatically determine the port, this message appears: **Setup was unable to access the SQL UDP port 1434**. Click **OK** to return to the **Database Information** page.

7. The Pre-Installation Auditor automatically runs and validates the server condition. The checks are passed if the server meets all requirements. If the tool flags warning on a specific issue, you can rectify them and click **Rerun**. Once all checks have passed, click **Finish**.



McAfee™ ePolicy Orchestrator™ Pre-Installation Auditor - 3.1.0.133

Checks

⚠ Hardware requirements
⚠ SQL Server Browser Service status
⚠ Trace flag
ⓘ Supported TLS protocols for SQL Server communication
✓ Operating System support
✓ Pending file rename operations
✓ Pending Windows tasks

Description

Checks whether the system meets the hardware requirements to install or upgrade McAfee ePO server. This check might take some time.

See McAfee ePO Installation Guide for more information.

Result

RAM:
Total available RAM: RAM Size : 7 GB.
Recommended RAM is 8 GB. Upgrade RAM before upgrading McAfee ePO for better performance.

See McAfee PD26914 for more information on this check.

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

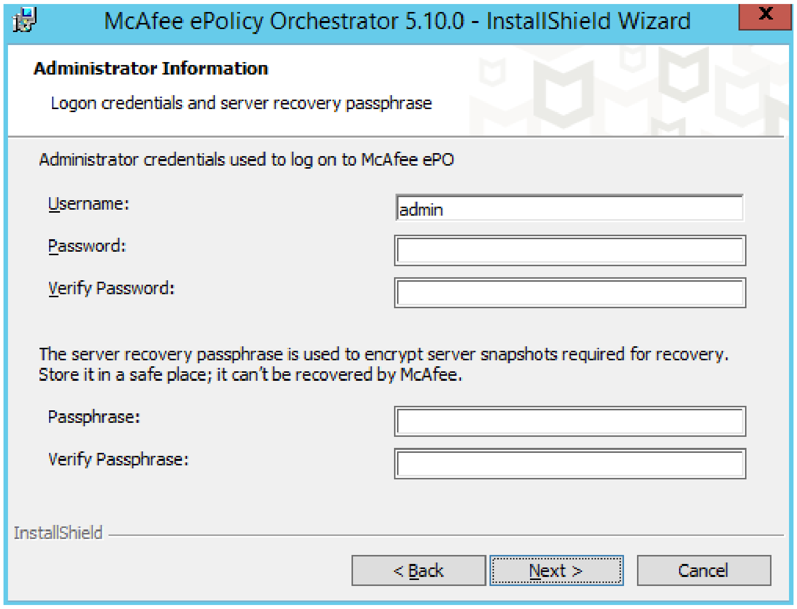
ⓘ **Important**

> The **Agent wake-up communication port** and **Agent broadcast communication port** can only be changed during and after installation. You cannot change the other port numbers after installation. For more information about the port information, see KB66797.

9. In **Administrator Information**, specify the login credentials and click **Next**.
   a. Type the user name and password you want to use for your primary administrator account.
   b. Type the server recovery passphrase.
   The passphrase must be of 14–200 characters, must not contain leading or trailing backslashes (\), spaces, double quotation marks ("), or characters below ASCII 32 or above ASCII 65535.

   ⓘ **Important**

   > Save the passphrase as you need it to decrypt the Disaster Recovery Snapshot records. McAfee does not store this passphrase and can't recover it.


McAfee ePolicy Orchestrator 5.10.0 - InstallShield Wizard

Administrator Information

Logon credentials and server recovery passphrase

Administrator credentials used to log on to McAfee ePO

Username: admin

Password:

Verify Password:

The server recovery passphrase is used to encrypt server snapshots required for recovery. Store it in a safe place; it can't be recovered by McAfee.

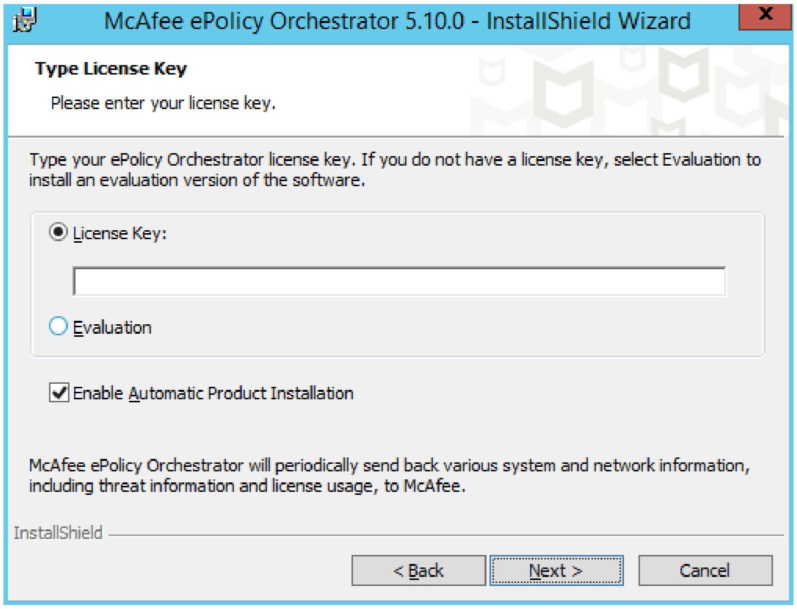
Passphrase:

Verify Passphrase:

10. In **Type License Key**, type your license key, then click **Next**.
    If you are evaluating the software and have not purchased the license, select **Evaluation** to install the software. The evaluation period is limited to 90 days.
    a. You can enable the software license after the installation.
    b. (Optional) You can select **Enable Automatic Product Installation** to automatically download the licensed products after installation.

Note

The **Enable Automatic Product Installation** option is enabled by default and only available if you have a license key.



McAfee ePolicy Orchestrator 5.10.0 - InstallShield Wizard

Type License Key

Please enter your license key.

Type your ePolicy Orchestrator license key. If you do not have a license key, select Evaluation to install an evaluation version of the software.

● License Key:

○ Evaluation

☑ Enable Automatic Product Installation

McAfee ePolicy Orchestrator will periodically send back various system and network information, including threat information and license usage, to McAfee.

11. In **Ready to install the Program**, you can decide whether to allow McAfee to collect system and software telemetry data, then click **Install** to begin installing the software.
12. Wait until the installation process is complete, then click **Finish** to exit the Setup program.

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

Results

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

A certificate warning appears if you are using a self-signed certificate to access McAfee ePO server through web console. Add the URL to the browser trusted sites.

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.

Set recovery model in SQL server

After upgrading to or installing McAfee ePO 5.10, a new SQL database is created, in addition to the existing McAfee ePO database, in this format:

```
ePO_<ePOServerName>_Events
```

When you configure SQL database backups, you must add the **ePO Events** database to your current backup plan.

McAfee ePO stores monthly event data in the **ePO Events** database, which handles threat information.

SQL server can be recovered in Full and Simple Recovery models. You can select a recovery model for **ePO Events** or any database attached to the SQL server.

Full recovery model

- By default, the **ePO Events** database is configured to use the Full Recovery Model.
- The Full Recovery Model includes the administrative overhead of periodically backing up the Transaction log for your McAfee ePO database.
- If a disaster recovery is needed, the data and events database must be restored to avoid historical data loss.

ⓘ **Warning**

> The size of the Transaction log continues to grow if you don't perform periodic backups of the Transaction log when the **ePO Events** database is in **Full Recovery** mode. The log grows until it consumes all available disk space, so it is important to perform regular Transaction log backups. Full and differential SQL backups do not truncate the Transaction log.

Simple recovery model

- Set the **Simple Recovery** mode, if the regular Transaction log backup is not required.
- Simple recovery model performs a full backup of McAfee ePO database excluding Transaction logs.
- If there is a disaster, you can recover only to the last full backup. All changes that occurred after the last full backup are lost.
- The Simple Recovery Model is an acceptable solution for most enterprise customers because the data lost in a disaster is usually event data since the last full backup.

Installing McAfee ePO on a cloud server

Using an AWS server for McAfee ePO

You can use Amazon Web Services to install McAfee ePO.

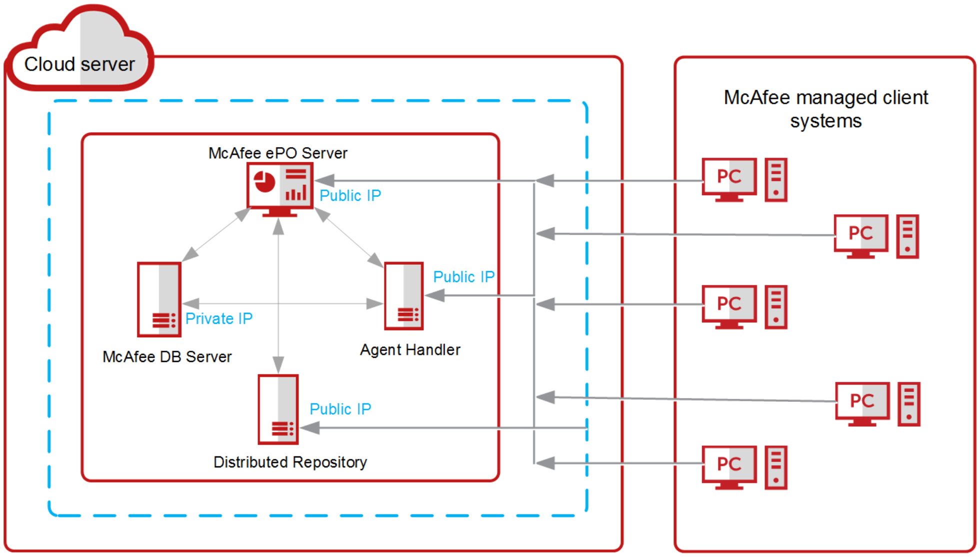
For more information, see https://aws.amazon.com/quickstart/.

Using a Microsoft Azure server for McAfee ePO

Installing McAfee ePO on a Microsoft Azure virtual server allows you to resize your server as your network grows, eliminating the chance of hardware failure.

