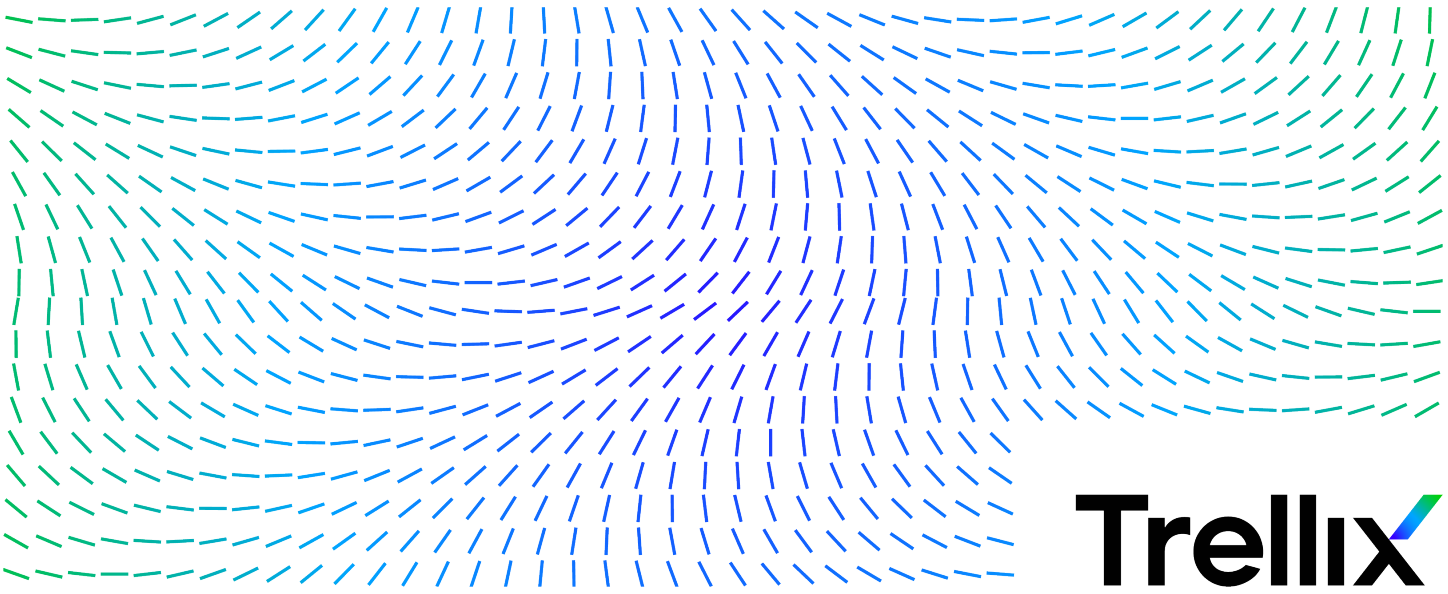
McAfee Agent 5.7.x Product Guide



Trellix

Contents

Product overview. 5

Overview. 5

Product name conventions. 5

Key features. 6

How it works. 9

Supporting Security-Enhanced Linux Confinement. 11

Supporting Security-Enhanced Linux (SELinux) confinement. 11

Configuring McAfee Agent policies. 12

McAfee Agent policy settings. 12

Configuring General policy. 15

Priority event forwarding. 15

Retrieve system properties. 16

Safe install using Product Deployment Incompatibility check (McAfee ePO On-Premises). 17

Configuring Repository policy. 19

Select a repository (McAfee ePO On-Premises). 19

Configure proxy settings for the agent. 20

Configuring Product Improvement Program policy (McAfee ePO On-Premises). 22

Product Improvement Program capability in McAfee Agent. 22

Enable the software on the McAfee ePO server. 22

Enforce policy to enable the software on client systems. 23

How the Custom Properties policy works. 23

Configure Custom Properties policy. 25

Configure client task to control access. 26

Working with the agent from McAfee ePO. 27

How agent-server communication works. 27

The agent-server communication interval. 27

Handling interruptions in agent-server communication. 28

Wake-up calls and tasks. 28

How SuperAgents work (McAfee ePO On-Premises). 30

SuperAgent wake-up calls. 31

Convert McAfee Agent to SuperAgent. 31

SuperAgent caching and communication interruptions. 32

SuperAgent hierarchy. 35

Creating a hierarchy of SuperAgents. . . . 36
Communicating through a RelayServer. . . . 37
Enable relay capability. . . . 38
Peer-to-peer communication. . . . 39
Downloading content updates from peer agents. . . . 39
Best practices for using peer-to-peer communication. . . . 40
Enable peer-to-peer service. . . . 40
Collect McAfee Agent statistics. . . . 41
Change the language for the agent interface and event log. . . . 42
Configure selected systems for updating (McAfee ePO On-Premises). . . . 43
Respond to policy events. . . . 43
Scheduling client tasks. . . . 44
Run client tasks immediately (McAfee ePO On-Premises). . . . 45
Locate inactive agents. . . . 46
Viewing clients pending for reboot. . . . 46
Identifying duplicate agent GUIDs (McAfee ePO On-Premises). . . . 47
Correct duplicate agent GUIDs (McAfee ePO On-Premises). . . . 47
Verify policy changes with system properties. . . . 48

Changing the agent management modes. . . . 50
How to change McAfee Agent management modes. . . . 50
Change from unmanaged to managed mode on Windows systems. . . . 51
Change from managed to unmanaged mode on Windows systems (McAfee ePO On-Premises). . . . 52
Change from unmanaged to managed mode on non-Windows platforms. . . . 52
Change from managed to unmanaged mode on non-Windows platforms (McAfee ePO On-Premises). . . . 53

Running agent tasks from the managed system. . . . 54
Using the system tray icon. . . . 54
Make the system tray icon visible and update security settings. . . . 55
Updates from the managed system. . . . 55
McAfee Agent command-line options. . . . 56
Using the maconfig command-line tool (McAfee ePO On-Premises). . . . 57

Agent logs. . . . 61
Viewing McAfee Agent logs. . . . 61
View McAfee Agent Status Monitor. . . . 63
View McAfee Agent product log from McAfee ePO (McAfee ePO On-Premises) using Single System Troubleshooting . . . 63

Additional information. . . . 64

McAfee Agent files and folders. 64
McAfee Agent feature support. 66
Available interface language versions. 69

Frequently asked questions. 72

Product overview

Overview

McAfee® Agent is the client-side component that provides secure communication between McAfee® ePolicy Orchestrator® (McAfee® ePO™) and managed products.

The agent also serves as an updater for McAfee products.

Systems can be managed by the McAfee ePO server only if they have an agent installed. While running silently in the background, the agent:

- Installs products and their upgrades on managed systems.
- Updates security content such as the V3 DAT files or AMCore Content Package associated with McAfee® Endpoint Security.
- Enforces policies and schedules tasks on managed systems.
- Gathers information and events from managed systems, and sends them to McAfee ePO.

The term *agent* is used in these contexts in McAfee ePO:

- Agent — The basic operating mode for McAfee Agent, providing a communication channel to McAfee ePO and local services for managed products.
- SuperAgent — An agent that acts as an intermediary between McAfee ePO and other agents in the same network broadcast segment. The SuperAgent caches information received from McAfee ePO, the Master Repository, or a mirrored Distributed Repository, and distributes it to the agents in its network subnet.
  Configure a SuperAgent in every subnet when managing agents in larger networks.

Note

SuperAgent is not available on McAfee ePO Cloud.

Product name conventions

This guide covers multiple versions of McAfee ePO management platform. When content applies to only one platform, the platform name appears with the content.

McAfee ePO	The umbrella term for all McAfee ePO management platforms. When used in this guide, the content applies to all platforms.
McAfee ePO On-Premises	The locally installed (on-premises) version of McAfee ePO.

McAfee ePO Cloud	The cloud version of McAfee ePO.
MVISION ePO	The MVISION version of McAfee ePO.

Key features

McAfee Agent architecture is single threaded and asynchronous based on services (messaging) architecture. In messaging-based architecture, the services communicate using a common language. This reduces the use of system resources, such as number of threads, number of handles, memory, and CPU.

McAfee Agent 5.0.x is the minimum required version for McAfee ePO Cloud.

(McAfee ePO On-Premises) McAfee Agent 5.6.x supports McAfee ePO 5.3.x or later.

The McAfee Agent 5.x.x extension manages all previous versions of McAfee Agent (4.8.x and 5.0.x). But, previous versions of the McAfee Agent management extension cannot manage McAfee Agent 5.x.x clients.

McAfee Agent includes these features:

Manifest based policy

When using McAfee Agent 5.x.x with McAfee ePO, the manifest based policy improves the scalability of McAfee ePO. McAfee Agent fetches only the changed policy settings from McAfee ePO, using fewer resources for comparing or merging settings. Also, McAfee ePO doesn't have to compute the changed policies at each agent-server communication. This helps save network bandwidth every time a policy update is downloaded.

Persistent connection

When performing an agent-server communication, McAfee Agent keeps the communication channel with McAfee ePO alive, so that multiple requests and responses such as property upload, policy download, and events upload are passed between the agent and the Agent Handler in the same TCP connection. Once the communication is complete, the connection is closed.

Previous versions of McAfee ePO required multiple TCP connections from McAfee Agent during a single agent-server communication. This required more network bandwidth, whereas keeping the connection alive reduces the network bandwidth.

Sensor services

McAfee Agent uses sensor services to track system events and take actions on the client system. There are two types of sensor services:

- User sensors — Detects the logged on users on the client system using operating system APIs and apply the user-based policies accordingly.
- Network sensors — Detects the network connectivity status using operating system network APIs and determines if the agent functionality such as pulling updates from the repository or communicating to McAfee ePO should be performed.

Peer-to-peer communication

To retrieve updates and install products, McAfee Agent communicates with McAfee ePO. These updates might be available with the agents in the same subnet. With peer-to-peer communication, McAfee Agent downloads updates from the peer agents in the same subnet, reducing bandwidth consumption between McAfee ePO and McAfee Agent.

Remote provisioning

You can use remote provisioning to:

- Convert an unmanaged McAfee Agent to managed — Use the command-line switch to convert McAfee Agent mode from unmanaged to managed (that is, provision to McAfee ePO).
- Migrate from one McAfee ePO to another — Use the command-line switch to migrate McAfee Agent from one McAfee ePO to another.

See *Changing agent management modes* for more details.

Third-party software authentication

McAfee Agent supports third-party integration, such as integration with software developed by SIA partners. For these third-party software to communicate with McAfee Agent, the software should have Message Bus Certificates for mutual authentication. We have added MsgbuscertupdaterPackage.zip on SDM and other source locations which certify third-party software to communicate with McAfee Agent.

Note

The MsgbuscertupdaterPackage.zip package is downloaded automatically at the client nodes. This default download task is also scheduled to download the package at 12 a.m. (local time) every day.

Self-protection

McAfee Agent protects unauthorized access to all internal Agent assets such as the databases, files, folders, and registries using McAfee VSCore. The admin can choose to enable or disable the service protection with McAfee Agent self-protection policy.

Because McAfee Agent 5.0.5 or later doesn't consume SysCore in its installer, it doesn't upgrade or install SysCore on the system. This makes McAfee Agent installer lightweight and reduces the size of the package and installation time. Once a supported version of SysCore (15.3.0.673 or later) is installed on the system, McAfee Agent starts using its protection capabilities, enables self-protection for files, folders, registry, services, and executables.

Installer improvements

In the event of shutdown or restart, McAfee Agent now provides additional information to the user when products are being deployed onto the system.

If the user initiates system shutdown or restart when the agent is deploying products, McAfee Agent notifies the user that the shutdown can't continue. If continued, this might cause stability issues to the operating system. The user can still continue with the shutdown operation. Once the product deployment is complete, the user can reinitiate shutdown later by clicking `Cancel` on the notification displayed. If not, the system automatically continues for shutdown.

Note

McAfee product updates such as DAT and content updates are not affected by this new feature.

(McAfee ePO On-Premises) Smart Scheduler

Smart Scheduler is a feature provided by McAfee Agent for use with McAfee® Endpoint Security for Servers. Smart Scheduler minimizes the performance impact on VDI or virtual servers with efficient scheduling of CPU intensive tasks based on overall CPU load.

Note

Smart Scheduler supports VMware ESXi, Citrix XenServer, Microsoft Hyper-V, Microsoft Azure, and Amazon Web Services. This feature is not supported on physical systems.

For more details about configuring Smart Scheduler, see the McAfee Endpoint Security for Servers product documentation.

(McAfee ePO On-Premises) Incompatibility check

McAfee Agent 5.6.0 checks for incompatibility with McAfee products before it is deployed on the client system using the McAfee ePO deployment task. McAfee Agent has in-built content driven incompatibility specification list which controls the McAfee product installation using the McAfee ePO deployment task.

McAfee Agent 5.6.0 has the capability to block the deployment of incompatible McAfee products on the client system, which is based on the incompatibility specification list.

Management platform support

Below table shows the management platform support for McAfee Agent features and functionality.

