McAfee Endpoint Security 10.7.x Installation Guide

Contents

Upgrade to version 10.7.x

You can use multiple deployment methods to upgrade to McAfee Endpoint Security 10.7.x on your endpoints. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

The method you choose for deploying the product software to endpoints depends on not only your environment and your goals for the installation, but also your preferences and department policies for tools.

Deciding which deployment method to use

Upgrading more than one product?	Using third-party tool?	Using McAfee ePO?	Use this method
Yes			Endpoint Upgrade Assistant
No	Yes		• IBM BigFix • Microsoft System Center Configuration Manager (SCCM) • Tanium Deploy
No	No	Yes	• McAfee ePO 5.10.x or McAfee ePO 5.9.x • McAfee MVISION ePO
No	No	No	Product installer (SetupEP)

Using McAfee ePO 5.10.x–5.9.x

You can use a deployment task in McAfee ePO 5.10.x or 5.9.x to upgrade to Endpoint Security 10.7.x on your endpoints. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

Deployment tasks can be set up as continuous (for endpoints in specific groups or with specific tags) or fixed (for a static set of endpoints).

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that products installed on endpoints are supported.
   - Verify that you're aware of compatibility requirements for other installed products.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   - Verify that endpoint users have permission to access the user temp folder (KB85033).
   - Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).

     Note: Best practice: Use the latest version of the McAfee SysPrep utility when upgrading from version 10.5.3 or earlier, or when new software or policy configurations are used in software metering, software monitoring, or rights management. Check with technical support for the latest version of McAfee SysPrep.
   - Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
   - If you plan to save custom product settings, review your settings, client tasks, and assignments, consolidating them where possible. Remove duplicates and unused objects.
2. Upgrade product extensions and installation packages on McAfee ePO.
3. Update content files on McAfee ePO.
4. Deploy product software to endpoints.
5. After the installation:
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   - Review the policy settings that are new or changed in Endpoint Security 10.7.x.

Upgrade product extensions and installation packages

When using McAfee ePO 5.10.x or 5.9.x to upgrade to McAfee Endpoint Security 10.7.x, you need to upgrade the product extensions and installation packages on the McAfee ePO server. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

The product extensions manage policies and tasks on the McAfee ePO server and the installation packages install Endpoint Security on your endpoints. You can retrieve them through McAfee ePO or from the McAfee Product Downloads site. When you check in the installation packages, you need to choose the repository branch where to store them.

Task

1. In McAfee ePO, select Menu → Software → Software Catalog (Software Manager on version 5.9.x).
2. From the Category list, expand Endpoint Security, then click Bundles.
3. In the right pane, select the bundle that suits your environment:

Bundle name	What's included
McAfee Endpoint Security	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Client Proxy
McAfee Endpoint Security Adaptive Threat Protection	◦ Endpoint Security Platform ◦ Threat Prevention

Bundle name	What's included
	◦ Firewall ◦ Web Control ◦ Adaptive Threat Protection ◦ Client Proxy

4. From the Actions column, click Check In All.
5. Select the checkbox to accept the license agreement.
6. Select the branch where to check in the installation packages, then select Check In.

Results

When check-in is complete, the product extensions are listed on the Extensions page and the installation packages are listed in the Master Repository. Based on the bundle installed, you can view the respective extensions and packages in these locations.

Extension	Navigation
Endpoint Security Platform	Menu → Extension → McAfee → Endpoint Security
Endpoint Security Threat Prevention	
Endpoint Security Firewall	
Endpoint Security Web Control	
Endpoint Security Adaptive Threat Protection	
Threat Detection Reporting	Menu → Extension → McAfee → Threat Detection Reporting You can view this extension only if you have checked in the McAfeeEndpoint Security Adaptive Threat Protection bundle.

Packages	Navigation
AMCore Content Package	Menu → Master Repository
DAT	
Endpoint Security Adaptive Threat Protection	
Endpoint Security Exploit Prevention Content	
Endpoint Security Firewall	
Endpoint Security Platform	
Endpoint Security Threat Prevention	
Endpoint Security Web Control	
Threat Intelligence Exchange Module Content	

Update content files

Make sure that the latest content files for antimalware and exploit prevention are updated on the McAfee ePO server as part of any installation. Content files are released regularly to protect against the latest known threats.

McAfee releases new Adaptive Threat Protection Rules for ATP in AMCore content.

Task

1. In McAfee ePO, select Menu → Automation → Server Tasks.
2. Edit the Update Master Repository server task.
3. Click the Actions tab.
4. For the Repository Pull action, make sure that the following are set:
   - Source site: McAfeeHttp
   - Package types: All packages
5. Click Save.
6. For the Update Master Repository server task, click Run.

Results

The Master Repository includes the AMCore Content Package and the Endpoint Security Exploit Prevention Content Package, which are required by Endpoint Security.

Deploy product software to endpoints

You can use a deployment task in McAfee ePO 5.10.x or 5.9.x to upgrade to Endpoint Security 10.7.x on multiple endpoints. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

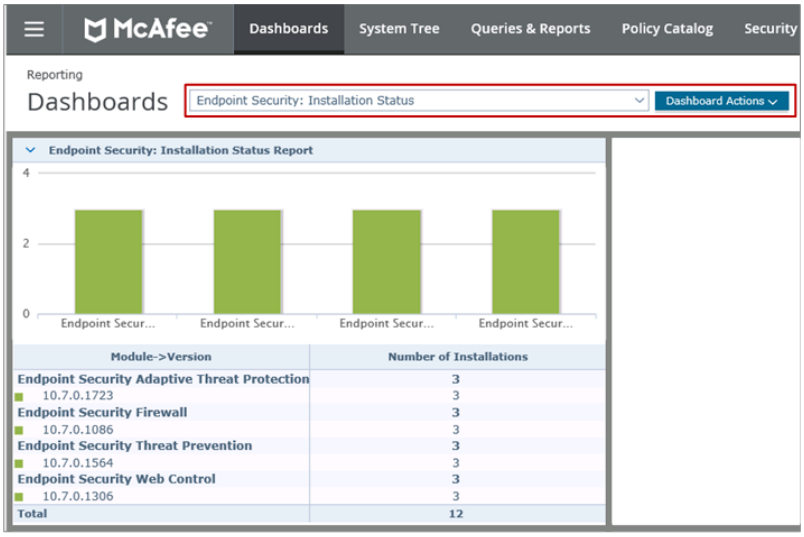
Product deployment tasks are the simplest type of task to set up.

Task

1. In McAfee ePO, select Menu → Software → Product Deployment.
2. On the Product Deployment page, click New Deployment.
3. On the New Deployment page:
   a. Enter a name for the deployment.
   b. Select each module you want to deploy from the Package drop-down list, clicking + Add another package each time you want to select another one.
      Endpoint Security Platform is required for other modules to be installed.
   c. Select the endpoints to deploy to.
   d. Configure any other settings, then click Save at the top of the page.
      The Product Deployment page opens with your new project added to the list of deployments. Also, a client task is automatically created with the deployment settings.
4. Check the status of the deployment on the Product Deployment page.
   From the list on the left side of the page, click the deployment task to display its details.

Results

To verify that Endpoint Security installed on your endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that version 10.7.xxxx is installed on the correct number of endpoints.



Using Endpoint Upgrade Assistant

You can use Endpoint Upgrade Assistant to upgrade other McAfee products when you upgrade to Endpoint Security 10.7.x. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x. You can also upgrade from legacy products like VirusScan Enterprise.

Endpoint Upgrade Assistant detects McAfee products in your environment and determines the minimum version needed to remain compatible with Endpoint Security 10.7.x, then lets you upgrade all of them with a single deployment task.

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that products installed on endpoints are supported.
   - Verify that you're aware of compatibility requirements for other installed products.
   - Get your grant number in the email from McAfee that confirmed your subscription. You need your grant number and this email address to download software.
   - Check for and install a new version of Endpoint Upgrade Assistant.
   - Check in the latest version of the McAfee Agent installation package to the McAfee ePO branch you plan to deploy upgrades from.
   - Download the latest version of McAfee SysPrep from McAfee Product Downloads, if one is available, and check it in to the McAfee ePO branch you plan to deploy upgrades from. Endpoint Upgrade Assistant runs McAfee SysPrep during upgrades to detect and allow trusted third-party software injectors.
     Note: Best practice: Use the latest version of the McAfee SysPrep utility when upgrading from version 10.5.3 or earlier, or when new software or policy configurations are used in software metering, software monitoring, or rights management. Check with technical support for the latest version of McAfee SysPrep.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   - Verify that endpoint users have permission to access the user temp folder (KB85033).
   - Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
   - If you plan to save custom product settings, review your settings, client tasks, and assignments, consolidating them where possible. Remove duplicates and unused objects.
   - If you're upgrading legacy products, such as VirusScan Enterprise, and want to save your custom product settings, install the Endpoint Migration Assistant.
2. Upgrade product extensions and installation packages on McAfee ePO.
3. Update content files on McAfee ePO.
4. Resolve issues blocking analysis.
5. Deploy products that Endpoint Upgrade Assistant cannot upgrade.
6. Deploy product software to endpoints.
7. After the installation:
   a. If you saved your custom product settings, verify that settings you configured in the previous version work as expected.
   b. Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   c. If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   d. Review the policy settings that are new or changed in Endpoint Security 10.7.x.

Upgrade product extensions and installation packages

When using Endpoint Upgrade Assistant to upgrade to McAfee Endpoint Security 10.7.x, you need to upgrade the product extensions and installation packages on the McAfee ePO server. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

The product extensions manage policies and tasks on the McAfee ePO server and the installation packages install Endpoint Security on your endpoints. You can retrieve them through McAfee ePO or from the McAfee Product Downloads site. When you check in the installation packages, you need to choose the repository branch where to store them.

Task

1. In McAfee ePO, select Menu → Software → Software Catalog (Software Manager on version 5.9.x).
2. From the Category list, expand Endpoint Security, then click Bundles.
3. In the right pane, select the bundle that suits your environment:

Bundle name	What's included
McAfee Endpoint Security	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Client Proxy
McAfee Endpoint Security Adaptive Threat Protection	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Adaptive Threat Protection ◦ Client Proxy

4. From the Actions column, click Check In All.
5. Select the checkbox to accept the license agreement.
6. Select the branch where to check in the installation packages, then select Check In.

Results

When check-in is complete, the product extensions are listed on the Extensions page and the installation packages are listed in the Master Repository. Based on the bundle installed, you can view the respective extensions and packages in these locations.

Update content files

Make sure that the latest content files for antimalware and exploit prevention are updated on the McAfee ePO server as part of any installation. Content files are released regularly to protect against the latest known threats.

McAfee releases new Adaptive Threat Protection Rules for ATP in AMCore content.

Task

1. In McAfee ePO, select Menu → Automation → Server Tasks.
2. Edit the Update Master Repository server task.
3. Click the Actions tab.
4. For the Repository Pull action, make sure that the following are set:
   - Source site: McAfeeHttp
   - Package types: All packages
5. Click Save.
6. For the Update Master Repository server task, click Run.

Results

The Master Repository includes the AMCore Content Package and the Endpoint Security Exploit Prevention Content Package, which are required by Endpoint Security.

Resolve issues blocking analysis

To see a full picture of environmental readiness, resolve issues that are blocking endpoints from being analyzed for their upgrade needs by Endpoint Upgrade Assistant.

Blocked endpoints are categorized as unmanaged, incompatible, or excluded. Endpoints can appear in multiple categories.

- Unmanaged endpoints must be put under management before being analyzed.
- Incompatible endpoints have issues related to hardware, memory, or operating system compatibility that block the analysis.
- Currently excluded endpoints have McAfee products installed on them that the tool does not support.

You can tag endpoints that require the same solution, then deploy products using a deployment task in McAfee ePO.

Exporting the analysis details allows you to search, sort, and filter the information more readily; for example, to identify endpoints that need client properties updated (which requires refreshing the McAfee ePO database).

Task

1. In McAfee ePO, select Menu → Software → Endpoint Upgrade Assistant.
2. Analyze upgrade requirements for your environment.
   a. Select McAfee Endpoint Security 10.7.x as the version to upgrade to.
   b. Select the endpoints to analyze. The time required to analyze your selection depends on the size of the McAfee ePO database and the number of endpoints selected.
   c. Click Analyze Environment.

   When the analysis is done, you can view it in the Environment Overview chart.
3. To see endpoints that can't be analyzed, check Blocked from upgrading on the Overview tab.
   Endpoints with similar issues are grouped, so that you can tag them. Each time you tag a group of endpoints, Endpoint Upgrade Assistant creates a tag called UA_<timestamp> in the McAfee ePO Tag Catalog.
4. To resolve the problems, click More Info to display details about the blocked endpoints, then follow these steps:

For this type of endpoint...	When this issue is present...	Do this...
Unmanaged	McAfee Agent is not installed.	Install a supported version.
Unmanaged	An unsupported version of McAfee Agent is installed.	Install a supported version.
Unmanaged	McAfee Agent is not in managed mode.	Enable managed mode.
Incompatible	Hardware, memory, or operating system does not meet minimum requirements.	Upgrade system components as needed.
Excluded	Products that the tool doesn't support.	Deploy those products outside of the tool.

5. Click Re-Analyze Environment.
   Endpoints that are no longer blocked are moved to one of the other tables.

Results

Once all endpoints have been analyzed, you can install other products that are required before upgrading to Endpoint Security 10.7.x.

Deploy products that cannot be upgraded

Because some McAfee products cannot be upgraded using Endpoint Upgrade Assistant, you need to upgrade them using another deployment method like deployment tasks in McAfee ePO.

You can tag endpoints that require the same solution, then deploy products using a deployment task in McAfee ePO.

Exporting the analysis details allows you to search, sort, and filter the information more readily; for example, to identify endpoints that need client properties updated (which requires refreshing the McAfee ePO database).

You can also view endpoints that require specific products and versions in the McAfee ePO System Tree and link to technical articles, when available.

Task

1. In McAfee ePO, select Menu → Software → Endpoint Upgrade Assistant.
2. Analyze upgrade requirements for your environment.
   a. Select McAfee Endpoint Security 10.7.x as the version to upgrade to.
   b. Select the endpoints to analyze. The time required to analyze your selection depends on the size of the McAfee ePO database and the number of endpoints selected.

c. Click Analyze Environment.

When the analysis is done, you can view it in the Environment Overview chart.

3. To see endpoints that you need to upgrade using McAfee ePO, check Require product upgrades on the Overview tab.
   Endpoints with similar issues are grouped, so that you can tag them. Each time you tag a group of endpoints, Endpoint Upgrade Assistant creates a tag called UA_<timestamp> in the McAfee ePO Tag Catalog.
4. Click More Info to display the steps required to complete each manual upgrade, including the product versions and number of restarts required.
5. (Optional) Click Product versions to display product details for the endpoints.
6. In McAfee ePO, create a deployment task to deploy the required client software to a group of endpoints, selecting the tag that you created in step 2.
7. When the required manual upgrades are complete, click Re-Analyze Environment.
   Endpoints that no longer require manual tasks are moved to the Ready for Upgrade Automation table.
8. Repeat these steps until no endpoints require manual product upgrades.

