McAfee Endpoint Security for Mac 10.5.0 - Installation Guide

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

1 Installing the software on a standalone Mac

Install the software on a standalone Mac using the wizard or from the command line.

Contents

Hardware and software requirements

Make sure that your standalone Mac meets these requirements for successful installation.

Component	Requirement
Hardware	Mac that can run the supported operating system configuration.
Operating system	• macOS High Sierra 10.13.x (client and server)  You must upgrade McAfee Agent to the platform compatibility update released for version 5.0.6 that supports macOS High Sierra before upgrading the operating system. Otherwise, the communication between the McAfee ePO server and the Mac fails, and you can't manage your Mac from McAfee ePO. For more information about the McAfee Agent version that supports macOS High Sierra, see KB51573. For information about McAfee Agent known issues, see KB83895. • macOS Sierra 10.12.x (client and server) — McAfee Agent 5.0.5 and later. • El Capitan 10.11.x (client and server) — McAfee Agent 5.0.5 and later.
Browser	Safari 10.1.1 and later Google Chrome 49 and later.

Install the software

Install the software on a standalone Mac using the wizard or the command line.

Before you begin

McAfee Endpoint Security for Mac doesn't support the co-existence of competitor's software in the Mac. You must uninstall competitor's software from the system before installation.

Tasks

- *Install the software using wizard* on page 6
  The wizard guides you through the steps to install the software on your standalone Mac.
- *Install the software from the command line (silent installation)* on page 6
  You can use the command line to install the software without user intervention.

Install the software using wizard

The wizard guides you through the steps to install the software on your standalone Mac.

Task

1 Download `McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.dmg` to a temporary location on your Mac, then double-click it to mount.

2 Double-click `McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.pkg` to open the wizard.

During the installation, the installer prompts you to select modules for installation. You can select one or multiple modules. To install a module later, you must start the installation wizard. If the modules are grayed out, it indicates that the installer has detected the competitor software on your Mac. You must uninstall it before installing the module. For more information, see McAfee Knowledgebase article KB78192.

3 Follow the prompts to install the software.

To install the module that you have already installed, you must start the installation wizard, then select the module as needed. When you re-install the module, the protection settings that you configured previously are retained.

Install the software from the command line (silent installation)

You can use the command line to install the software without user intervention.

Task

1 Download `McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.dmg` to a temporary location on your Mac, then double-click it to mount `McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.pkg`.

2 Copy the `McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.pkg` file to a temporary location on your Mac.

3 Open a Terminal window and change the working directory to the one where you saved the `McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.pkg` file.

4 Type the following command, then press **return**.

```
sudo installer -pkg
McAfee-Endpoint-Security-for-Mac-<version>-standalone-<build_number>.pkg -target /
```

5 Type the administrator password, then press **return**. The following message appears.

The Install was successful.

To install individual protection module using the command-line, see McAfee KnowledgeBase article KB84772.

Test the installation

Test the software to make sure that it is installed properly and can protect your Mac.

Tasks

- *Test the Threat Prevention feature* on page 7
  Access the EICAR standard anti-virus test file to test the **Threat Prevention** feature.
- *Test the Firewall feature* on page 7
  Test the Firewall feature by creating a rule. Consider a scenario where you want to create an allow rule for *www.intelsecurity.com*.
- *Test the Web Control feature* on page 8
  Make sure that the Web Control extension is added to the Safari browser, and appropriate rating appears for sites.

Test the Threat Prevention feature

Access the EICAR standard anti-virus test file to test the **Threat Prevention** feature.

This file is the combined effort by anti-virus vendors to implement one standard that customers can use to validate the anti-virus software.

Task

1 Go to the EICAR website http://www.eicar.org.

2 Click **DOWNLOAD ANTI MALWARE TESTFILE**, then click **DOWNLOAD**.

3 From the **Download area using the standard protocol http** section, click the file `eicar.com.txt`.

For the test to be successful, McAfee Endpoint Security for Mac displays a Notification `1 detection(s) found on your system.` with the relevant details.

Test the Firewall feature

Test the Firewall feature by creating a rule. Consider a scenario where you want to create an allow rule for *www.intelsecurity.com*.

Task

1 Click the McAfee menulet on the status bar, then select **Preferences**.

2 Click **Firewall**.

3 Click , type the administrator password, then click **OK**.

4 Select **Regular Mode**.

5 Click in the bottom left corner of the console to create a firewall rule.

   a Type a name of the rule in the **Rule Name** text box.

   b Select **Enabled** from the **Status** drop-down list.

   c Select **Allow** from the **Action** drop-down list.

   d Select **Outgoing** from the **Direction** drop-down list.