Feature	McAfee ePO On-Premises	McAfee ePO Cloud	MVISION ePO
RelayServer	Yes	Yes	Yes
Peer-to-peer	Yes	Yes	Yes
McAfee Smart Installer	Yes	Yes	Yes
Property collection	Yes	Yes	Yes
Policy enforcement	Yes	Yes	Yes
Task enforcement	Yes	Yes	Yes

Feature	McAfee ePO On-Premises	McAfee ePO Cloud	MVISION ePO
McAfee Agent Wake-up	Yes	Yes	Yes
Product Update	Yes	Yes	Yes
Product Deployment	Yes	Yes	Yes
Event Forwarding	Yes	Yes	Yes
Automatic McAfee Agent uninstall from McAfee ePO	Yes	Yes	Yes
Remote provisioning	Yes	Yes	Yes
Incompatibility check	Yes	No	Yes
SuperAgent	Yes	No	No
Run Client Task Now	Yes	No	No
Remote log access	Yes	No	No
User-based policy	Yes	Yes	Yes
Data channel support	Yes	No	No
Mirror Task	Yes	No	No
UNC repository updating	Yes	No	No

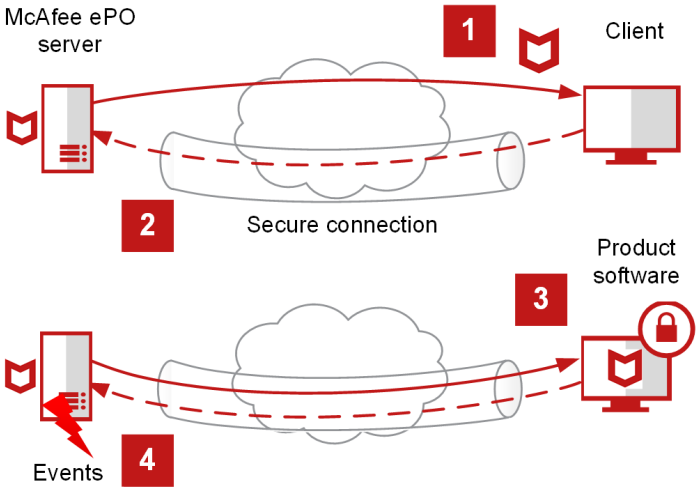
How it works

Installing the agent on client systems is required for managing your security environment through McAfee ePO.

This diagram shows how the McAfee Agent works when installed on client systems through McAfee ePO.

1. You install the McAfee Agent on a client.

2. The McAfee Agent establishes a secure connection between the client and McAfee ePO.
3. McAfee ePO downloads the product software to the client over the secure connection.
4. The McAfee Agent sends client events and other information back to McAfee ePO.



Supporting Security-Enhanced Linux Confinement

Supporting Security-Enhanced Linux (SELinux) confinement

McAfee Agent supports all processes to run in SELinux confined mode.

SELinux is a kernel security module that allows enforcement of access controls that are loaded at the start of a system.

You can use SELinux to confine programs and services as well as access to files, network, IPC, and other processes. SELinux RPM provides SELinux policies to confine all services installed by McAfee Agent. When you install McAfee Agent along with SELinux RPM, the SELinux modules create contexts for McAfee Agent processes, binaries, configuration files, log files, etc. and all Agent processes run in SELinux confinement.

Note

McAfee Agent SELinux is supported on RHEL 7.x and 8.x versions. For information about the supported RHEL versions, see KB51573.

When you enable McAfee Agent SELinux, the following are the default allowed directories for the processes and features to perform its operations.

- The command-line, maconfig and cmdagent tools, accesses the directory in /tmp, /var/tmp, /var/log, /var/McAfee/agent/logs.
- McAfee Agent processes access the directory in /var/McAfee/agent.
- Super Agent, peer-to-peer and relay accesses the directory in /var/McAfee/agent.

To change the allowed default directory to any other directory when you enable SELinux, you need to perform the steps mentioned in KB94454. For example, you can change the Super Agent or peer-to-peer repository from /var/McAfee/agent to /tests/test through McAfee Agent general policy from McAfee ePO by following the steps mentioned in KB94454.

Configuring McAfee Agent policies

McAfee Agent policy settings

McAfee Agent provides configuration pages for setting policy options that are organized into these categories: **General**, **Repository**, **Product Improvement Program**, **Troubleshooting**, and **Custom Properties**.

Before distributing McAfee Agent throughout your network, consider carefully how you want McAfee Agent to behave in the segments of your environment. Although you can configure McAfee Agent policy settings after they are distributed, we recommend setting them before the distribution, to prevent unnecessary impact on your resources.

Note

Only the difference in the policy settings is downloaded from the server when using McAfee Agent 5.0.0 or later.

General policy

Settings available for **General** policy are divided into following tabs.

Tab	Settings
General	• Policy enforcement interval • Use of system tray icon in Windows environments • Enabling system tray icon in a remote desktop session • (McAfee ePO On-Premises) McAfee Agent and **SuperAgent** wake-up call support • Whether to accept connections only from McAfee ePO • Yielding of the CPU to other processes in Windows environments • Restricting McAfee Agent processes, services, and registry keys change • Rebooting options after product deployment in Windows environments • The agent-server communication • Retrieving all system and product properties

SuperAgent	• Enabling RelayServer on McAfee Agent
	• Disabling discovery of RelayServers
	• (McAfee ePO On-Premises parameters):
	  • The repository path where the **SuperAgent** goes for product and update packages
	  • Specify the interval to flush lazy cache memory
	  • Specify the disk space for the lazy cache
	  • Specify the interval to purge the files from the disk
	  • Broadcast wake-up call to SuperAgent

Tab	Settings
	• Enabling lazy caching
Events	• Enabling/disabling priority event forwarding • Level of priority events forwarded • Interval between event uploads • Maximum number of events per upload
Logging	• Enabling/disabling application logging • Setting the log file size limit and rollover count • Level of logging detail • (McAfee ePO On-Premises) Enabling/disabling remote logging • (McAfee ePO On-Premises) Setting to enable remote access to logs **Note:** To know about enabling debug logging for McAfee Agent for non-Windows troubleshooting, see KB69542.
Updates	• Custom update log file location **Note:** For information about log file option requirements for McAfee Agent Product update, see KB85549. • Specifying post-update options (runs only after a successful update) • Downgrading DAT files • Enabling automatic update of McAfee products post deployment • Selecting update type and repository branch **Note:** The selected update type is considered for tasks that run post deployment of McAfee products and when you run **Update Security** using the system tray icon.
Peer-to-Peer	• Enable peer-to-peer communication on McAfee Agent to enable peer-to-peer client

Tab	Settings
	Note: Peer-to-peer policies are enabled by default for the McAfee Default policies and are disabled for the Large Organization Default policies. • Enable McAfee Agent to serve updates or installation files to peer agents • Specify the repository path • Specify the disk space for the updates on the peer-to-peer server • Specify the interval to purge the files from the peer-to-peer server repository
Deployment	• Enable McAfee Agent to perform incompatibility check during McAfee product deployment

Note

(McAfee ePO On-Premises) When importing **My Default General** policy from the McAfee ePO 4.6.6 server to the McAfee ePO 5.1.1 server, the policy values for **Peer-to-Peer** feature are replicated from **McAfee Default** policy rather than **My Default** policy on the McAfee ePO 5.1.1 server.

Repository policies

Repository policies settings can be configured using **Repositories** and **Proxy** tabs.

Note

On McAfee ePO Cloud, only **Proxy** server settings can be configured using the **Repository** policy.

Tab	Settings
(McAfee ePO On-Premises) **Repositories**	Repository selection
Proxy	Proxy configuration

Troubleshooting policies

Settings available for **Troubleshooting** policies are contained in one tab.

Tab	Settings
General	McAfee Agent user interface and log language

Product Improvement Program policies

Settings available for **Product Improvement Program** policies are contained in one tab.

Tab	Settings
Product Improvement Program	Allowing Product Improvement Program to collect anonymous diagnostic and usage data.

Custom Properties policies

Settings available for **Custom Properties** policies are contained in one tab.

Tab	Settings
Custom Properties	Determine end-user access permission to view or edit a particular custom property.

Configuring General policy

Priority event forwarding

You can configure McAfee Agent to forward events to McAfee ePO on a priority basis, if they are equal to or greater than a specified severity.

During normal operation, McAfee Agent and security software on the managed system generate software events regularly. These events are uploaded to the server at each agent-server communication, at a set upload interval and are stored in the database. These events can range from information about regular operation, such as when McAfee Agent enforces policies locally, to critical events, such as when a virus is detected and not cleaned. A typical deployment of McAfee Agent in a large network can generate thousands of these events an hour.

If you plan to use **Automatic Responses**, enable priority uploading of higher severity events for those features to function as intended. McAfee Agent sends lower priority events to McAfee ePO on later agent-server communication intervals.

Specific event severities are determined by the product that generates the events. You can enable priority uploading of events on the **Events** tab of the McAfee Agent policy pages.

The table lists the events generated by McAfee Agent with IDs and severity.

Event ID	Description	Severity
2401	Common update success	3
2402	Common update fail	4
2411	Deployment success	3
2412	Deployment fail	4
2413	McAfee Agent uninstall attempt	3
2422	Policy enforce fail	3
2427	Props collect fail	3

Retrieve system properties

Use McAfee Agent to retrieve system properties from managed systems.

Retrieve system properties to fetch information about the defined properties and installed programs on the managed systems.

At each agent-server communication, McAfee Agent sends information to McAfee ePO about the managed computer, including information about the software products that are installed.

The scope of the information depends on how you have configured:

- McAfee Agent policy that specifies whether to retrieve a full set of information about installed programs, or only a minimal set as defined by the McAfee products.
- (McAfee ePO On-Premises) The task setting that specifies whether to retrieve all properties defined by McAfee Agent policy, or only properties that have changed since the last agent-server communication. This setting is available when configuring an immediate or scheduled wake-up call.

Use **System Tree** actions to wake up McAfee Agent on non-Windows operating systems.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **General**. Click **Edit** to update a policy.

You can also edit the policy from **Policy Details** on the right pane.

Note

For McAfee ePO 5.9 or earlier and McAfee ePO Cloud, select **McAfee Agent** in the **Product** drop-down list and **General** in the **Category** drop-down list. Click a policy name to update it.

3. Deselect **Retrieve all system and product properties (recommended). If unchecked retrieve only a subset of properties.** to send system properties and minimal product properties.
   This is selected by default.
4. Click **Save**.
5. Select **Menu** → **Client Tasks** → **Client Task Catalog**.

   Note

   For McAfee ePO 5.9 or earlier and McAfee ePO Cloud, select **Menu** → **Policy** → **Client Task Catalog**.

6. In the **Client Task Types** list, select **McAfee Agent Wakeup**.
7. Click the name of an existing task, or click **New Task** and choose a **McAfee Agent Wakeup** task.
8. In **Options**, select **Send all properties defined by the agent policy** to retrieve all properties as defined by McAfee Agent policy, even if previously sent.
9. Click **Save**.

Safe install using Product Deployment Incompatibility check (McAfee ePO On-Premises)

McAfee Agent 5.6.0 checks for incompatibilities with McAfee products before it is deployed on the client system using a McAfee ePO deployment task.

How safe install works

Safe install checks the content hosted by McAfee, and McAfee Agent downloads the latest available version of the contents on the McAfee ePO server. This information is further propagated to all client systems as a policy setting. If a deployment task fails due to this policy setting, the information is sent to McAfee ePO using the install failure client events.

You can see the safe install errors in the install failure client event details in McAfee ePO. The following table shows the list of errors displayed on the **Client Event: Details** page.

Types of error
Incompatibility detected as dependent product is not installed
Incompatibility detected as incompatible product is installed or it is an unsupported version

Types of error
Incompatibility detected as conflict product is installed

Viewing the Product Deployment Incompatibility report

You can view the Product Deployment Incompatibility report using either **Dashboard** or **Queries & Reports**.

The Product Deployment Incompatibility queries display a bar chart with product incompatibilities detected during product deployment on the client system.

The following queries are available on the Product Deployment Incompatibility report:

- **Product Deployment Incompatibility Summary within 24 hours**
- **Product Deployment Incompatibility Summary within 7 days**

View the Product Deployment Incompatibility report using Dashboard

You can view the Product Deployment Incompatibility report using Dashboard on the McAfee ePO console.

Task

1. Select **Menu** → **Dashboards**.
2. Select **Product Deployment Incompatibility** from **McAfee Dashboards** pop down list.
   The Product Deployment Incompatibility report is displayed.

Results

View the Product Deployment Incompatibility report using Queries & Reports

You can view the Product Deployment Incompatibility report using **Queries & Reports** on the McAfee ePO console.

Task

1. Select **Menu** → **Queries & Reports**.

2. From **McAfee Groups**, select **Agent Management**.
   The list of queries is displayed. You can run queries to view the Product Deployment Incompatibility report.

Results

Configure safe install

Check for product incompatibilities using safe install during McAfee product deployments.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **General**.
   Click **Edit** to update a policy.
3. Click the **Deployment** tab.
4. Select **Enable Incompatibility check**.
5. Click **Save**.

Configuring Repository policy

Select a repository (McAfee ePO On-Premises)

Repositories are selected in a policy. McAfee products are updated from the repositories you specify in the Repository policies.

See McAfee ePO product documentation for details about Repositories and different types of repositories.