Results

Once endpoints are ready to upgrade, you can deploy Endpoint Security 10.7.x and other required software to endpoints.

Deploy product software to endpoints

When endpoints meet the requirements for upgrading, create a deployment task in Endpoint Upgrade Assistant to deploy Endpoint Security 10.7.x with other required McAfee products. Endpoint Upgrade Assistant creates a task using the McAfee ePO branch and product options that you selected on the Prepare and Overview tabs.

This method deploys the installation packages to all endpoints that are ready to upgrade.

Exporting the analysis details allows you to search, sort, and filter the information more readily; for example, to identify endpoints that need client properties updated (which requires refreshing the McAfee ePO database).

Task

1. In McAfee ePO, select Menu → Software → Endpoint Upgrade Assistant.
2. Analyze upgrade requirements for your environment.
   a. Select McAfee Endpoint Security 10.7.x as the version to upgrade to.
   b. Select the endpoints to analyze. The time required to analyze your selection depends on the size of the McAfee ePO database and the number of endpoints selected.
   c. Click Analyze Environment.

   When the analysis is done, you can view it in the Environment Overview chart.
3. To see the endpoints that Endpoint Upgrade Assistant can upgrade, check Ready for Upgrade Automation on the Overview tab.
4. Specify whether to upgrade compatible versions of McAfee Agent installed on endpoints.
5. To select the installation packages to deploy, click the Prepare tab, then select them.
   a. If you are upgrading legacy products, follow instructions in the Policy Migration section to migrate or convert custom settings that you want to save.
      - To migrate settings — Click Endpoint Migration Assistant to run Migration Assistant, which guides you through the process of migrating your policy settings. If you haven't installed Migration Assistant, install and run it now. If you've already migrated your settings, you can skip this step.
      - To convert other product settings — Click the link to the technical article for instructions.

   b. In the Packages Required for Upgrade Automation section, select the McAfee ePO branch to deploy the upgrade from.
   c. For each installation package listed, resolve issues that are highlighted in red under the Notes section.
      - Select product version to install — If multiple versions are checked in to the selected McAfee ePO branch, select the version you want.
        - To install a product — Select the version from the drop-down list.
        - To install an Endpoint Security update — Select the Hotfix number from the drop-down list.
        - To take no action on a product — Select Do not install or Do not upgrade.
      - Incompatible versions of this product were detected — Select a compatible version to upgrade to.

   d. If product extensions are required, install them on the McAfee ePO server.
   e. Click Refresh to confirm that your server is up to date.

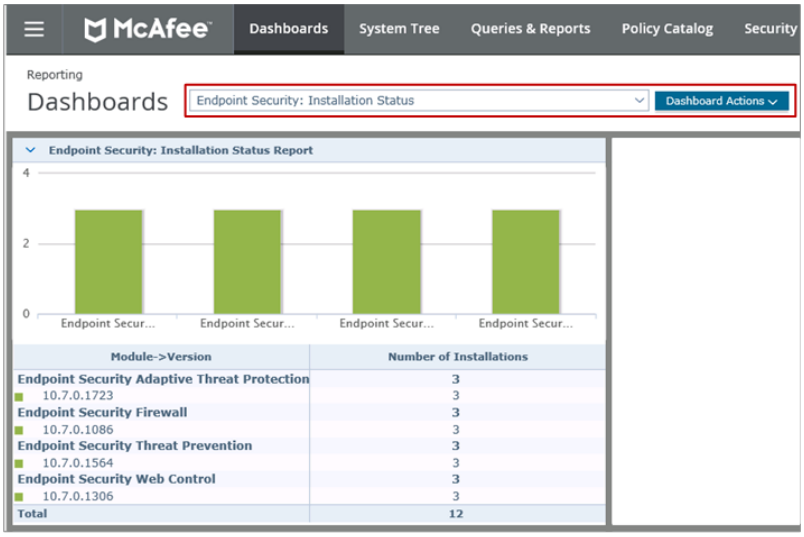
This refreshes only the information on the Prepare tab without fully re-analyzing your selected environment.

f. Repeat substeps c-e until all required software is checked in.
Best practice: If you plan to deploy upgrades using McAfee ePO, click Copy Command Line to copy the command-line options, then paste them into the product deployment task.

6. On the Deploy & Track tab, click Create Deployment Task.
   a. On the Create Deployment Task page, specify a name for the task.
   The branch and product options that you selected on the Prepare and Overview tabs appear. If you want to change them, cancel this task, select the correct settings on those tabs, then begin this step again.
   b. For Policy Migration, select the checkbox to acknowledge that one of the following is true:
      - You have migrated your legacy custom policies and client tasks that you want to save.
      - You want McAfee Default policy settings to be enforced.
      - You aren't migrating your settings.
   c. Specify when to run the deployment task.
   d. Select the endpoints to upgrade.
   By default, both workstations and servers are upgraded. To change this, you can select individual endpoints from a list.
   e. Click Create, verify that the information for the task is correct, then click OK.
7. On the Deploy & Track tab, under Deployment Status, verify that the deployment task completed successfully.

Results

To verify that Endpoint Security installed on your endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that version 10.7.xxxx is installed on the correct number of endpoints.



Using a third-party tool

You can use a third-party deployment tool like Microsoft System Center Configuration Manager, IBM BigFix, or Tanium Deploy to upgrade to McAfee Endpoint Security 10.7.x on your endpoints with a command line. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

You can retrieve the installation packages from the McAfee Product Downloads site using a valid grant number.

This method lets you install Endpoint Security using the same tool and automated processes that you use to install other products in your environment.

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that products installed on endpoints are supported.
   - Verify that you're aware of compatibility requirements for other installed products.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.

- Get your grant number in the email from McAfee that confirmed your subscription. You need your grant number and this email address to download software.
- Have this information ready for deployment: a descriptive name for the deployment task, the file name for the installer, and the command line to run the deployment (for example, `setupEP.exe ADDLOCAL="tp,atp,fw,wc"`).
- Verify that endpoint users have permission to access the user temp folder (KB85033).
- Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).

  Note: Best practice: Use the latest version of the McAfee SysPrep utility when upgrading from version 10.5.3 or earlier, or when new software or policy configurations are used in software metering, software monitoring, or rights management. Check with technical support for the latest version of McAfee SysPrep.
- Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
- If you plan to save custom product settings, review your settings, client tasks, and assignments, consolidating them where possible. Remove duplicates and unused objects.

2. Upgrade product extensions on McAfee ePO.
3. Update content files on McAfee ePO.
4. Download installation packages.
5. Deploy product software to endpoints.
6. After the installation:
   - If you saved your custom product settings, verify that settings you configured in the previous version work as expected.
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   - Review the policy settings that are new or changed in Endpoint Security 10.7.x.

Upgrade product extensions

When using a third-party tool to upgrade to McAfee Endpoint Security 10.7.x, you need to upgrade the product extensions on the McAfee ePO server. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

The product extensions manage policies and tasks on the McAfee ePO server. You can retrieve them through McAfee ePO or from the McAfee Product Downloads site.

Task

1. In McAfee ePO, select Menu → Software → Software Catalog (Software Manager on version 5.9.x).
2. From the Category list, expand Endpoint Security, then click Extensions.
3. In the right pane, select the bundle that suits your environment:

Bundle name	What's included
McAfee Endpoint Security	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Client Proxy
McAfee Endpoint Security Adaptive Threat Protection	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Adaptive Threat Protection ◦ Client Proxy

4. From the Actions column, click Check In All.
5. Select the checkbox to accept the license agreement.
6. Click Check In.

Results

When check-in is complete, the product extensions are listed on the Extensions page.

Update content files

Make sure that the latest content files for antimalware and exploit prevention are updated on the McAfee ePO server as part of any installation. Content files are released regularly to protect against the latest known threats.

McAfee releases new Adaptive Threat Protection Rules for ATP in AMCore content.

Task

1. In McAfee ePO, select Menu → Automation → Server Tasks.
2. Edit the Update Master Repository server task.
3. Click the Actions tab.
4. For the Repository Pull action, make sure that the following are set:
   - Source site: McAfeeHttp
   - Package types: All packages
5. Click Save.
6. For the Update Master Repository server task, click Run.

Results

The Master Repository includes the AMCore Content Package and the Endpoint Security Exploit Prevention Content Package, which are required by Endpoint Security.

Download installation packages

To upgrade to Endpoint Security 10.7.x using a third-party deployment tool, you must download the installation packages from the McAfee Product Downloads site. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

The installation packages install Endpoint Security on your endpoints. You can retrieve the installation packages from the McAfee Product Downloads site using a valid grant number.

Task

1. Go to McAfee Product Downloads.
2. Enter the grant number and email address associated with the product, then click Submit.
   The My Products page displays information about your licensed products.
3. In the Find Products section under Filters, select Endpoint Security for the Category.
   A table displays your licensed Endpoint Security products.
4. Navigate through the table to locate and select McAfee Endpoint Security.
   A table displays all the product files that are available to download.
5. In the Available Downloads section, under Filters, select Installation for the Type.
   The table displays information about each downloadable installation package, including the release date, file size, and notes.
6. Select the Endpoint Security Standalone Install package, version 10.7.x.xxxx.
7. In Windows, move the downloaded installation packages to a location that your deployment tool can access, then expand the compressed folder.

Results

The installation packages are ready to deploy to your endpoints.

Deploy product software to endpoints

Upgrade to McAfee Endpoint Security 10.7.x on multiple endpoints using the installation packages and a third-party deployment tool. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

These steps vary depending on the tool. See the documentation for your third-party deployment tool for specific deployment details.

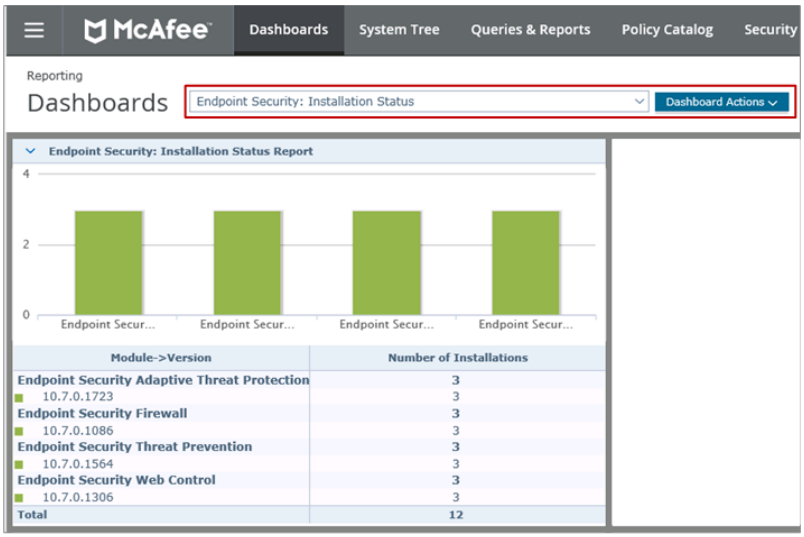
Task

1. Follow the steps required in your tool for creating an application to deploy and install the software on your endpoints, then specify the installation packages to deploy.
   You need to manually select the installation packages that you downloaded for the product modules.
2. Enter a command line for installing the product.
   For the installation command line, enter `setupEP.exe` with the options required for your environment.

   Best practice: Use `setupEP.exe ADDLOCAL="tp,atp,fw,wc"` to install all the product modules on endpoints without displaying notifications or interrupting user activity.
3. Specify the information and options required for your environment.
   These vary depending on your tool. Some examples might be:
   - **To detect whether the product needs to be installed** — Specify a detection method for determining whether the product is already installed, such as a file, a registry key, or an .msi product code. For example, Endpoint Security 10.7.x doesn't need to be deployed to systems where the HKEY_LOCAL_MACHINE registry key SOFTWARE\McAfee\Endpoint\AV includes a value for ProductVersion that is equal to 10.7.x.
   - **To configure the user experience** — Specify options for running the installer on the endpoint (for example, whether users need to be logged on, whether installation is hidden, and estimated and maximum installation times).
   - **To check whether other required products need to be upgraded** — Specify any dependencies for required products and versions. For example, if you specify McAfee Agent version 5.6.x and an earlier version is installed, it will be upgraded before Endpoint Security 10.7 is installed.

Results

To verify that Endpoint Security installed on your endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that version 10.7.xxxx is installed on the correct number of endpoints.



Using MVISION ePO

You can create a deployment link in McAfee MVISION ePO to upgrade to Endpoint Security 10.7.x on your own endpoint, then send it to users so they can upgrade their endpoints. The link downloads and installs the software on each endpoint. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

When you use MVISION ePO to install Endpoint Security, users can initiate the installation on their endpoints when it's convenient.

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that products installed on endpoints are supported.
   - Verify that you're aware of compatibility requirements for other installed products.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.

- Verify that endpoint users have permission to access the user temp folder (KB85033).
- Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).
- Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
- If you plan to save custom product settings, review your settings, client tasks, and assignments, consolidating them where possible. Remove duplicates and unused objects.

2. Deploy product software to endpoints.
3. After the installation:
   - If you saved your custom product settings, verify that settings you configured in the previous version work as expected.
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   - Review the policy settings that are new or changed in Endpoint Security 10.7.x.

Deploy product software to endpoints

To upgrade to Endpoint Security 10.7.x on endpoints managed by McAfee MVISION ePO, you need to generate a deployment link that can be used to download and install the new version of the product on your endpoints. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

Task

1. In MVISION ePO, select Menu → Software → Product Deployment to open the Install Products page.
2. Edit the Group Name value as needed.
3. Select an operating system from the Platform drop-down list.
4. Select Endpoint Protection Software options, then keep the defaults or select the products to include.
5. Under Advanced Options, select Software is automatically updated to the latest version.
6. Click Done to open the Install Protection on Other Computers dialog box.
   - To install on your endpoint, click Download Installer.
   - To create a deployment link for users:
     - Click Copy URL to Clipboard.
     - Send the deployment link to your users, along with instructions for using it to install Endpoint Security on their endpoints.
     - To install on an endpoint, open the email that contains the deployment link, then click that link or enter it in a browser window.

Results

To verify that users have installed Endpoint Security on each endpoint, select Menu → Systems → System Tree, click Systems, then for each endpoint you sent the URL to confirm that the Endpoint Security 10.7 modules are listed on the Product tab (for example, Endpoint Security Threat Prevention 10.7.x.xxxx.x).

On self-managed endpoints

Upgrade to McAfee Endpoint Security 10.7.x on endpoints that aren't managed by a network management platform. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

1. Before the installation:
   - Verify that the endpoint meets the minimum requirements (KB82761), installed products are supported (Supported upgrade paths), and you're aware of compatibility requirements (How the installer handles other installed products).
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   - Verify that you have permission to access the user temp folder (KB85033).
   - Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
   - Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).

Note: Best practice: Use the latest version of the McAfee SysPrep utility when upgrading from version 10.5.3 or earlier, or when new software or policy configurations are used in software metering, software monitoring, or rights management. Check with technical support for the latest version of McAfee SysPrep.