An Azure virtual server provides the same features and performance as locally configured hardware. This diagram shows the basic configuration of McAfee ePO installed on an Azure server.

Cloud server with McAfee ePO configuration



Limitations

There are some limitations that you need to consider when a server initiated communication is required.

- If the McAfee ePO server or the Agent Handler can't communicate with the Agents in a private network, then these features will not work.
  - Push agent doesn't work — Use a VPN to overcome this limitation.
  - Wake up agent using Agent Handler doesn't work — Use a VPN or configure DXL to overcome this limitation.
  - Run client task using an Agent Handler doesn't work — Use a VPN or configure DXL to overcome this limitation.

- If the McAfee ePO server or the Agent Handler can't communicate with remote servers in private networks, then these features will not work.
  - Distributed repositories such as SuperAgent, FTP, HTTP, and UNC will not work.
  - Registered server that cannot communicate with the McAfee ePO server will not work.
  - If McAfee ePO can't reach the SMTP server, the email service doesn't work.

Note

If McAfee ePO can communicate with agents and remote servers, then these features work as expected; provided the required ports are configured in Azure Security Rules.

Port requirements

Configure these ports to establish an uninterrupted communication between McAfee ePO server, repositories, and the agents.

TCP ports 80 and 443 are the default ports used for communication between McAfee ePO and the McAfee Agent. You can change the ports while installing McAfee ePO.

The Azure Inbound Security Rules must allow this communication. For details about port requirements, see KB66797.

In addition to the ports mentioned in the article, the following table lists the ports that you need to configure for these servers:

Server type	Port details
Distributed Server	• Configure port 2049 in the McAfee ePO server outbound security group. • Configure port 2049 in the distributed repository server inbound security group.
CSR Report Server	• Configure port 9112 in the McAfee ePO server outbound security group. • Configure port 9111, 9112, 9121 and 9129 in CSR report server inbound security group.
Syslog Server	• Configure port 6514 in the McAfee ePO server outbound security group. • Configure port 6514 in Syslog server inbound security group.

Note

McAfee Agent 5.x and later does not support port 80.

Configure the Microsoft Azure server for McAfee ePO

On the Azure server, you must create a virtual server and start a Virtual Machine (VM) instance to install McAfee ePO.

Before you begin

You must have a Microsoft Azure account to complete this task.

Perform these steps to install and configure McAfee ePO in an Azure server to manage your clients.

Task

1. Get an Azure account from https://azure.microsoft.com/.
2. Log on to the Azure console and configure your virtual server.
    a. Start a VM instance.

    Note

    > Select the location for your virtual server nearest to most of your McAfee ePO managed systems.

    b. Configure Inbound Security Rules on Azure.
    In Azure, a firewall is called as Inbound Security Rules and must be created to allow a McAfee Agent to connect to the McAfee ePO server.

    Note

    > Make sure that you configure your Inbound Security Rules according to McAfee ePO server port requirements.

    c. Capture the Azure instance public DNS name, or IP address, that Azure created.

    Note

    > Assign an elastic IP address to the public DNS name or IP address.
3. Use Remote Desktop Connection and the DNS name, or public IP address, to connect to the Azure server.
4. Install McAfee ePO using software provided by McAfee and information from the Azure SQL database server.
5. Create a McAfee Agent URL or McAfee Agent installation package.

Results

The McAfee ePO server starts managing your systems.

Install McAfee ePO on an Azure server

Installing McAfee ePO on an Azure server is similar to installing the software on a physical server.

Before you begin

- The Azure server must be created.
- You must know the SQL Server name.

Task

1. Connect to Azure server using Remote Desktop Connection and the configured static IP address or DNS name.
2. Start the McAfee ePO installation process.
3. In **Database Information**, enter the name of the Microsoft SQL Server configured.

   By default, the McAfee ePO SQL Server name is <AzureServerName>\EPOSERVER.

4. Complete the McAfee ePO server installation.
5. (Optional) Create a backup image of your Azure server. See Azure documentation for instructions.

Results

You have a McAfee ePO server installed and configured that you can connect to from a remote browser using this format:

```
https://<EPO Server PUBLIC DNS Name>:<port>
```

Update McAfee ePO public DNS name

You must update the McAfee ePO public DNS name in the console.

Before you begin

McAfee ePO must be installed on your Azure server.

Task

1. Select **Menu** → **Configuration** → **Server Settings**.
2. Select **McAfee ePO Server Public DNS** from the **Setting Categories** pane and click **Edit**.
3. Enter the Public DNS name and click **Save**.

Manage your Agent Handlers

You can install an Agent Handler on your Azure server similar to installing an Agent Handler on a physical server.

Before you begin

McAfee ePO must be installed on your Azure server.

To install and configure an Agent Handler, see the product guide for McAfee ePO.

Task

Use an Elastic Load Balancer (ELB) with your Agent Handler to distribute the traffic.

- If an Agent Handler is used without a Load Balancer:
  - Go to **Menu** → **Configuration** → **Agent Handlers**.
  - Click **Agent Handlers** under **Handler Status**.
  - Click the **Handler DNS Name** in the **Handler List**.
  - Enter the **Published DNS Name** and the **Published IP address**.
  - Click **Save**.
- If an Agent Handler is used with a Load Balancer:
  - Configure ELB on Microsoft Azure management console.
    - Add Agent Handler VMs.
    - Configure Azure Security Rules for ELB according to port requirements of Agent Handler.
  - For information about how to configure the Load Balancer, see the product guide for McAfee ePO.

Distributed Repository connections

There are different types of repositories from where the McAfee Agent retrieves the security content to keep the environment up to date.

The packages in the **Main Repository** are replicated to a distributed repository in the network.

You can create different users for different types of repository and associate them while sharing the folder.

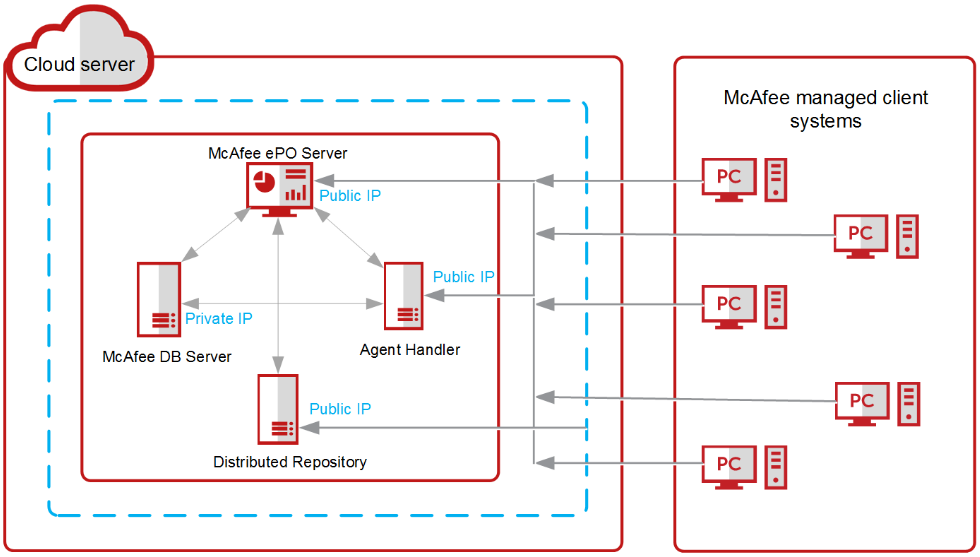
For Universal Naming Convention (UNC) repository, install NFS in the repository server and share the UNC folder using NFS sharing. Open NFS port 2049 in the McAfee ePO server and in the Repository server.

Using a Google Cloud Platform (GCP) server for McAfee ePO

Installing McAfee ePO on a GCP allows you to resize your server as your network grows, eliminating the chance of hardware failure.

A GCP virtual server provides the same features and performance as locally configured hardware. This diagram shows the basic configuration of McAfee ePO installed on a GCP server.

Cloud server with McAfee ePO configuration



Limitations

There are some limitations that you need to consider when a server initiated communication is needed.

- If the McAfee ePO server or the Agent Handler can't communicate with the Agents in a private network, then these features don't work.
  - Push agent doesn't work — Use a VPN to overcome this limitation.
  - Wake up agent using Agent Handler doesn't work — Use a VPN or configure DXL to overcome this limitation.
  - Run client task using an Agent Handler doesn't work — Use a VPN or configure DXL to overcome this limitation.
- If the McAfee ePO server or the Agent Handler can't communicate with remote servers in private networks, then these features don't work.
  - Distributed repositories such as SuperAgent, FTP, HTTP, and UNC doesn't work.
  - Registered server that can't communicate with the McAfee ePO server doesn't work.
  - If McAfee ePO can't reach the SMTP server, the email service doesn't work.

Note

If McAfee ePO can communicate with agents and remote servers, then these features work as expected; provided the needed ports are configured in Firewall.

Port requirements

Configure these ports to establish an uninterrupted communication between McAfee ePO server, repositories, and the agents.

TCP ports 80 and 443 are the default ports used for communication between McAfee ePO and the McAfee Agent. You can change the ports while installing McAfee ePO.

The GCP firewall rules must allow this communication. For details about port requirements, see KB66797.

In addition to the ports mentioned in the article, the following table lists the ports that you need to configure for these servers:

Server type	Port details
Distributed Server	• Configure port 2049 in the McAfee ePO server firewall rule. • Configure port 2049 in the distributed repository server inbound security group.
CSR Report Server	• Configure port 9112 in the McAfee ePO server firewall rule. • Configure port 9111, 9112, 9121 and 9129 in CSR report server inbound security group.
Syslog Server	• Configure port 6514 in the McAfee ePO server firewall rule. • Configure port 6514 in Syslog server inbound security group.

Note

McAfee Agent 5.x and later does not support port 80.

Configure GCP on McAfee ePO

On GCP, you must create a virtual server and start a Virtual Machine (VM) instance to install McAfee ePO.

Before you begin

You must have a GCP account to complete this task.

Perform these steps to install and configure McAfee ePO in GCP to manage your clients.