McAfee Agent can update from any repository in its repository list based on the policy setting. These repository policies allow you to specify the most efficient means for designating a source repository for updates. You can select repositories based on ping time, subnet distance, or from a preset list.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **Repository**. Click **New Policy** to create a policy or select **Edit** → **Duplicate** on the right pane for the **My Default** policy name to create a policy based on the default.

Note

For McAfee ePO 5.9 or earlier, select **McAfee Agent** from the **Product** drop-down list, and **Repository** in the **Category** drop-down list. Click **New Policy** to create a policy, or select **Duplicate** in the **Actions** column for the **My Default** policy name to create a policy based on the default.

3. Type a name for the policy, then click **OK**.
4. Click a policy name to update it.
5. On the **Repositories** tab, select **Use this repository list** (the McAfee ePO server-managed repository list), or **Use other repository list** (a locally controlled repository list that is not managed by the McAfee ePO server).
6. Choose a basis for selecting a repository.

Selection method	Definition
Ping time	The shortest round-trip elapsed time between sending an echo request to a remote ICMP-enabled system and receiving a response from that system. Ping timeout can be configured to control the maximum time taken for a response from the remote ICMP-enabled system. The default is 30 seconds, minimum is 5, and maximum is 60.
Subnet distance	The fewest hops an ICMP packet makes while traversing the network from a local system to a remote system. The maximum number of hops can be used to control the packet traversal. The default is 15 hops, minimum is 1, and maximum is 30.
Use order in repository list	A user-defined list of repositories based on locally determined preferences. You can sequence and enable or disable specific distributed repositories on the **Repositories** tab of the McAfee Agent policy pages. Allowing McAfee Agent to update from any distributed repository ensures that they get the update in the sequence configured by the McAfee ePO administrator.

Note

McAfee Agent selects a repository each time a change occurs in the repository list, IP address, or Repository policy option.

Configure proxy settings for the agent

You might need to configure proxy settings if an agent is having trouble accessing the Internet. The proxy is supported on Windows, Macintosh, and Linux operating systems.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **Repository**. Click **Edit** to update a policy.

   Note

   For McAfee ePO 5.9 or earlier and McAfee ePO Cloud, select **McAfee Agent** from **Product** drop-down list and **Repository** from **Category** drop-down list.

3. From the list of policies, select any policy listed on this page other than **McAfee Default**.
4. Click **Proxy**.
5. Select your preferred option:

   - Select **Do not use a proxy** if your agent does not require a proxy to access the Internet.
   - Select **Use Internet Explorer settings (For Windows) / System Preferences settings (For Mac OSX)/ System environment variables (For Linux)**, then enable **Allow user to configure proxy settings**.

   Note

   On Linux systems, you can add or modify the proxy information in the /etc/ma.d/ma_environment.conf file. Restart the McAfee Agent services once you add or modify the proxy information. The proxy information in a ma_environment.conf file can be as shown below:

   ```
   http_proxy=<proxy_url>:<proxy_port>
   HTTP_PROXY=<proxy_url>:<proxy_port>
   https_proxy=<proxy_url>:<proxy_port>
   HTTPS_PROXY=<proxy_url>:<proxy_port>
   no_proxy=<localhost>
   all_proxy=<proxy_url>:<proxy_port>
   ```

   To configure the proxy settings for McAfee Agent, and to allow continuous communication with McAfee ePO when a user session is logged out, use the netsh command to set the proxy.

   ```
   netsh winhttp import proxy source =ie (if the proxy already configured in IE)
   or
   netsh winhttp set proxy <proxy>:<port>
   ```

   - Select **Manually configure the proxy settings** if you need a proxy other than Internet Explorer, and configure the following settings:
     - Select a form for the address of the source HTTP or FTP location where the agent pulls updates.
       - **DNS Name**
       - **IPv4**
       - **IPv6**

- Type the DNS name or IP address and port numbers of the HTTP or FTP source. If appropriate, select **Use these settings for all proxy types**.
- Select **Specify exceptions** to designate systems that do not require access to the proxy.
- Select **Use HTTP proxy authentication** and **Use FTP proxy authentication**, then provide a user name and credentials.

6. Click **Save**.

Configuring Product Improvement Program policy (McAfee ePO On-Premises)

Product Improvement Program capability in McAfee Agent

McAfee Agent 5.5.2 or later replaces the Product Improvement Program (PIP) with a new, more efficient, and more secure product telemetry framework.

To simplify the management experience, the new framework is integrated with McAfee Agent management extension and client. This integration eliminates the need for a separate PIP extension. McAfee Agent 5.6.0 or later installer removes any previously installed PIP extension and PIP client. To make these changes as transparent as possible, we have maintained the name of the Server Setting in McAfee ePO and maintained previous PIP settings with this new capability.

Purpose

McAfee uses the data that is collected by the agent. The data collected is:

- Analyzed by McAfee to improve product features and customers' experience with the product.
- Used by McAfee Technical Support for troubleshooting.

Privacy protection

The data collected by McAfee Agent will be used only for product improvement and Technical Support. The system-specific data will be filtered or used in aggregate form, unless it is required for Technical Support. For details about McAfee Privacy Notice, see https://www.mcafee.com/enterprise/en-us/about/legal/privacy.html.

Enable the software on the McAfee ePO server

You can configure the McAfee ePO server settings to enable Product Improvement Program capability.

Task

1. Click **Menu** → **Configuration** → **Server Settings**, select **Product Improvement Program** from the **Setting Categories**, then click **Edit**.
2. Select **Yes** to allow McAfee to collect anonymous diagnostic and usage data, then click **Save**.

Enforce policy to enable the software on client systems

You can manage Product Improvement Program on multiple client systems using the McAfee Agent PIP policy.

Before you begin

Make sure you enable the Product Improvement Program server settings before enforcing the policies.

Task

1. Click **Menu** → **Systems** → **System Tree**, then select a group in the **System Tree**.
   All systems within this group (but not its subgroups) appear in the details pane.
2. Select the required systems, then click **Actions** → **Agent** → **Set Policy & Inheritance**.
3. Select **McAfee Agent** as the **Product**, **Product Improvement Program** as the **Category**, then select the required policy.
   See the ePolicy Orchestrator product documentation for more information about creating and editing policies.
4. Select whether to **Reset inheritance** or **Break inheritance**, then click **Save**.

How the Custom Properties policy works

You can configure the Custom Properties policy to report any text value as part of system properties. You can also determine which Custom Properties are set on the client system.

These system properties can be used to tag and identify managed systems to perform actions such as assign policies, tasks, and sort systems in the **System Tree**. You can configure Custom Properties policy to determine which custom properties are set on the client system.

Custom Properties features include:

- Eight default Custom Properties.
- McAfee ePO administrator can perform the following actions:
  - Set Custom Properties remotely from the McAfee ePO console.
  - Allow or deny system administrators to view a particular custom property using registry or command-line options.
  - Allow or deny system administrators to edit a particular custom property using installer or command-line options.
  - Grant one-time edit permission to system administrators to change a particular custom property that has write access revoked.
- A custom property that is empty can be overwritten by system administrators regardless of write policy set.

Note

Starting with McAfee Agent 5.0.5, you can set up to eight Custom Properties. When using McAfee Agent 5.0.5 with earlier versions of McAfee ePO (before 5.9.0), the first four (1–4) Custom Properties are reported as part of system properties that can be effectively used for tagging, queries, and quick find features. The remaining four (5–8) Custom Properties can't be used for tagging features and are reported as part of McAfee Agent product properties.

The following table explains the behavior of Custom Properties on the System Properties page for different versions of McAfee ePO and McAfee Agent.

McAfee ePO	McAfee Agent	Custom Properties supported by McAfee Agent	Custom Properties supported by McAfee ePO	Custom property tagging	Properties reported on McAfee Agent tab	Custom Properties reported as system property
(McAfee ePO On-Premises) 5.1.x and 5.3.x	5.0.4 and earlier	4	4	4	4	4
(McAfee ePO On-Premises) 5.1.x and 5.3.x	5.0.5 and later	8	4	4	8	4
(McAfee ePO Cloud) 5.6.x	5.0.4 and earlier	4	4	4	4	4
(McAfee ePO Cloud) 5.6.x	5.0.5 and later	8	4	4	8	4
5.9.0 and later	5.0.4 and earlier	4	8	8	4	4
5.9.0 and later	5.0.5 and later	8	8	8	8	8

The custom properties field does not support use of double quotation marks ("). you can use the single quotation mark (') as an alternative. For example:

```
maconfig.exe -custom -prop1 "'quoted text' 1"
```

System administrators' action on Custom Properties is based on the following policy conditions:

- If the **Allow edit** option is enabled in the policy, system administrators can change a custom property multiple times using the `maconfig/frminst` command.
    - At the command prompt, execute the following `maconfig` commands as needed.
        - Windows: `maconfig.exe -custom -prop1 "prop1" -prop2 "prop2".....-prop8 "prop8"`
        - Non-Windows: `maconfig -custom -prop1 "prop1" -prop2 "prop2".....-prop8 "prop8"`
    - frminst command-line options
        - Windows: `frminst.exe /install=Agent /customProps1="prop1" /customProps2="prop2"...../customProps8="prop8"`
- If the **Allow edit** option is disabled in the policy, system administrators:
    - Can edit a custom property if the value on the client system is blank.
    - Can edit a custom property once if McAfee ePO administrator grants **One-time edit permission** to the property.
    - Can't edit a custom property if the property already contains a value, and is not permitted with one-time access.
- If **Allow view** is enabled in the policy, system administrators can view the custom property value from the registry or using the `cmdagent` command.
    - At the command prompt, execute the following `maconfig` commands as needed.
        - Windows: `cmdagent.exe -x`
        - Non-Windows: `cmdagent -x`
- If the **Allow view** option is disabled in the policy, system administrators can't view the custom property value from the registry or using the `cmdagent` command.

Configure Custom Properties policy

Determine which properties of the Custom Properties policy are set on client systems.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **Custom Properties**. Click **Edit** to update a policy.
   For McAfee ePO 5.9 or earlier and McAfee ePO Cloud, select **McAfee Agent** from Product list, then select **Custom Properties** from the Category list.

3. Click **New Policy**, type the policy name, then click **OK**.
4. Click the new policy name you created from the Policy Catalog page.
5. Set the **Allow view** and **Allow edit** options for each Custom Property as needed.
6. Click **Save**.

Configure client task to control access

Use a client task to remotely set Custom Properties on client systems.

Task

1. Select **Menu** → **Client Tasks** → **Client Task Catalog**.

   Note

   For McAfee ePO 5.9 or earlier and McAfee ePO Cloud, select **Menu** → **Policy** → **Client Task Catalog**.

2. From the **Client Task Types** list, select **McAfee Agent** → **Custom Properties**.
3. Click **New Task**, select **Custom Properties** as task type, then click **OK**.
4. Type a name and description for the task.
5. In **Custom Properties**, configure these fields as needed:
   - **Set Values** — Enable or disable setting custom property value through a task.
     - **Overwrite client system values**:
       - If enabled, a new value overwrites the existing value regardless of the value set on the client system.
       - If disabled and property is empty on the client system, a new value is set.
     - **Value** — A new value that needs to be set on the client system.
   - **Grant one-time edit permission** — Enable or disable McAfee ePO administrator to grant one-time edit permission through a task.
     - **One-time edit permission** — Grant one-time permission for system administrators to edit a particular custom property on the client system.
6. Click **Save**.

Working with the agent from McAfee ePO

How agent-server communication works

McAfee Agent communicates with McAfee ePO periodically to send events and make sure that all client system settings are up to date.

These communications are referred as agent-server communication. During each agent-server communication, McAfee Agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to McAfee Agent, and the repository list if it has changed since the last agent-server communication. McAfee Agent enforces the new policies locally on the managed system and applies any task or repository changes.

Note

Repository is not available on McAfee ePO Cloud.

McAfee ePO uses an industry-standard Transport Layer Security (TLS) network protocol for secure network transmissions.

When McAfee Agent is first installed, it calls into the server in 45 seconds. After, McAfee Agent calls in when one of the following occurs:

- The agent-server communication interval (ASCI) elapses.

  Note

  After upgrading McAfee Agent extension on MVISION ePO, the minimum ASCI value changes to 60 minutes for existing customer policies if its earlier ASCI value is less than 60 minutes. For more information, see KB94254. There is no change in the minimum ASCI value for the On-premise ePO.

- Wake-up calls are sent from McAfee ePO or Agent Handlers.
- A scheduled wake-up task runs on the client systems.
- Communication is initiated manually from the managed system (using the **Agent Status** monitor or command line).
- A "Run Immediately" client task runs on the client systems.

Note

For details about how to troubleshoot agent-server communication failures in McAfee Agent 5.x.x, see KB90603.

The agent-server communication interval

The **agent-server communication interval** (ASCI) determines how often the agent calls into McAfee ePO.

The ASCI is set on the **General** tab of the McAfee Agent policy page. The default setting of 60 minutes means that McAfee Agent contacts McAfee ePO once every hour. When deciding whether to change the interval, consider that McAfee Agent performs each of the following actions at each ASCI:

- Collects and sends its properties.
- Sends non-priority events that have occurred since the last agent-server communication.
- Receives new policies and tasks. This action might trigger other resource-consuming action based on tasks, and or schedules received.
- Enforces policies.