- If you plan to save your product settings, check that they're set up correctly and up to date.

2. Run product installer on endpoint.
3. After the installation:
   - Manually update your endpoint with the latest version of the content files required by Endpoint Security for AMCore, Exploit Prevention, and Adaptive Threat Protection.
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   - Review the product settings that are new or changed in Endpoint Security 10.7.x.

Run the product installer

On a self-managed endpoint, running the product installer on the endpoint is the simplest way to upgrade to McAfee Endpoint Security 10.7.x. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

Task

1. Download the Endpoint Security .zip file, unzip the contents of the file, then double-click `setupEP.exe`.
   If you purchase the product online, you receive an email with instructions and a URL for downloading the product.
2. On the License Agreement page, click Accept.
3. Resolve any conflicts detected by the installer.
   The installer tries to remove conflicting virus-detection and firewall software products automatically. If it can't, it prompts you to remove them manually, then prompts you to restart the endpoint.
   - If you restart the endpoint immediately, installation resumes afterward.
   - If you restart the endpoint later, run the installer again at your earliest convenience.
4. On the Install Options page, select the product modules to upgrade.
   As a best practice, we recommend that you upgrade all product modules to the version 10.7.x.
   Endpoint Security Platform (the Common module) installs automatically with the first module you install.
5. Select whether to save your settings.
6. Click Install.
   A dialog box shows the progress of the installation and notifies you when it is complete. You can cancel the installation at any time, if needed.
7. Click Finish to close the installer.
   As a best practice, we recommend restarting the endpoint after the upgrade completes.

Results

To verify that Endpoint Security installed on the endpoint, open the Windows Control Panel and check that version 10.7.x of each product module you selected to install appears. You can also check that no errors or failure messages appear in the installation log file.

Install version 10.7.x for the first time

You can use multiple deployment methods to install McAfee Endpoint Security 10.7.x on your endpoints.

The method you choose for deploying the product software to endpoints depends on not only your environment and your goals for the installation, but also your preferences and department policies for tools.

Deciding which deployment method to use

Using third-party tool?	Using McAfee ePO?	Use this method
Yes		• IBM BigFix • Microsoft System Center Configuration Manager (SCCM) • Tanium Deploy
No	Yes	• McAfee ePO 5.10.x or McAfee ePO 5.9.x • McAfee MVISION ePO
No	No	Product installer (SetupEP)

Using McAfee ePO 5.10.x–5.9.x

You can use a deployment task in McAfee ePO 5.10.x or 5.9.x to install Endpoint Security 10.7.x on your endpoints.

Deployment tasks can be set up as continuous (for endpoints in specific groups or with specific tags) or fixed (for a static set of endpoints).

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that you're aware of compatibility requirements for other installed products.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   - Verify that endpoint users have permission to access the user temp folder (KB85033).
   - Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).
   - Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
2. Install product extensions and installation packages on McAfee ePO.
3. Update content files on McAfee ePO.
4. Deploy product software to endpoints.
5. After the installation:
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   - Configure your policy settings for your environment, as needed.

Install product extensions and installation packages

When using McAfee ePO 5.10.x or 5.9.x to install McAfee Endpoint Security 10.7.x, you need to install the product extensions and installation packages on the McAfee ePO server.

The product extensions manage policies and tasks on the McAfee ePO server and the installation packages install Endpoint Security on your endpoints. You can retrieve them through McAfee ePO or from the McAfee Product Downloads site. When you check in the installation packages, you need to choose the repository branch where to store them.

Task

1. In McAfee ePO, select Menu → Software → Software Catalog (Software Manager on version 5.9.x).
2. From the Category list, expand Endpoint Security, then click Bundles.
3. In the right pane, select the bundle that suits your environment:

Bundle name	What's included
McAfee Endpoint Security	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Client Proxy
McAfee Endpoint Security Adaptive Threat Protection	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Adaptive Threat Protection ◦ Client Proxy

4. From the Actions column, click Check In All.
5. Select the checkbox to accept the license agreement.
6. Select the branch where to check in the installation packages, then select Check In.

Results

When check-in is complete, the product extensions are listed on the Extensions page and the installation packages are listed in the Master Repository. Based on the bundle installed, you can view the respective extensions and packages in these locations.

Update content files

Make sure that the latest content files for antimalware and exploit prevention are updated on the McAfee ePO server as part of any installation. Content files are released regularly to protect against the latest known threats.

McAfee releases new Adaptive Threat Protection Rules for ATP in AMCore content.

Task

1. In McAfee ePO, select Menu → Automation → Server Tasks.
2. Edit the Update Master Repository server task.
3. Click the Actions tab.
4. For the Repository Pull action, make sure that the following are set:
   - Source site: McAfeeHttp
   - Package types: All packages
5. Click Save.
6. For the Update Master Repository server task, click Run.

Results

The Master Repository includes the AMCore Content Package and the Endpoint Security Exploit Prevention Content Package, which are required by Endpoint Security.

Deploy product software to endpoints

You can use a product deployment task in McAfee ePO 5.10.x or 5.9.x to install McAfee Endpoint Security 10.7.x on multiple endpoints.

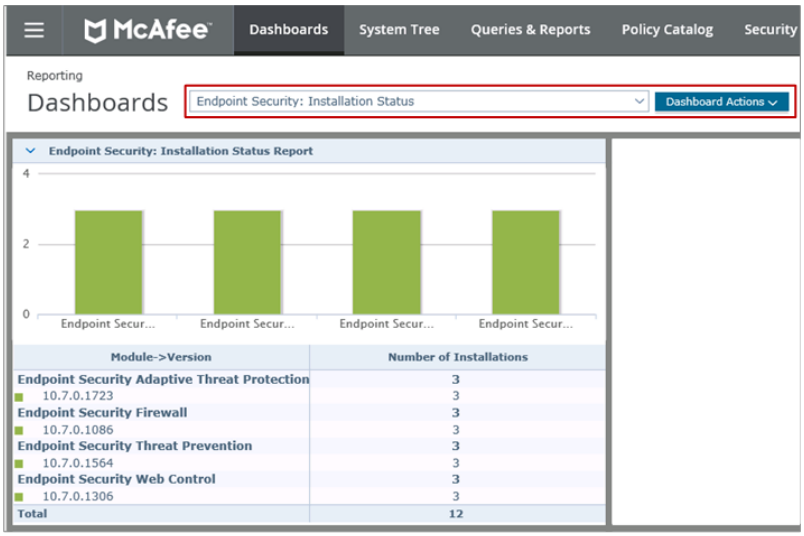
Product deployment tasks are the simplest type of task to set up.

Task

1. In McAfee ePO, select Menu → Software → Product Deployment.
2. On the Product Deployment page, click New Deployment.
3. On the New Deployment page:
   a. Enter a name for the deployment.
   b. Select each module you want to deploy from the Package drop-down list, clicking + Add another package each time you want to select another one.
      Endpoint Security Platform is required for other modules to be installed.
   c. Select the endpoints to deploy to.
   d. Configure any other settings, then click Save at the top of the page.
      The Product Deployment page opens with your new project added to the list of deployments. Also, a client task is automatically created with the deployment settings.
4. Check the status of the deployment on the Product Deployment page.
   From the list on the left side of the page, click the deployment task to display its details.

Results

To verify that Endpoint Security installed on your endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that version 10.7.xxxx is installed on the correct number of endpoints.



Using a third-party tool

You can use a third-party deployment tool like Microsoft System Center Configuration Manager, IBM BigFix, or Tanium Deploy to install McAfee Endpoint Security 10.7.x on your endpoints with a command line.

You can retrieve the installation packages from the McAfee Product Downloads site using a valid grant number.

This method lets you install Endpoint Security using the same tool and automated processes that you use to install other products in your environment.

1. Before the installation:
   a. Verify that all endpoints meet the minimum requirements (KB82761).
   b. Verify that you're aware of compatibility requirements for other installed products.
   c. Get your grant number in the email from McAfee that confirmed your subscription. You need your grant number and this email address to download software.
   d. Have this information ready for deployment: a descriptive name for the deployment task, the file name for the installer, and the command line to run the deployment (for example, `setupEP.exe ADDLOCAL="tp,atp,fw,wc"`).
   e. On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   f. Verify that endpoint users have permission to access the user temp folder (KB85033).

g. Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).
h. Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
2. Install product extensions on McAfee ePO.
3. Update content files on McAfee ePO.
4. Download installation packages.
5. Deploy product software to endpoints.
6. After the installation:
   a. Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   b. If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   c. Configure your policy settings for your environment, as needed.

Install product extensions

When using a third-party tool to install McAfee Endpoint Security 10.7.x, you need to install the product extensions on the McAfee ePO server.

The product extensions manage policies and tasks on the McAfee ePO server. You can retrieve them through McAfee ePO or from the McAfee Product Downloads site.

Task

1. In McAfee ePO, select Menu → Software → Software Catalog (Software Manager on version 5.9.x).
2. From the Category list, expand Endpoint Security, then click Extensions.
3. In the right pane, select the bundle that suits your environment:

Bundle name	What's included
McAfee Endpoint Security	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Client Proxy
McAfee Endpoint Security Adaptive Threat Protection	◦ Endpoint Security Platform ◦ Threat Prevention ◦ Firewall ◦ Web Control ◦ Adaptive Threat Protection ◦ Client Proxy

4. From the Actions column, click Check In All.
5. Select the checkbox to accept the license agreement.
6. Click Check In.

Results

When check-in is complete, the product extensions are listed on the Extensions page.

Update content files

Make sure that the latest content files for antimalware and exploit prevention are updated on the McAfee ePO server as part of any installation. Content files are released regularly to protect against the latest known threats.

McAfee releases new Adaptive Threat Protection Rules for ATP in AMCore content.

Task

1. In McAfee ePO, select Menu → Automation → Server Tasks.

2. Edit the Update Master Repository server task.
3. Click the Actions tab.
4. For the Repository Pull action, make sure that the following are set:
   - Source site: McAfeeHttp
   - Package types: All packages
5. Click Save.
6. For the Update Master Repository server task, click Run.

Results

The Master Repository includes the AMCore Content Package and the Endpoint Security Exploit Prevention Content Package, which are required by Endpoint Security.

Download installation packages

To install Endpoint Security 10.7.x using a third-party deployment tool, you must download the installation packages from the McAfee Product Downloads site.

The installation packages install Endpoint Security on your endpoints. You can retrieve the installation packages from the McAfee Product Downloads site using a valid grant number.

Task

1. Go to McAfee Product Downloads.
2. Enter the grant number and email address associated with the product, then click Submit.
   The My Products page displays information about your licensed products.
3. In the Find Products section under Filters, select Endpoint Security for the Category.
   A table displays your licensed Endpoint Security products.
4. Navigate through the table to locate and select McAfee Endpoint Security.
   A table displays all the product files that are available to download.
5. In the Available Downloads section, under Filters, select Installation for the Type.
   The table displays information about each downloadable installation package, including the release date, file size, and notes.
6. Select the Endpoint Security Standalone Install package, version 10.7.x.xxxx.
7. In Windows, move the downloaded installation packages to a location that your deployment tool can access, then expand the compressed folder.

Results

The installation packages are ready to deploy to your endpoints.

Deploy product software to endpoints

Install McAfee Endpoint Security 10.7.x on multiple endpoints using the installation packages and a third-party deployment tool.

These steps vary depending on the tool. See the documentation for your third-party deployment tool for specific deployment details.

Task

1. Follow the steps required in your tool for creating an application to deploy and install the software on your endpoints, then specify the installation packages to deploy.
   You need to manually select the installation packages that you downloaded for the product modules.
2. Enter a command line for installing the product.
   For the installation command line, enter `setupEP.exe` with the options required for your environment.

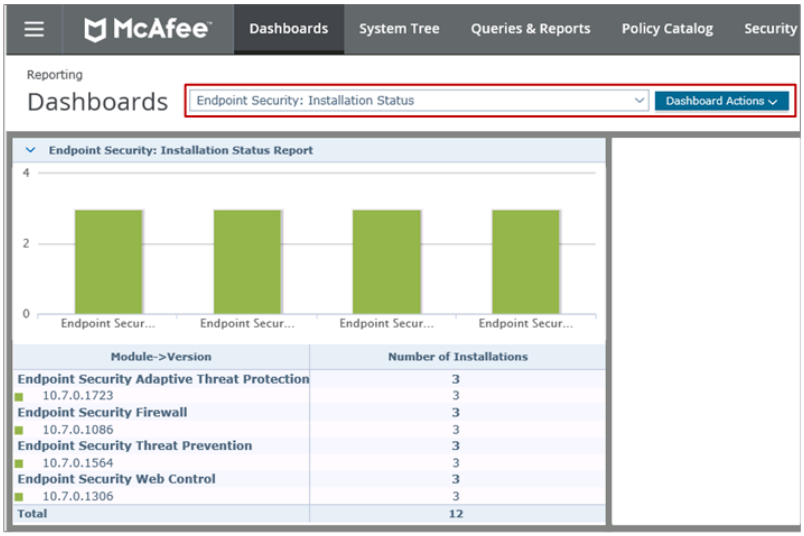
   Best practice: Use `setupEP.exe ADDLOCAL="tp,atp,fw,wc"` to install all the product modules on endpoints without displaying notifications or interrupting user activity.
3. Specify the information and options required for your environment.
   These vary depending on your tool. Some examples might be:
   - **To detect whether the product needs to be installed** — Specify a detection method for determining whether the product is already installed, such as a file, a registry key, or an .msi product code. For example, Endpoint Security 10.7.x doesn't need

to be deployed to systems where the HKEY_LOCAL_MACHINE registry key SOFTWARE\McAfee\Endpoint\AV includes a value for ProductVersion that is equal to 10.7.x.

- **To configure the user experience** — Specify options for running the installer on the endpoint (for example, whether users need to be logged on, whether installation is hidden, and estimated and maximum installation times).
- **To check whether other required products need to be upgraded** — Specify any dependencies for required products and versions. For example, if you specify McAfee Agent version 5.6.x and an earlier version is installed, it will be upgraded before Endpoint Security 10.7 is installed.

Results

To verify that Endpoint Security installed on your endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that version 10.7.xxxx is installed on the correct number of endpoints.



Using MVISION ePO

You can create a deployment link in McAfee MVISION ePO to install Endpoint Security 10.7.x on your own endpoint, then send it to users so they can install it on their endpoints The link downloads and installs the software on each endpoint.

When you use MVISION ePO to install Endpoint Security, users can initiate the installation on their endpoints when it's convenient.

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that you're aware of compatibility requirements for other installed products.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   - Verify that endpoint users have permission to access the user temp folder (KB85033).
   - Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).
   - Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
2. Deploy product software to endpoints.
3. After the installation:
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - Configure your policy settings for your environment, as needed.

Deploy product software to endpoints

To install Endpoint Security 10.7.x on endpoints managed by McAfee MVISION ePO, you need to generate a deployment link that can be used to download and install the product on your endpoints.