Task

1. Get a GCP account from https://cloud.google.com.
2. Log on to the GCP console and configure your virtual server.
3. Create a GCP server.
4. In GCP, firewall rules must be created to allow McAfee Agent to connect to the McAfee ePO server.

   Important

   Make sure that you configure your firewall rules according to McAfee ePO server port requirements.

5. Install McAfee ePO using software provided by McAfee and information from the SQL database server.

   For more information, see the list of supported SQL servers.

Results

The McAfee ePO server starts managing your systems.

Install McAfee ePO on a GCP server

Installing McAfee ePO on a GCP server is similar to installing the software on a physical server.

Before you begin

- The GCP server must be created.
- You must know the SQL Server name.

Note

If you are using GCP cloud SQL service for McAfee ePO database, see KB94509 for more information.

Task

1. Connect to the GCP server using Remote Desktop Connection and the configured static IP address or DNS name.
2. Start the McAfee ePO installation process.
3. In **Database Information**, enter the name of the Microsoft SQL Server configured.

   By default, the McAfee ePO SQL Server name is <GCPServerName>\EPOSERVER.

4. Complete the McAfee ePO server installation.
5. (Optional) Create a backup image of your GCP server. See GCP documentation for instructions.

Results

You have a McAfee ePO server installed and configured that you can connect to from a remote browser using this format:

```
https://<GCPServerName>:<port>
```

Update McAfee ePO public DNS name

You must update the McAfee ePO public DNS name in the console.

Before you begin

McAfee ePO must be installed on your GCP server.

Task

1. Select **Menu** → **Configuration** → **Server Settings**.
2. Select **McAfee ePO Server Public DNS** from the **Setting Categories** pane and click **Edit**.
3. Enter the Public DNS name and click **Save**.
4. Run the query, `update [EPOServerInfo] set RmdSecureHttpPort='443'` on the McAfee ePO database to enable the secured port 443 for McAfee ePO DNS.

Results

The McAfee ePO public DNS name is updated, `https://<Public DNS NAME>:<port>`.

Manage your Agent Handlers in the GCP environment

You can install an Agent Handler on your GCP server similar to installing an Agent Handler on a physical server.

Before you begin

McAfee ePO must be installed on your GCP server.

To install and configure an Agent Handler, see the product guide for McAfee ePO.

Task

Use an Elastic Load Balancer (ELB) with your Agent Handler to distribute the traffic.

- If an Agent Handler is used without a Load Balancer:
  - Go to **Menu** → **Configuration** → **Agent Handlers**.
  - Click **Agent Handlers** under **Handler Status**.
  - Click the **Handler DNS Name** in the **Handler List**.
  - Enter the **Published DNS Name** and the **Published IP address**.
  - Click **Save**.
- If an Agent Handler is used with a Load Balancer:
  - Configure ELB on GCP management console.
    - Add Agent Handler VMs.
    - Configure GCP Firewall Rules for ELB according to port requirements of Agent Handler.

For information about how to configure the Load Balancer, see the product guide for McAfee ePO.

Distributed Repository connections

There are different types of repositories from where the McAfee Agent retrieves the security content to keep the environment up to date.

The packages in the **Main Repository** are replicated to a distributed repository in the network.

You can create different users for different types of repository and associate them while sharing the folder.

For Universal Naming Convention (UNC) repository, install NFS in the repository server and share the UNC folder using NFS sharing. Open NFS port 2049 in the McAfee ePO server and in the Repository server.

Installing McAfee ePO in a cluster environment

McAfee ePO provides high availability for server clusters with Microsoft Cluster Server (MSCS) software.

Installing the software into your Microsoft Cluster Server environment requires additional steps. Cluster installation is supported on Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, and Windows Server 2019.

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

Cluster installation terminology

This terminology is used in the cluster installation instructions.

Term	Definition
Data drives	Required by Microsoft Cluster Server and McAfee ePO. For information about setting up data drives, see the Microsoft documentation. This 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.

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 Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, and Windows Server 2019.

- McAfee ePO supports two-node cluster environments only. Environments with more than two nodes are not supported.
- Microsoft Cluster Server is set up and running on a cluster of two servers.
- Data drives present and available to all nodes in the cluster according to Microsoft guidelines.
- 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.

Create the McAfee ePO application role

The McAfee ePO application role is required to allow Microsoft Cluster Services to control McAfee ePO.

Before you begin

The steps required to create a McAfee ePO application role might vary depending on the setup and configuration of your cluster environment. For more information, see the Microsoft documentation.

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 select **Bring Online**.

Add the data drive

The data drive is the location where you install McAfee ePO.

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 McAfee ePO installation, then click **OK**.

Install McAfee ePO software on each cluster node

Run the Cluster installation on each of the nodes.

Task

1. Log on to the Windows Server system to be used as the first node of the McAfee ePO server cluster.
   Use an account with local administrator permissions.
2. Locate the software you downloaded from the McAfee website and extract the files to a temporary location. Right-click **Setup.exe** and select **Run as Administrator**.
   The executable is located in the downloaded McAfee ePO installation folder.

   ⚠ **Caution**

   > 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. Click **Next**.
3. On the **Setup Type** page, select the **Cluster** option, then click **Next**.
4. In the **Choose Destination Location** page, specify the path for the shared data drive, then click **Next**.
   Use the same path for each node.
5. On the first node in the Set Virtual Server Settings page, provide this identifying information for the McAfee ePO cluster:

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

   On subsequent nodes, the Virtual Server IP address, Virtual Cluster name, and Virtual Cluster FQDN are automatically provided. You must add the Cluster Configuration Passphrase to each subsequent node.
6. The installer searches for SQL Servers. If the installer finds any SQL Servers, it automatically moves to the next stage and the servers that it finds can be selected from a drop-down list.
   If it doesn't find any SQL Servers, a dialog box appears asking if you want to search again. Click **No** to continue to the next step where the SQL Server information can be entered manually.
7. In the **Database Information** step, specify information for your database, then click **Next**.
   a. Specify the **Database Server** and **Database Name**.

Database Server	If the installer found the SQL Server in the previous step, select your server from the drop-down list. If the server is not listed, enter the information manually by typing the name of the SQL Server. If you are using dynamic SQL ports, enter the name of the SQL Server and the name of the SQL instance separated by a backslash. For example, if your SQL Server is called SQL Server and you are using the default instance name of MSSQLSERVER, enter `SQLServer\MSSQLSERVER`.
Database Name	This value is automatically populated with the name of the database. Enter a new database name to change the value.

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

Windows authentication	From the **Domain** menu, select the domain of the user account for accessing the SQL Server from the drop-down list. If the required domain is not listed, type the domain name, user name, and password.
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. **Note:** The **Domain** menu is grayed out when using SQL authentication.

c. Click **Next**.

The installer attempts to connect to the SQL Server using the credentials given. If the installer can't automatically determine the port, this message appears: **Setup was unable to access the SQL UDP port 1434**. Click **OK** to return to the **Database Information** page. However, the SQL Server TCP port field is now available. Enter the port and click **Next**.

8. The Pre-Installation Auditor automatically starts. Review the results and correct any failures, then click **Rerun**. Once all checks have passed, click **Finish**.
9. In the **HTTP Port Information** step, review the default port assignment, then click **Next** to verify that the ports are not already in use on this system.

Important

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**.

10. 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 server recovery passphrase.
    The passphrase includes 14–200 characters, must not contain leading or trailing backslashes (\), spaces, double quotation marks ("), or characters below ASCII 32 or above ASCII 65535.

    Important

    Keep a record of this passphrase; you need it to restore McAfee ePO using the Disaster Recovery Snapshot records and McAfee can't recover it.

11. In the **Type License Key** step, type your license key, then click **Next**.
    If you don't have a license key, you can select **Evaluation** to continue installing the software in evaluation mode. The evaluation period is limited to 90 days. You can enter a license key after installation is complete from the McAfee ePO Settings or Software Catalog. Optionally, if you want McAfee ePO to automatically download the products you are licensed for after the installation completes, select **Enable Automatic Product Installation**. For more information, see *Automatic Product Installation*.

    Note

    The **Enable Automatic Product Installation** option is enabled by default and only available if you have a license key.

12. Accept the **McAfee End User License Agreement** and click **OK**.
13. From the **Ready to install the Program** dialog box, decide if you want to allow McAfee to collect system and software telemetry data, then click **Install** to begin installing the software.
14. When the installation is complete, do not select **Yes, I wish to launch McAfee ePolicy Orchestrator now**. Click **Finish** to exit the Setup program on the first cluster node.
15. In Failover Cluster Manager, move the **ePO application role** to the second node of the cluster by right-clicking the role, then select **Move** → **Select Node**. Select the second node of the cluster and click **OK**.
    The role moves to the second node of the cluster.
    Alternatively, shut down the first cluster node server: this automatically moves the role to the second node.
16. Log on to the Windows Server computer to be used as the second node of the McAfee ePO server cluster.
    Use an account with local administrator permissions.
17. Locate the software you downloaded from the McAfee website and extract the files to a temporary location. Right-click **Setup.exe** and select **Run as Administrator**.
    The executable is located in the downloaded McAfee ePO installation folder.

    Caution

    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. Click **Next**.

18. On the **Setup Type** page, select the **Cluster** option, then click **Next**.
19. In the **Choose Destination Location** page, click **Change**, and browse to the location on the shared drive where McAfee ePO was installed in step 4, then click **OK** → **Next**.
20. In the **Set Virtual Server Settings** step, the details for the McAfee ePO Virtual Server IP address, McAfee ePO Virtual Cluster name, and McAfee ePO Virtual Cluster FQDN are already populated. Enter the Cluster Configuration Passphrase that you chose in step 5 and click **Next**.
21. From the **Ready to install the Program** dialog box, decide if you want to allow McAfee to collect system and software telemetry data, then click **Install** to begin installing the software.
    The install process on the second node completes much more quickly than on the first node.
22. When the installation is complete, do not select **Yes, I wish to launch McAfee ePolicy Orchestrator now**. Click **Finish** to exit the Setup program on the first cluster node.

Create the Generic Service resources

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

Create three generic service resources.