Although these activities do not overload any one computer, several factors can cause the cumulative demand on the network, McAfee ePO, or **Agent Handlers** to be significant, including:

Note

Agent Handlers are not available on McAfee ePO Cloud.

- Number of systems managed by McAfee ePO
- If your organization has stringent threat response requirements
- If the network or physical location of clients in relation to servers or **Agent Handlers** is highly distributed
- If there is inadequate available bandwidth

In general, if your environment includes these variables, you want to perform agent-server communications less often. For individual clients with critical functions, you might want to set a more frequent interval.

Handling interruptions in agent-server communication

When a client system can't connect with McAfee ePO, you must resolve the issue to re-establish communication.

Communication interruptions can happen for many of reasons, and the agent-server connection algorithm is designed to reattempt communication if its first attempt fails.

McAfee Agent tries to establish connection using one of these methods. If all these methods fail, McAfee Agent tries to connect again during the next ASCI.

- IP address
- Fully qualified domain name
- NetBIOS name
- Relay
- Proxy

Wake-up calls and tasks

A wake-up call triggers an immediate agent-server communication rather than waiting for the current interval to elapse.

Note

Use **System Tree** actions to wake up McAfee Agent.

There are two ways to issue a wake-up call:

- **Manually from the server** — The most common approach and requires an open wake-up communication port.
- **On a schedule set by the administrator** — Useful when a policy requires manual agent-server communication. The administrator can create and deploy a wake-up task, which wakes up McAfee Agent and initiates agent-server communication.

Some reasons for issuing a wake-up call are:

- You make a policy change that you want to enforce immediately, without waiting for the scheduled ASCI.
- (McAfee ePO On-Premises) You created a task that you want to run immediately. The **Run Task Now** option creates a task, then assigns it to specified client systems and sends wake-up calls.
- A query generated a report indicating that a client is out of compliance, and you want to test its status as part of a troubleshooting procedure.

(McAfee ePO On-Premises) If you converted a particular McAfee Agent to a **SuperAgent**, it can issue wake-up calls to designated network broadcast segments. **SuperAgent** distributes the bandwidth impact of the wake-up call.

Send manual wake-up calls to individual systems

Manually send a wake-up call to managed systems when you make policy changes and want to enforce them before the next agent-server communication.

Task

1. Select **Menu** → **Systems** → **System Tree**, then select the group that contains the target systems.
2. Select the systems from the list, then click **Actions** → **Agent** → **Wake Up Agents**.
3. Make sure the systems you selected appear in the **Target Systems** section.
4. (McAfee ePO On-Premises) Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call** as appropriate.
5. Accept the default **Randomization** (0 minutes) or type a different value (0–60 minutes). Consider the number of systems that are receiving the wake-up call when it is sent immediately, and how much bandwidth is available. If you type `0`, agents respond immediately.
6. To send incremental product properties as a result of this wake-up call, deselect **Retrieve all properties...**. The default is to send full product properties.
7. To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.
8. Enter the **Number of attempts**, **Retry interval**, and **Cancel after** settings for this wake-up call if you do not want the default values.

9. (McAfee ePO On-Premises) Select whether to wake up agent using **All Agent Handlers**, **Last Connected Agent Handlers**, or **Selected Agent Handler**.
10. Click **OK** to send a wake-up call.

Send manual wake-up calls to a group (McAfee ePO On-Premises)

Manually send a wake-up call to an entire group of managed systems when you make policy changes and want to enforce them before the next agent-server communication.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. Select the target group from the **System Tree** and click the **Group Details** tab.
3. Click **Actions** → **Wake Up Agents**.
4. Make sure that the selected group appears next to **Target group**.
5. Select whether to send the wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.
6. Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call**.
7. Accept the default **Randomization** (0 minutes), or type a different value (0–60 minutes). If you type `0`, agents awaken immediately.
8. To send minimal product properties as a result of this wake-up call, deselect **Retrieve all properties...**. The default is to send full product properties.
9. To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.
10. Click **OK** to send a wake-up call.

How SuperAgents work (McAfee ePO On-Premises)

A SuperAgent is a distributed repository which is designed to reduce the load on McAfee ePO. McAfee ePO manages how the SuperAgent is replicated.

The SuperAgent caches information received from McAfee ePO, the **Master Repository**, an HTTP, or an FTP repository, and distributes it to the agents in its broadcast domain. Configure a **SuperAgent** in every broadcast domain when managing agents in larger networks.

The Lazy Caching feature allows the SuperAgent to retrieve data from McAfee ePO only when requested by a local agent system. Creating a hierarchy of SuperAgents with lazy caching further saves bandwidth and minimizes the load on McAfee ePO.

A SuperAgent also broadcasts wake-up calls to other agents on the same network subnet. The **SuperAgent** receives a wake-up call from McAfee ePO, then wakes up the agents in its subnet.

Note

This broadcast is an alternative to sending ordinary wake-up calls to each agent in the network or sending agent wake-up task to each computer.

SuperAgent wake-up calls

SuperAgent contacts all agents in the same subnet using the **SuperAgent** wake-up call.

SuperAgent distributes the bandwidth load of concurrent wake-up calls. Instead of sending wake-up calls from the server to every McAfee Agent, the server sends the **SuperAgent** wake-up call to **SuperAgents** in the selected System Tree segment.

The process is:

1. Server sends a wake-up call to all **SuperAgents**.
2. **SuperAgents** broadcast a wake-up call to McAfee Agent in the same broadcast domain.
3. All notified McAfee Agent (McAfee Agent notified by a **SuperAgent** and all **SuperAgents**) exchange data with McAfee ePO or Agent Handler.

When you send a **SuperAgent** wake-up call, McAfee Agent without an operating **SuperAgent** on their broadcast domain are not prompted to communicate with the server.

SuperAgent deployment tips

To deploy enough **SuperAgents** to the appropriate locations, first determine the broadcast domains in your environment and select a system (preferably a server) in each domain to host a **SuperAgent**. If you use **SuperAgents**, make sure that every McAfee Agent is assigned a **SuperAgent**.

McAfee Agent and **SuperAgent** wake-up calls use the same secure channels. Make sure that the following ports are not blocked by a firewall on the client:

- McAfee Agent wake-up communication port (8081 by default).
- McAfee Agent broadcast communication port (8083 by default).

Convert McAfee Agent to SuperAgent

Configure **SuperAgent** policy settings to convert McAfee Agent to **SuperAgent**.

Task

1. Select **Menu** → **Systems** → **System Tree** → **Systems** tab, then select the required group under **System Tree**.
   All systems in this group appear in the details pane
2. Select the required system, then click **Actions** → **Agent** → **Edit Policies on a Single System**.
   The **Policy Assignment** page for that system appears.

3. From the **Product** drop-down list, select **McAfee Agent**.
   The policy categories are listed with the system's assigned policies.
4. Click **Edit Assignment** under **Actions** corresponding to the **General** policy category.
5. Next to the **Inherit from** option, select **Break inheritance and assign the policy and settings below** to inherit the policies from.
6. From the **Assigned policy** drop-down list, select **My Default** policies, then click **Edit Policy**.

   Note

   You can also create a policy by clicking **New policy**.

7. On the **SuperAgent** tab, next to **Repository options**, enable **Convert agents to SuperAgents** to allow broadcasting of wake-up calls.
8. Click **Save**.
9. Send a wake-up call.

SuperAgent caching and communication interruptions

The **SuperAgent** caches the contents of its repository in a way that minimizes the load on McAfee ePO.

If an agent has been converted to a **SuperAgent**, it can cache content from McAfee ePO, the distributed repository, or other **SuperAgent** to distribute locally to other agents, reducing load on McAfee ePO.

Note

SuperAgent caching with repository replication is not recommended. The **SuperAgent** can't cache content from McAfee HTTP or FTP repositories.

How LazyCaching works

The **LazyCaching** feature allows the **SuperAgent** to retrieve data from the configured repositories only when requested by a local agent. When a client system first requests content, the **SuperAgent** assigned to that system downloads the requested content from its configured repositories and caches that content. The cache is updated when a newer version of the requested package is available in the **Master Repository**. Creating a hierarchy of **SuperAgents** with **LazyCaching** further saves bandwidth and minimizes the load on McAfee ePO. When a hierarchical structure of **SuperAgent** is created, the child **SuperAgent** receives the requested content update from its parent's cache.

The **SuperAgent** is guaranteed only to store content required by the agents assigned to it because it does not pull any content from the repositories until requested from a client. This minimizes traffic between the **SuperAgent** and the repositories. While the **SuperAgent** is retrieving content from the repository, client system requests for that content are paused.

To enable LazyCaching, go to **Menu** → **Policy** → **Policy Catalog** → **McAfee Agent** → **General** → **SuperAgent**, then select **Enable LazyCaching**.

Important

The **SuperAgent** must have access to the repository. Without this access, agents receiving updates from the **SuperAgent** never receive new content. Make sure that your **SuperAgent** policy includes access to the repository.

Agents configured to use the **SuperAgent** as their repository receive the content cached in the **SuperAgent** instead of directly from McAfee ePO. This improves agent system performance by keeping most network traffic local to the **SuperAgent** and its clients.

If the **SuperAgent** is reconfigured to use a new repository, the cache is updated to reflect the new repository.

How communication interruptions are handled

When a **SuperAgent** receives a request for content that might be outdated, the **SuperAgent** tries to contact McAfee ePO to see if new content is available. If the connection tries time out, the **SuperAgent** distributes content from its own repository instead. This content transfer is done to make sure that the requester receives content even if that content might be outdated.

Important

Do not use **SuperAgent** caching with global updating. These features serve the same function in your managed environment, keeping your distributed repositories up to date. But, they are not complementary features. Use **SuperAgent** caching when limiting bandwidth usage is your primary consideration. Use **Global Updating** when quick enterprise updating is your primary consideration. See McAfee ePO product documentation for more details about **Global Updating**. **SuperAgent** caching with repository replication is not recommended.

Set flush interval for LazyCaching

Configure a flush interval on the **SuperAgent** policy page to remove content from the **SuperAgent** memory if the content is outdated.

The next time the **SuperAgent** receives a content request after the flush interval, it downloads the requested file hash. If there is a mismatch in the file hash, the outdated content is removed and the latest files are retrieved and served to the agent.

Task

1. Select **Menu** → **Systems** → **System Tree** → **Systems** tab, then select the required group under **System Tree**.
   All systems in this group appear in the details pane.
2. Select the required system, then click **Actions** → **Agent** → **Edit Policies on a Single System**.
   The **Policy Assignment** page for that system appears.
3. From the **Product** drop-down list, select **McAfee Agent**.
   The policy categories are listed with the system's assigned policies.
4. Click **Edit Assignment** under **Actions** corresponding to the **General** policy category.
5. Next to the **Inherit from** option, select **Break inheritance and assign the policy and settings below** to inherit the policies from.

6. From the **Assigned policy** drop-down list, select **My Default** policies, then click **Edit Policy**.

   Note

   You can also create a policy by clicking **New policy**.

7. On the **SuperAgent** tab, next to **Repository options**, enable these options:
   - **Convert agents to SuperAgents**
   - **Use systems running SuperAgents as distributed repositories**
8. Enter valid repository path and enable **Enable LazyCaching**.

   Note

   Make sure that one or more repositories are enabled.

9. Enter the flush interval.
   You can set the flush interval between 0–300 minutes.
10. Click **Save**.
11. Send a wake-up call.

Set purge interval for LazyCaching

Configure the interval for the **SuperAgent** to purge cache content that is no longer in use.

The cache content is downloaded when a client system requests for an update. The previous content update files might still be available in the local disk, but might not be listed in the Replica.log file. If a file is not listed, it is purged. By default the cache content is purged every day.

Note

The Replica.log file contains information about files and folder in its respective directory. Every directory in the repository contains a Replica.log file.

Task

1. Select **Menu** → **Systems** → **System Tree** → **Systems** tab, then select the required group under **System Tree**.
   All systems in this group appear in the details pane.
2. Select the required system, then click **Actions** → **Agent** → **Edit Policies on a Single System**.
   The **Policy Assignment** page for that system appears.
3. From the **Product** drop-down list, select **McAfee Agent**.
   The policy categories are listed with the system's assigned policies.
4. Click **Edit Assignment** under **Actions** corresponding to the **General** policy category.

5. Next to **Inherit from** option, select **Break inheritance and assign the policy and settings below** to inherit the policies from.
6. From the **Assigned policy** drop-down list, select **My Default** policies, then click **Edit Policy**.

   Note

   You can also create a policy by clicking **New policy**.

7. On the **SuperAgent** tab, next to **Repository options**, enable these options:
   - **Convert agents to SuperAgents**
   - **Use systems running SuperAgents as distributed repositories**
8. Enter the valid repository path then enable **Enable LazyCaching**.

   Note

   Make sure that one or more repositories are enabled.

9. Enter the maximum disk quota in GB.
10. Enter the purge interval in days.
11. Click **Save**.
12. Send a wake-up call.

Best practices for using SuperAgent

Traffic between locations can be reduced by ensuring best practices when enabling **SuperAgent** in your network.