6 In the **Network Protocol (IPv4)**, section:
   a Select **Any Local IP Address** for **Local**.
   b Click , select **Fully Qualified Domain Name** for **Remote**, then type the **Domain Name**.
7 In the **Transport Protocol** section, select **All Protocols**.
8 Open the browser, type the website name, then press **return**.

Test the Web Control feature

Make sure that the Web Control extension is added to the Safari browser, and appropriate rating appears for sites.

Tasks

- *Verify the extension installation* on page 8
  Make sure that the Web Control extension is added to the Safari browser.
- *Test the site rating feature* on page 8
  Make sure that the **Web Control** feature displays the appropriate rating for sites.

Verify the extension installation

Make sure that the Web Control extension is added to the Safari browser.

Task

1 Start the Safari browser.
2 On the Menu bar, click **Safari**, then select **Preferences**.
3 In the **Extension** dialog box, you can see **McAfee Web Control 10.1** with **Enable Web Control** selected.

Test the site rating feature

Make sure that the **Web Control** feature displays the appropriate rating for sites.

Before you begin
You must have enabled **Web Control** in **Preferences**.

Task

1 Start the Safari browser.
2 In the address bar, type `www.mcafee.com`, then press **return**.
3 You must see the Green rating McAfee on the left top of the browser page.

Upgrading the software

McAfee Endpoint Security for Mac supports upgrading the software and migrating the configuration from the previous versions of the software.

Supported upgrades on a standalone Mac

McAfee Endpoint Security for Mac supports upgrading the software and migrating the preferences from the previous versions of the software.
You can upgrade the software from:

- McAfee® Endpoint Protection for Mac 2.3.0
- McAfee Endpoint Security for Mac 10.x
- McAfee® VirusScan™ for Mac 9.8.0

Upgrading from McAfee Endpoint Protection for Mac 2.3.0

When you upgrade the software, the respective preferences are migrated according to the modules you select.

When you upgrade the software from the previous version, the existing software is removed completely but the preferences for all modules are saved. When you install a module, the respective preferences are migrated.

For example:

If you select...	Migrated preferences...
Threat Prevention	Anti-malware
Firewall	Desktop Firewall
Web Control	None

Since Application Protection module is not part of McAfee Endpoint Security for Mac, the Application Protection preferences are migrated only when you install the McAfee® Application Protection 2.3.0 software. For more information, see *McAfee Application Protection* product guide.

When you migrate the preferences from McAfee Endpoint Protection for Mac or McAfee VirusScan for Mac, the **Quarantine** scan action is migrated to **Delete**, and the **Notify** scan action is migrated to **Deny**.

Upgrading from McAfee Endpoint Security for Mac 10.x

When you upgrade the software, the respective existing preferences are migrated according to the module you select. For example:

If you select...	Migrated preferences...
Threat Prevention	Threat Prevention
Firewall	Firewall
Web Control	Web Control

Upgrading from McAfee VirusScan for Mac 9.8.0

When you upgrade the software, the existing anti-malware preferences are migrated.

Upgrade the software on a standalone Mac

You can upgrade the software and migrate the existing configuration settings.

Before you begin

Before upgrading the software, make sure that your system meets all requirements.

Task

1 Install the software using the wizard.

For more information, see *Install the software using wizard*.

2 Make sure that all existing preferences are migrated to the new version.

Default settings

Once installed, McAfee Endpoint Security for Mac starts protecting the Mac immediately based on the default configurations defined. Refer to these default settings, and configure them for your environment.

General

Feature	Default settings
Threat Prevention	Enabled
Firewall	Enabled
Web Control	Enabled

Threat Prevention

Feature	Default settings

Threat Prevention	**On-Access Scan**:
	• **Scan files while** — Write
	• **Maximum scan time for a file** — 45 seconds for a file.
	  • **When a virus is found** — Clean
	  • **If clean fails** — Delete
	  • **When a spyware is found** — Clean
	  • **If clean fails** — Delete
	  • **Enable McAfee GTI** — Enabled.
	  • **Sensitivity Level** — Medium.
	  Also scan:
	  • **Archives & Compressed Files** — Disabled
	  • **Apple Mail messages** — Disabled
	  • **Network Volumes** — Disabled

	On-Demand Scan: • **When a virus is found** — Clean • **If clean fails** — Delete • **When a spyware is found** — Clean • **If clean fails** — Delete • **Enable McAfee GTI** — Enabled. • **Sensitivity Level** — Medium. • **Archives & Compressed Files** — Enabled • **Apple Mail messages** — Enabled • **Network Volumes** — Disabled

Feature	Default settings
	• **Scheduled Scan Option** • **Scan only when the system is idle** — Enabled. • **Do not scan when the system is on battery power** — Enabled.
	Exclusions — None