Task

1. In the Failover Cluster Manager, right-click the **ePO** application role, then select **Add Resource** → **Generic Service**.
2. On the **New Resource Wizard**, select the ePolicy Orchestrator Application Server service, then click **Next**.
3. On the **Confirmation** page, click **Next** to create the service, then click **Finish** to create the generic service.
4. Repeat steps 1–3 for the ePolicy Orchestrator Server service and the ePolicy Orchestrator Event Parser service.
   The newly created generic service resources are listed on the **Resources** tab of Failover Cluster Manager under the **Roles** section. Follow these steps to configure these resources.
5. Right-click the ePolicy Orchestrator Application Server resource, then select **Properties**. In the **Properties** dialog box, select the **Dependencies** tab, add the following dependencies, then click **Apply** → **OK**.
   a. Server Name resource
   b. Shared Storage resource
6. Right-click the ePolicy Orchestrator Server resource, then select **Properties**. In the **Properties** dialog box, remove anything in the Startup Parameters field and enter a single space character. The service will not start with any parameters specified.
7. Select the **Dependencies** tab, add **ePolicy Orchestrator Application Server resource** as the dependency, then click **Apply** → **OK**.
8. Right-click the ePolicy Orchestrator Event Parser resource, then select **Properties**. In the **Properties** dialog box, select the **Dependencies** tab, add the following dependencies, then click **Apply** → **OK**.
   a. Server Name resource
   b. Shared Storage resource
9. In Failover Cluster Manager, right-click the **ePO application role** and select **Start Role** to bring the **ePO application role** online.

Test the McAfee ePO cluster installation

When the McAfee ePO role is online and running in Failover Cluster Manager, use this task to make sure that the software functions in a failover situation.

Task

1. From a separate system, open a web browser and log on to the McAfee ePO console. The URL for the console is https://<Server Name Resource>:<console port>, where <Server Name Resource> is the server name used when the Client Access Point was created, and <console port> is the console port chosen during setup (8443 by default).
2. In Failover Cluster Manager, move the McAfee ePO application role to the other node of the cluster by right-clicking the role, then select **Move** → **Select Node**. Select the other node of the cluster and click **OK**.
   The role moves to the other node of the cluster.
   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.
3. Manually refresh your browser session. If failover is successful, you are redirected to the McAfee ePO logon page.

Setting up your McAfee ePO 5.10.0 environment

After installing McAfee ePO 5.10.0, get up-and-running quickly by configuring the essential features of your McAfee ePO server.

1. Install the McAfee licensed products on the McAfee ePO server.
    a. Automatic Installation
    b. Manual Installation
2. Add your systems to the System Tree.
3. Choose a deployment method to deploy McAfee Agent to your systems to manage them through McAfee ePO management console.
4. Deploy the McAfee licensed products to your systems.
5. Configure product updates in your managed systems.
6. Define proxy settings, if you use a proxy server in your network environment.
7. Enable McAfee ePO 5.10.0 license.
8. Confirm that your systems are managed by McAfee ePO.
9. Confirm that your protection software stops a sample threat. For information about how to use the EICAR anti-malware test with McAfee products, see KB59742.
10. Confirm the threat response in McAfee ePO.

Install products automatically on your McAfee ePO server

During an automatic installation, McAfee ePO downloads and installs all McAfee products approved for your McAfee ePO license.

Before you begin

- To automatically install, you must have selected **Enable Automatic Product Installation** during the McAfee ePO installation.
- **Automatic Product Installation** process runs immediately after the ePO installation and finishes before you log on.
- If installation of all or any product fails, the **Automatic Product Installation** page appears when you initially log on to McAfee ePO.You can click **Retry** to try the product installation again.

Task

1. On your McAfee ePO server desktop, click the **Launch ePolicy Orchestrator** icon.
2. When the log-on screen appears, type your credentials and select a default language for the console.
   The **Product Installation Status** software automatically starts downloading and installing the licensed software available to your organization. The page displays this information:
    - **Products** — All licensed software and the latest available version.
    - **Status** — The progress of the product's installation.
3. Wait for the status of each product to change to **Complete**.

4. To know more about the product installation status information, navigate to **Software Catalog** in ePO console: **Menu** → **Software** → **Software Catalog**. Search for a product to view the status.

   Note

   If any product installation fails, select the checkbox next to the product name to retry installation. If a product repeatedly fails during **Automatic Product Installation**, contact Technical Support, or click **OK** to exit the **Automatic Product Installation** page and begin setting up the McAfee ePO server.

Install products manually on your McAfee ePO server

Your McAfee licensed products must first be checked in to the McAfee ePO server before they can be installed on managed systems.

- If you have selected the **Enable Automatic Product Installation**, the products are installed along with the ePO installation.
- If you didn't select the **Enable Automatic Product Installation** option during the McAfee ePO installation, you can manually check in products on the McAfee ePO server.

Task

1. On your McAfee ePO server desktop, click the **Launch ePolicy Orchestrator** icon.
2. When the Log On screen opens, type your credentials and select a default language for the console.
   The default dashboard appears the first time you log on to ePO.
3. Select **Menu** → **Software** → **Software Catalog**.
4. In the **Software Catalog** page **Category** list, filter by product categories, or use the search box to find your software.
5. When you have located the correct software, select **Check In All**.
6. Under **Check In**, review and accept the product details and End User License Agreement (EULA), select the **Client Package Branch**, then click **Check In** to complete the operation.

Add systems to the System Tree

McAfee uses McAfee Agent to communicate with the security products. To deploy McAfee Agent initially, you must add systems manually to the **System Tree** .

Before you begin

- McAfee ePO server must be connected to the target systems with local administrator access.

Task

1. Use `ping` commands to test the ability to successfully resolve and connect from the McAfee ePO server to managed systems.

2. To confirm the `Admin$` share folder on Windows target systems is accessible from the McAfee ePO server, click Windows **Start** → **Run**, then type the path to the target system's `Admin$` share, specifying system name or IP address. For example, type `\\<System Name>\Admin$`.
   If the systems are properly connected over the network, if your credentials have sufficient rights, and if the Admin$ share folder is present, a Windows Explorer dialog box appears.
3. Select **Menu** → **Systems** → **System Tree**, then click **New Systems** on the **System Tree** page.
4. From the **New Systems** page, click **Push agents and add systems to the current group** and **Browse**.
5. From the **NT Domain Credentials** dialog box, type this information and click **OK**.
   - **Domain** — Type the domain name with your target systems. Use a period (".") to represent a local (non-domain) account.
   - **User Name** — Type your user name.
   - **Password** — Type your password.
6. On the **Browse for Systems** page, select the domain server from the **Domain** list.
7. Select the systems or groups of systems to add to the System Tree, then click **OK**.
   The systems you selected appear in the **Target Systems** field, separated by commas.
8. In **Agent Version**, select **Windows** or **Non-Windows** and the version from the list.
9. In **Credentials for agent installation**:
   - Type the domain name.
   - Type your domain user name.
   - Type the domain password.
   - Select the **Remember my credentials for future deployments** checkbox.
10. Use the defaults for the final settings and click **OK**.

Results

After McAfee Agent successfully establishes communication with ePO the status is set to **Managed State**. Now you can deploy other McAfee software products on those managed system through ePO. The systems you selected are added to the

System Tree and appear as **Unmanaged** in the **Managed State** column. This process can take several hours to complete.

Define proxy settings

If you use a proxy server in your network environment, you must specify the proxy settings on the **Server Settings** page.

Task

1. Select **Menu** → **Configuration** → **Server Settings**, select **Proxy Settings** from the **Setting Categories**, then click **Edit**.
2. Select **Configure the proxy settings manually**, provide the specific configuration information your proxy server uses for each set of options, then click **Save**.

Enable McAfee ePO license

Your license key entitles you to a full installation of ePO 5.10.0, and populates the Software Catalog with the licensed McAfee products your company owns.

Without a license key, ePO runs in evaluation mode. Once the evaluation period expires, ePO ceases to function. You can add a license key at any time during or after the evaluation period.

Task

1. Select **Menu** → **Configuration** → **Server Settings**, select **License Key** from the **Setting Categories**, then click **Edit**.
2. Type your **License Key** and click **Save**.

Confirm that your protection software stops a sample threat

Run a sample threat on a managed system to test that your protection software detects and stops it.

Before you begin

Endpoint Security must be installed on the managed system to run the anti-malware test file.

You can also test the software from ePO as they are managed. In this example we consider the software is ENS and test its successful function.

To run an anti-malware test file, you can log on to the test system locally or remotely.

Task

1. Log on to the test system with administrator rights.
2. Using a web browser, connect to the EICAR site:
   `http://www.eicar.org/86-0-Intended-use.html`
3. Follow the instructions to download and run the 68-Byte eicar.com anti-malware test file.
4. In Windows, click **Start** → **All Programs** → **McAfee** → **McAfee Endpoint Security**, then click **Status**.
   A threat Summary lists the type of threat and the number of threats received.
5. Click **Event Log** to display the threat events in the **Event** table and remove the sample threat.
   The bottom pane of the Event table lists the threat event details.

Confirm the threat response in McAfee ePO

Knowing where to look for threat events in McAfee ePO is an important part of protecting your managed systems.

Before you begin

You must run the EICAR anti-malware test file to see any threat events.

Task

1. Log on to the McAfee ePO and select **Menu** → **Reporting** → **Dashboards**.
2. In the title bar of the **Dashboards** list, select a dashboard.
   - **ePO Summary** — Displays recent threats in the **Malware Detection History** line chart.
   - **Executive Dashboard** — Displays a **Malware Detection History** line chart.
   - **Threat Events** — Displays recent threats in these dashboards:
     - **Most Numerous Threat Event Descriptions** table
     - **Threat Events by System Tree Group** table and pie chart
     - **Threat Event Descriptions in the Last 24 Hours** table and pie chart
     - **Threat Events in the Last 2 Weeks** line chart
3. Select **Menu** → **Reporting** → **Threat Event Log** to see a description the recent threat.
   Information in the table includes:
   - Event Generated Time
   - Event ID
   - Event Description
   - Event Category
   - Threat Target IPv4 Address
   - Action Taken
   - Threat Type
4. Click the event in the table to see all threat details.
5. To see the detailed information about the affected system, click **Go to related Systems**.