- Enable **SuperAgent** servers on PCs or virtual systems. Don't enable a **SuperAgent** server on laptops or other mobile devices.
- Avoid setting up **SuperAgent** servers on systems with poor network connectivity or are connected using VPN.
- Set up at least one **SuperAgent** per subnet to reduce the network load. Each **SuperAgent** can handle 1024 requests concurrently.
- If you set up **SuperAgent Hierarchical Update**, make sure that your hierarchy of **SuperAgents** is no more than three levels.
- Configure the **Max. disk quota** to be greater than the disk space requirement for all commonly used applications and their updates.

  For example, if the DAT file size is 150 MB and the average product update size is 100 MB, the purging disk quota should be more than 250 MB.

SuperAgent hierarchy

A hierarchy of **SuperAgents** can serve agents in the same network with minimum network traffic utilization.

A **SuperAgent** caches the content updates from McAfee ePO or distributed repository and distributes it to the agents in the network, reducing the load on McAfee ePO. It is always ideal to have more than one **SuperAgent** to balance the network load.

Note

Make sure that you enable **Lazy caching** before you set the **SuperAgent** hierarchy.

Creating a hierarchy of SuperAgents

Use the **Repository** policy to create the hierarchy. We recommend that you create a three level hierarchy of **SuperAgents** in your network.

Creating a hierarchy of **SuperAgents** avoids repetitive download of the content update from McAfee ePO or distributed repository. For example, in a client network with multiple **SuperAgents** (**SuperAgent** 1, **SuperAgent** 2, **SuperAgent** 3, and **SuperAgent** 4) and a distributed repository, configure the hierarchy so that the client systems receive the content updates from their respective **SuperAgents** (**SuperAgent** 2, **SuperAgent** 3, or **SuperAgent** 4). The **SuperAgent** 2, 3, and 4 receive and cache updates from **SuperAgent** 1, and the **SuperAgent** 1 receives and caches updates from the distributed repository.

In the previous example, **SuperAgent** 2, **SuperAgent** 3, and **SuperAgent** 4 are configured as **SuperAgents** for the client systems in their respective broadcast domain.

Note

The **SuperAgents** can't cache content from McAfee ePO HTTP or FTP repositories.

When creating a hierarchy, make sure that the hierarchy doesn't form a cycle of **SuperAgent**; for example **SuperAgent** 1 is configured to pull updates from **SuperAgent** 2, **SuperAgent** 2 is configured to pull updates from **SuperAgent** 3, and **SuperAgent** 3 in turn is configured to pull updates from **SuperAgent** 1.

To make sure that the parent **SuperAgent** is up to date with the latest content update, **SuperAgent** wake-up calls broadcast must be enabled.

Note

If the **SuperAgents** don’t serve agents with latest content update, agent falls back to the next repository configured in the policy.

Arrange SuperAgents in a hierarchy

Creating a hierarchy of **SuperAgents** with lazy caching further saves bandwidth and minimizes the wide-area network traffic.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **General**.

   Note

   For McAfee ePO 5.9 or earlier, select **McAfee Agent** in the **Product** drop-down list and **General** in the **Category** drop-down list.

3. Click the **My Default** policy to start editing the policy. To create a policy, click **New Policy**.

   Note

   The **McAfee Default** policy can't be changed.

4. On the **SuperAgent** tab, select **Convert agents to SuperAgents** to convert the agent to a **SuperAgent** and update its repository with latest content.
5. Select **Use systems running SuperAgents as distributed repository** to use the systems that host **SuperAgents** as update repositories for the systems in its broadcast segment. Then, provide the **Repository Path**.
6. Select **Enable Lazy caching** to allow **SuperAgents** to cache content when it is received from McAfee ePO.
7. Click **Save**.
   The **Policy Catalog** page lists the **General** policies.
8. Change the **Category** to **Repository**, then click the **My Default** policy to start editing the policy. If you want to create policy, click **New Policy**.
9. On the **Repositories** tab, select **Use order in repository list**.
10. Click **Automatically allow clients to access newly-added repositories** to add new **SuperAgent** repositories to the list. Then, click **Move to Top** to arrange the **SuperAgents** in a hierarchy.

    Note

    Arrange the hierarchy of the repositories so that the parent **SuperAgent** is always at the top of the repository list.

11. Click **Save**.
    After setting the **SuperAgent** hierarchy, you can create and run the **McAfee Agent Statistics** task to collect a report of network bandwidth saving.

Communicating through a RelayServer

Enabling relay capability in your network converts a McAfee Agent to a **RelayServer**. A McAfee Agent with relay capability can access McAfee ePO, Agent Handler, or the distributed repository listed in `Sitelist.xml`.

A McAfee Agent discovers each **RelayServer** in the network at every agent-server communication, and caches details for the first five unique servers to respond. If the connection fails or the required content update isn't available, McAfee Agent connects to the first **RelayServer** in its cached list.

Relay capability can be enabled on McAfee Agent that does not have direct connectivity to McAfee ePO or **Agent Handler** to bridge communication between the client systems and McAfee ePO. You can configure more than one McAfee Agent as a **RelayServer** to maintain network load balance.

Note

Agent Handler is not available on McAfee ePO Cloud.

When a McAfee Agent uses relay to communicate with McAfee ePO, the connections are established in two parts; first between McAfee Agent and the **RelayServer**, and second between the **RelayServer** and McAfee ePO. These connections are maintained during the communication.

Enable relay capability

Configure and assign policies on an agent to convert it to a RelayServer.

Note

If enabling a non-Windows system as a **RelayServer**, make sure that you manually add an exception for the `macmnsvc`, `masvc`, `macompatsvc`, and `Mue_InUse` processes and the service manager port to the `iptables` and `ip6tables`.

Task

1. Select **Menu** → **Systems** → **System Tree** → **Systems** tab, then select the required group under **System Tree**.
   All systems in this group appear in the details pane.
2. Select the required system, then click **Actions** → **Agent** → **Edit Policies on a Single System**.
   The **Policy Assignment** page for that system appears.
3. From the **Product** drop-down list, select **McAfee Agent**.
   The policy categories are listed with the system's assigned policies.
4. Click **Edit Assignment** under **Actions** corresponding to the **General** policy category.
5. Next to the **Inherit from** option, select **Break inheritance and assign the policy and settings below** to inherit the policies from.
6. From the **Assigned policy** drop-down list, select **My Default** policies, then click **Edit Policy**.

   Note

   You can also create a policy by clicking **New policy**.

7. On the **SuperAgent** tab, select these **Relay Client options** as appropriate:

- Select **Enable Relay Communication** to allow agents to discover RelayServers in the network.
- Select **Disable Discovery** to disable UDP broadcast (discovery) in the client network to detect RelayServer.
  - Specify the RelayServer IP address or Host name and Port number through which the agent communicates with McAfee ePO in the network.

8. Select these **ReleayServer options** as appropriate:
   - Select **Enable RelayServer** to enable relay capability on an agent.
     - Configure the **Service Manager port** to **8083**

     Note

     Enable relay capability in the organization's network. A **RelayServer** can't connect to McAfee ePO using proxy settings.

   Note

   To disable the relay capability on McAfee Agent, deselect **Enable Relay Communication** and **Enable RelayServer** respectively.

9. Click **Save**.
10. Send a wake-up call.

Results

After the first ASCI, the status of the **RelayServer** is updated in the **McAfee Agent Properties** page or the McTray UI on the client system.
The log file `macmnsvc_<hostname>.log` is saved in these locations:

- On a Windows client system — `<ProgramData>\McAfee\Agent\Logs`
- On a non-Windows client system — `/var/McAfee/agent/logs`

Peer-to-peer communication

Downloading content updates from peer agents

Downloading updates and installation files from peers (agents in the same broadcast domain) reduces the load on McAfee ePO.

A McAfee Agent can be configured as a peer-to-peer server or client as needed. Configuring a McAfee Agent as a peer-to-peer server enables it to provide updates to others in the broadcast domain when requested. A peer-to-peer server has local disk space allocated to cache updates. By default, the peer-to-peer server caches 512 MB of updates at `<agent data folder>\data \mcafeeP2P`, but the cache size and location can be customized. You can also configure the policy to purge updates cached in the local disk.

When an agent requires a content update, it tries to discover peer-to-peer servers with the content update in its broadcast domain. On receiving the request, the agents configured as peer-to-peer servers check if they have the requested content and respond back to the agent. The agent requesting the content downloads it from the peer-to-peer server that responds first.

Note

Enable the policy option **Enable Peer-to-Peer Communication** to allow the client system to discover peer-to-peer servers in the broadcast domain.

The peer-to-peer server uses HTTP to serve content to clients.

If a McAfee Agent can't discover a peer-to-peer server or the content update among its peers in the broadcast domain, it falls back to the repository, as configured in the policy.

Peer-to-peer communication uses port 8082 to discover peer servers and port 8081 to serve peer agents with updates.

Peer-to-peer server purges the content based on the disk quota and purge interval configuration.

Best practices for using peer-to-peer communication

Traffic between locations can be reduced by following best practices when enabling peer-to-peer communication in your network.

- We recommend that you enable peer-to-peer servers on PCs or virtual systems. Enabling peer-to-peer server on laptops or other mobile devices is not recommended.
- We recommend that you disable peer-to-peer servers on the systems that have poor network connectivity or are connected using VPN.
- When deploying McAfee Agent or managed products, or updating the products on large number of systems, we recommend that you enable peer-to-peer client on all systems. This limits the network traffic in the local subnet during the deployment or update.
- Peer-to-peer communication is enabled by default. If your organization restricts peer-to-peer communication, disable the peer-to-peer policy.
- We recommend that you configure the **Max disk quota** always greater than the size of sum of commonly used application and updates (For example, if the DAT file size is 150 MB and the average product update size is 100 MB, the peer-to-peer disk quota should be more than 250 MB).

Enable peer-to-peer service

To reduce the load on McAfee ePO, enable peer-to-peer service in your broadcast domain.

Note

Peer-to-peer service is enabled by default in **McAfee Default** and **My Default** policies.

Task

1. Select **Menu** → **Systems** → **System Tree** → **Systems** tab, then select the required group under **System Tree**.
   All systems in this group appear in the details pane.
2. Select the required system, then click **Actions** → **Agent** → **Edit Policies on a Single System**.
   The **Policy Assignment** page for that system appears.
3. From the **Product** drop-down list, select **McAfee Agent**.
   The policy categories are listed with the system's assigned policies.
4. Click **Edit Assignment** under **Actions** corresponding to the **General** policy category.
5. Next to the **Inherit from** option, select **Break inheritance and assign the policy and settings below** to inherit the policies from.
6. From the **Assigned policy** drop-down list, select **My Default** policies, then click **Edit Policy**.

   Note

   You can also create a policy by clicking **New policy**.

7. On the **Peer-to-Peer** tab, select these options as appropriate:
   - Select **Enable Peer-to-Peer Communication** to allow McAfee Agent to discover and use peer-to-peer servers in the network.
   - Select **Enable Peer-to-Peer Serving** to enable McAfee Agent to serve content to peer agents.
8. Click **Save**.
9. Send a wake-up call.

Collect McAfee Agent statistics

Run the **McAfee Agent Statistics** client task on the managed systems to collect the statistics.

Collect **RelayServer** statistics and network bandwidth saved by **Peer-to-Peer** communication and **SuperAgent** hierarchy.

Note

SuperAgent hierarchy is not available on McAfee ePO Cloud.

Task

1. Select **Menu** → **Systems** → **System Tree** → **Systems**, then select a group under the **System Tree**.
   The details pane lists all systems in the group.
2. Select a system, then click **Actions** → **Agent** → **Edit Tasks on a Single System** to display the system's client tasks.
3. Click **Actions** → **New Client Task Assignment**.
4. From the product list, select **McAfee Agent**, then select **McAfee Agent Statistics** as the **Task Type**.

5. Click **Create New task**.
6. Select the required option, then click **Save**.

Note

Once the task is deployed on the client system and the status is reported to McAfee ePO, the statistics are reset to 0.

Results

To see the statistics collected by McAfee Agent, create and run a new **Agent Statistics Information** query.

Change the language for the agent interface and event log

Force the agent on a target system to run and publish log entries in the selected language.

You can change the agent user interface and logging language on a managed system with a McAfee ePO policy. This setting forces the agent on the target system to run and publish log entries in the selected language.

Note

Individual McAfee security software products control some text. This text might follow regional or locale settings.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. From **Products**, select **McAfee Agent** → **Troubleshooting**.

Note

For McAfee ePO 5.9 or earlier and McAfee ePO Cloud, select **McAfee Agent** in the **Product** drop-down list and **Troubleshooting** in the **Category** drop-down list.

3. Click the name of a policy to change, or duplicate an existing policy.
   The **McAfee Default** policy can't be changed.
4. Select **Select language used by agent: (Windows, Mac OSX and EWS agents only)** and select a language from the drop-down list.
5. Click **Save**.

Results

When you assign this policy to a system, the agent on that system runs and publishes log messages in the selected language. If this language does not match the active windows system locale, the log messages appearing in the **Agent Monitor** user interface might not be legible.

Note

Regardless of language selection, some log messages are always published in English to aid McAfee in troubleshooting customer issues.

Configure selected systems for updating (McAfee ePO On-Premises)

Choose a set of packages that are updated immediately when **Update Now** is selected on one or more managed systems.