Task

1. In MVISION ePO, select Menu → Software → Product Deployment to open the Install Products page.
2. Edit the Group Name value as needed.
3. Select an operating system from the Platform drop-down list.
4. Select Endpoint Protection Software options, then keep the defaults or select the products to include.
5. Under Advanced Options, select Software is automatically updated to the latest version.
6. Click Done to open the Install Protection on Other Computers dialog box.
   - To install on your endpoint, click Download Installer.
   - To create a deployment link for users:
     - Click Copy URL to Clipboard.
     - Send the deployment link to your users, along with instructions for using it to install Endpoint Security on their endpoints.
     - To install on an endpoint, open the email that contains the deployment link, then click that link or enter it in a browser window.

Results

To verify that users have installed Endpoint Security on each endpoint, select Menu → Systems → System Tree, click Systems, then for each endpoint you sent the URL to confirm that the Endpoint Security 10.7 modules are listed on the Product tab (for example, Endpoint Security Threat Prevention 10.7.x.xxxx.x).

On self-managed endpoints

Install McAfee Endpoint Security 10.7.x on endpoints that aren't managed by a network management platform.

1. Before the installation:
   - Verify that all endpoints meet the minimum requirements (KB82761).
   - Verify that you're aware of compatibility requirements for other installed products.
   - On endpoints running Microsoft Windows 10 October 2018 Update or later, verify that the case-sensitivity attribute is disabled for folders in your source and target installation paths and \Windows\System32\drivers.
   - Verify that you have permission to access the user temp folder (KB85033).
   - Provide accurate reputation values to McAfee Global Threat Intelligence by running McAfee GetClean (KB73044).
   - Detect and allow trusted third-party software to make sure that they work with Endpoint Security by running McAfee SysPrep (KB89860).

     Note: Best practice: Use the latest version of the McAfee SysPrep utility when upgrading from version 10.5.3 or earlier, or when new software or policy configurations are used in software metering, software monitoring, or rights management. Check with technical support for the latest version of McAfee SysPrep.
2. Run product installer on endpoint.
3. After the installation:
   - Manually update your endpoint with the latest version of the content files required by Endpoint Security for AMCore, Exploit Prevention, and Adaptive Threat Protection.
   - Disable the Windows firewall to avoid conflicts with Endpoint Security Firewall rules.
   - If third-party applications aren't working correctly after you install Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules, temporarily enable Adaptive Mode.
   - Configure your settings as needed.

Run the product installer

On a self-managed endpoint, running the product installer on the endpoint is the simplest way to install McAfee Endpoint Security 10.7.x.

Task

1. Download the Endpoint Security .zip file, unzip the contents of the file, then double-click `setupEP.exe`.
   If you purchase the product online, you receive an email with instructions and a URL for downloading the product.
2. On the License Agreement page, click Accept.
3. Resolve any conflicts detected by the installer.

The wizard tries to remove conflicting virus-detection and firewall software products automatically. If it can't, it prompts you to remove them manually, then prompts you to restart the endpoint.

- If you restart the endpoint immediately, installation resumes afterward.
- If you restart the endpoint later, run the installer again at your earliest convenience.

4. If you don't want to install all product modules with the default settings, select new settings on the Install Options page.
   Endpoint Security Platform (the Common module) installs automatically with the first module you install.
5. Click Install.
   A dialog box shows the progress of the installation and notifies you when it is complete. You can cancel the installation at any time, if needed.
6. Click Finish to close the installer.
   As a best practice, we recommend restarting the endpoint after the upgrade completes.

Results

To verify that Endpoint Security installed on the endpoint, open the Windows Control Panel and check that version 10.7.x of each product module you selected to install appears. You can also check that no errors or failure messages appear in the installation log file.

Things to know before the installation

What is installed with Endpoint Security 10.7.x

McAfee Endpoint Security 10.7.x is made up of multiple product modules that are installed by default when you install the product bundle.

Endpoint Security includes these modules:

- McAfee® Endpoint Security Threat Prevention
- McAfee® Endpoint Security Firewall
- McAfee® Endpoint Security Web Control
- McAfee® Endpoint Security Adaptive Threat Protection (ATP) — Requires Threat Prevention

Endpoint Security includes these additional components:

- McAfee® Endpoint Security Platform — Installed on the McAfee ePO server and the endpoint before Threat Prevention, Firewall, or Web Control (previously named the Common module).
- McAfee® Threat Detection Reporting — Installed on the McAfee ePO server for use with Adaptive Threat Protection.

McAfee Endpoint Security is available on McAfee ePO in two different bundles. Select the bundle that suits your environment.

Bundle name	Details
McAfee Endpoint Security	• Endpoint Security Platform • Threat Prevention • Firewall • Web Control • Client Proxy
McAfee Endpoint Security Adaptive Threat Protection	• Endpoint Security Platform • Threat Prevention • Firewall • Web Control • Adaptive Threat Protection • Client Proxy

If you are downloading McAfee Endpoint Security from Download portal, then select the required extensions and packages from these products:

Product name	Extensions	Packages
McAfee Endpoint Security	• Endpoint_Security_Platform_*Version*_extension.zip • Firewall_*Version*_extension.zip • Threat_Prevention_*Version*_extension.zip • Web_Control_*Version*_extension.zip	• Endpoint_Security_Platform_*Version*_client.zip • Firewall_*Version*_client.zip • Threat_Prevention_*Version*_client.zip • Web_Control_*Version*_client.zip
McAfee Endpoint Security Adaptive Threat Protection	• Threat_Detection_Reporting_*Version*_extension.zip • Adaptive_Threat_Protection_*Version*_extension.zip	• Adaptive_Threat_Protection_*Version*_client.zip

For optimal performance and protection, install the same version of the Endpoint Security modules.

Supported upgrade paths

When upgrading from Endpoint Security version 10.2.x, 10.5.x, or 10.6.x, or from legacy products like VirusScan Enterprise 8.8, the installer saves your custom settings (if that option is selected), removes the existing product software, and installs Endpoint Security 10.7.x.

If McAfee® MVISION Endpoint is installed, the installer removes the product software before installing Endpoint Security, but does not save product settings.

For optimal performance and protection, upgrade all Endpoint Security modules to the latest version.

You can upgrade these products to Endpoint Security 10.7.x:

- McAfee® Endpoint Security 10.2.x
- McAfee® Endpoint Security 10.5.x
- McAfee® Endpoint Security 10.6.x
- McAfee® VirusScan® Enterprise 8.8
- McAfee® Host Intrustion Prevention (McAfee Host IPS) 8.0
  Note: Host Intrusion Prevention can run alongside Endpoint Security. Whenever McAfee Host IPS Firewall is installed and enabled, Endpoint Security Firewall is disabled, even if enabled in the policy settings.
- McAfee® SiteAdvisor Enterprise 3.5
- McAfee® Endpoint Security Threat Intelligence 10.2

Best practice: If you are moving to Endpoint Security from a legacy product (VirusScan Enterprise, McAfee Host IPS, SIteAdvisor Enterprise, or Threat Intelligence), run the McAfee® Endpoint Upgrade Assistant. With this tool you can also run the Endpoint Migration Assistant, which saves and converts your existing settings to use with Endpoint Security.

Compatibility with other installed products

Before you install McAfee Endpoint Security 10.7.x, check that other products running on your endpoints are compatible. If any products are not compatible, follow instructions to resolve conflicts.

The installer detects existing virus-detection or firewall products on the endpoint, checks for compatibility, and tries to uninstall the software. If it can't, it prompts the user to cancel the installation, uninstall the incompatible software manually from the Windows Control Panel, then resume the installation.

Additionally, these products can affect the installation requirements for Endpoint Security or the way that Endpoint Security features are configured after installation.

If...	Then...
Common Event Enabler (CEE)/Common AntiVirus Agent (CAVA) is running	To install with CAVA support, use the `/CAVA` command-line option. To upgrade a previous version with CAVA, use the command-line option. Otherwise, the upgrade occurs without CAVA.
McAfee® Application Control and McAfee® Change Control are running	Install Endpoint Security first, then Application Control and Change Control. Otherwise, disable the Memory Protection and Script As Updater features in Application Control and Change Control before installing Endpoint Security.
McAfee Client Proxy is installed	Web Control disables itself automatically if it detects a web gateway appliance or if McAfee Client Proxy is installed *and* in redirection mode.

Best practices for setting up your test environment

As part of your planning process, schedule time to thoroughly test the installation on a subset of representative endpoints, to research and resolve any issues discovered, and to verify the results before installing across your environment.

Progressive (test) deployments typically catch issues that you don't want to experience on a wide-scale, mass deployment. For example, you can avoid issues related to specific programs or files in your environment that you might not have considered.

For best results, make sure the test environment represents your production environment as closely as possible. When selecting endpoints for your test environment, identify the variables in your production environment that you need to include and the groups and endpoints that are available for testing.

- Do not include endpoints that are essential to your daily operations.
- Select endpoints that reflect the diversity of your environment.
- To identify representative endpoints for each group and remote location, consider this information:
    - McAfee product combinations and versions
    - Operating systems
    - Servers and workstations
    - Policy settings and exclusions
    - Third-party products
- Test on a subset of servers before upgrading your entire server environment.

Endpoint Upgrade Assistant

McAfee® Endpoint Upgrade Assistant is a tool that assists with upgrading endpoints to the latest version of Endpoint Security. The tool also upgrades other McAfee products at the same time to maintain compatibility.

Administrators can use Endpoint Upgrade Assistant to:

- Analyze endpoints, detect the supported McAfee products that are installed, and determine the minimum requirements for upgrading to Endpoint Security.
- Upgrade older versions of Endpoint Security or legacy products like VirusScan Enterprise to the latest version of Endpoint Security.
- Remove incompatible McAfee products.
- Upgrade incompatible products to recommended versions.
- Prepare, deploy, and track product upgrades throughout the environment.

Endpoint Upgrade Assistant is bundled with McAfee ePO 5.10.x. If you're using McAfee ePO 5.9.x, you need to download it from the McAfee Product Downloads site and install it.

Components

Endpoint Upgrade Assistant includes these components:

- Endpoint Upgrade Assistant product extension — Installed on the McAfee ePO server. Collects and analyzes the data about the environment. Displays the requirements for upgrading and the status of deployment tasks.
- Endpoint Upgrade Automation installation package — Deployed to endpoints along with the installation packages for the products you're upgrading. Manages upgrades on endpoints: removes incompatible versions of existing products, installs compatible versions, and reports deployment status to Endpoint Upgrade Assistant.

When you install the product extension, a copy of the Upgrade Automation installation package is checked in automatically to each McAfee ePO branch. You can deploy upgrades from any branch.

If you need to change the product modules or settings included in the default installation package, you can use the Package Creator tool that is bundled with Endpoint Upgrade Assistant to generate a custom package.

How it works

Endpoint Upgrade Assistant is a tool that analyzes your McAfee ePO environment, reports the information you need to prepare for an upgrade, and deploys and tracks their status.

Analyzing your environment

Endpoint Upgrade Assistant analyzes the McAfee ePO database, determines the software installed on endpoints in your environment, and reports:

- Minimum requirements for upgrading to Endpoint Security.
- Other McAfee products running on endpoints that require an upgrade to maintain compatibility with Endpoint Security.
- Problems that prevent upgrades.

By default, Endpoint Upgrade Assistant runs an analysis automatically in the background when it's installed, then re-analyzes your environment weekly. It displays results in the Environmental Overview section at the top of the tool's interface. It also displays a notification on the McAfee ePO landing page when 80% of your endpoints are ready to upgrade.

You can configure options for analyzing, like selecting groups of endpoints or specifying a different schedule, and re-analyze your environment whenever you need to. You can also change when upgrade notifications appear in McAfee ePO.

Reporting upgrade readiness

Endpoint Upgrade Assistant displays data about endpoints and software in your environment, which you can use to identify endpoints that are:

- Blocked from analyzing — You need to resolve the blocking issue, then re-analyze the endpoints.
- Running products that Endpoint Upgrade Assistant can't upgrade — You need to upgrade these products, then re-analyze the endpoints.
- Ready to upgrade — You can use Endpoint Upgrade Assistant to select the products and versions to deploy, verify that all required software is available, then upgrade these endpoints with a single deployment task.

Tagging endpoints for upgrades

Endpoints with similar issues are grouped, so that you can tag them. Each time you tag a group of endpoints, Endpoint Upgrade Assistant creates a tag called UA_<timestamp> in the McAfee ePO Tag Catalog. This lets you tag all the endpoints that require the same upgrade, then create a deployment task that deploys the upgrade to them, even if the endpoints are in different System Tree groups.

Deploying installation packages

When your endpoints are ready to upgrade, Endpoint Upgrade Assistant supports multiple options to deploy the installation packages that include all selected products and the Upgrade Automation client software.

- **Deployment task** — Use a deployment task that was created with Endpoint Upgrade Assistant or with McAfee ePO to deploy the installation packages to all selected endpoints. You can track the status of deployment tasks from Endpoint Upgrade Assistant.
- **Third-party tool** — Use a third-party deployment tool like Microsoft System Center Configuration Manager or IBM BigFix to deploy the installation packages to all selected endpoints. You can use the same tool and automated processes that you use to upgrade other products in your environment.
- **Custom installation package** — Use a McAfee ePO deployment task or third-party tool to deploy a custom installation package to all selected endpoints. Use the Endpoint Upgrade Assistant Package Creator tool to create the custom package.

For more information about using Endpoint Upgrade Assistant, you can watch the product training video.

What happens on endpoints during upgrades

The installation package for Upgrade Automation is deployed to endpoints during upgrades, along with the installation packages for the products you're upgrading. Upgrade Automation runs on the endpoint, determines which tasks are required to install the product upgrades included in the client deployment package, then performs the required tasks in a defined sequence.

For example, Upgrade Automation checks for pending Windows updates and conflicting products on the endpoint, and it determines whether it needs to remove existing products or upgrade them to a new version.

On each endpoint, Upgrade Automation performs the following tasks to upgrade Endpoint Security and other products you've selected. It skips the tasks required for upgrading products you didn't select.

1. Downloads the checked-in software packages for the products you want to upgrade, then verifies that they're the correct product versions.
2. Verifies that no Windows updates are pending. If updates are pending, the Upgrade Automation process exits so that updates can be applied.

   For example, if a Windows Update has been downloaded and not applied, or a required reboot following a Windows Update has not been performed, you need to manually complete the pending actions, then start the Upgrade Automation upgrade again.
3. Verifies that no conflicting products exist on the endpoint.
4. Harvests local policies for VirusScan Enterprise and McAfee Host IPS.
5. Removes VirusScan Enterprise, McAfee Host IPS, and Threat Intelligence Exchange (TIE) for VirusScan Enterprise.
6. Upgrades McAfee Agent (if selected), installs Endpoint Security and Adaptive Threat Protection, and then applies the local policies.
7. Installs the selected updates for Endpoint Security and Adaptive Threat Protection.
8. Installs McAfee Data Exchange Layer Client or upgrades it to the selected version.
9. Installs McAfee Active Response Client or upgrades it to the selected version.
10. Installs McAfee Application Control and McAfee Change Control or upgrades them to the selected version.
11. Upgrades McAfee Data Loss Prevention to the selected version.
12. Sends telemetry data to McAfee when installation is complete.