Confirm that your systems are being managed by ePO

After deploying McAfee Agent and the licensed products, make sure that your systems are listed in the **System Tree** and appear as managed.

Before you begin

You must have deployed the McAfee Agent and downloaded the product software to your systems.

Task

1. Select **Menu** → **Systems** → **System Tree**, then click the **Systems** tab to show a list of managed systems.

Note

If no systems appear, click **This Group and All Subgroups** in the **Preset** list.

2. In the **Managed State** column, confirm that **Managed** appears next to each system.
   If **Unmanaged** appears in the **Managed State** column, the system was added to the **System Tree** but the McAfee Agent and product software are not installed on the system.
3. To view details about a system, select the system name to open the **Systems Information** page.

Upgrade to McAfee ePO 5.10.x

Upgrading your existing McAfee ePO environment involves careful planning and preparation for a smooth and successful process.

The McAfee ePO upgrade process consists of three phases:

Phase 1: Before you upgrade — Check that your McAfee ePO server meets all requirements, download the McAfee ePO software and tools, and back up your databases and directories.

Phase 2: Day of upgrade — Stop Agent Handler and McAfee ePO services, start and complete the InstallShield Wizard, and upgrade Agent Handlers.

Phase 3: After you upgrade — Complete the post-upgrade checklist and migrate SHA-1 certificates to SHA-2 or higher.

Before you upgrade

Pre-upgrade checklist

The pre-upgrade checklist identifies what to do before you begin your upgrade, so you have a successful upgrade and limited downtime.

1. Plan for a successful upgrade	
□	Read the release notes.
□	Gather required information.
□	Download the Pre-Installation Auditor.
□	Download McAfee ePO software.
□	Run the Pre-Installation Auditor to check for issues that could cause the upgrade to fail, and compatibility of installed products.
□	

2. Prepare your environment	
□	Back up McAfee ePO databases and directories.
□	Update database server certificates.

Planning your McAfee ePO upgrade

Before you start the McAfee ePO upgrade, make sure that you have the information you need.

Review documentation

Read the release notes for your version of McAfee ePO, particularly these sections:

- Supported upgrade paths
- Supported environments
- Known issues

Gather required information

- Grant number

Note

If you need help with your grant number, contact Customer Service.

- Database server and database name
- Database server credentials, including domain if authenticating with Windows credentials
- Primary McAfee ePO administrator account credentials
- Disaster Recovery passphrase

Download the tools and software you need to upgrade

Before you upgrade McAfee ePO, download the Pre-Installation Auditor and McAfee ePO installation software packages from the Product Downloads site.

Task

1. Go to the **Product Downloads** site: https://www.mcafee.com/enterprise/en-us/downloads.html
2. Type your grant number and email address, and click **Submit**.

Note

> If you need help with your grant number, contact Customer Service.

3. On the **My Products** page, click **McAfee ePolicy Orchestrator**.
   Make sure **Show only latest version** is selected.
4. On the **Available Downloads** page:
   a. Click **Install - ePolicy Orchestrator Version 5.10.0**.
   b. Click **ePO - Pre-Installation Auditor tool**.
   c. Click **Update # for ePolicy Orchestartor 5.10.0 Version 5.10.0**.

   Note

   > The number corresponds with the latest available update. The update is needed when the McAfee ePO upgrade successfully completes.

5. Extract the downloaded .zip to a temporary location.

   Caution

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

Checking your system for compatibility using the PIA tool

Before you install or upgrade McAfee ePO, run the Pre-Installation Auditor (PIA) tool to reduce or prevent upgrade issues. Running the tool automates the verification tasks included in the upgrade process.

Running a Product Compatibility check

The PIA tool runs a Product Compatibility Check to verify that your managed products are compatible with the latest version of McAfee ePO. If it finds discrepancies, the tool creates a list of blocked or disabled product extensions.

- Blocked extensions — Upgrade of McAfee ePO is blocked.
- Disabled extensions — Upgrade continues, but extension isn't initialized until a compatible replacement is installed.

For a complete list of the checks the PIA performs and information about how to run it at any time, see KB71825.

Back up McAfee ePO databases and directories

Before upgrading McAfee ePO, back up your databases and directories to make sure you can recover your McAfee ePO environment if the upgrade is unsuccessful.

Before you begin

Make sure that you have your Disaster Recovery snapshot passphrase. If you don't know it, see Change the server recovery passphrase.

Task

1. Run a successful Disaster Recovery Snapshot server task. For details, see Disaster Recovery.
2. Back up all McAfee ePO databases and directories. For details, see KB66616.

Update your database server certificates

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

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 KB87731.

Note

TLS 1.0 is disabled by default for communication to external servers, such as SQL Server. For more information about TLS support, see KB90222.

Task

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

Day of upgrade

Upgrade checklist

The upgrade checklist identifies actions that must be performed when you upgrade McAfee ePO.

Important

You must complete all steps in the pre-upgrade checklist before you upgrade McAfee ePO.

Extra steps are required if you installed McAfee ePO in a cluster environment. For information about cluster environment, see *Upgrade your McAfee ePO cluster server*.

☐	Confirm you have successfully backed up your McAfee ePO databases and directories.
☐	Stop Remote Agent Handlers.

□	Prepare McAfee ePO services for upgrade.
□	Run the InstallShield Wizard.
□	Upgrade Agent Handlers (if applicable).

Stop Agent Handler and McAfee ePO services

If you use Agent Handlers in your environment, you must stop McAfee services on each Agent Handler server before the upgrade.

Before you begin

- Complete all steps in the *Pre-upgrade checklist*.

Task

1. Stop Remote Agent Handler services.
   a. Press **Windows+R**, type `services.msc`, then click **OK**.
   b. Stop the **ePolicy Orchestrator Server Service** and **ePolicy Orchestrator Event Parser Service**.
2. Stop McAfee ePO services.
   a. Press **Windows+R**, type `services.msc`, then click **OK**.
   b. Stop these services:
      - **ePolicy Orchestrator Server Service**
      - **ePolicy Orchestrator Event Parser Service**
      - **ePolicy Orchestrator Application Server**
3. Start the **ePolicy Orchestrator Application Server** service.

Run the InstallShield Wizard

Run the InstallShield Wizard to upgrade your McAfee ePO server.

Tip

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

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 folder where it was extracted.

   Important

   > 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 select **Run as 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. To install the listed software, click **Next**.
5. In the **Database Information** step:
   1. Confirm that the automatically selected **Database Server** and **Database Name** are correct.
   2. Specify the type of credentials to use from the lists.
6. Specify which type of **Database Server Credentials** to use, then click **Next**.

   - **Windows authentication** — From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. 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.

   Tip

   > The **Domain** menu is grayed out when using SQL authentication.

   The McAfee ePO Pre-Installation Auditor runs, analyzing your McAfee ePO environment to make sure it meets all requirements.
7. In the **Administrator Information** step:
   1. For the **Username**, replace the default `admin` if necessary, and type your primary Administrator account user name.
   2. For the **Password**, type your primary Administrator account password.
   3. For the **Server recovery password**, type a passphrase to encrypt Disaster Recovery Snapshot records.

      The passphrase includes 14–200 characters, must not contain leading or trailing backslashes (\), spaces, double quotation marks ("), or characters below ASCII 32 or above ASCII 65535.

      Note

      > Keep a record of this password. If you ever want to restore McAfee ePO from a Disaster Recovery snapshot, you need this password to decrypt the Disaster Recovery Snapshot records.
   4. Click **Next**.
8. In the **Type License Key** step, click **Next**.

Your existing license key is automatically populated in the field and the Product Compatibility Check runs.

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**.
11. When the upgrade is complete, click **Next**, click **Finish**, then optionally select to restart the server.

    Note

    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.**

Results

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

Upgrade your Agent Handlers

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

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

Task

1. Copy the Agent Handler folder, included in the McAfee ePO software installation package, to the system.
2. Right-click **Setup.exe** and select **Run as Administrator** 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. Accept the default destination or select a different destination, then click **Next**.
6. Configure the McAfee ePO server information.
    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 8443.
    c. Type the name and password of a user with McAfee ePO Global Administrator rights, and click **Next**.
    d. Provide the password for access to the McAfee ePO SQL database, then click **Next**. The **Database Information** page is populated with these McAfee ePO server settings.

        - **Database Server** with instance name, as in DB-SERVER\SERVERNAME.
        - Authentication type.

- **Domain** name where the database server is hosted if using Windows authentication.
- **User name** and **Password**.
- **Database name** if not provided automatically.

7. Click **Install** to start the installation.
   The installation continues without any additional input. When the wizard is complete, click **Finish**.

Upgrade your McAfee ePO cluster server

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

Before you begin

Make sure your current environment is supported for the upgrade to McAfee ePO 5.10.x.

Task

1. In Failover Cluster Manger on the active node, open the **ePO group**.
2. Make sure that the primary node is the active server.
3. Take this Generic Service resource offline, then delete it:
   - ePolicy Orchestrator Application Server
4. Do not change these resources, which are required for a successful upgrade:
   - Data drive
   - McAfee ePO virtual IP address
   - McAfee ePO virtual Network Name
5. Open the **Services Control Manager** and start each of these services on the primary node:
   - ePolicy Orchestrator Application Server
   - ePolicy Orchestrator Event Parser service
   - ePolicy Orchestrator Server service
6. Install the new McAfee ePO software on the primary node.
7. In Failover Cluster Manager, move the **ePO application role** to the second node of the cluster: right-click the role, select **Move** → **Select Node**. Select the second node of the cluster and click **OK**.
   The role moves to the second node of the cluster.
   (Optional) Shut down the first cluster node server, which automatically moves the role to the second node.
8. Install your new McAfee ePO software on the second node.
9. Create the new Generic Service resources.
   For information about how to create the Generic Service resources, see Create the Generic Service resources.

After you upgrade

Post-upgrade checklist

After the upgrade is complete, perform a quick health check on your McAfee ePO server.

Note

> McAfee ePO 5.10 can no longer connect to a registered server that requires TLS certificates but does not support TLS 1.1 or 1.2. For more information, see Update your database server certificates.