Typical reasons for using this functionality include:

- Updating selected systems when troubleshooting
- Distributing new DATs or signatures to many systems, or all systems, immediately
- Updating selected products, patches, or service packs that have been deployed previously

Task

1. Select **Menu** → **Systems** → **System Tree**, then select the systems to be updated.
2. Click **Actions** → **Agent** → **Update Now**.
   - Select **All packages** to deploy all update packages in the repository.
   - Select **Selected packages** to specify which update packages to deploy. Deselect the packages that you do not want to deploy.

   Note

   Deploying patches and service packs from the **Evaluation** or **Previous** repositories is designed to allow update testing on a limited subset of systems before a broader deployment. We recommend moving approved patches and service packs to the **Current** repository when they are ready for general deployment.
3. Click **OK.**

Respond to policy events

Set up an automatic response in McAfee ePO that is filtered to see only policy events.

Task

1. Select **Menu** → **Automation** → **Automatic Responses** to open the **Automatic Responses** page.
2. Click **New Response**.
3. Enter a **Name** for the response, and an optional **Description**.
4. Select **ePO Notification Events** for the **Event group**, and **Client**, **Threat**, or **Server** for the **Event type**.
5. Click **Enabled** to enable the response, then click **Next**.
6. From **Available Properties**, select **Event Description**.
7. Click **...** in the **Event Description** row and choose an option:
    - **Agent failed to collect properties for any point products** — This event is generated and forwarded when a property collection failure first occurs. A subsequent success event is not generated. Each failing managed product generates a separate event.
    - **Agent failed to enforce policy for any point products** — This event is generated and forwarded when a policy enforcement failure first occurs. A subsequent success event is not generated. Each failing managed product generates a separate event.
8. Enter remaining information into the filter as needed, then click **Next**.
9. Select **Aggregation**, **Grouping**, and **Throttling** options as needed.
10. Choose an action type and enter a behavior depending on the action type, then click **Next**.
11. Review the summarized response behavior. If correct, click **Save**.

Results

The automatic response performs the described action when a policy event occurs.

Scheduling client tasks

When assigning a client task to systems in the **System Tree**, you can schedule them to run based on various intervals such as Daily, Weekly, and Monthly.

On the **Client Task Assignment Builder** page, configure whether a task runs on a schedule.

If you disable scheduling, you must run the task from the **System Tree** → **Systems** page by clicking **Actions** → **Agent** → **Run Client Task Now**.

Note

Run Client Task Now is not available on McAfee ePO Cloud.

Client tasks can be scheduled to run at these intervals:

- **Daily** — Specifies that the task runs every day at a specific time, on a recurring basis between two times of the day, or a combination of both.
- **Weekly** — Specifies that the task runs on a weekly basis. Such a task can be scheduled to run on a specific weekday, all weekdays, weekends, or a combination of days. You can schedule a task to run at a specific time on the selected days, or on a recurring basis between two times on the selected days.
- **Monthly** — Specifies that the task runs on a monthly basis. Such a task can be scheduled to run on one or more specific days or weekdays of each month at a specific time.
- **Once** — Starts the task on the time and date you specify.
- **At System Startup** — Starts the task the next time you start the client.
- **At logon** — Starts the task the next time you log on to the client.
- **Run immediately** — Starts the task immediately.

Note

After the task is run for the first time, it will not run again.

Also you can:

- Configure the start and end dates when the client task is available or unavailable to run at the scheduled intervals.
- Specify the time when the task begins.
- Specify whether to run the task only once at the Start time, or to continue running until a later time. You can also specify the interval when the task runs during this interval.
- Specify whether the task runs at the local time on the managed system or Coordinated Universal Time (UTC).
- Configure task behavior and what happens if the task runs too long, or whether the task runs if it was missed.
- Specify whether to run the task randomly in a specific interval.

Run client tasks immediately (McAfee ePO On-Premises)

When McAfee ePO communicates with McAfee Agent, you can run client tasks before the next agent-server communication using the **Run Client Task Now** action.

Such client tasks reach the agent using the Datachannel communication. This allows agent to run these client tasks immediately.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. Select one or more systems where you want to run a task.
3. Click **Actions** → **Agent** → **Run Client Task Now**.
4. Select the **Product** as **McAfee Agent** and the **Task Type**.
5. To run an existing task, click the **Task Name** then click **Run Task Now**.
6. To define a new task, click **Create New Task**.
    a. Enter the information appropriate to the task you are creating.

Results

The **Running Client Task Status** page appears, and displays the state of all running tasks. When the tasks are complete, the results can be viewed in the **Server Task Log**.

Locate inactive agents

An inactive McAfee Agent is one that has not communicated with McAfee ePO in a user-specified time period.

It's possible for agents to become disabled, or for users to uninstall them. In other cases, the system hosting McAfee Agent might have been removed from the network. We recommend performing regular weekly searches for systems with these inactive agents.

Task

1. Select **Menu** → **Reporting** → **Queries & Reports**.
2. In the **Groups** list, select **McAfee Groups**, then select **Agent Management** group.
3. Click **Run** in the **Inactive Agents** row to run the query.
   The default configuration for this query finds systems that have not communicated with McAfee ePO in the last 30 days.

Results

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication.

Note

(McAfee ePO On-Premises) The query results allow you to take actions on the systems identified, including ping, delete, wake up, and redeploy McAfee Agent.

Viewing clients pending for reboot

McAfee ePO administrators can identify the client systems that are pending for reboot using the **Product Reboot Pending** dashboard on the McAfee ePO console.

Note

This dashboard is not available on McAfee MVISION ePO.

McAfee ePO administrators can restart the client systems that require a reboot before scheduling the installation or upgrade deployment tasks for the point products to avoid the possible unknown installation or upgrade failures. Reboot is detected only

for the McAfee point products and Windows update that requires a reboot. The Reboot Pending status from a client system is sent as part of system properties, which gets updated during the next scheduled ASCI and on a manual property collection.

Task

1. Select **Menu** → **Dashboards**.
2. Select **Product Reboot Pending** from **McAfee Dashboards** pop down list.
   The Product Reboot Pending dashboard is displayed. The color indicator can be one of the following:
   - Red - The system require a reboot.
   - Green - The reboot process is complete.

Identifying duplicate agent GUIDs (McAfee ePO On-Premises)

When client systems with duplicate GUIDs attempt to communicate with an Agent Handler, they generate sequencing errors, which indicate a GUID problem. The **Managed Systems** query result type tracks this information about the sequence errors.

- The number of sequence errors for each system in the **Managed Systems Sequence Errors** property.
- The date and time of the last sequence error in the **Managed Systems Last Sequence Error** property.

The tracked information is incorporated into one of the available predefined queries:

- **Systems with High Sequence Errors**
- **Systems with no Recent Sequence Errors**

Two predefined tasks help manage GUID problems.

- **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs**

  This task deletes the systems that have many sequencing errors and classifies the agent GUID as problematic. As a result, the agent is forced to generate a new GUID. The threshold number of sequencing errors is set in the query **Systems with High Sequence Errors**.

- **Duplicate Agent GUID - Clear error count**

  Sequencing errors can occur occasionally for inconsequential reasons. This task clears the count of sequencing errors in systems that have not had any recent sequencing errors. This cleanup task does not remove any problematic GUIDs. The threshold value for defining recent is set in the query **Systems with no Recent Sequence Errors**.

Correct duplicate agent GUIDs (McAfee ePO On-Premises)

Agents with duplicate GUIDs can be automatically identified and removed with a server task.

You can schedule this task to run periodically, or run it immediately.

Task

1. Select **Menu** → **Automation** → **Server Tasks**, then edit the **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs** task.

   Note

   To run this task immediately, click **Run**. The **Server Task Log** page appears after running the task.

2. On the **Description** page, select **Enabled**.
   - To run the task with the default configuration, click **Save**.
   - To configure the **Actions** and **Schedule** tabs, click **Next**.
3. On the Actions page, select **Actions** → **Run Query**.
4. Select one of these queries from the **System Management** category, then click **OK**.
   - **System with high Sequence errors**
   - **Systems with no recent Sequence errors**
5. From the **Sub-Actions** drop-down list, select one of these, then click **Next**.
   - **Clear Agent GUID Sequence Error Count**
   - **Move Agent GUID to Duplicate List and Delete systems**
6. Set a schedule for running the task, then click **Next**.
7. Review your settings, then click **Save**.

Verify policy changes with system properties

When you make changes to a policy, make sure that the changes match the properties retrieved from a system.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. On the **Systems** tab, click the row corresponding to the system you want to examine.

Results

Information about the system's properties, installed products, and McAfee Agent appears. The top of the **System Information** page contains **Summary**, **Properties**, and **Threat Events** windows. It also displays **System Properties**, **Products**, **Threat Events**, and **McAfee Agent** tabs.

Changing the agent management modes

McAfee Agent operates in two modes, managed and unmanaged.

- Managed mode — McAfee Agent connects and communicates with McAfee ePO to manage McAfee product updates.
- (McAfee ePO On-Premises) Unmanaged mode — McAfee Agent doesn't connect or communicate with McAfee ePO, but pulls updates from McAfee HTTP or FTP servers.

How to change McAfee Agent management modes

McAfee Agent can be toggled between unmanaged mode and managed mode.

(McAfee ePO On-Premises) Some of the more recent McAfee products that use AutoUpdate, such as McAfee Endpoint Security, are installed with McAfee Agent in updater mode. To start managing these products with McAfee ePO, you can enable McAfee Agent that is already on the system by changing its management mode.

Changing the existing McAfee Agent on each system to managed mode saves significant network bandwidth over deploying McAfee Agent installation package. But, existing McAfee products were probably installed with an older version of McAfee Agent, which is *not* automatically upgraded to the latest version on McAfee ePO.

(McAfee ePO On-Premises) In some situations, you might want to change a system that is managed by McAfee ePO to updater (unmanaged) mode. Information is provided for changing from managed mode to unmanaged mode.

Before changing the McAfee Agent mode, consider the following:

- By default, `FrmInst.exe` is installed on client system in this location:
  - Windows (32-bit) – `C:\Program Files\McAfee\Agent`.
  - Windows (64-bit) – `C:\Program Files\McAfee\Agent\x86`.
- Do not change the McAfee Agent installation folder without removing and reinstalling McAfee Agent. The agent that you enable might be in a different folder than the agent that you deploy in your network by another method.
- Assigning sorting filters or domain names to specific **System Tree** segments saves time. Without such designations, systems are placed in **Lost & Found** and you must move them from that location.
- Export `agentfipsmode` file from this location with the mentioned files and rename the `reqseckey.bin` and `srpubkey.bin` to `req2048seckey.bin` and `sr2048pubkey.bin` respectively.
  - Windows (32-bit) – `C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3000\Install\0409\`
  - Windows (64-bit) – `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Software\Current \EPOAGENT3000\Install\0409\`

Change from unmanaged to managed mode on Windows systems

Change the agent from unmanaged mode to managed mode to connect and communicate with McAfee ePO.

On Windows systems, you have three methods to change the management mode of the agent:

Note

Only remote provisioning method is available on McAfee ePO Cloud to change the management mode of the agent.

- Use the installer package Framepkg

Send the installer file `Framepkg.exe` from McAfee ePO to the unmanaged system, then run it on the system from an administrator account.

- Locally provision with maconfig
  - Send `Sitelist.xml`, `srpubkey.bin`, `reqseckey.bin`, `req2048seckey.bin`, and `sr2048pubkey.bin` from McAfee ePO to the unmanaged system.
  - Run one of these on the target system (requires administrator rights).
    - Using `frminst`

32-bit Windows	`C:\Program Files\McAfee\Agent\frminst.exe /install=agent /siteinfo =<full path>\Sitelist.xml`
64-bit Windows	`C:\Program Files\McAfee\Agent\x86\frminst.exe /install=agent /siteinfo =<full path>\Sitelist.xml`

    - Locally provisioning using `maconfig`

```
maconfig.exe -provision -managed -dir "directory location where the sitelist.xml and security keys were exported"
```

- Remotely provision with maconfig

Run the following command on the target system.

```
maconfig.exe -provision -managed -auto -dir "temp location to copy keys"
 -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]
```

For example,

```
maconfig -provision -managed -auto -dir "C:\Windows\Temp"
 -epo ePOServerMachine [-user admin] [password password123]
```

Change from managed to unmanaged mode on Windows systems (McAfee ePO On-Premises)

Remove Windows systems from the **System Tree** to change them to unmanaged mode.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. Select the systems to change to unmanaged mode.
3. Click **Actions**, select **Directory Management**, then click **Delete.**
4. Select **Remove McAfee Agent on next agent-server communication** and confirm the deletion. The selected system is no longer managed by McAfee ePO and now functions only as an updater.

Results

This uninstalls McAfee Agent if no other managed products are installed on the system.

Change from unmanaged to managed mode on non-Windows platforms

You have two methods to change McAfee Agent mode on non-Windows systems. You can change the mode using local or remote provisioning using maconfig.

Before you begin

Perform the following:

1. Download and extract the McAfee Agent package (Example: MAxxxLNX.zip and MAxxxMAC.zip) to a temporary location.
2. Copy the DXL.zip and contrib.ini files to the /var/McAfee/agent/data/contrib folder.

Remote provisioning

- To change the mode using remote provisioning, run the following command:

```
maconfig  -provision -managed -auto -dir "temp location to copy keys" -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]
```

Local provisioning (McAfee ePO On-Premises)

- To change the mode using local provisioning, follow these steps:

- On the target system, locate the `maconfig` file in the binaries subfolder of the `ma` folder.