Products that it can upgrade

Endpoint Upgrade Assistant can upgrade supported versions of Endpoint Security and legacy products to Endpoint Security 10.7.x. It also upgrades other supported McAfee products to maintain product compatibility, using a single deployment task.

Earlier versions of Endpoint Security

Upgrade Automation attempts to upgrade Endpoint Security 10.2.x, 10.5.x, or 10.6.x. If it can't, it removes the existing version and installs Endpoint Security 10.7.x.

Additional considerations:

- If you select a product update, it is also installed.
- If McAfee Host Intrusion Prevention is installed, you can choose to keep it.

Legacy products

When upgrading these supported legacy products, Upgrade Automation removes the existing product and installs the new product.

This legacy product...	Is upgraded to...
McAfee® VirusScan Enterprise 8.8 or later	• Endpoint Security Threat Prevention • Endpoint Security Adaptive Threat Protection (Optional; Requires Endpoint Security Threat Prevention)
McAfee® Host Intrusion Prevention (McAfee Host IPS) 8.0 or later	Endpoint Security Firewall (Optional)
McAfee® SiteAdvisor Enterprise 3.5 or later	Endpoint Security Web Control (Optional)
McAfee® Threat Intelligence Exchange (TIE) for VirusScan Enterprise 1.x or later	Removed

Additional considerations:

- If you select a product update, it is also installed.
- If you want to keep your custom settings, you must migrate them before upgrading to Endpoint Security. If you don't do this before running Endpoint Upgrade Assistant, you are prompted to migrate them when preparing endpoints for upgrade.
- If McAfee Host Intrusion Prevention is installed, you can choose to keep it.

McAfee Agent

If Endpoint Upgrade Assistant determines that McAfee Agent version 4.6 or later needs to be upgraded to support Endpoint Security 10.7, it is upgraded to version 5.0.3.222 or later when Endpoint Security is upgraded.

If a compatible version of McAfee Agent is on an endpoint, you can select whether to upgrade it.

Other McAfee products

You can deploy upgrades for these additional McAfee products when you upgrade to Endpoint Security 10.7.x by selecting the version you want to upgrade to. The selected version of most of these products can be installed during the upgrade if an earlier version isn't already installed.

This McAfee product...	Installs selected version if product isn't already installed?
McAfee® Application Control and McAfee® Change Control 7.0 or later	Yes
McAfee® Active Response 2.2 or later (Requires Endpoint Security Adaptive Threat Protection)	Yes
McAfee® Data Loss Prevention (McAfee DLP) 9.2–11.2	No
McAfee® Data Exchange Layer (DXL) Client 4.0 and earlier	Yes

Compatibility with other installed products

Endpoint Upgrade Assistant can't upgrade endpoints where unsupported McAfee products are installed.

Products that Endpoint Upgrade Assistant ignores

If these products are running, you can use Endpoint Upgrade Assistant to upgrade to Endpoint Security 10.7. Endpoint Upgrade Assistant doesn't interact with these products.

Product	Versions
McAfee® File and Removable Media Protection (FRP)	4.3.1.153 and later
McAfee® Drive Encryption	7.1.1 and later

Products to upgrade using another method

If these products are running, you need to upgrade them using another method before you can use Endpoint Upgrade Assistant to upgrade to Endpoint Security 10.7.x. Endpoint Upgrade Assistant reports these endpoints as Requires product upgrades on the Overview tab.

Product	Versions
McAfee Host Intrusion Prevention	7.0 and earlier
McAfee® MOVE AntiVirus	All versions
McAfee VirusScan Enterprise	8.5 and earlier
McAfee® VirusScan(R) Enterprise for Offline Virtual Images	All versions
McAfee® VirusScan(R) Enterprise for SAP	All versions
McAfee® VirusScan® Enterprise for Storage	All versions

Required McAfee ePO permissions

Some features of Endpoint Upgrade Assistant require additional McAfee ePO permissions.

If you can't analyze your environment or deploy upgrades, check that you have the required additional permissions.

Permission set	Required permission	Required for...
McAfee Agent	View and change task settings	Deploying upgrades
Server tasks	View Scheduler tasks; view Scheduler task results in the Server Task Log	Analyzing the environment
Software	View packages	Analyzing the environment
Systems	• Create and edit tags and tag groups • View the System Tree tab • Apply, exclude, and clear tags	Analyzing the environment
System Tree access	• Can search on the following nodes and portions of the System Tree: My Organization	Analyzing the environment

Permission set	Required permission	Required for...
	• Can access the following nodes and portions of the System Tree: My Organization	

Managing upgrade information

Endpoint Upgrade Assistant uses several McAfee ePO features that assist you with planning and implementing your upgrade strategy.

Using queries and reports

Each time it analyzes an environment, Endpoint Upgrade Assistant creates a query that you can view in McAfee ePO under Queries & Reporting. Use these queries to create reports containing the information you need to plan and track your upgrades, then save them in PDF format.

Endpoint Upgrade Assistant queries display results from the last System Tree or group you analyzed. Data from previous analyses is overwritten.

Exporting endpoint details

System administrators can search, sort, filter, and validate Endpoint Upgrade Assistant results by downloading the information for a selected category in comma-separated values (CSV) format. Use this information for purposes such as debugging, identifying the endpoints required for upgrades, and resolving differences between the reported and expected status of endpoints.

- Export Systems — Creates a list of endpoints with their name, path, and type (server or workstation).
- Export System and Product Details — Adds the products and versions running on endpoints. You can sort by product to create a list of all endpoints running each version of each product (for example, outdated versions of McAfee Agent).
- View Systems — Displays the corresponding endpoints that you can export.

Tag management

By default, Endpoint Upgrade Assistant deploys upgrades to all the endpoints you have tagged with the UA_<timestamp> tag. To deploy to a subset of tagged endpoints, use one of these methods:

- **In Endpoint Upgrade Assistant** — From the landing page, select a System Tree group to analyze. Endpoint Upgrade Assistant analyzes only endpoints in that group. When you create a new tag, it includes only endpoints in the selected group.
- **In McAfee ePO** — Create a new tag, then copy endpoints with Endpoint Upgrade Assistant tags into the new tag.

Install the latest version of Endpoint Upgrade Assistant

Before upgrading, download and install a newer version of Endpoint Upgrade Assistant if one is available. Endpoint Upgrade Assistant notifies you when a newer version is available. The latest version includes support for the latest McAfee product versions and features.

Endpoint Upgrade Assistant is installed automatically with some versions of McAfee ePO. If it isn't already installed in your environment, you need to install it on the McAfee ePO server.

During installation, the extension is installed on the McAfee ePO server. Also, the Endpoint Upgrade Automation client package is checked in to all branches of McAfee ePO, so that you can deploy upgrades from any branch. During upgrades, Upgrade Automation is deployed with the product software to perform the upgrade on the endpoint.

If you plan to generate custom installation packages, you must also install the version of Endpoint Upgrade Assistant Package Creator that matches your other Endpoint Upgrade Assistant components. The correct version of Package Creator is bundled with the Endpoint Upgrade Assistant product extension and the Upgrade Automation installation package that is deployed to endpoints during upgrades.

Task

1. In McAfee ePO, click Software → Extensions.
2. Select Endpoint Upgrade Assistant from the list, then note the version number.
3. Click Menu → Software → Software Catalog (Software Manager on version 5.9.x), then:
   a. From the Category list, click Utilities & Connectors.

b. In the right pane, expand Endpoint Upgrade Assistant and Package Creator.
c. Check-in EUA extension.
d. (Optional) Search for Endpoint Upgrade Assistant Package Creator and download to the same version as Endpoint Upgrade Assistant, if needed. Required only to generate custom installation packages.

You can also log on to the McAfee Product Downloads site to search for new versions, using the grant number and email address associated with your product subscription.

Configure upgrade readiness notifications

Endpoint Upgrade Assistant displays a notification in McAfee ePO server by default when 80% of the endpoints in your environment are ready to upgrade. You can configure different settings as needed.

Task

1. On the Endpoint Upgrade Assistant landing page:

To...	Do this...
Change when the notification appears	For Display logon message when percentage of systems ready to upgrade exceeds, type a different number in the text box. **Example:** To display the notification when 75% or more of the endpoints in your environment are ready to upgrade, change the number in the text box to 75.
Hide the notification	For Display logon message when percentage of systems ready to upgrade exceeds, type a higher number in the text box. **Example:** If the notification says that 80% of the endpoints in your environment are ready to upgrade, change the number in the text box to 81 or higher. McAfee ePO won't display the notification again until more endpoints are ready to upgrade.
Hide the notification and the upgrade readiness data on the Endpoint Upgrade Assistant landing page	For Enable Endpoint Assistant landing page, select No from the drop-down list.

2. Click Save.

Results

Notifications are displayed when and where you have specified.

Sending telemetry data to McAfee

Upgrade Automation includes a telemetry feature that collects and sends anonymous deployment data to McAfee. This data is used to improve product robustness and performance in future releases.

The telemetry feature collects the following anonymous data:

- Product name (EUA)
- Product version
- Iteration number
- List of products installed prior to upgrade
- List of products installed post upgrade
- List of completed upgrade progress milestones
- Command line used for upgrade
- MD5 hash of machine GUID
- Machine locale (LCID)
- Success/failure of deployment
- Return code from Endpoint Upgrade Assistant
- Exit Description from Endpoint Upgrade Assistant

You can disable this feature by configuring an option when you generate a custom installation package or create a deployment task using McAfee ePO.

Other ways to install and upgrade

Installation command-line interface

Use the command-line interface to customize installation of Endpoint Security 10.7. You can specify commands when creating McAfee ePO deployment tasks. You can also run `setupEP.exe` using a third-party tool or the Windows command prompt on the endpoint.

Syntax: Deployment task options

When creating a deployment task in McAfee ePO, in the Command line box, you can enter the commands listed in the *Deployment task and setupEP.exe command-line options* table.

When using the `setupEP.exe` command line on the endpoint, or installing on the endpoint using a third-party tool, the command-line syntax for installation is:

```
installation_path\setupEP.exe [ADDLOCAL="tp,fw,wc,atp"] [ command_args setupEP_command_args]
```

- *installation_path* — The folder where you extracted the installation package.
- *command_args* — Commands in the *Deployment task and setupEP.exe command-line options* table.
- *setupEP_command_args* — Commands in the *setupEP.exe command-line options* table

These options are available when installing with a deployment task in McAfee ePO or by running `setupEP.exe` from the command line on the endpoint.

Options are not case sensitive.

Deployment task and setupEP.exe command-line options

Option	Parameters	Description	Notes
`CAVA="thread_count"`	*thread_count* — (Optional) Specifies the number of scanning threads to use.	Installs Endpoint Security with support for the Common AntiVirus Agent (CAVA). Requires Threat Prevention.	Required when upgrading from a previous version of Endpoint Security with CAVA. This option disables the blocking cache in the on-access scanner, increases the number of on-access scanning threads to 200, and enables network scanning, to ensure that all files from CAVA are scanned. You can also specify a different number of scanning threads. See How to install Endpoint Security with support for CAVA (KB88973) for more information.
`INSTALLDIR="path"`	*path*	Specifies where to install the product files on the endpoint.	The installer creates an Endpoint folder at the specified location and installs the product to this folder. By default, product files are installed in the folder C:\Program Files\McAfee\Endpoint Security.

Option	Parameters	Description	Notes
`/log"path"` `/l"path"`	*path*	Specifies where to save the installation log files for tracking installation events.	The installer creates an Endpoint folder at the specified location and saves the log files to this folder. By default, log files are saved in the Windows System TEMP folder C:\windows\Temp\McAfeeLogs.
`/l*v"path"`	*path*	Specifies where to save the installation log files and verbose (more descriptive) logging entries.	
`/nocontentupdate`		Does not automatically update product content files on the endpoint as part of the installation process.	Content files include the latest AMCore, Exploit Prevention, and Adaptive Threat Protection content files required for Endpoint Security. **Caution:** Update content files to ensure that the endpoint is fully protected. If you don't update them during installation, schedule an update as soon as possible.
`/override"program"`	`hips` — McAfee Host Intrusion Prevention	Overrides and removes the specified conflicting product.	
`/quarantinefolder="path"`	*path*	Specifies the location of the Quarantine folder where detected threats are placed. The folder path is limited to 190 characters.	By default, the Quarantine folder is located in the folder <SYSTEM_DRIVE>\Quarantine.

These additional options are available when running `setupEP.exe` from the command line on the endpoint.

setupEP.exe command-line options

Option	Parameters	Description
`ADDLOCAL="tp,fw,wc,atp"`	• `tp` — Threat Prevention • `fw` — Firewall • `wc` — Web Control • `atp` — Adaptive Threat Protection	Specifies individual product modules to install in silent mode. Before you can install `atp`, `tp` must be installed. **Best practice:** For optimal performance and protection, install the same version of the Endpoint Security modules or upgrade all modules to the latest version. **Tip:** When using `ADDLOCAL`, there are no endpoint notifications or user interactions. It behaves like `/qn` is

Option	Parameters	Description
		specified. To change this behavior, you can specify `/q!` or `/qb`.

`/qn` or `/quiet`
`/qb!` or `/passive`
`/qb`
	• `qb!` — Shows only a progress bar. Users cannot cancel the installation while it is in progress (passive mode).
	• `qb` — Shows a progress bar and a Cancel button. Users can cancel the installation while it is in progress, if needed.
	• `qn` — Hides all installation notifications (silent mode). Users have no interaction.
	Note: When using `ADDLOCAL` to install, this is the default behavior and you do not need to specify it.
		Specifies how users interact with the installer.

`/import` *file*	*file*	Imports settings from the specified file.
`/module <TP,FW,WC,ATP,ESP>`	• `TP` — Threat Prevention • `FW` — Firewall • `WC` — Web Control • `ATP` — Adaptive Threat Protection • `ESP` — Resources shared by product modules.	Applies imported settings to the specified product modules.
`/nopreservesettings`		Does not save your product settings when upgrading to Endpoint Security. By default, settings are preserved.
`/policyname` *name*	*name*	Assigns the specified settings to endpoints where the product is installed.
`/unlock` *password*	*password*	Unlocks the client interface using the specified password.

Examples: Deployment task and setupEP command-line options

To run these example commands:

- **In McAfee ePO** — On the Create Deployment Task page, type options in the Command line box.
- **On the endpoint** — Open a command prompt in Windows, then change to the location where you extracted the installation package.
- **In a third-party deployment tool** — When creating a deployment task, for the installation command line enter `setupEP.exe` with the options required for your environment.

  Best practice: Use `setupEP.exe ADDLOCAL="tp,atp,fw,wc"` to install all the product modules on endpoints without displaying notifications or interrupting user activity.