□	Confirm you can log on and access different areas of the McAfee ePO console.
□	Update your certificates to SHA-2 if a warning appears on the McAfee ePO logon screen. For details, see Migrate Certificate Authority Hashtag Algorithm from SHA-1 to SHA-2 or higher.
□	Verify connectivity by sending an agent wake-up call to one or more systems.
□	Verify McAfee ePO is operating correctly by running a query or server task.
□	Make sure that your policies, tasks, product deployments, and repositories reflect the choices you made when you set up your environment.
□	Test the connection to all your registered servers. If any server fails that uses SSL, it might need to be updated to support TLS 1.1 or higher for McAfee ePO to successfully connect to it.
□	Apply the available update to McAfee ePO and all Agent Handlers. For details, see McAfee ePO Cumulative Updates.
□	Enable any server tasks you disabled before upgrading.
□	Enable Windows updates to make sure that your servers receive the latest updates for your operating system.
□	Apply the latest update when the upgrade is complete.

Migrate Certificate Authority Hashing Algorithm from SHA-1 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:

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

Important

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

1. Log on as an administrator, then select **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 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 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**.

ⓘ **Important**

> Make sure that the distribution percentage is as close to 100% as possible before you continue. Otherwise, pending systems might not receive the newly generated certificates and won't be able 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**.
6. Stop and start these services:
   a. Stop the 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.
   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.

9. Re-install any agents that use the old certificates to restore agent-server communication.

McAfee ePO cumulative updates

McAfee ePO 5.10.0 introduces a new strategy where we release cumulative updates instead of patches. Updates address product defects and often introduce new features. Because updates are cumulative, you only need to apply the latest available update.

Updates are on the product download site and the Software Catalog. When a new update is released, the previous update is removed from the product download site and Software Catalog so only the latest update is available.

Updates are posted with the following naming convention: **EPO 5.10.0 Update #**

Install the latest update on your McAfee ePO server

Before you begin

Make sure your system meets these requirements before installing the latest update:

- McAfee ePO 5.10.0 is installed.
- Administrator permissions are needed.
- Have a recent snapshot and a backup of the McAfee ePO database and installation directory.
- Have a minimum of 2-GB disk space is available to copy, extract, and apply updates.

Follow these actions before running the updater tool:

- Standalone environment
  - Stop the McAfee ePO Application Server Service (Tomcat).
  - Stop the Agent Handler Service, including Remote Agent Handler Service (Apache).
  - Stop the Event Parser Service.
  - Close all other File Explorer windows.
- Cluster environment
  - Bring the Generic Service resources offline (Apache, TomCat, and Event Parser).
  - Copy and extract the contents of McAfee ePO 5.10.0 Update13.zip to the data drive.
  - Run this update on one node.

Note

> These steps apply to all Remote Agent Handlers; perform these steps on each Agent Handler in your environment after you install the latest update.

Task

1. Download McAfee ePO 5.10.0 Update 13 package from ePO **Software Catalog** or from McAfee product downloads site.
2. Copy and extract the update package to your McAfee ePO server.
3. Run **ePOUpdater.exe** from the folder where you extracted the update package.
4. Enter the database password and click **Continue**.
5. Review the list of fixes in the **Current Update(s) to be installed** dialog box and click **Continue**.

   Note

   > Click **Details** to view the file types based on version, action being taken, plug-in name (if applicable), and the destination folder where the files are updated.

6. In the **Apply Update** pop-up window, select the checkbox if you want the updater tool to migrate the *McAfeeFtp* source site to point to the HTTP server.

   Note

   > The service provider that McAfee uses to host our FTP service no longer provides FTP capabilities. McAfee uses HTTP sites to update content for McAfee products. For more information about End of Support for the FTP option to access CommonUpdater download sites, see KB91260.

   By default, the option to update *McAfeeFtp* source site details are automatically selected. If you continue with this option, the updater tool changes to the *McAfeeFtp* source site setting.

   These properties are updated:

Property name	Before upgrade	After upgrade
Source Site Name	McAfeeFtp	McAfeeFtpMigrated
Source Site ID	McAfeeFtp	McAfeeFtpMigrated
Location	ftp.nai.com/CommonUpdater	update.nai.com/Products/CommonUpdater
Protocol	FTP	HTTP
Port	21	80

Note

If you choose not to update *McAfeeFtp* source site details using the updater tool, you can deselect the checkbox and manually update source site details later.

7. Click **OK** to apply the update.

   Note

   An error message appears if services do not stop. In the error message, click **OK** then manually stop the McAfee ePO services, and click **Re-Apply**. This option doesn't apply to McAfee ePO in a Windows Cluster environment.

8. Verify that **Successful** is highlighted in green after the update completes.
   For McAfee ePO in a Windows cluster, make sure that the generic services are online in the McAfee ePO role. Only run the update on one node in the cluster.
9. After successful installation of the update on the first node, perform the cluster failover to log on to the second node. Perform the repair operation on the second node to complete the McAfee ePO Update installation.
10. Click **Finish**.

    Note

    For McAfee ePO in a Windows cluster, make sure that the generic services are online in McAfee ePO role. Starting the services might take a few minutes to complete.

11. **(Optional)** Repeat these steps on all Agent Handlers.

Install the latest build on your McAfee ePO server

Follow these steps to install the latest build of ePO 5.10 Update 13 (2.0.0.1235) over the older build of Update 13.

Task

1. Log on to McAfee ePO as administrator.
2. Copy and extract the update package to your McAfee ePO server.
3. Run **ePOUpdater.exe** from the folder where you extracted the update package.
4. Enter the database password and click **Continue**.
5. Select Previously installed Updates and click **Repair**.
6. Click **Finish**.

Install the latest update on Remote Agent Handlers

Run the Updater tool on the McAfee ePO server before running it on Remote Agent Handlers.

Task

1. Run the Updater tool on the McAfee ePO server.
2. Run the Updater tool on Remote Agent Handlers.
3. Make sure that these services aren't running.
    - Agent Handler Service including Remote Agent Handlers (Apache)
    - Event Parser Service
4. Start the Updater tool.

Verify the update installation

Verify that the update successfully completed.

Task

1. From McAfee ePO, select **Menu** → **Server Settings** → **Server Information**.
2. Verify the latest update number appears in the **Update Installed** as **Update 13 (2.0.0.1235)**.

Roll back updates

McAfee ePO updates allow you to roll back an update without going through a disaster recovery process. You can only roll back the last update you applied.

Before you begin

Stop these services:

- McAfee ePO Application Server Service (Tomcat)
- Agent Handler Service including Remote Agent Handler Service (Apache)
- Event Parser Service

Note

These steps apply to all Remote Agent Handlers; perform these steps on each Agent Handler in your environment after you install the latest update.

Task

1. Log on to McAfee ePO as administrator.
2. Copy and extract the update package to your McAfee ePO server.
3. Run **ePOUpdater.exe** from the folder where you extracted the update package.
4. Click **Rollback**. Verify if the **Rollback** button changes to **Successfully Rolled Back** in green.
5. Click **Finish**.
6. Verify the entry for **Update Version** doesn't appear on the McAfee ePO console under **Menu** → **Server Settings** → **Server Information**.
   For more information, see *Verify the update installation*.

   In a cluster environment:

   - Bring all services offline in Cluster Manager.
   - Perform Rollback operation in primary/secondary node.
   - Perform failover to another node.
   - Run McAfee ePO 5.10.0 Update 13. In the pop-up window, click **OK**.
   - A message appears when rollback is successful. Click **OK**.
7. **(For McAfee ePO 5.10.0 Update 9 or before)** Enter the database password and click **Continue**.
8. **(For McAfee ePO 5.10.0 Update 9 or before)** Expand **Previous Installed Update(s)**, then click **Rollback**.
9. **(For McAfee ePO 5.10.0 Update 9 or before)** Wait for the green box to show the message **Successfully Rolled Back**.
10. **(For McAfee ePO 5.10.0 Update 9 or before)** Click **Finish**.

Use Silent Mode to install a McAfee ePO update

Use the command line to install scripted files in **Silent Mode** on the McAfee ePO 5.10 server and Agent Handler servers.

Note

This feature is only supported with McAfee ePO 5.10 Update 5.

Task

1. Log on as administrator to the server hosting McAfee ePO.
2. Copy and extract the McAfee ePO update .zip package to the server hosting McAfee ePO.
3. As administrator, open the command prompt:
   a. Run the install.bat file, located here: %EPOHOTFIX_ROOT_PATH%\resources\app.
      For example, C:\ePO CU BUILDS\ePOUpdater-2.0.0.679\resources\app\install.bat.
   b. Enter the command **install.bat [your password]** and replace the default password with your McAfee ePO database server password.
      For example, C:\Users\cloudadmin.WIN-QFN79SPC5U4.000\Desktop\CU BUILDS\ePOUpdater-2.0.0.679\resources\app> install.bat Welcome123.
4. Verify the installation:
   - If the latest update is installed, the message **Update is already installed** appears.
   - If the update isn't installed, the service restarts and the installation runs.

   For more information, see Verify the update installation.

Troubleshooting installation

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 section, contact Technical Support after you have taken these steps:

1. Verify that you have met the minimum installation requirements.
2. Review the release notes and click the link to the McAfee Knowledge Base 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 write down any message codes that appear.
5. Gather the installation log files from C:\Program Data\McAfee\ePO.

Common installation messages with 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 McAfee ePO 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 1366x768 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.
McAfee ePO software requires that your computer is running Windows Server 2008, Windows Server 2012, or Windows Server 2016.	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.
McAfee ePO 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.

Message	Cause	Solution
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 Technical Support for assistance.	Setup is unable to read the license information required to install the software.	Contact 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 McAfee ePO license has expired.	Your license to use the software has expired.	Contact your administrator or designated McAfee representative.
This system is not currently configured with a static IP address, which is recommended for the McAfee ePO server.	The computer where you are 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.