Firewall

Feature	Default settings
Firewall	• **Regular Mode** — Enabled

Web Control

Feature	Default settings

Web Control	• **Rating Actions for Sites**
	  • **Red** — Block
	  • **Yellow** — Warn
	  • **Unrated** — Allow
	  • **Unverified** — Allow
	• **Enable Web Category Blocking** — Enabled
	• **Block and Allow List** — None

Update

Feature	Default settings
Update	In **Repository List** • **Repository Name** — McAfeeHttp, McAfeeFtp In **Proxy Settings** • **Proxy settings** — Configure proxy settings manually In **Schedule** • **Schedule** — Daily at 4:45 PM (local time)

Logging

Feature	Default settings
Logging	In **Enable Debug Logging** • **Threat Prevention** — Disabled • **Firewall** — Disabled • **Web Control** — Disabled

Recommended post-installation tasks

Perform these tasks to make sure that the protection configuration does not affect the business routines.

Task	Description
Update the content files	After installation, McAfee Endpoint Security for Mac automatically updates the content files to protect the Mac from the latest threats. By default, this update is scheduled at 4.45 pm local time every day. When the files are updated for the first time, it may take longer time to download the full content. The subsequent updates will be incremental. You can view the content files last update details in the **Console** page.
Perform an on-demand scan	Run an on-demand-scan to scan the local volumes, after you install the software to clean the infected files that are not accessed by but reside in the Mac. Configure the **On-Demand Scan** task to define: • The items to scan (files, folders, and drives) • Set frequency of scan (daily, weekly, monthly, or immediately) • Define the action when malware is found (**Delete** or **Clean**)
Threat Prevention	McAfee Endpoint Security for Mac comes with the default settings. Verify that the default settings are consistent with your organization policies and provides complete protection against malware.
Firewall	McAfee Endpoint Security for Mac comes with the *stateful* Firewall enabled, which protects your Mac from the moment the product is installed. The firewall comes with a set of default rules that enable your Mac to access the necessary services. We recommend that you review the default rules to make sure that your Mac can access the necessary services according to your organization policies. The rules are processed using a top-down approach with the implicit default block rule that denies all traffic. This rule can't be modified.
Web Control	Review the default Web Control settings and update the **Block and Allow List** in such a way that you can access business-critical sites and block unwanted sites. The **Block and Allow List** overrides other settings such as **Enable Web Category Blocking** and **Rating Actions for Sites**.

Uninstall the software

Remove the software from the standalone Mac.

Tasks

- *Uninstall the software from a standalone Mac* on page 12
  You can uninstall the software or specific modules from a Mac using the command line.

Uninstall the software from a standalone Mac

You can uninstall the software or specific modules from a Mac using the command line.

Before you begin

You must have administrator rights to uninstall the software.

Task

1 Open a Terminal window.

2 Type the following command, then press **return**.

To remove...	Use this command...
All modules	`sudo /usr/local/McAfee/uninstall EPM`
Threat Prevention module	`sudo /usr/local/McAfee/uninstall ThreatPrevention`
Firewall module	`sudo /usr/local/McAfee/uninstall Firewall`
Web Control module	`sudo /usr/local/McAfee/uninstall WebControl`

The uninstallation command is case sensitive.

3 Type the administrator password when prompted.

When **Uninstallation** is enabled in Endpoint Security Common policy, uninstalling the software using the command line prompts you to type the password set by your McAfee ePO server administrator.

When the software is uninstalled, the following message appears:

Product has been uninstalled successfully.

When you uninstall the software, the McAfee Agent is not uninstalled from the system. This is because that it might be used by other products. Refer to the product guide of your McAfee Agent version for more information.

2 Installing the software on systems managed with McAfee ePO

Install and manage the software on a system that is managed with McAfee ePO.

McAfee ePO is an extensible management platform that enables centralized policy management and enforcement of your security products and the systems where they are installed.

It also provides comprehensive reporting and product deployment capabilities, all through one point of control. You can deploy security products, patches, and service packs to the managed systems in your network.

Contents

System requirements

Make sure that these requirements are met and you have administrator permission.

Component	Requirements
Hardware	Mac that can run with the supported operating system configuration.
Operating system	• macOS High Sierra 10.13.x (client and server) You must upgrade McAfee Agent to the platform compatibility update released for version 5.0.6 that supports macOS High Sierra before upgrading the operating system. Otherwise, the communication between the McAfee ePO server and the Mac fails, and you can't manage your Mac from McAfee ePO. For more information about the McAfee Agent version that supports macOS High Sierra, see KB51573. For information about McAfee Agent known issues, see KB83895. • macOS Sierra 10.12.x (client and server) — McAfee Agent 5.0.5 and later. • El Capitan 10.11.x (client and server) — McAfee Agent 5.0.5 and later.
Browser	Safari 10.1.1 and later. Google Chrome 49 and later.
McAfee ePolicy Orchestrator	5.3.2 and later

Component	Requirements
McAfee® Endpoint Security extensions	10.5.4 and later
McAfee Endpoint Security license extension	10.2.0 This license extension is mandatory to view the features that are supported for Windows and Mac operating systems.