To...	Add these options in the deployment task	Run this command from the command line
Install Firewall and Web Control (and Common, if needed).	`ADDLOCAL="fw,wc"`	`setupEP.exe ADDLOCAL="fw,wc"`
Install the product modules using a third-party deployment tool. By default,	`ADDLOCAL="tp,atp,fw,wc"`	`setupEP.exe ADDLOCAL="tp,atp,fw,wc"`

To...	Add these options in the deployment task	Run this command from the command line
there are no notifications on the endpoint or user interaction.		
Install the product modules under D:\Installed Programs\Mcafee\Endpoint Security instead of the default location (C:\Program Files\McAfee\Endpoint Security).	`INSTALLDIR="D:\Installed Programs"`	`setupEP.exe INSTALLDIR="D:\Installed Programs"`
Save product log files under D:\Log Files instead of the default location (C:\Windows\Temp\McAfeeLogs).	`/l"D:\Log Files"`	`setupEP.exe /l"D:\Log Files"`
Save product log files under D:\Log Files and specify verbose logging.	`/l*v"D:\Log Files"`	`setupEP.exe /l*v"D:\Log Files"`
Remove McAfee Host Intrusion Prevention automatically during installation.	`/override"hips"`	`setupEP.exe /override"hips"`
Create a Quarantine folder at D:\reports\Quarantine instead of the default location (<SYSTEM_DRIVE>\Quarantine).	`/quarantinefolder="D:/reports"`	`setupEP.exe /quarantinefolder="D:/reports"`
Install Threat Prevention with support for CAVA and increase the number of on-access scanning threads to 220.	`ADDLOCAL="tp" CAVA="220"`	`setupEP.exe ADDLOCAL="tp" CAVA="220"`
Install Adaptive Threat Protection (and Threat Prevention and Common) automatically without updating the product content files during installation.	`ADDLOCAL="atp" /nocontentupdate`	`setupEP.exe ADDLOCAL="atp" /nocontentupdate`
Import settings from the file called `mysettings`.		`setupEP.exe /import mysettings`
Import settings from the file called `mysettings` to Threat Prevention and Firewall.		`setupEP.exe /import mysettings /module TP,FW`
Install the product modules using a third-party deployment tool. By default, there are no notifications on the endpoint or user interaction.		`setupEP.exe ADDLOCAL="tp,atp,fw,wc"`

Download and install Endpoint Security on McAfee ePO

If you can't get the Endpoint Security 10.7.x product extensions and installation packages from the Software Catalog (Software Manager on McAfee ePO 5.9.x), you can download them from the McAfee Product Downloads site, then install them on the McAfee ePO server.

Best practice: For optimal performance and protection, install the same version of the Endpoint Security modules or upgrade all modules to the latest version.

Task

1. Go to McAfee Product Downloads.
2. Enter the grant number and email address associated with the product, then click Submit.
   The My Products page displays information about your licensed products.
3. In the Find Products section under Filters, select Endpoint Security for the Category.
   A table displays your licensed Endpoint Security products.
4. To download the extensions and packages of McAfee Endpoint Security do the following:
   a. Navigate through the table to locate and select McAfee Endpoint Security.
      A table displays all the product files that are available to download.
   b. In the Available Downloads section under Filters, select Extension for the Type, then click the product extension for each product module that you want to download to your default downloads folder.
      - Endpoint Security Platform extension Version 10.7.x.xxxx (Required for Threat Prevention, Firewall, and Web Control)
      - Endpoint Security Threat Prevention extension Version 10.7.x.xxxx
      - Endpoint Security Firewall extension Version 10.7.x.xxxx
      - Endpoint Security Web Control extension Version 10.7.x.xxxx

      The product extensions are now ready to install on the McAfee ePO server.
   c. In the Available Downloads section under Filters, select Package for the Type, then click the installation package for each product module that you want to download to your default downloads folder.
      - Endpoint Security Platform – Full Install Version 10.7.x.xxxx (Required for Threat Prevention, Firewall, and Web Control)
      - Endpoint Security Threat Prevention – Full Install Version 10.7.x.xxxx
      - Endpoint Security Firewall – Full Install Version 10.7.x.xxxx
      - Endpoint Security Web Control – Full Install Version 10.7.x.xxxx

      The installation packages are now ready to install on the McAfee ePO Master Repository.
5. (Optional) To download the extensions and packages of McAfee Endpoint Security Adaptive Threat Protection do the following:
   a. Navigate through the table to locate and select McAfee Endpoint Security Advance Threat Protection.
      A table displays all the product files that are available to download.
   b. In the Available Downloads section under Filters, select Extension for the Type, then click the product extension that you want to download to your default downloads folder.
      - Threat Detection Reporting extension Version 1.0.x.xxxx
      - Endpoint Security Adaptive Threat Protection – Full Install Version 10.7.x.xxxx (Requires Threat Prevention)

      The product extensions are now ready to install on the McAfee ePO server.
   c. In the Available Downloads section under Filters, select Package for the Type, then click the installation package that you want to download to your default downloads folder.
      - Endpoint Security Adaptive Threat Protection – Full Install Version 10.7.x.xxxx (Requires Threat Prevention)

      The installation packages are now ready to install on the McAfee ePO Master Repository.
6. To install the downloaded Endpoint Security extensions on McAfee ePO:
   a. Click Menu → Software → Extension and click Install Extensions.
   b. Browse the required extension and click OK.
      The Install Extension table displays the extension details.
   c. Click OK.
   d. Repeat the steps to install other extensions.

   When the installation is complete, the product extensions are listed on the Extensions page.
7. To check in the downloaded Endpoint Security packages on McAfee ePO:
   a. Click Menu → Software → Master Repository.
   b. Click Check In Package and in the Package tab, browse the required client package.
   c. Click Next.
   d. In the Package Options tab, select the required option in the Branch and click Save.
   e. Repeat the steps to check-in the other packages.

   When the check-in is complete, you can view the installed Endpoint Security packages in the Master Repository.

Deploy packages generated with Endpoint Upgrade Assistant using McAfee ePO

You can use a deployment task in McAfee ePO 5.10.x or 5.9.x to upgrade to Endpoint Security 10.7.x on your endpoints with an installation package that you create using Endpoint Upgrade Assistant.

If you used Endpoint Upgrade Assistant to tag the endpoints that you plan to upgrade, you can select the tag when you create the deployment task in McAfee ePO. You can also select a custom installation package that you generated using Endpoint Upgrade Assistant Package Creator.

Task

1. In McAfee ePO, select Menu → Software → Product Deployment.
2. On the Product Deployment page, click New Deployment.
3. On the New Deployment page:
   a. Enter a name for the deployment.
   b. From the Product and Components section, select the Upgrade Automation package that you created with Endpoint Upgrade Assistant.
   c. From the Tag Catalog, select the Upgrade Automation tag that you created with Endpoint Upgrade Assistant.
   d. Specify other options as needed.
      - Installation options — Upgrade Automation supports several command-line options.
      - McAfee Agent options — Upgrade Automation supports most options for installing or upgrading McAfee Agent.
   e. Click Save at the top of the page.
      The Product Deployment page opens with your new project added to the list of deployments. Also, a client task is automatically created with the deployment settings.

Upgrade Automation command-line options

The Upgrade Automation client software included in the installation package for upgrades managed with Endpoint Upgrade Assistant supports these command-line options for deployment tasks that you create using McAfee ePO.

Best practice: If you don't want to enter deployment task options manually, click **Copy Command Line** in Endpoint Upgrade Assistant to copy to the Windows clipboard the command-line options that match your selections on the Overview and Prepare tabs.

Option	Description
`--keepma`	Do not upgrade versions of McAfee Agent that are compatible with Endpoint Security.
`--ma="[arguments]"`	Install or upgrade McAfee Agent using the specified command-line arguments. These arguments are not supported: • `/REMOVE` • `/FORCEUNINSTALL` • `/RELAY`
`--excludefw`	Do not deploy Endpoint Security Firewall. The module won't be downloaded and installed.
`--excludewc`	Do not deploy Web Control. The module won't be downloaded and installed.
`--installdlp=[version]`	Upgrade McAfee DLP to the specified version. The deployment task fails if the software isn't checked in to the selected McAfee ePO branch.
`--installatp`	Install Adaptive Threat Protection.

Option	Description
`--installdxl`	Install or upgrade Data Exchange Layer. The deployment task fails if the software isn't checked in to the selected McAfee ePO branch.
`--installmacc`	Install or upgrade McAfee Application Control and McAfee Change Control. The deployment task fails if the software isn't checked in to the selected McAfee ePO branch.
`--installmar`	Install or upgrade Active Response. The deployment task fails if the software isn't checked in to the selected McAfee ePO branch.
`-update=[updatenumber]`	Install the specified update during the Endpoint Security upgrade.
`--tag[=1-4]` where: 1–4 specifies one of four Custom fields	Report endpoint events in a Custom field on the System Properties tab in the McAfee ePO System Details page. For example, `--tag=3` reports endpoint events in the Custom 3 field, and `--tag` or `--tag=1` reports in the Custom 1 field.
`--exitondllinjector`	Stop the Endpoint Security upgrade if McAfee SysPrep returns a failure message. In this case, the software on the endpoint is not removed, to ensure that the endpoint is always protected.
`--ignorebatterylevel`	Ignore battery charge level if the endpoint is a mobile computer.
`--ignoreensoscheck`	Don't verify the version of Windows running on the endpoint before installing Endpoint Security. By default, Upgrade Automation verifies that a compatible version of Windows is running on the endpoint you plan to upgrade. If it's incompatible, no upgrade occurs. Use this option to proceed with the upgrade regardless of the Windows version. **Best practice:** Allowing Upgrade Automation to verify the version of Windows helps to prevent upgrade failures caused by product incompatibility.
`--log=[path]`	Save the Upgrade Automation installation log file in the specified location. For example, `--log=C:\mcafeeEUALOGS` creates the C:\mcafeeEUALOGS\ folder and saves the log file at that location.
`--notelemetry`	Do not collect and send anonymous telemetry data from Upgrade Automation.
`--retryafterreboot`	• If Endpoint Security fails to install on the first attempt — Do not initiate a restart automatically. Wait until the endpoint restarts, then attempt to install Endpoint Security.

Option	Description
	• If Endpoint Security is manually installed before the endpoint restarts — Detect that the product is installed, then cancel the pending installation.

Compatibility of command-line options

Command-line options are case sensitive. If you enter an invalid or an unrecognized option, Endpoint Upgrade Assistant doesn't start the upgrade and closes without making any changes to endpoints.

Specifying multiple options can result in conflicting actions. Here's how Endpoint Upgrade Assistant resolves conflicting command-line options:

Options	Result
`--tag=2 --keepma`	• Does not upgrade McAfee Agent if it is compatible with Endpoint Security. • Reports endpoint events in the Custom 2 field on the System Properties tab in the McAfee ePO System Details page.

Upgrade and install on self-managed endpoints using a command line

Upgrade the software

To upgrade to McAfee Endpoint Security 10.7.x on a self-managed endpoint with custom options like silent installation, run the installer from the command line. You can upgrade from version 10.2.x, 10.5.x, or 10.6.x.

Information is reported in the installation log file. You can specify an option to display a progress window, if needed.

Best practice: For optimal performance and protection, upgrade all Endpoint Security modules to the latest version.

Task

1. Copy the product files to the endpoint where you plan to install it.

   Depending on how you purchased the product, you might need to download product files from a download site or copy them from a disc.
2. Open a Command Prompt window, navigate to the folder where you copied the files, then type this command and any applicable parameters, which are not case-sensitive:

   ```
   setupEP.exe [parameters]
   ```

   As a best practice, we recommend restarting the endpoint after the installation has completed.

Results

To verify that Endpoint Security installed on the endpoint, open the Windows Control Panel and check that version 10.7.x of each product module you selected to install appears. You can also check that no errors or failure messages appear in the installation log file.

Install the software for the first time

To install McAfee Endpoint Security 10.7.x on a self-managed endpoint with custom options like silent installation, run the installer from the command line.

Information is reported in the installation log file. You can specify an option to display a progress window, if needed.

Best practice: For optimal performance and protection, install the same version of the Endpoint Security modules.

Task

1. Copy the product files to the endpoint where you plan to install it.

   Depending on how you purchased the product, you might need to download product files from a download site or copy them from a disc.

2. Open a Command Prompt window, navigate to the folder where you copied the files, then type this command and any applicable parameters, which are not case-sensitive:

   ```
   setupEP.exe [parameters]
   ```

   As a best practice, we recommend restarting the endpoint after the installation has completed.

Results

To verify that Endpoint Security installed on the endpoint, open the Windows Control Panel and check that version 10.7.x of each product module you selected to install appears. You can also check that no errors or failure messages appear in the installation log file.

Deploy custom packages generated with Package Designer

Use Endpoint Security Package Designer 10.7.x to generate custom Endpoint Security 10.7.x installation packages that you can deploy to your endpoints with McAfee ePO 5.10.x , 5.9.x or a third-party deployment tool.

Why use Package Designer

Package Designer lets you generate custom installation packages that:

- Meet specific requirements — For example, preconfigure port exclusions to ensure that vital communications are not blocked when Firewall is installed, or preconfigure settings required for compliance with security regulations.
- Replace the default settings with custom settings
- Install Endpoint Security with settings in place — Settings take effect as soon as installation is complete, rather than waiting for the first policy enforcement.
- Reduce the size of the installation package.
- Remove unneeded files.

How Package Designer works

The default installation package contains...	Package Designer 10.7 lets you...
McAfee Default settings	Replace them with preconfigured, custom settings
Installers required to install Endpoint Security: • All product modules • On 64-bit and 32-bit Windows operating systems • Any required monthly updates and Hotfixes	Remove unused installers for: • Product modules you don't plan to install • 64-bit or 32-bit installers • Monthly updates and Hotfixes

To generate the custom installation package, you can run Package Designer on an endpoint where Endpoint Security 10.7.x is installed. Package Designer uses the current settings and installation packages on the endpoint as the source for the custom package. You can also run Package Designer on any endpoint that has access to the installation files and policy settings you plan to include in the custom package. Deploy the custom package to endpoints using a McAfee ePO deployment task or a third-party deployment tool.

Best practice: To prevent a policy enforcement from overwriting the custom settings, run Package Designer on an unmanaged endpoint. Alternatively, you can customize the settings using McAfee ePO, push the updated settings to the endpoint where Package Designer is installed, then run Package Designer on the endpoint.

Package Designer 10.7 is required to customize packages for Endpoint Security 10.7.x.

Before you begin

- If they are not available in the Software Catalog (Software Manager on McAfee ePO 5.9.x), download these installation packages from the McAfee Product Downloads site:
    - Endpoint Security Package Designer Version 10.7.x.xxxx
    - Endpoint Security Platform – Full Install Version 10.7.x.xxxx (Required for Threat Protection, Firewall, and Web Control)
    - Endpoint Security Threat Prevention – Full Install Version 10.7.x.xxxx
    - Endpoint Security Firewall – Full Install Version 10.7.x.xxxx
    - Endpoint Security Web Control – Full Install Version 10.7.x.xxxx

- Endpoint Security Adaptive Threat Protection – Full Install Version 10.7.x.xxxx (Requires Threat Prevention)

Best practice: For optimal performance and protection, install the same version of the Endpoint Security modules or upgrade all modules to the latest version.