Message	Cause	Solution
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

McAfee 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
AH5100-Install-MSI.log	Agent Handler installation	C:\ProgramData \McAfee\ePO	This file logs all Agent Handler installation details including: • Installer actions • Installation failures

File name	Log type	Location	Description
AH5100-ahetupdll.log	Temporary	%temp% (on the Agent Handler server)	Logs Agent Handler back-end events.
core-install.log	Temporary	%temp%\McAfeeLogs\ePO5100-Troubleshoot\MFS	Generated when the installer calls the MFS ANT installer. Provides information about: • Creation of server database tables • Installation of server components **Note:** This file is deleted if the installation succeeds.
epo-install.log	Installation	C:\ProgramData\McAfee\ePO	Created when the installer calls the ANT installer.
EPO5100-Checkin-Failure.log	Installation	C:\ProgramData\McAfee\ePO	Generated when installer fails to check in any of these package types: • Extensions • Plug-ins • Deployment packages • Agent packages
EPO5100-CommonSetup.log	Installation	C:\ProgramData\McAfee\ePO	Contains 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
EPO5100-Install-MSI.log	Installation	C:\ProgramData\McAfee\ePO	The primary installation log. Contains installation details such as installer actions and installation failures.

File name	Log type	Location	Description
<ExtensionFileName>.cmd	Temporary	%temp%\McAfeeLogs \ePO5100-troubleshoot \OutputFiles	Created by the installer. Contains the command (sent to Remote-Client) to check in extensions. **Note:** If the installation succeeds, these files are deleted.
MFS5100-CommonSetup.log	Installation	C:\ProgramData \McAfee\ePO	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 **Note:** This file is not present until after initial service startup.
Errorlog.<CURRENT_DATETIME>	Apache	[InstallDir] \Apache2\logs	Contains Apache service details.

File name	Log type	Location	Description
			Note: 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 (1)	Contains McAfee ePO Application Server service details. **Note:** 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. **Note:** 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. **Note:** This file is not present until after the McAfee ePO Application Server service is started for the first time.
Replication_<serverName>.log	Server	[InstallDir]\DB \Logs	The McAfee ePO server replication log file. This file is generated only when all these criteria are true: • There are distributed repositories. • A replication task has been configured.

File name	Log type	Location	Description
			- 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 **Note:** 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. **Note:** 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. **Tip:** Enable this file for the minimum time to capture the required information, because the resulting files grow rapidly.

1 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 5.5.0 for Windows.

McAfee Agent 5.5.0 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 • Policy enforcement • Scheduling of tasks • Agent server communication • Update sessions
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.

McAfee Agent 5.5.0 file name	Log type	Location	Description
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` **Note:** 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 during installation. McAfee Agent error logs are named using the convention <filename>_error.log.

For example, when performing client tasks, information is normally logged in McScript.log. Errors that occur are logged in McScript_error.log.

Error logs only contain details about errors.

Note

After installation, the McAfee Agent logs are located in %ProgramData%.

Adding an SSL certificate to trusted collection

Supported browsers warn about a server’s SSL certificate if it cannot verify the certificate.

By default, the McAfee ePO server uses a self-signed certificate for SSL communication with the browser, which the browser does not trust. A warning message displays every time you visit the McAfee ePO console.

To stop this warning message from appearing, do one of the following:

- Add the McAfee ePO server certificate to the browser's collection of trusted certificates.
- Add the certificate for every browser that interacts with McAfee ePO. If the browser certificate changes, add the server certificate again.
- (Recommended) Replace the default McAfee ePO server certificate with a valid certificate signed by a certificate authority (CA) that the browser trusts. You only need to add the certificate once for web browsers in your environment.
- If the server host name changes, replace the server certificate with a new trusted CA certificate.

For more information, see KB72511.

To replace the McAfee ePO server certificate, you must first obtain the certificate signed by a trusted CA. You must also obtain the certificate’s private key and its password (if it has one). Then you can use all these files to replace the server’s certificate.

The McAfee ePO server expects the server certificate to use these formats: PKCS7, PEM encoded, DER encoded, or PKCS12 file with extensions .cer, .crt, .p12, or .p7b.

The McAfee ePO browser expects the linked files to use PEM for private keys.

If the server certificate or private key is not in these formats, convert to one of the supported formats before replacing the default certificate.

If your organization requires a higher standard of encryption, replace the default SHA-256 certificate with one that uses SHA-384 or higher.

Replace the server certificate

Update the default server certificate used for HTTPS communication with browsers.

Before you begin

You must have access to the new certificate and private key files.

Task

1. Open the **Edit Server Certificate** page.
   a. Select **Menu** → **Configuration** → **Server Settings**.

   b. From the **Setting Categories** list, select **Server Certificate**, then click **Edit**.

2. Browse to the server certificate file, then click **Open**.

   Note

   > You can create your own self-signed certificate with OpenSSL.

3. If needed, type the PKCS12 certificate password and alias name.
4. Browse to the private key file, then click **Open**.
5. If needed, type the private key password, then click **Save**.
6. Restart McAfee ePO for the change to take effect.

Install the security certificate for Internet Explorer

Prevent the certificate prompt from appearing every time you log on by installing the security certificate.

Task

1. From your browser, open McAfee ePO. The **Certificate Error: Navigation Blocked** page appears.
2. Click **Continue to this website (not recommended)** to open the logon page. The address bar is red, indicating the browser cannot verify the security certificate.
3. To the right of the address bar, click **Certificate Error** to display the **Certificate Invalid** warning.
4. At the bottom of the warning, click **View certificates** to open the **Certificate** dialog box.

   Caution

   > Do not click **Install Certificate** on the **General** tab. If you do, the process fails.

5. Select the **Certification Path** tab, then select **Orion_CA_<servername>**, and click **View Certificate**. Another dialog box opens to the **General** tab, displaying the certificate information.
6. Click **Install certificate** to open the **Certificate Import Wizard**.
   a. Click **Next** to specify where the certificate is stored.
   b. Select **Place all certificates in the following store**, then click **Browse** to select a location.
   c. Select the **Trusted Root Certificate Authorities** folder from the list, click **OK**, then click **Next**.
   d. Click **Finish**. In the **Security Warning** that appears, click **Yes**.
7. Close the browser.
8. Change the target of the McAfee ePO desktop shortcut to use the NetBIOS name of the McAfee ePO server instead of "localhost."
9. Restart McAfee ePO.

Results

Now when you log on to McAfee ePO, you are no longer prompted to accept the certificate.

Install the security certificate for Firefox

You can install the security certificate when using Firefox 3.5 or later, so that the warning dialog box does not appear every time you log on.

Task

1. From your browser, open McAfee ePO. The **This Connection is Untrusted** page appears.
2. Click **I Understand the Risks** at the bottom of the page.
3. Click **Add Exception**.
4. Click **Get Certificate**. The **Certification Status** information is populated and the **Confirm Security Exception** button is enabled.
5. Make sure that **Permanently store this exception** is selected, then click **Confirm Security Exception**.

Results

Now when you log on to McAfee ePO, you are no longer prompted to accept the certificate.

Install Agent Handlers

Install Agent Handlers in your environment to help manage agent-server communication and load balancing. You can install 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.

Each McAfee ePO server contains a main Agent Handler. Installing more Agent Handlers can help manage an increased number of products and systems managed by one McAfee ePO server in situations where the CPU and IO on the database server is not overloaded.
Agent Handlers require the same high-speed network access to your database as the primary McAfee ePO server.

ⓘ **Attention**

> Install additional Agent Handlers in the same data center as the SQL Server. Do not install Agent Handlers in remote locations or you risk impacting the performance of the entire McAfee ePO environment.

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.

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. Right-click **Setup.exe** and select **Run as Administrator** 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. Accept 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**.

   ⓘ **Important**

   > 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. Configure the server information.
   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 8443, the same port used for client-to-server authenticated communication.
   c. Type the name and password of a user with McAfee ePO Global Administrator rights, and click **Next**.

d. Provide the password for access to the McAfee ePO SQL database, then click **Next**.

The **Database Information** page is populated with these McAfee ePO server settings.

- **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.
8. When installation is complete, enable your Agent Handler from the McAfee ePO interface.

Restoring McAfee from a Disaster Recovery Snapshot

Disaster Recovery Snapshot prerequisites

Make sure these requirements are in place before you begin restoring McAfee ePO from a Disaster Recovery Snapshot.

- McAfee ePO SQL database containing a valid Disaster Recovery Snapshot.
- User name and password for a global administrator account that uses McAfee ePO authentication.
- The Disaster Recovery passphrase for the snapshot in the database.
- Install McAfee ePO 5.10.2428.67 or later in Primary Node after enabling the **Restore DB** option.
- Failover to the secondary node and complete the installation without enabling the **Restore DB** option. During this process expect unavailability of Tomcat service.
- If you apply McAfee ePO 5.10.0 Update 13 after taking snapshot on the previous McAfee ePO 5.10.0 server, you must perform disaster recovery with McAfee ePO 5.10.2428.67 or later, then perform the repair function with McAfee ePO 5.10.0 Update 13.
- When snapshot is taken on McAfee ePO 5.10.0 Update 13, during Disaster Recovery restore, ePO package 5.10.0.2428.67 or later automatically performs the repair for Update 13, that means manual repair is not needed post Disaster Recovery restore.

For more details about the Disaster Recovery process, see the product guide for McAfee ePO.

Restore McAfee ePO software in a single-server environment

Restore McAfee ePO from the snapshot stored in a McAfee ePO database. You can do this by reinstalling the McAfee ePO software on a server with the **Restore ePO from an existing database** option enabled and configuring the installation to use an existing McAfee ePO database.

Before you begin

Gather this information and complete these steps before beginning your installation. These steps make sure that your McAfee ePO software can communicate with the SQL Server hosting the McAfee ePO database.

- If you are using dynamic ports for your SQL Server, verify that the SQL Browser Service is running.
- If you are not using dynamic ports for your SQL Server, make sure that you know the ports that your SQL instance is using.
- Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.

Note

McAfee Agent uses either the last known IP address, DNS name, or NetBIOS name of the McAfee ePO server. If you change any one of these values, make sure that McAfee Agent has a way to locate the server. The easiest way to do that is to retain the existing DNS record, and change it later to direct the McAfee ePO server's new IP address. After McAfee Agent successfully connects to the McAfee ePO server, it downloads an updates Sitelist.xml with the current information.