Requirements for Adaptive Threat Protection

Component	Requirements
McAfee Endpoint Security Adaptive Threat Protection extensions	10.5.4 and later
McAfee Endpoint Security for Mac license extension	10.2.0
TIE server	2.1.0 and later
McAfee Data Exchange Layer Broker	3.1.0 and later
McAfee Data Exchange Layer client	3.1.0 and later
McAfee Endpoint Security Threat Prevention	10.5.4 and later
McAfee Endpoint Security Common	10.5.4 and later
McAfee Endpoint Security for Mac Threat Prevention client	10.5.0 and later
Threat Intelligence Exchange module content for Mac	1.0.0

Check in the package to the McAfee ePO server

You can check in the package using the Software Manager or check in the package manually.

Tasks

- *Check in the package using Software Manager* on page 16
  Check in McAfee Endpoint Security for Mac using the Software Manager.
- *Check in the package manually* on page 16
  Manually check in the McAfee Endpoint Security for Mac deployment package to the McAfee ePO Master Repository to manage the software.

Check in the package using Software Manager

Check in McAfee Endpoint Security for Mac using the Software Manager.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Software** | **Software Manager**.
3. From the **Product Categories** list under **Software (By Label)**, select **McAfee Endpoint Security for Mac 10.5**, select the package file, then click **Check in All**.
4. On the summary page, accept the **McAfee End User License Agreement**, then click **OK**.

Check in the package manually

Manually check in the McAfee Endpoint Security for Mac deployment package to the McAfee ePO Master Repository to manage the software.

Task

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

1. Download the .zip file from the McAfee download site to a temporary location on the McAfee ePO server.
2. Log on to the McAfee ePO server as an administrator.
3. Select **Menu** | **Software** | **Master Repository** | **Check In Package**.
   a. For **Package type**, select **Product or Update (.ZIP)**.
   b. Click **Choose File**, select the file, click **Choose**, then click **Next**.
   c. Select **Current** as the branch.
4. Click **Save**.

You must check in the Threat Intelligence Exchange module content for Mac (JTIContent-macOS-<version>Release-xxx.zip) manually.

Install the extensions on the McAfee ePO server

Install the extensions on the McAfee ePO server to be able to configure and deploy policies for managed systems.

You must install these extensions in this order to enable the features of the product:

- Endpoint Security for Mac License — Endpoint Security for Mac license extension to view the operating system-specific tag in the policy and task options.
- Endpoint Security Platform — Endpoint Security Common policy extension.
- These product modules as required:
  - Endpoint Security Threat Prevention extension.
  - Endpoint Security Firewall extension.
  - Endpoint Security Web Control extension.
- Product help extension.

Tasks

- *Install the extensions using Software Manager* on page 17
  Install the extensions using the Software Manager.
- *Install the extensions manually* on page 18
  Manually install Endpoint Security extensions on the McAfee ePO server.

Install the extensions using Software Manager

Install the extensions using the Software Manager.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu**, **Software**, then click **Software Manager**.
3. From the **Software Manager** | **Product Categories** | **Software (By Label)**, select **Endpoint Security** | **McAfee Endpoint Security for Mac 10.5**, select from the right pane, then check in the extensions.

Install the extensions manually

Manually install Endpoint Security extensions on the McAfee ePO server.

You must install the extensions to enable the features of the product.

Task

1 Log on to the McAfee ePO server as an administrator.

2 Select **Menu** | **Software** | **Extensions**, then click **Install Extension**.

3 Click **Choose File** and select the extension, then click **OK**.

You must install the extensions in this order:

- Endpoint Security for Mac License — Endpoint Security for Mac license extension to view the operating system-specific tag in the policy and task options.
- Endpoint Security Platform — Endpoint Security Common policy extension.
- These product modules as required:
  - Endpoint Security Threat Prevention extension.
  - Endpoint Security Firewall extension.
  - Endpoint Security Web Control extension.
- Product help extension.

After installing the Endpoint Security extensions, you can use the migration tasks to migrate McAfee Endpoint Protection for Mac 2.3 or McAfee VirusScan for Mac 9.8 policies and tasks. For more information, see Endpoint Security migration help.

Install the client software on a managed system using the installation URL

McAfee ePO administrators can create an installation URL to install Endpoint Security for Mac client software on managed systems.

It is a method for the user on the managed system to install the software themselves.

Tasks

- *Create an installation URL* on page 18
  Create an installation URL and send it to the users so that they can install McAfee Agent on their managed systems.
- *Install the software with an installation URL on a managed system* on page 19
  The user accesses the URL to install the client software on a managed system.