- On the endpoint where you plan to run Package Designer:
  - Install Package Designer 10.7.x.
  - Install Endpoint Security 10.7.x, or make sure the endpoint has access to the installation packages.
  - Configure settings on the endpoint as needed, or make sure the endpoint has access to the custom settings.

Deploy custom packages generated with Endpoint Upgrade Assistant Package Creator

Use Endpoint Upgrade Assistant Package Creator to generate a custom Endpoint Security 10.7.x installation package for upgrades that you manage with Endpoint Upgrade Assistant. The custom package includes the Endpoint Upgrade Automation client software, which manages the upgrade on the endpoints, and you can deploy it to your endpoints using McAfee ePO 5.10.x, 5.9.x, or a third-party deployment tool.

Why use Endpoint Upgrade Assistant Package Creator

Endpoint Upgrade Assistant Package Creator lets you create custom installation packages when you need to:

- Meet specific requirements — For example, preconfigure port exclusions to ensure that vital communications are not blocked when Firewall is installed, or preconfigure settings required for compliance with security regulations.
- Replace the default settings with custom settings
- Install Endpoint Security with settings in place — Settings take effect as soon as installation is complete, rather than waiting for the first policy enforcement.
- Reduce the size of the installation package.
- Remove unneeded files.

Use Endpoint Upgrade Assistant to create custom installation packages that contain the product installation packages for:

- McAfee Agent — You can specify whether to upgrade McAfee Agent when a compatible version is installed on an endpoint.
- Required McAfee products.
- The latest Endpoint Security update — You can specify whether to include the update.
- Upgrade Automation client software — Manages the upgrade of multiple products on the endpoint.

Endpoint Upgrade Assistant Package Creator generates a single installation package that contains everything needed to upgrade multiple products on your endpoints. No additional downloads are required during the upgrade process. Package Creator lets you select some of the files to include and options for deploying them.

Best practice: Because it contains the installer for McAfee Agent, use Endpoint Upgrade Assistant Package Creator to generate a deployment package when you plan to move endpoints to a new McAfee ePO server during the upgrade.

Supported deployment methods

Choose the type of installation package to save based on your deployment method:

If you plan to deploy with...	Save the file as...	Then check in the file to the...
A third-party deployment tool	An executable application	Repository for your third-party tool This is a self-extracting .exe file that extracts the installers, then runs Upgrade Automation to automatically upgrade endpoints with the selected options.
McAfee ePO	A package .zip file	McAfee ePO server Endpoint Upgrade Assistant Package Creator validates the package while creating it.

Best practice: If you plan to generate more than one custom package, assign a unique label to each one, then save them for future use. You must enable Advanced mode to use this feature.

Before you begin

In addition to prerequisites for deploying a standard installation package, you need to meet these prerequisites for creating and deploying a custom installation package.

- Download the latest version of Endpoint Upgrade Assistant Package Creator from the Software Catalog (Software Manager on McAfee ePO 5.9.x) or the McAfee Product Downloads site.
- Download the latest version of McAfee SysPrep from the McAfee Product Downloads site, if one is available, and check it in to the McAfee ePO branch you plan to deploy upgrades from. Endpoint Upgrade Assistant runs McAfee SysPrep during upgrades to detect and allow trusted third-party software injectors.
- On the endpoints where you plan to deploy the custom package, make sure you have system permissions.
- Identify a location for saving the custom package — Select a location that McAfee ePO or your third-party deployment tool can access.
- Have this information ready for deployment: a descriptive name for the deployment task, the file name for the installer, and the command line to run the deployment (for example, `setupEP.exe ADDLOCAL="tp,atp,fw,wc"`).
- On the endpoint where you plan to run Endpoint Upgrade Assistant Package Creator:
    - Make sure that you have administrator credentials.
    - Install the Microsoft .NET 4.5 Framework class library.
    - Configure screen resolution no lower than 1280 x 720.
    - Install Endpoint Security 10.7.x and configure settings as needed.
    - Install Endpoint Upgrade Assistant Package Creator.
- Check and increase the package size limit, if needed, in McAfee ePO before uploading large packages.

Download the McAfee Agent frame package file

Endpoint Upgrade Assistant Package Creator needs a compatible installation package for McAfee Agent, to include in the custom installation package that it generates. You need to download this installation package, called a frame package, from your target McAfee ePO server.

The correct file is named FramePkg.exe. Files named SmartInstaller.exe or Frminst.exe don't work.

Task

1. In McAfee ePO, select System Tree → New Systems.
2. For How to add systems, select Create and download agent installation package.
3. For version, select Windows and 5.0.5 or later.
4. Click OK to download a valid McAfee Agent installation package from your McAfee ePO server.

Generate the package using Package Creator

Use Endpoint Upgrade Assistant Package Creator to generate custom installation packages when upgrading other products with McAfee Endpoint Security 10.7.x. You can deploy the custom packages with McAfee ePO or a third-party tool. Package Creator requires Endpoint Upgrade Assistant.

Task

1. Open Package Creator, specify the product modules to install, then click Next.
    a. Specify the locations of the installers for Endpoint Security.
    This installs the required modules: Threat Prevention, Adaptive Threat Protection (if selected), and Endpoint Security Platform (Common).
    b. Select other Endpoint Security modules to install, as needed.
    Best practice: For optimal performance and protection, install the same version of the Endpoint Security modules or upgrade all modules to the latest version.
    c. Select updates to install for Endpoint Security and Adaptive Threat Protection, as needed.
2. Specify other McAfee products to install, then click Next.
    a. Specify the location of the installation package for McAfee Agent, called a frame package (FramePkg.exe).
    b. Select whether to upgrade versions of McAfee Agent that are compatible with Endpoint Security.
    c. Specify the locations of the installers for optional McAfee products to install.

3. Select package deployment options, then click Next.
   a. Select the type of product installer to generate:
      - A package (.zip) file to deploy with McAfee ePO.
      - An executable application to install with third-party tools: specify the name and location for the installer.
   b. (Optional) Specify a custom location for the log files created on the endpoint where you run Package Creator and the endpoints where you deploy the installer.
   c. (Optional) Specify a later version of McAfee SysPrep to install.
   d. (Optional) Select command-line options to use.
4. (Optional) In the upper-left corner of Package Creator, right-click the McAfee icon, then select Advanced to display additional options.
   - Under McAfee Agent, enter McAfee Agent command-line options to use, if needed.
   - Under Select package deployment method, enter a unique package code, if needed. This lets you generate multiple custom installation packages that can all be checked in to the same repository at the same time.
5. Verify that you've specified the correct information, then click Create.

Results

The custom installation package is ready to deploy.

Deploy with a third-party tool

Use your third-party deployment tool to deploy an executable, custom installer that you generated with Endpoint Upgrade Assistant Package Creator to your endpoints. The custom installer contains installation packages for McAfee Endpoint Security 10.7.x and other required McAfee products.

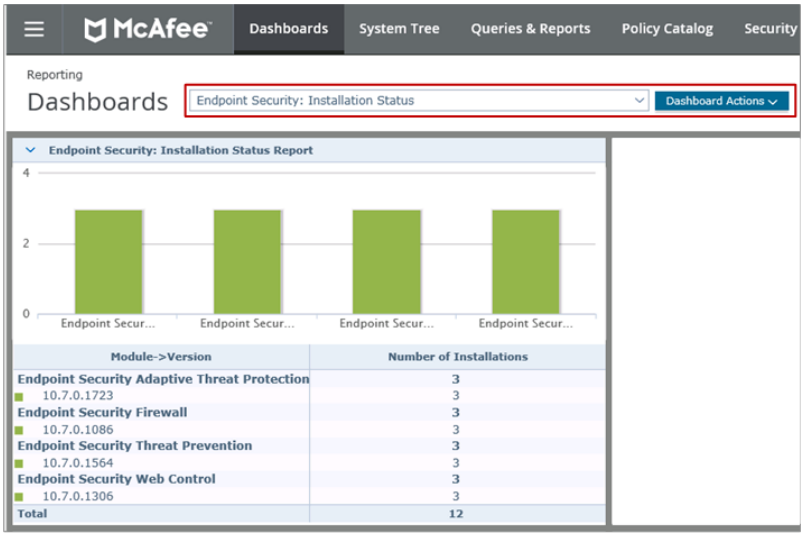
These steps vary depending on the tool. See the documentation for your third-party deployment tool for specific deployment details.

Task

1. Import the installer that you created with Package Creator into your third-party deployment tool.
2. Specify the information and options required for your environment.
   These vary depending on your tool. Some examples might be:
   - **To detect whether the product needs to be installed** — Specify a detection method for determining whether the product is already installed, such as a file, a registry key, or an .msi product code. For example, Endpoint Security 10.7.x doesn't need to be deployed to systems where the HKEY_LOCAL_MACHINE registry key SOFTWARE\McAfee\Endpoint\AV includes a value for ProductVersion that is equal to 10.7.x.
   - **To configure the user experience** — Specify options for running the installer on the endpoint (for example, whether users need to be logged on, whether installation is hidden, and estimated and maximum installation times).
   - **To check whether other required products need to be upgraded** — Specify any dependencies for required products and versions. For example, if you specify McAfee Agent version 5.6.x and an earlier version is installed, it will be upgraded before Endpoint Security 10.7 is installed.

Results

To verify that Endpoint Security installed on your endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that version 10.7.xxxx is installed on the correct number of endpoints.



Create a custom settings file to import

When you want to install McAfee Endpoint Security 10.7.x on a new endpoint with custom settings, command-line tools let you import settings that you have saved (also called exported) to a file.

How the command-line tools work

This method of installing the software with custom settings requires two command-line tools:

- On the endpoint where Endpoint Security is installed — Run `ESConfigTool` with the export option to save the settings to a file. This tool is located in the Endpoint Security Platform folder (C:\Program Files\McAfee\Endpoint Security\Endpoint Security Platform, by default.
- On the endpoint where you want to install Endpoint Security — Run `SetupEP` with the import option to install the product and overwrite the default settings with the settings in the file.

Before you begin

In additional to the requirements for installing on self-managed endpoints, you need to:

- On the endpoint where Endpoint Security is installed — Configure the product settings for your needs.
- On the endpoint where you plan to install Endpoint Security — Make sure that:
    - You have administrator rights.
    - You know the password to unlock Endpoint Security Client, if the interface mode is not set to Full access. You'll be asked to enter it on the command line.

Save (Export) your custom settings

To install McAfee Endpoint Security 10.7.x locally on an endpoint with preconfigured settings, save the settings to a file that the installer can import. Use the `ESConfigTool` utility to save the custom settings, then use a `SetupEP` command-line installation to import them.

This tool exports all settings for the selected product modules to a location that you specify.

Best practice: To create custom packages that include custom policies and client software for deployment with McAfee ePO, use the Endpoint Security Package Designer.

For option definitions, run : `ESConfigTool.exe`.

Task

1. In Endpoint Security, configure your settings.
2. Open a command prompt window in Windows.
3. Run `ESConfigTool` to export your settings to `<file_name>` and save this file to a folder that is not protected by McAfee.

   ```
   ESConfigTool.exe /export <file_name> [/module <TP|FW|WC|ATP|ESP> ]
   ```

   The folder containing `ESConfigTool` is protected, so use a different, writable location for the export location.

   Example:

```
ESConfigTool.exe /export C:\ENS\firewall.policy /module FW
```

This example exports the Firewall settings to C:\ENS\firewall.policy.

Results

When you're ready to install Endpoint Security with the saved settings, use the `SetupEP` utility with the `/import` command-line option.

Command-line options for exporting custom settings

You can configure these options when using `ESConfigTool` to save custom Endpoint Security 10.7.x settings to a file.

Run `ESConfigTool` from the command line on an endpoint where Endpoint Security 10.7.x is installed.

Syntax: ESConfigTool command line interface

installation_path\ESConfigTool.exe /export *file* [*command_args*] [/plaintext]]

installation_path\ESConfigTool.exe /import *file* [*command_args*] [/policyname *name*]]

- *installation_path* - C:\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform by default
- *command_args* - One of the commands in the *ESConfigTool command-line options* table

Options are not case sensitive.

ESConfigTool command-line options

Option	Parameters	Description
`/export` *file*	*file*	Saves settings to a file with the specified name and location. **Note:** Save this file to a folder that is not protected by McAfee. The folder containing `ESConfigTool` is protected, so use a different, writable location for the export location.
`/import` *file*		Imports the settings from the specified file name. The file must be encrypted.
`/module <TP|FW|WC|ATP|ESP>`	• `TP` — Threat Prevention • `FW` — Firewall • `WC` — Web Control • `ATP` — Adaptive Threat Protection • `ESP` — Resources shared by product modules.	Specifies which product module settings to export or import.
`/unlock` *password*	*password*	Specifies the password to unlock the client interface.
`/plaintext`		Specifies descriptive comments in human-readable format when exporting settings.
`/policyname`	*name*	Specifies the name of the policy to import.

Examples: ESConfigTool command line interface

Open a command prompt and change to the installation location of the `ESConfigTool` command. By default, `ESConfigTool` is located in the C:\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform folder.

To...	Run this command
Export settings for Threat Prevention and Firewall to the file C:\ENS \preconfigured.policy when the Endpoint Security Client interface mode is set to Full access.	`ESConfigTool.exe /export C:\ENS\preconfigured.policy /module TP FW`
Export settings for all product modules to the file C:\ENS \preconfigured.policy when the Endpoint Security Client interface mode is set to Full access.	`ESConfigTool.exe /export C:\My Programs\Endpoint\preconfigured.policy/ module TP FW WC ATP ESP`
Unlock the Endpoint Security Client and export settings for all product modules to the file C:\ENS \preconfigured.policy.	`ESConfigTool.exe /export C:\My Programs\Endpoint\preconfigured.policy / module TP FW WC ATP ESP /unlock MyStrongPassword`
Import settings for all product modules from the file C:\ENS \preconfigured.policy.	`ESConfigTool.exe /import C:\My Programs\Endpoint\preconfigured.policy / module TP FW WC ATP ESP`

Troubleshooting Endpoint Security installations and upgrades

Error codes and messages

McAfee installer errors

The McAfee Endpoint Security installer displays an error message or code, depending on your installation method, when an unexpected condition occurs that it can't fix. Use this list to find an error message, an explanation of the condition, and any action you can take to correct it.