Note

We recommend that you change the FQDN first, and use the same IP address so that McAfee Agent on the end nodes communicates to the Agent Handler or the McAfee ePO server using the last known IP address. After successful communication, McAfee Agent will update the new FQDN of the server. Once all systems communicate successfully using the IP address, you can change the IP address as McAfee Agent knows the new FQDN.

Note

Monitor the process because you might need to restart your system.

Task

1. If you have 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.
2. Using an account with local administrator permissions, log on to the Windows Server that you want to restore McAfee ePO to.
3. Extract the files to a temporary location, and double-click **Setup.exe**.
   The version of McAfee ePO being restored must be the same as the version used to create the snapshot in the database. You can download the correct version from the McAfee website.

   Important

   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.
4. Select **Restore ePO from an existing database snapshot** and click **Next** to begin the installation process.
5. In the Install additional software step, any remaining prerequisites are listed. To install them, click **Next**.
6. In the Destination Folder step, click either:
   - **Next** — Install your McAfee ePO software in the default location (C:\Program Files (x86)\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 as needed. When finished, click **OK** → **Next**.
7. In the Database Information step, either select the SQL Server name from the Database Server drop-down list or manually enter the name of the SQL Server.

8. In the Database Name field, enter the name of the existing McAfee ePO database containing the snapshot, specify the type of Database Server Credentials to use, then click **Next**.
   - **Windows authentication** — From the Domain menu, enter the domain of the user account you're going to use to access the SQL Server. Enter the user name and password for an account with sufficient permissions to access the SQL Server hosting the McAfee ePO database.
   - **SQL authentication** — Enter the user name and password for an account with sufficient permissions to access the SQL Server hosting the McAfee ePO database.

   The Domain menu is grayed out when using SQL authentication.

   You might need to specify 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 TCP port 1433, and to determine if a dynamic port is in use by querying the SQL Browser service on UDP port 1434. If those ports fail, you are prompted to provide a SQL Server TCP port.
9. In the HTTP Port Information step, review the default port assignments, then click **Next** to verify that the ports are not already in use on this system.
10. In the Administrator Information step, type the user name and password you used for your previously existing McAfee ePO global administrator account.
11. Type the Keystore Encryption passphrase (also known as the Snapshot passphrase) for the snapshot in the McAfee ePO database.
12. Click **Install** to begin the installation.
13. When installation is complete, click **Finish** to exist the InstallShield wizard.
14. If you restored McAfee ePO to a server with a different IP address and DNS name than your previously existing server, configure a way to allow your managed systems to connect to your new McAfee ePO server.
    There are several ways to achieve this depending on your DNS vendor. The most common way is to create a CNAME record in DNS that redirects requests to the old DNS name to the IP address of the new McAfee ePO server. For more information about this process, see Microsoft documentation.
15. If you stopped the Agent Handlers in step 1, and restored McAfee ePO to a system with the same server name and IP address that it had previously, 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.
    If you restored McAfee ePO to a system with a different name or IP address, see *Restore Agent Handler connections*.

Results

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

Restore McAfee ePO software in a cluster environment

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

Before you begin

Gather this information and complete these steps before beginning your installation. These steps ensure that your McAfee ePO software can communicate with the SQL Server hosting the McAfee ePO database.

- If you are using dynamic ports for your SQL Server, verify that the SQL Browser Service is running.
- If you are not using dynamic ports for your SQL Server, ensure that you know the ports that your SQL instance is using.
- Make sure that the TCP/IP Protocol is enabled in the SQL Server Configuration Manager.

Restoring the McAfee ePO software in a Microsoft Cluster Server environment is similar to installing the software initially.

Tip

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

Task

1. If you have 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.
2. Using an account with local administrator permissions, log on to the Windows Server (the first node of the cluster) used as the restore McAfee ePO server.
3. If needed, in the Failover Cluster Manager, create the McAfee ePO application role, Client Access Point, and shared data drive resources.
   For more information, see *Installing Software in a Cluster environment* .
4. Extract the files to a temporary location, and double-click **Setup.exe**.
   The version of McAfee ePO being restored must be the same as the version used to create the snapshot in the database. You can download the correct version from the McAfee website.

   Important

   > 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. Select **Restore ePO from an existing database snapshot** and click **Next** to begin the 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 **Change** to 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 as needed. When finished, click **OK**.

   Important

   > Make sure that you specify a destination folder that is accessible from all nodes of the cluster.

8. In the Set Virtual Server Settings step, provide the Virtual Server IP address, McAfee ePO Virtual Cluster Name, McAfee ePO Virtual Cluster FQDN, and Cluster Configuration Passphrase, then click **Next**.
9. In the Database Information step, either select the SQL Server name from the Database Server drop-down list or manually enter the name of the SQL Server.
10. In the Database Name field, enter the name of the existing McAfee ePO database containing the snapshot, specify the type of Database Server Credentials to use, then click **Next**.

    - **Windows authentication** — From the Domain menu, enter the domain of the user account you're going to use to access the SQL Server. Enter the user name and password for an account with sufficient permissions to access the SQL Server hosting the McAfee ePO database.
    - **SQL authentication** — Enter the user name and password for an account with sufficient permissions to access the SQL Server hosting the McAfee ePO database.

    The Domain menu is grayed out when using SQL authentication.

    You might need to specify 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 TCP port 1433, and to determine if a dynamic port is in use by querying the SQL Browser service on UDP port 1434. If those ports fail, you are prompted to provide a SQL Server TCP port.

11. In the HTTP Port Information step, review the default port assignments, then click **Next** to verify that the ports are not already in use on this system.
12. In the Administrator Information step, type the user name and password you used for your existing McAfee ePO global administrator account.
13. Type the Keystore Encryption passphrase (also known as the Snapshot passphrase) for the snapshot in the McAfee ePO database.
14. Click **Install** to begin the installation.
15. When the installation has completed on the first node, click **Finish**, and move the **ePO Application role** to the second node.

    Note

    You can also shut down the first note, forcing the role to move to the second node.

16. On the second node, run the McAfee ePO installer.

    Important

    Do not select the **Restore ePO from an existing database snapshot** option.

17. In the Destination Folder step, click **Change**, browse to the destination on the shared data drive where McAfee ePO is installed, and click **OK** → **Next**.
18. In the Set Virtual Server Settings step, the Virtual Server IP address, McAfee ePO Virtual Cluster Name, and McAfee ePO Virtual Cluster FQDN fields are automatically populated. Type the Cluster Configuration Passphrase and click **Next**.
19. Click **Install** to start the installation on the second node, then click **Finish**.
    This process takes much less time than the installation on the first node.

20. Create the three Generic Service resources. When finished, bring the **ePO Application Role** online.
    For more information, see *Installing software in a cluster environment*.
21. If you stopped the 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.
22. Confirm that McAfee ePO is functioning correctly, and test the cluster function by moving the **ePO Application Role** to the other node.

Results

After completing these steps, your McAfee ePO software is restored.

Restore Agent Handler connections

If you restored McAfee ePO to a system with a new name or IP address, you must change the Agent Handler settings to connect to the restored server.

Task

1. On the Agent Handler server, extract the McAfee ePO software installation package to a temporary location.
2. In the extracted folder, open the Agent Handler folder, and double-click **Setup.exe** to start the McAfee Agent Handler InstallShield wizard.
3. Click **Next** to begin the change process.
4. From the **Program Maintenance** dialog box, select **Modify** to change which program features are installed, then click **Next**.
5. 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 8443.
    c. Type the **ePO Admin User Name** and **ePO Admin Password** of a user with global administrator rights.
    d. Click **Next**.
    The installer contacts the McAfee ePO server and obtains the details for the SQL Server hosting the McAfee ePO database. The SQL Server and database details, except for the password, are already populated.
6. Enter the password for the account you specified and click **Next**.
7. Click **Install** to start the changes to the installation.
8. When installation is complete, click **Finish**.

Results

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

Using McAfee ePO in FIPS mode

FIPS basics

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).

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 cryptographic modules to meet the requirements for FIPS-compliance.

Validated FIPS 140-2 cryptographic modules used by McAfee ePO

Cryptographic module	Certificate number	Link
RSA BSAFE Crypto-C Micro Edition (Crypto-C ME) 4.1.2	2294	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2294
Bouncy Castle FIPS Java API (BC-FJA) 1.0.1	3152	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3152
OpenSSL FIPS Object Module 2.0.16	2398	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2398

Cryptographic module	Certificate number	Link
Note: This module is used only for TLS communication between McAfee ePO and the McAfee Agent.		

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

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.

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.

Note

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 an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module.

The cryptographic boundary defines this perimeter and contains the set of hardware, software, and firmware that implements valid security functions. Only the approved set of interfaces can access the cryptographic modules inside the cryptographic boundary. No other mechanism 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

Important

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 can't be used in FIPS mode. Check new versions of McAfee products for further information about FIPS compliance as they are released.

Install 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

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.

   Important

   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.

Important

> 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 Agent Handler is in FIPS 140-2 mode

View the server.ini file to make sure that Agent Handler 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.

Verify that the Apache server is in FIPS 140-2 mode

The Apache server contains a FIPS enablement configuration setting.

Task

1. Browse to the Agent Handler installation folder. The default folder is C:\Program Files (x86)\McAfee\ ePolicy Orchestrator.
2. Browse to the Apache configuration folder: apache2\conf
3. Using a text editor, open the httpd.conf file and search for **SSLFIPS**.
    - Off — Apache mod_ssl is not configured for FIPS enablement.
    - On — Apache mod_ssl is configured for FIPS enablement.

Verify that the application server is in FIPS 140-2 mode

View the Security Mode to make sure that the McAfee ePO application server is running in FIPS mode.

Task

Select **Menu** → **Configuration** → **Server Settings** → **Security Keys**, then confirm that **Security Mode** is **FIPS 140-2**.

Remove the software

Uninstall McAfee ePO

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

Before you begin

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 can't regenerate these keys later.

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

   Note

   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.

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.

COPYRIGHT