Create an installation URL

Create an installation URL and send it to the users so that they can install McAfee Agent on their managed systems.

Task

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

1 Log on to the McAfee ePO server as an administrator.

2 Select **Menu** | **Dashboards**, then select **Getting Started with ePolicy Orchestrator** from the drop-down list.

3 On the **Product Deployment** page, click **Start Deployment**, define these settings, then click **Deploy**.

- **System Tree Group**
- **McAfee Agent**
- **Software and Policies**
- **Auto Update**

4 On the **Initial Product Deployment Summary** page, click **OK**.

On the Dashboard page, the installation URL appears under **Product Deployment** section.

5 Email the URL with instructions to install the client software on the system.

After successful installation, McAfee Agent checks back with the McAfee ePO server for assigned tasks for that system group, then installs the software accordingly.

Install the software with an installation URL on a managed system

The user accesses the URL to install the client software on a managed system.

Before you begin

Make sure that your managed system meets the hardware and software requirements.

You must have an installation URL that you created or received from your administrator.

Task

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

1 Open a browser window, paste the installation URL in the address bar, then press **Enter**.

2 Follow the on screen instructions.

3 If the installation does not start automatically, click **Install**.

Deploy the client software from McAfee ePO

Use McAfee ePO to deploy the client software to systems in your network that are managed.

To deploy the software from McAfee ePO with the On-Access Scan option disabled, you can use the McAfee Agent command-line option to pass the **oasoff** parameter in the deployment task. The command-line option is available in the Client Task Catalog page under the Products and Components section. By default, the software is installed with the On-Access Scan option enabled.

For Adaptive Threat Protection, if you are using TIE server, you also need to deploy the McAfee Data Exchange Layer client and McAfee Data Exchange Layer broker.

To make sure that On-Access Scan is disabled, configure the McAfee Endpoint Security Threat Prevention On-Access Scan policy with the **Enable On-Access Scan** option is unselected.

Task

1 Log on to the McAfee ePO server as an administrator.

2 Select **Menu** | **Systems** | **System Tree**, then select a group or systems.

3 On the **Assigned Client Tasks** tab, click **Actions**, then click **New Client Task Assignment**.

4 Complete these options, then click **Create New Task**:
   a For product, select **McAfee Agent**.
   b For task type, select **Product Deployment**.
5 On the **Client Task Catalog** page:
   a Type a name for the task.
   b Select **Mac** as the target platform.
   c In **Products and components**, select the product, select **Install** as the action, then click **Save**.


You can add more products by using  .

6 On the **Client Task Assignment Builder** page:
   a Select the task, then click **Next**.
   b Schedule the task to run immediately, click **Next** to view a summary of the task, then click **Save**.
7 In the **System Tree**, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
8 Select **Force complete policy and task update**, then click **OK**.

Test the installation

After deploying the software, verify that the client software is installed and updated correctly on managed systems.

Task

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

1 Wait for client systems to report back to the McAfee ePO server (typically after an hour).
2 On the McAfee ePO console, select **Menu** | **Dashboards**, then select **Endpoint Security: Installation Status** for a complete list of managed systems and their installation status.

Remove the software from a managed system

Remove the client software from a managed system and remove the extensions from the McAfee ePO server.

Tasks

- *Remove the software extensions* on page 20
  Remove the McAfee Endpoint Security for Mac extensions from the McAfee ePO server.
- *Remove the software from client systems* on page 21
  Create a client task on the McAfee ePO server to remove McAfee Endpoint Security for Mac from your managed systems.

Remove the software extensions

Remove the McAfee Endpoint Security for Mac extensions from the McAfee ePO server.

Task

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

1 Log on to the McAfee ePO server as an administrator.

2 Select **Menu** | **Software** | **Extensions**.

3 In the left pane, select the extension, then click **Remove**.

4 Select **Force removal, bypassing any checks or errors**, then click **OK**.

Remove the software from client systems

Create a client task on the McAfee ePO server to remove McAfee Endpoint Security for Mac from your managed systems.

Task

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

1 Log on to the McAfee ePO server as an administrator.

2 Select **Menu** | **Systems** | **System Tree**, then select a group or systems.

3 Click the **Assigned Client Tasks** tab, then click **New Client Task Assignment**.

4 Complete these options, then click **Create New Task**.

   a For products, select **McAfee Agent**.

   b For task type, select **Product Deployment**.

5 On the **Client Task Catalog** page:

   a Type a name for the task.

   b Select **Mac** as the target platform.

   c In **Products and components**, select the product, select **Remove** as the action, then click **Save**.

6 On the **Client Task Assignment Builder** page:

   a Select the task, then click **Next**.

   b Schedule the task to run immediately, then click **Next** to view a summary of the task, then click **Save**.