Linux	`/opt/McAfee/agent/bin`
Macintosh	`/Library/McAfee/agent/bin`

- Open a terminal window on the target system.
- Export `Sitelist.xml`, `srpubkey.bin`, `reqseckey.bin`, `req2048seckey.bin`, `sr2048pubkey.bin`, and `agentfipsmode` from McAfee ePO to a temporary location on the target system.
- Run the following command:

```
maconfig -provision -managed -dir "directory location where the sitelist.xml and security keys were exported"
```

Change from managed to unmanaged mode on non-Windows platforms (McAfee ePO On-Premises)

Changing McAfee Agent mode on non-Windows systems must be done manually.

Task

1. On the target system, locate the `maconfig` file in the binaries subfolder of the `ma` folder.

Linux	`/opt/McAfee/agent/bin`
Macintosh	`/Library/McAfee/agent/bin`

2. Open a terminal window on the target system.
3. Run the following command:

```
/opt/McAfee/agent/maconfig -provision -unmanaged -nostart
```

Note

The optional `-nostart` parameter indicates that McAfee Agent does not restart after changing mode.

Running agent tasks from the managed system

Using the system tray icon

The system tray icon provides a collection point for actions that can be performed on a client system. Every McAfee managed product provides actions and information to the system tray icon.

The system tray icon resides in the Windows system tray on the client system and provides an interface to products installed on that system.

Option	Function
Update Security	Triggers immediate updating of all installed McAfee software products. This includes application of updates and hotfixes, as well as DAT and signature updates. **Note:** This feature is available only if enabled in the agent policy.
(McAfee ePO On-Premises) **Quick Settings**	Links to certain product menu items that are frequently used.
(McAfee ePO On-Premises) **Manage Features**	Displays links to the administrative console of managed products.
(McAfee ePO On-Premises) **Scan Computer for**	Starts McAfee programs, such as VirusScan Enterprise, that scan systems on-demand and detect malware.
View Security Status	Displays the current system status of managed McAfee products, including current events.
McAfee Agent Status Monitor	Triggers the Agent Status Monitor, which: • Displays information about the collection and transmission of properties. • Sends events. • Enforces policies.

Option	Function
	• Checks for new policies and tasks.
About...	Displays system and product information, including the agent, McAfee ePO, or Agent Handler with which McAfee Agent communicates, product versions, and the software products being managed. Also displays if the system is managed or unmanaged. If it is a managed system, displays if these features are enabled. • (McAfee ePO On-Premises) SuperAgent • Peer-to-peer • Relay capability

Make the system tray icon visible and update security settings

Allow users to update security settings by making the system tray icon visible.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. On the **Assigned Policies** tab, select **McAfee Agent** in the **Product** drop-down list.
3. Click the name of a policy that is in the **General** category.
4. Select **Show the McAfee system tray icon (Windows only)**.

    • To allow users to update security on-demand, select **Allow end users to update security from the McAfee system tray menu**.

    When selected, users who are running McAfee Agent can update all products when an update package is present in the repository.

    • To allow users to enable McAfee system tray icon in a remote desktop session, select **Enable McAfee system tray icon in a remote desktop session**.
5. When you have completed your changes to the default configuration, click **Save**.

Updates from the managed system

Security updates from a Windows-managed system are possible, but the functionality is disabled by default to control when updates occur.

If you want to allow Windows users to update all McAfee products on their managed systems, you must enable this functionality. The icon can't be used to update applications selectively. The user can update all items in the repository, or none of them.

When the user selects **Update Security**, these items are updated with the contents of the designated repository:

- Patch releases
- Legacy product plug-in (.DLL) files
- Service Pack releases
- SuperDAT file (SDAT*.EXE) packages
- Supplemental DAT (Extra.DAT) files
- DAT files
- Antivirus engines
- Managed product signatures

McAfee Agent command-line options

Use the Command Agent tool to perform selected McAfee Agent tasks from the managed system.

Different Command Agent tools are available for Windows and non-Windows operating systems.

- Windows — cmdagent.exe
- Non-Windows — cmdagent

The Command Agent tool is installed on the managed system at the time of McAfee Agent installation. Perform this task locally on managed systems. It must be run from an Administrator command prompt.

The Command Agent tool file is located in the McAfee Agent installation folder. By default, this location is:

- Windows — <Program Files>\McAfee\Agent
- Linux — /opt/McAfee/Agent/bin
- Macintosh —/Library/McAfee/Agent/bin

Using multiple switches per command can start multiple concurrent agent-server communications and can cause policy errors. For example, `CmdAgent.exe /p`. Make sure you use only one switch per command. These switches are case sensitive. Switches on non-Windows systems use a **-** instead of **/**.

Command-line options

Parameter	Description
`/c`	Checks for new policies. McAfee Agent contacts McAfee ePO for new or updated policies, then enforces them immediately on receipt.
`/e`	Prompts McAfee Agent to enforce policies locally.

Parameter	Description
`/p`	Sends properties to McAfee ePO.
`/s`	Displays the McAfee Agent monitor on Windows client systems.
`/f`	Forwards events from client systems to McAfee ePO.
`/i`	McAfee Agent information.
`/h`	Lists all switches with their description.
`-l`	Set location of the log file.

You can use McAfee Agent Return Codes with installation and removal scripts to allow the script to continue to the next step or stop depending on the code returned. The two return codes are:

- **0** — Success
- **-1** — Failure

For a code -1, the parameter is invalid or it failed to open one of the global events for the framework service. Make sure that the service is running, the user has administrator rights, and you are using a valid command line.

Using the maconfig command-line tool (McAfee ePO On-Premises)

The command-line tool, maconfig, is provided with McAfee Agent for Linux.

It is installed with McAfee Agent and its default location is `/opt/McAfee/agent/bin`.

With `maconfig` you can perform operations such as:

- Provision agent to McAfee ePO
- Set custom properties
- Set log level
- Provision agent to MVISION ePO (applicable only for MLOS based nDLP appliances)

Command-line switches

Use these command-line switches with the `maconfig` tool to perform operations.

Parameter	Description
`-provision`	Provisions the agent in managed or unmanaged mode.
`-enforce`	Enforces the agent policies or configurations locally.
`-managed`	Provisions the agent in managed mode.
`-unmanaged`	Provisions the agent in unmanaged mode.
`-auto`	Uses McAfee ePO credentials.
`-dir`	Uses McAfee ePO files from a specific directory.
`-epo`	Specifies McAfee ePO IP address and port.
`-mvisionepoenv`	Provision to MVISION ePO using the configuration provided in *.ini* file (for example: "`/temp/config.ini`").
`-user`	Specifies McAfee ePO administrator's user name.
`-password`	Specifies McAfee ePO password.
`-custom`	Sets custom properties. You can set more than one custom property.
`-prop1 "string value" -prop2 "string value" ... -propN "string value"`	Value of custom property. Specify the value for each of your custom property.
`-license`	Sets license key.
`-loglevel`	Sets log level number(0(Disable)\1(Info)\2(Debug)\3(Detail)).
`-noguid`	Deletes GUID entries.
`-start`	Starts the agent.

Parameter	Description
`-stop`	Stops the agent.
`-help`	Displays Help for maconfig.

Examples

- **Provision the agent to McAfee ePO**

This command provisions a specified McAfee ePO to the local system that runs this command.

```
maconfig -provision -managed -auto -epo <ePO IP> -user <ePO admin username> -password <ePO admin password>
```

- **Set custom properties**

This command allows you to set custom properties that are reported back to McAfee ePO and are displayed in the system properties.

```
maconfig -custom -prop1 "string value1" -prop2 "string value2"
```

- **Set log level**

This command allows you to configure the level of agent activity that is recorded.

```
maconfig -enforce -loglevel 3
```

- **Provision the agent to MVISION ePO (applicable only for nDLP appliances)**

This command provisions agent to MVISION ePO. The tenant or an endpoint administrator logs into the endpoint device and runs `maconfig`. The `maconfig` uses the following parameters to obtain the agent configuration data. The `maconfig` initiates provisioning of agent after retrieving the configuration data.

Run the `maconfig -provision -managed -auto - mvisionepoenv <config file path>` command to provision agent.

For example, `maconfig -provision -managed -auto -mvisionepoenv /tmp/config.ini`

Where, `config.ini` contains the following parameters:

- `-srt : <srt_token>` You can obtain registration token from MVISION ePO. For more information about obtaining registration token, see *McAfee MVISION ePO Product Guide*.
- `-iam_url:`
- `-epo_url:`
- `-proxy_url:`
- `-proxy_port:`

- `-proxy_user:`
- `-proxy_password:`
- `-connection_timeout:` The default value is set to 30 seconds.
- `-transfer_timeout:` The default value is set to 300 seconds.
- `-epo_endpoint:` The default value is `frameworkconfig`.

Inputs to `srt`, `iam_url`, and `epo_url` are mandatory. The `proxy_url`, `proxy_port`, `epo_endpoint`, `connection_timeout`, and `transfer_timeout` are optional fields. If you provide `proxy_url`, then providing `proxy_port` is mandatory. Optionally, you can provide `proxy_user` and `proxy_password` for authentication. Otherwise, proxy details are optional parameters. If you provide `epo_endpoint`, it is appended at the end of `epo_url`.

Agent logs

Viewing McAfee Agent logs

The McAfee Agent log is a condensed log that can be viewed from the client system.

McAfee Agent Status Monitor — You can open the **McAfee Agent Status Monitor** window from the McAfee Agent tray icon (McTray).

Single System Troubleshooting — You can view the McAfee Agent logs of a managed system from the McAfee ePO console remotely for troubleshooting. You can enable remote logging by enabling the **Enable Remote Logging** option under the **General** policy **Logging** tab. The default line limit for the remote log is 200 lines and can go up to 5000 lines.

McAfee Agent product logs — You can record all McAfee Agent activities related to policy enforcement, agent-server communication, product deployment, update logging, and event forwarding in the respective log files.

You can configure the **Logging** policy options under the **General** policy tab to enable McAfee Agent logging on the managed systems and McAfee ePO. Configuring the **Application Logging** option allows McAfee Agent to record the activities in the McAfee Agent log files. In addition to the information stored in the McAfee Agent log, you can view detailed log that contains troubleshooting messages. You can enable detailed logging by enabling the **Enable detailed logging** option. The default file size is 2 MB and can go up to 100 MB. The default rollover count is 1 and can go up to 10.

You can view all installation-related activities in the installation log files.

By default, the McAfee Agent logs on Windows client systems are saved in <ProgramData>\McAfee\Agent\Logs.

The Windows installation logs on the client system are saved in:

- %TEMP%\McAfeeLogs, if the McAfee Agent is installed or upgraded manually.
- C:\Windows\Temp\McAfeeLogs, if McAfee Agent is installed using push or deployment task on McAfee ePO.

The Non-Windows installation logs on client system are saved in /var/log/ if McAfee Agent is installed using McAfeeSmartInstall.

Whenever there is a manifest integrity failure or an error in the policy database validation, the McAfee Agent logs an error message in the mapolicy_<hostname>.log file. The maximum file size is 5 MB for 1 rollover count and there is no impact on this file size by the McAfee Agent policy.

The table lists the McAfee Agent logs and installation log files for Windows and Non-Windows client systems.

McAfee Agent logs (Windows)	McAfee Agent logs (Non-Windows)	Installation logs (Windows)	Installation logs (Non-Windows)
masvc_<hostname>.log	masvc_<hostname>.log	Frminst_<hostname>.log	McAfeeSmartInstall_<sys time stamp>.log
macmnsvc_<hostname>.log	macmnsvc_<hostname>.log	Frminst_<hostname>_error.log	mcupdater_<hostname>
macompatsvc_<hostname>.log	macompatsvc_<hostname>.log	MFEAgent.msi.<system time stamp>.log	
McScript.log	McScript.log	McAfeeSmartInstall_<system time stamp>.log	
McScript_error.log	McScript_error.log	mcupdater_<hostname>.log	
McScript_deploy.log	McScript_deploy.log		
McScript_deploy_error.log	McScript_deploy_error.log		
marepomirror.log	mcupdater_<hostname>.log		
marepomirror_error.log	McAfeeSmartInstall_<system time stamp>.log		
UpdaterUI_<hostname>.log	mcupdater_<hostname>.log		
UpdaterUI_<hostname>_error.log			
McTray_<hostname>.log			
mfemactl.log			
mfemactl_c.log			
mapolicy_<hostname>.log	mapolicy_<hostname>.log		

View McAfee Agent Status Monitor

The McAfee Agent log files are useful for determining the McAfee Agent status or for troubleshooting.

Task

1. On the managed system, right-click the McAfee Agent icon in the system tray, then select **McAfee Agent Status Monitor**.

   Note

   McAfee Agent icon is available in the system tray only if the **Show McAfee system tray icon (Windows only)** policy is set in McAfee ePO on the **General** tab of the McAfee Agent policy pages.

2. Click **Save Contents to Desktop** to save the contents of the McAfee Agent log to a file.
   A file called Agent_Monitor.log is saved on your desktop.
3. When finished viewing the McAfee Agent log, click **Close**.