7 In the **System Tree**, select the systems or groups for which you assigned the task, then click **Wake Up Agents**.

8 Select **Force complete policy and task update**, then click **OK**.

Installing Adaptive Threat Protection

Adaptive Threat Protection is an optional Endpoint Security module that analyzes content and decides what to do based on file reputation, rules, and reputation thresholds.

Adaptive Threat Protection works with Endpoint Security Threat Prevention and McAfee Data Exchange Layer. You must have checked in Common extension, Endpoint Security Threat Prevention, and Data Exchange Layer packages in the Master Repository of the McAfee ePO server before installing Adaptive Threat Protection.

Adaptive Threat Protection is not supported on standalone systems and systems managed by McAfee ePO Cloud.

Overview of Adaptive Threat Protection installation process

Complete these tasks to install and use Adaptive Threat Protection in managed network environments.

Tasks related to the TIE server are required only when the TIE server is installed.

1 Install the McAfee Endpoint Security for Mac product files on McAfee ePO.
   - At a minimum, install the Endpoint Security Threat Prevention and Endpoint Security Common extensions. These are installed as part of the McAfee Endpoint Security for Mac bundle.
   - Check in the McAfee Endpoint Security for Mac product deployment package to the **Master Repository**.

2 Download and check in the product components to McAfee ePO.

3 (Required for TIE server only.) Install the Data Exchange Layer product files on McAfee ePO.
   - Install the Data Exchange Layer extension.
   - Check in the Data Exchange Layer product deployment package to the Master Repository.

4 Install the Adaptive Threat Protection product files on McAfee ePO.
   - Install the Adaptive Threat Protection extension.
   - Check in the Adaptive Threat Protection product deployment package to the **Master Repository**.

5 Deploy the correct version of McAfee Agent to managed systems.

6 (Required for TIE server only.) Deploy the Data Exchange Layer package to managed systems.

7 Deploy Endpoint Security (at least Threat Prevention and Common) and Adaptive Threat Protection to managed systems.

   You can use a single deployment task for steps 6 and 7. In the deployment task, Adaptive Threat Protection must be the last item in the **Products and Components** list. This ensures that Endpoint Security Threat Prevention and Data Exchange Layer is present when Adaptive Threat Protection is installed.

8 Verify the deployment.

9 (Required for TIE server only.) Install and configure the Threat Intelligence Exchange (TIE) server. See the *McAfee Threat Intelligence Exchange Product Guide*.

Using Adaptive Threat Protection on managed systems

You can use McAfee ePO to configure, manage, deploy, and enforce Adaptive Threat Protection policies. Once configured, you can then use queries and dashboards to monitor your environment for threats.

Components

Adaptive Threat Protection can integrate with these components:

- **TIE server** — A server that stores information about file and certificate reputations, then passes that information to other systems.
- **Data Exchange Layer** — Clients and brokers that enable bidirectional communication between the Adaptive Threat Protection module on the managed system and the TIE server.
- Threat Prevention and Data Exchange Layer modules are mandatory to install Adaptive Threat Protection. Data Exchange Layer (including client software) is required for Adaptive Threat Protection to communicate with TIE server.

These components are installed as McAfee ePO extensions and add several new features and reports.

How Adaptive Threat Protection works

Adaptive Threat Protection functions differently, depending on whether TIE server is deployed:

- If the TIE server isn't present and the system is connected to the Internet, Adaptive Threat Protection uses McAfee GTI for reputation decisions.
- If If the TIE server isn't present and the system isn't connected to the Internet, Adaptive Threat Protection determines the file reputation using information about the local system.
- If the TIE server is present, Adaptive Threat Protection uses the Data Exchange Layer framework to share file and threat information instantly across the whole enterprise.

Check in the Adaptive Threat Protection components to McAfee ePO

Check in the required Adaptive Threat Protection components to the McAfee ePO server. If you plan to install the TIE server, you also need to download and check in the Data Exchange Layer.

> **Before you begin**
>
> The Endpoint Security for Mac product files (at least the Threat Prevention and Common packages) are installed on the McAfee ePO server, and the Endpoint Security for Mac client product deployment package is added to the Master Repository.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Software** | **Software Manager**.
3. Check in the McAfee Data Exchange Layer package (Required only for TIE Server):
   a. From **Management Solutions**, select **McAfee Data Exchange Layer 3.1.0** or later.
   b. Check in the **DXL Platform** (or Bundle) package.
4. Check in the Adaptive Threat Protection package.
   a. From **Endpoint Security**, select **McAfee Endpoint Security Adaptive Threat Protection 10.5**.
   b. Check in the **Endpoint Security Adaptive Threat Protection** package.

Deploy the client software from McAfee ePO

Use McAfee ePO to deploy the client software to systems in your network that are managed.

To deploy the software from McAfee ePO with the On-Access Scan option disabled, you can use the McAfee Agent command-line option to pass the **oasoff** parameter in the deployment task. The command-line option is available in the Client Task Catalog page under the Products and Components section. By default, the software is installed with the On-Access Scan option enabled.

For Adaptive Threat Protection, if you are using TIE server, you also need to deploy the McAfee Data Exchange Layer client and McAfee Data Exchange Layer broker.

To make sure that On-Access Scan is disabled, configure the McAfee Endpoint Security Threat Prevention On-Access Scan policy with the **Enable On-Access Scan** option is unselected.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, then select a group or systems.

3 On the **Assigned Client Tasks** tab, click **Actions**, then click **New Client Task Assignment**.

4 Complete these options, then click **Create New Task**:

   a For product, select **McAfee Agent**.

   b For task type, select **Product Deployment**.

5 On the **Client Task Catalog** page:

   a Type a name for the task.

   b Select **Mac** as the target platform.

   c In **Products and components**, select the product, select **Install** as the action, then click **Save**.

   You can add more products by using +.

6 On the **Client Task Assignment Builder** page:

   a Select the task, then click **Next**.

   b Schedule the task to run immediately, click **Next** to view a summary of the task, then click **Save**.

7 In the **System Tree**, select the systems or groups where you assigned the task, then click **Wake Up Agents**.

8 Select **Force complete policy and task update**, then click **OK**.

Verify the deployment

After installing the Adaptive Threat Protection components, verify the deployment to managed systems. If you plan to install the TIE server, also verify deployment for the McAfee Data Exchange Layer.

Task

1 Log on to the McAfee ePO server as an administrator.

2 In the **System Tree**, click the group or system name, then click the **Products** tab.

3 Verify that the following components are listed:

- McAfee Agent.
- McAfee Data Exchange Layer client.
- Endpoint Security Platform.
- McAfee Endpoint Security Threat Prevention.
- Endpoint Security Adaptive Threat Protection.

Uninstall Adaptive Threat Protection

Remove the software from managed systems remotely from McAfee ePO or locally at the managed systems. You can continue to use other Endpoint Security modules after uninstalling Adaptive Threat Protection.

With Adaptive Threat Protection installed, to uninstall Endpoint Security Threat Prevention, you must first uninstall Adaptive Threat Protection, then uninstall Threat Prevention.

Tasks

- *Remove the software from client systems* on page 21
  Create a client task on the McAfee ePO server to remove McAfee Endpoint Security for Mac from your managed systems.
- *Uninstall the software from managed systems using commands* on page 25
  You can uninstall Adaptive Threat Protection module from the managed Mac using the command line.

Remove the software from client systems

Create a client task on the McAfee ePO server to remove McAfee Endpoint Security for Mac from your managed systems.

Task

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

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. Click the **Assigned Client Tasks** tab, then click **New Client Task Assignment**.
4. Complete these options, then click **Create New Task**.
   a. For products, select **McAfee Agent**.
   b. For task type, select **Product Deployment**.
5. On the **Client Task Catalog** page:
   a. Type a name for the task.
   b. Select **Mac** as the target platform.
   c. In **Products and components**, select the product, select **Remove** as the action, then click **Save**.
6. On the **Client Task Assignment Builder** page:
   a. Select the task, then click **Next**.
   b. Schedule the task to run immediately, then click **Next** to view a summary of the task, then click **Save**.
7. In the **System Tree**, select the systems or groups for which you assigned the task, then click **Wake Up Agents**.
8. Select **Force complete policy and task update**, then click **OK**.

Uninstall the software from managed systems using commands

You can uninstall Adaptive Threat Protection module from the managed Mac using the command line.

Before you begin

You must have administrator rights to uninstall the software.

Task

1 Open a Terminal window.

2 Type the following command, then press return.

```
sudo /usr/local/McAfee/uninstall ATP
```

The uninstallation command is case sensitive.

3 Type the administrator password when prompted.

When Uninstallation is enabled in Endpoint Security Common policy, uninstalling the software using the command line prompts you to type the password set by your McAfee ePO server administrator.

3 Installing the software on a system managed with McAfee ePO Cloud

Install and manage the software on a system that is managed with McAfee ePO Cloud.

McAfee ePO Cloud is an extensible management platform that enables centralized policy management and enforcement of your security products and the systems where they are installed.

It also provides comprehensive reporting and product deployment capabilities, all through a single point of control. Using McAfee ePO Cloud, you can deploy security products, patches, and service packs to the managed systems in your network.

Contents

McAfee ePO Cloud components

These components make up McAfee ePO Cloud software.