View McAfee Agent product log from McAfee ePO (McAfee ePO On-Premises) using Single System Troubleshooting

You can view the McAfee Agent product log of a managed system from the McAfee ePO console remotely.

Before you begin

- Make sure that McAfee Agent can communicate with McAfee ePO.
- Enable the **Enable Remote Logging** option under the McAfee Agent **General** → **Logging** policy tab.

Task

1. Select **Menu** → **Systems** → **System Tree**, then select the system for which you want to collect the product log.
2. From the **Actions** drop-down list, select **Agent**, then select **Single System Troubleshooting** to view the product log.
3. Click **Collect**, then click **Download**.

   Note

   The download option is available only after the product log collection is complete. The task completion status for a system is queued if the **Run Client Task Now** and **Update Now** tasks are in progress. Single System Troubleshooting requests through multiple sessions invoke an error message — `The selected system cannot use this feature as the system cannot be reached`.

   A file called <Machine_Name>_productlogs.zip is downloaded. Extract the contents in the folder to view the product logs.

Additional information

McAfee Agent files and folders

When you install the agent, the files are stored in different locations depending on the operating system.

Note

The DXL client is automatically installed with McAfee Agent 5.6.0. The DXL files are stored in the respective `Data Exchange Layer` folder based on the operating system.

Folder content	Operating system	Location
Installation files	Windows (32-bit and 64-bit) • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`<PROGRAMFILES>\McAfee\Agent`
	Linux	`/opt/McAfee/agent/`
	Macintosh	`/Library/McAfee/agent`
Data files	Windows (32-bit and 64-bit) • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`<Documents and Settings>\All Users\Application Data\McAfee\Agent` If the operating system does not have a Documents and Settings folder, the default location is `<System_Drive>\ProgramData\McAfee\Agent`
	Linux and Macintosh	`/var/McAfee/agent/`
Configuration and management information (including GUID and agent	Linux and Macintosh	`/etc/ma.d/`

Folder content	Operating system	Location
version) needed to manage products		
Script for starting and stopping the agent manually and when called by the system	Linux	`/etc/init.d/ma`
	Macintosh	`/Library/StartupItems/ma`
Installation log files	Windows • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`%TEMP%\McAfeeLogs`
Agent log files	Windows • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`<Documents and Settings>\All Users\Application Data\McAfee\Agent\Logs` If the operating system does not have a Documents and Settings folder, the default location is `<System_Drive>\ProgramData\McAfee\Agent\Logs`
	Linux and Macintosh	`/var/McAfee/agent/logs`
Peer-to-peer repository path	Windows • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`<Documents and Settings>\All Users\Application Data\McAfee\Agent\data\mcafeeP2P` If the operating system does not have a Documents and Settings folder, the default location is `<System_Drive>\ProgramData\McAfee\Agent\data\McAfeeP2P`
	Linux and Macintosh	`/var/McAfee/agent/data/McAfeeP2P`

Folder content	Operating system	Location
(McAfee ePO On-Premises) Lazy cache repository path	Windows • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`<Documents and Settings>\All Users\Application Data\McAfee\Agent\data\McAfeeHttp` If the operating system does not have a Documents and Settings folder, the default location is `<System_Drive>\ProgramData\McAfee\Agent\data\McAfeeHttp`
	Linux and Macintosh	`/var/McAfee/agent/data/McAfeeHttp`
Database path	Windows • Windows 7–10 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2	`<Documents and Settings>\All Users\Application Data\McAfee\Agent\DB` If the operating system does not have a Documents and Settings folder, the default location is `<System_Drive>\ProgramData\McAfee\Agent\DB`
	Linux and Macintosh	`/var/McAfee/agent/db`

McAfee Agent feature support

The table lists the McAfee Agent features and its platform support.

Features supported on McAfee ePO

Feature	Windows	Non-Windows
64-bit Native	Partially	Yes **Note:** McAfee Agent 5.0.5 or later supports Macintosh and McAfee Agent 5.0.4 or later supports Linux.

Feature	Windows	Non-Windows
	Note: Most of the McAfee Agent services are in 64-bit. To support other managed products, a few McAfee Agent services or processes are retained in 32-bit.	
RelayServer	Yes	Yes
Peer-to-peer	Yes	Yes
Policy-enabled application service logging	Yes	Yes
Policy-enabled debug logging	Yes	Yes
Configurable log rotation	Yes	Yes
McAfee Agent upgrade from McAfee ePO	Yes	Yes
McAfee Smart Installer	Yes	Yes
Property collection	Yes	Yes
Policy enforcement	Yes	Yes
Task enforcement	Yes	Yes
McAfee Agent Wake-up	Yes	Yes
Product Update	Yes	Yes
Product Deployment	Yes	Yes
Event Forwarding	Yes	Yes

Feature	Windows	Non-Windows
IPv4, IPv6, and mixed-mode compatibility	Yes	Yes
Managed product plug-in Architecture support	Yes	Yes
Secure Communication	Yes	Yes
CmdAgent	Yes	Yes
Run Immediately scheduling	Yes	Yes
Run Once scheduling	Yes	Yes
Run missed task scheduling	Yes	Yes
System startup scheduling	Yes	Yes
At logon scheduling	Yes	No
Automatic McAfee Agent uninstall from McAfee ePO	Yes	No
Cluster node property reporting	Yes	No
McAfee Agent status monitor	Yes	No
McTray application support	Yes	No
Remote provisioning	Yes	Yes
Incompatibility check	Yes	Yes

Features supported on McAfee ePO On-Premises only

Feature	Windows	Non-Windows
SuperAgent	Yes	Yes
Run Client Task Now	Yes	Yes
Remote log access	Yes	Yes
User-based policy	Yes	Macintosh only
McAfee Agent deployment from McAfee ePO	Yes	Linux and Macintosh only
Data Channel support	Yes	Yes
Managed and unmanaged modes	Yes	Yes
Agent Handler accessibility	Yes	Yes
Mirror Task	Yes	No
UNC repository updating	Yes	No

Available interface language versions

The agent is available in multiple languages. The default language that is installed is based on the locale of the operating system.

The Windows client systems support these languages.

Language	Language code
Portuguese (Brazil)	0416
Chinese (Simplified)	0804
Chinese (Traditional)	0404

Language	Language code
Czech	0405
Danish	0406
Dutch	0413
English	0409
Finnish	040b
French	040c
German	0407
Italian	0410
Japanese	0411
Korean	0412
Norwegian	0414
Polish	0415
Portuguese	0416
Russian	0419
Spanish	0c0a
Swedish	041d
Turkish	041f

McAfee Agent on Macintosh client systems supports English, Japanese, French, German, and Spanish.

McAfee Agent on all other supported non-Windows client systems supports only English.

Using multiple languages in your environment

You might need to use more than one language in your environment. This requires additional steps to make sure that the appropriate character sets for your chosen languages are supported. Follow these suggestions to make sure that all characters for each language are properly displayed in the McAfee Agent monitor.

- Configure your operating systems to use Unicode support for McAfee Agent.
- Install the appropriate operating system language packs on the systems to display language-specific characters.

Frequently asked questions

Here are answers to frequently asked questions.

McAfee Smart Installer

Note

For a consolidated list of common questions and answers for McAfee Agent 5.x.x, see KB75298.

Is the McAfee Smart Installer URL accessible on the Internet?

Yes. You can access the McAfee Smart Installer URL using the Internet if your McAfee ePO is accessible over a public network.

Can I restrict the McAfee Smart Installer URL to be used only a specific number of times or number of days?

Yes. The McAfee Smart Installer URL can be used for a predefined number of times.

Can I run the McAfee Smart Installer if I don't have administrator rights on the client system?

No. The user must have administrator rights to install McAfee Agent on client systems.

Remote Provisioning

Is there a temporary credential available that can be shared with end users for remote provisioning? I do not want to share my McAfee ePO administrator credentials.

No. The user needs administrator credentials to connect to McAfee ePO.

Peer-to-Peer communication

Is peer-to-peer information displayed on the Agent monitor?

No. These details are available in the detailed logs.

How many concurrent connections does a peer-to-peer server support?

A peer-to-peer server supports 10 connections concurrently.

How does a peer-to-peer client get updated content?

When an agent requires a content update, it tries to discover peer-to-peer servers with the content update in its broadcast domain. On receiving the request, the agents configured as peer-to-peer servers check if they have the requested content and respond back to the agent. The agent requesting the update, downloads the content update from the peer-to-peer server that responded first.

What type of content does a peer-to-peer server provide?

A peer-to-peer server provides all content available in its McAfee ePO repositories.

Can I configure the disk quota for peer-to-peer content?

Yes. See *Enable peer-to-peer service* for details.

General

Why do I see many McAfee Agent processes for Linux?

The McAfee runtime environment uses Linux Native threads through the Light Weight Process implementation. Using Linux Native threads causes each thread to show as a separate process on the client computer.

(McAfee ePO On-Premises) How can I change the language of McAfee Agent during installation?

Run this command on the client system.

```
framepkg.exe /install=agent /uselanguage=<Locale ID>
```

(McAfee ePO On-Premises) Are there best practices or important considerations for upgrading McAfee Agent?

Any action that generates network traffic must be carefully considered. Because McAfee ePO is used to deploy products, updates, and McAfee Agent, a McAfee ePO administrator's actions can negatively affect the network. Though the McAfee Agent installation package is not large by itself, it can have significant impact on a network if sent to thousands of systems at once. So, apply careful planning to any deployment effort.

Before checking in the new package, make sure you:

- Disable Global Updating — Checking in a McAfee Agent package with Global Updating enabled can cause the new version of McAfee Agent to be deployed even if the **Product Deployment** task is not enabled.
- Disable the **Product Deployment** Task — If the **Product Deployment** task is still enabled from the previous deployment, the new version causes deployments to begin according to the configured schedule. To reduce the risk of existing task execution, send the task change to client systems before checking in the new package.

Before deploying McAfee Agent:

- Enable **Product Deployment** task below Directory level — Do not set the **Product Deployment** task at the root level. Schedule **Product Deployment** tasks at a site level, or even at the group level, if needed, to reduce the number of systems downloading the new McAfee Agent at the same time.
- Randomize **Product Deployment** tasks — Do not configure the **Product Deployment** task to start at a set time for the entire site. Using the randomization feature in the task allows the network traffic to be spread out over a specified time.

(McAfee ePO On-Premises) How can I redirect the communication from a McAfee Agent to a new McAfee ePO server?

Use one of these installation methods to redirect communication from a McAfee Agent to a new McAfee ePO server. See McAfee ePO product documentation for alternate methods.

Method	Action
Using FrmInst.exe	1. On McAfee ePO, navigate to C:\Program Files\McAfee\ePO\DB\Software\Current \ePOAgent3000\Install\0409. 2. Copy these files to a temporary location on the client system. • Sitelist.xml file • sr2048pubkey.bin • srpubkey.bin (the server public key)

Method	Action
Note: This method is supported only on Windows.	• agentfipsmode file • reqseckey.bin (the initial request key) • req2048seckey.bin 3. Run this command on the client system. `FrmInst.exe /SiteInfo=<Temporary_folder_path>\Sitelist.xml`

Using remote provisioning commands	Run this command on the client system.
	`maconfig -provision -managed -auto -dir "temp location to copy keys" -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]`
	For example,
	`maconfig -provision -managed -auto -dir "/temp" -epo ePOServerMachine [-user admin] [password password123]`

How can I redirect the communication from a McAfee Agent to a new McAfee ePO Cloud server?

Use this installation method to redirect communication from McAfee Agent to a new McAfee ePO Cloud server. See McAfee ePO Cloud product documentation for alternate methods.

Method	Action

Using remote provisioning commands	Run this command on the client system.
	`maconfig -provision -managed -auto -dir "temp location to copy keys" -epo ePOServerMachine [-user ePO-User-name] [-password epo-admin-password]`
	For example,
	`maconfig -provision -managed -auto -dir "/temp" -epo ePOServerMachine [-user admin] [password password123]`

How does McAfee ePO sort McAfee Agent at the first connection?

When McAfee Agent is installed on a system, a unique GUID is created based on the MAC address and computer name of the system. McAfee Agent then connects to McAfee ePO in a randomized interval.
At that connection, McAfee ePO uses these system properties to see if McAfee Agent is populated in the **System Tree**. A new object is created in the **System Tree** if this search doesn't find a match. The location for the new object is also based on this sort order.

System properties used when Sorting Criteria is disabled	System properties used when Sorting Criteria is enabled
Agent GUID	Agent GUID
Domain Name	IP address and Tags evaluated for the computer
Computer Name	Domain Name
IP address	Computer Name

If an entry is found that is listed in the search order, McAfee Agent lists the client system in the correct group. If it does not find any of the above, it then lists the client in the **Lost & Found** group at the **My Organization** level.

What are the ports used by McAfee Agent?

Ports	Protocols	Traffic direction
8081	TCP	(McAfee ePO On-Premises) Inbound connection from McAfee ePO or Agent Handler. Peer-to-peer server serves content, Relay connections established.
8082	UDP	Inbound connection to McAfee Agent. Peer-to-peer server discovery, RelayServer discovery.
8083	UDP	RelayServer discovery for previous versions of McAfee Agent.

Note

If peer-to-peer service and RelayServer are disabled, these ports are not open.

COPYRIGHT

Trellix