- **McAfee ePO Cloud** — The center of your managed environment. McAfee ePO Cloud delivers security policies and tasks, controls updates, and processes events for all managed systems.
- **McAfee Agent** — A vehicle of information and enforcement between the McAfee ePO Cloud and each managed system. The agent retrieves updates, ensures task implementation, enforces policies, and forwards events for each managed system.
- **Master Repository** — The central location for all McAfee updates and signatures, residing on McAfee ePO Cloud. The Master Repository retrieves user-specified updates and signatures from McAfee.

Hardware and software requirements

Make sure that your standalone Mac meets these requirements for successful installation.

Component	Requirement
Hardware	Mac that can run the supported operating system configuration.
Operating system	• macOS High Sierra 10.13.x (client and server) You must upgrade McAfee Agent to the platform compatibility update released for version 5.0.6 that supports macOS High Sierra before upgrading the operating system. Otherwise, the communication between the McAfee ePO server and the Mac fails, and you can't manage your Mac from McAfee ePO. For more information about the McAfee Agent version that supports macOS High Sierra, see KB51573. For information about McAfee Agent known issues, see KB83895. • macOS Sierra 10.12.x (client and server) — McAfee Agent 5.0.5 and later. • El Capitan 10.11.x (client and server) — McAfee Agent 5.0.5 and later.
Browser	Safari 10.1.1 and later Google Chrome 49 and later.

Installation overview

In McAfee ePO Cloud environment, administrators can deploy the software remotely to managed Mac, or ask users to install it locally.

McAfee sets up each McAfee ePO Cloud account on an offsite management server and notifies the local administrator when products are ready to install on managed Mac systems. Administrators then typically create and send an installation URL to ePolicy Orchestrator administrators for installation of client software on Mac systems.

McAfee sends the credentials to you through registered email. If you have not previously activated and configured an account, see the McAfee ePO Cloud product guide for instructions.

McAfee Endpoint Security for Mac supports both URL installation and deployment tasks. As an administrator, you can choose the method that best suits your needs.

1 Make sure that all managed Mac systems meet the hardware and software requirements.

2 Open the management console. Open a browser and log on to your McAfee ePO Cloud account.

3 Create the installation URL.

4 Send the installation URL to all Mac users to install the McAfee Agent and product software.

5 Deploy the client software with default or custom settings to managed Mac in one of these ways.

- **Schedule product deployment tasks** — Run product deployment tasks to deploy the software on managed Mac.
- **Create an installation URL** — Create an installation URL, then email it to users with instructions about installing the product on their Mac.
- Verify that the client software is installed and up to date on all managed Mac.

Accessing the McAfee ePO Cloud account

These are the high level actions to set up the McAfee ePO Cloud account.

1 The enterprise administrator requests access to use McAfee ePO Cloud.

2 McAfee emails the McAfee ePO Cloud URL and logon information to the enterprise administrator.

3 Log on to the McAfee ePO Cloud server.

Install the client software on a managed systems using the installation URL

Create an installation URL and send it to users to install the client software on managed systems.

Tasks

- *Create an installation URL* on page 29
  Create an installation URL to install the software on managed systems.
- *Install the software with an installation URL* on page 30
  The managed system user can install the software on a local system with an installation URL.

Create an installation URL

Create an installation URL to install the software on managed systems.

Task

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

1 Log on to McAfee ePO Cloud as an administrator.

2 Click **Menu** | **Getting Started** | **Customize**.

3 On the **Customize Software Installation** page, define these settings, then click **Done**.

- **Group Name** — Type a name of the group.
- **Operating System** — Select **McAfee Agent for Mac**.
- **Software and Policies** — Select **McAfee Endpoint Security** software modules as required.
- **Auto Update** — Select this option to download updates for the software.

The default policies and tasks of the module are selected by default.

4 Click **Done**.

5 From the **Dashboards** drop-down list, select **Getting Started with ePolicy Orchestrator**.

On the right side pane under **Getting Started**, the URL that you created appears.

6 Email the URL with installation instructions to the system user.

After successful installation, McAfee Agent checks back with the McAfee ePO server for assigned tasks for that system group, then installs the software accordingly.

Install the software with an installation URL

The managed system user can install the software on a local system with an installation URL.

Before you begin

- Make sure that your system meets the hardware and software requirements.
- You must have an installation URL that you created or received from your administrator.

Task

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

1. Open a browser window, paste the installation URL in the address bar, then press **Enter**.
2. Follow the on-screen instructions.

Deploy the client software from McAfee ePO Cloud

Deploy the client software to systems in your network that are managed.

Task

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

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Software** | **Product Deployment**
3. In the **Product Deployment** page, define these settings, then click **Save**.
   - **Name**
   - **Description**
   - **Type**
   - **Auto Update**
   - **Package**
   - **Language**
   - **Branch**
   - **Command line**
   - **Select the systems**
   - **Select a start time**

Index