Message	Description	Solution
`Conflicting McAfee product(s) found.`	Error code: 16002 Displays temporarily in Windows Defender Security Center after a restart. The installer detected one or more conflicting McAfee products on the endpoint that it can't remove automatically.	Uninstall the conflicting products, then try installing again.
`Administrator rights required.`	Error code: 16002 You must have administrator rights to run the installer.	Log on as an administrator, then launch the installer.
`Invalid Package.`	Error code: 16003 Invalid package found. Please verify that you have a valid package.	Download a valid package file, then try installing the product again.
`Removal failed.`	Error code: 16007 The installer couldn't remove a previous version of this product (such as a beta version) or a legacy product (such as VirusScan Enterprise or SiteAdvisor Enterprise) from the endpoint.	Remove these products manually before installing Endpoint Security. Contact Technical Support if the issue persists.
`Installer failed to launch.`	Error code: 16008 The installer was not able to launch.	Contact Technical Support.
`Restart required.`	Error code: 16015 The installer requires an endpoint restart to **continue** the installation.	Restart the endpoint to continue with the installation. **Best practice:** For third-party deployments, it is not possible to display a restart prompt on endpoints. Check whether the third-party tool you are using provides an option to show a restart prompt based on this return code.
`Restart required.`	Error code: 16016 The installer requires an endpoint restart to **complete** the installation.	Restart the endpoint to complete the installation.
`Restart pending.`	Error code: 16017	Restart the endpoint to continue with the installation.

Message	Description	Solution
	An endpoint restart from a previous installation or removal operation is pending.	
`Incompatible software removal failed.`	Error code: 16018 The installer tried and failed to remove one or more incompatible software products it detected on the endpoint.	Remove these products manually before installing Endpoint Security.
`Installation failed.`	Error code: 16019 The installer was interrupted before it finished installing Endpoint Security. It made no changes to your endpoint.	Run the installer again at a later time.
`Setup cannot run from a directory with case sensitivity enabled.`	The installer was run from a path where one or more folders are case sensitive.	In Windows, disable the case-sensitive attribute for the folder, then run installation again.
`Install path invalid. Invalid Install Path - Install path or one of its parent directories is case sensitive.`	One or more folders in the path where the installer attempted to install Endpoint Security are case sensitive.	In Windows, disable the case-sensitive attribute for the folders or specify a different path, then run installation again. When installation is complete, these folders are automatically protected against enabling the case-sensitive attribute. This prevents issues with upgrades and updates.
`Installation failed. McAfee Endpoint Security installation failed because the case-sensitivity attribute is enabled for the installation folders you specified.`	One or more folders in the path where the installer attempted to install Endpoint Security are case sensitive.	In Windows, disable the case-sensitive attribute for the folder or specify a different folder, then run installation again. When installation is complete, this folder is automatically protected against enabling the case-sensitive attribute. This prevents issues with upgrades and updates.
`<attempted action is> violating the rule "Core Protection - Protect core McAfee folders against enabling the Windows case-sensitivity attribute."`	The Endpoint Security self-protection feature blocked an attempt to enable the case-sensitivity attribute for one or more folders in a critical path.	An action was blocked in accordance with the definition of the rule that was described in the event message. You can read more about troubleshooting this issue in KB85494.
`Installation canceled.`	Error code: 16020 The user canceled the installation before it completed. The installer made no changes to the user's endpoint.	Run the installer again.
`Migration failed.`	Error code: 16025 The installer tried to migrate settings from a legacy product, but it encountered an error.	Run the installer again at a later time.

Message	Description	Solution
`Your system is not protected. Your previous security software was uninstalled, but the installer was interrupted before McAfee Endpoint Security was installed. Call McAfee support for assistance as soon as possible.`	Error code: 16029, 16030, 16031 The installer was interrupted before Endpoint Security was installed. Your previous software was uninstalled, but no other changes were made to your endpoint.	To protect your endpoint against threats, contact Technical Support as soon as possible.
`Your system is not fully protected. The installer could not install [product name]. Call McAfee support for assistance.`	Error code: 16032 One or more Endpoint Security product modules failed to install. Your previous software was uninstalled.	To fully protect your endpoint against threats, call Technical Support as soon as possible.
`Policy import failed.`	Error code: 16502 The installer installed Endpoint Security successfully, but couldn't import the specified policy.	Check that you selected the proper data to import. Contact Technical Support if the issue persists.
`Policy import failed.`	Error code: 17001 The installer couldn't import the specified policy.	Check that you selected the proper data to import. Contact Technical Support if the issue persists.
`Installation failed and then rollback failed.`	Error code: 17002 The installer couldn't install Endpoint Security or roll back the changes it made to the user's endpoint.	Check the installation logs on the endpoint and contact Technical Support for assistance.
`Installation canceled and then rollback failed.`	Error code: 17003 The installation was canceled before it completed. The installer couldn't roll back the changes it made to the user's endpoint.	Check the installation logs on the endpoint and contact Technical Support for assistance.
`Another installation wizard is already running.`	Error code: 1618 Another installation is already in progress.	Complete that installation before proceeding with the new installation.
`Endpoint Security Platform is not running!`	The system tray icon also is gray with a red exclamation point. An unknown third-party injection into McAfee code might have been detected.	Check whether McAfee detected an unknown third-party, then run McAfee SysPrep if needed. You can read more about troubleshooting this issue in KB88029.
`The request was rejected because its size (<size>) exceeds the configured maximum (<size>).`	You attempted to check in a client package to the McAfee ePO Master Repository that exceeds the maximum size allowed. This issues occurs because of a limitation on product package sizes.	Use Package Designer to remove unneeded installers from the installation package. Or you can also increase the size limit for uploaded files in McAfee ePO.

Windows errors

Windows displays these error messages when an unexpected condition occurs while installing McAfee Endpoint Security 10.7.x. Use this information to find an explanation of the condition and a solution.

Message	Description	Solution
`Installation failed.`	The installer couldn't install Endpoint Security. It made no changes to the system.	See MsiExec.exe and InstMsi.exe Error Messages for descriptions of specific error codes. If the issue persists, contact Technical Support.
`Threat service has stopped. Restart it now.`	After restarting a system, this message appears in the Virus & threat protection page in Windows Defender Security Center. Threat Prevention tries to send the Endpoint Security security status to the Security Center service. This fails because the Security Center service is not in a running state immediately after a restart. After about two minutes, when the Security Center service is in a running state, Threat Prevention successfully sends the security status and the message no longer appears.	Ignore this message when displayed temporarily after a restart. The security status is automatically corrected about two minutes after the restart.

Endpoint Upgrade Assistant errors

Errors related to upgrades using Endpoint Upgrade Assistant are logged in the Upgrade Automation log file on the endpoint. This log file also contains error codes for custom packages and installers generated with Package Creator.

Code	Description of issue
112	System hardware doesn't meet requirements. Endpoint Upgrade Assistant won't continue.
113	Operating system incompatible. Can't install Endpoint Security 10.5.2 on Windows 10 RS4 or later.
114	Operating system incompatible. Can't install Endpoint Security 10.5.3 on Windows 10 RS4 or later.
115	Operating system incompatible. Endpoint Security, OS mismatch. Can't install Endpoint Security 10.5.4 or 10.6 on Windows 10 October 2018 Update (1810/RS5) or later.
116	Operating system incompatible. Can't install Endpoint Security 10.5.5 or 10.6.1 on Windows 10 April 2019 Update (1903/19H1) or later.
1010	The command line is invalid. Endpoint Upgrade Assistant won't continue.
1618	Endpoint Upgrade Assistant is already running.
3010	Endpoint Security installation encountered an issue, such as an incompatible Exploit Prevention driver, that has been resolved. Restart the endpoint, then installation resumes automatically.
3020	Upgrade completed successfully. Restart the endpoint to activate the upgraded McAfee DLP agent.
5010	The Endpoint Product Removal tool has been run on this endpoint. Endpoint Upgrade Assistant won't continue.

Code	Description of issue
5020	Products incompatible with Endpoint Security detected on endpoint using registry keys. Endpoint Upgrade Assistant won't continue.
5030	Products incompatible with Endpoint Security detected on endpoint using MSI codes. Endpoint Upgrade Assistant won't continue.
5040	Incompatible version of McAfee DLP detected on endpoint. Endpoint Upgrade Assistant won't continue.
5050	Incorrect McAfee Application Control and McAfee Change Control name.
5060	Incompatible version of McAfee Data Exchange Layer Client detected. Endpoint Upgrade Assistant won't continue.
5070	Incompatible version of McAfee® Endpoint Encryption for Files and Folders detected. Endpoint Upgrade Assistant won't continue.
5080	Incompatible version of McAfee Endpoint Encryption for PC detected. Endpoint Upgrade Assistant won't continue.
6010	Unsupported version (10.2) of Endpoint Security detected on endpoint. Endpoint Upgrade Assistant won't continue.
6020	Unsupported version (10.5) of Endpoint Security detected on endpoint. Endpoint Upgrade Assistant won't continue.
6030	Endpoint Security installation encountered an error. Contact Technical Support for assistance.
6040	Incompatible version of VirusScan Enterprise detected on endpoint. Endpoint Upgrade Assistant won't continue.
6050	Incompatible version of McAfee Host Intrusion Prevention detected on endpoint. Endpoint Upgrade Assistant won't continue.
6055	McAfee SysPrep closed with errors. Endpoint Upgrade Assistant won't continue.
6080	A later version of Endpoint Security is already installed.
7000	Failed to copy Endpoint Upgrade Assistant files.
7010	Incompatible version of McAfee Host Intrusion Prevention detected on endpoint. Endpoint Upgrade Assistant won't continue.
7020	Incompatible version of McAfee Host Intrusion Prevention content detected on endpoint. Endpoint Upgrade Assistant won't continue.
8010	McAfee DLP upgrade encountered an issue. Contact Technical Support for assistance.
8020	Endpoint Security Adaptive Threat Protection installation encountered an issue. Contact Technical Support for assistance.
8050	McAfee Active Response installation encountered an issue. Contact Technical Support for assistance.
9010	Endpoint Security Web Control installation encountered an issue. Contact Technical Support for assistance.

Code	Description of issue
9020	Endpoint Security Firewall installation encountered an issue. Contact Technical Support for assistance.
9030	VirusScan Enterprise installation encountered an issue. Contact Technical Support for assistance.
9040	Endpoint Security Platform installation encountered an issue. Contact Technical Support for assistance.
9050	Restart required after the last Windows Update. Endpoint Upgrade Assistant won't run if it detects a restart pending after a Windows Update. Restart the endpoint, then start the upgrade again.
9060	McAfee Data Exchange Layer installation or upgrade encountered an issue. Contact Technical Support for assistance.
9061	McAfee Application Control and McAfee Change Control installation or upgrade encountered an issue. Contact Technical Support for assistance.
9070	Endpoint Security Platform update installation encountered an issue. Contact Technical Support for assistance.
9071	Endpoint Security Threat Prevention update installation encountered an issue. Contact Technical Support for assistance.
9072	Endpoint Security Firewall update installation encountered an issue. Contact Technical Support for assistance.
9073	Endpoint Security Web Control update installation encountered an issue. Contact Technical Support for assistance.
9074	Endpoint Security Adaptive Threat Protection update installation encountered an issue. Contact Technical Support for assistance.
-1	Endpoint Security installation failed. Contact Technical Support for assistance.

Installation log files

McAfee Endpoint Security 10.7.x installation files

The McAfee Endpoint Security 10.7.x installer tracks details about installation, uninstallation, and migration in log files that you can use to verify results and troubleshoot problems.

Default location of installation log files

By default, the installer saves the installation log files to this location:

When...	Log location	Path
Deploying remotely (using McAfee ePO or a third-party tool)	Windows System TEMP folder	C:\Windows\TEMP\McAfeeLogs
Running the installer locally on the endpoint	User TEMP folder — %Temp% \McAfeeLogs	C:\Users\username\AppData\Local \Temp\McAfeeLogs

Endpoint users must have permission to access the file.

The path for the installation log location can include case-sensitive folders. After installation, the Endpoint Security self-protection feature prevents changing the case sensitivity of the endpoint log location configured in the Common Options policy or moving the log location to a case-sensitive folder.

Changing the location of installation log files

Use one of these command-line options to change the location for the log files:

```
/log"install_log_path"
/l"install_log_path"
/l*v"install_log_path"
```

where:

- `"install_log_path"` — Specifies where to save the installation log files.
  The installer creates an `Endpoint` folder at the specified location and saves the log files to this folder.
- `*v` — Specifies verbose (more descriptive) logging entries.

Example

```
/l"D:\Log Files"
```

Installs the product log files under `D:\Log Files\EndPoint\`.

Support for case sensitivity (Microsoft Windows 10 October 2018 Update or later)

The installer can save logs to a folder with a case-sensitive path. After installation, the Endpoint Security self-protection feature prevents you from changing the case sensitivity of the Endpoint Security client log location configured in the Common Options policy or moving that log location to a case-sensitive folder.

Installation and migration log files

Check these log files for details about installation and migration.

Log file name	Type of information
McAfee_<module>_Install_<%timestamp%>.log	Installation log for each product module.
McAfee_<Module>_Bootstrapper_<%timestamp%>.log	Bootstrapper for each product module.
McAfee_Endpoint_BootStrapper_<%timestamp%>.log	Bootstrapper for the Master installer (SetupEP) on self-managed systems.
McAfee_<Module>_CustomAction_Install_<%timestamp%>.log	MSI Custom Action for each product module.
McAfee_Endpoint_CompetitorUninstaller.log	Removal of incompatible virus-protection and firewall products.
McAfee_Endpoint_Security_Migration_xxx.log	Removal of legacy products. Example: McAfee_Endpoint_Security_Migration_McAfee VirusScan Enterprise_8.8_06042015195245175.log
McAfee_<module>_Migration_Plugin.log	Preserve and restore status of migrated legacy settings, per module. Example: McAfee_TP_Migration_Plugin.log
McAfee_ESP_Migration_Plugin.log	Legacy settings migrated to the Common Options policy.

Uninstallation log files

Check these log files for details about removing the product.

Log file name	Type of information
McAfee_<Module>_UnInstall<%timestamp%>.log	Uninstallation log for each product module.
McAfee_<Module>_CustomAction_Uninstall<%timestamp%>.log	MSI Custom Action for each product module for uninstallation.
McAfee_CommonUninst<%timestamp%>.log	Uninstallation log for Common module (which is uninstalled with last product module).
McAfee_ Common_VScore_Uninstall<%timestamp%>.log	Log for VSCore driver removal by Common module.
McAfee_ Firewall_FireCore_Uninstall<%timestamp%>.log	Log for FireCore driver removal by Common module. (Created only for versions 10.5.2 and earlier.)
McAfee_ ThreatPrevention_Caspercore_Uninstall<%timestamp%>.log	Log for CasperCore driver removal by Threat Prevention.
McAfee_ ThreatPrevention_ELAM_AVDriver_Uninstall<%timestamp%>.log	Log for ELAM driver removal by Threat Prevention. (Created only for versions 10.5.2 and earlier.)
McAfee_ ThreatPrevention_EP_Uninstall<%timestamp%>.log	Log for Exploit Prevention removal by Threat Prevention. (Created only for versions 10.5.2 and earlier.)

Upgrade Automation and Endpoint Upgrade Assistant Package Creator files

Events that occur during upgrades to McAfee Endpoint Security 10.7.x that are managed using Endpoint Upgrade Assistant are reported in the Upgrade Automation log file on the endpoints where they occur. Additionally, Package Creator reports events related to generating or deploying custom installation packages to the same log file.

The Upgrade Automation software, which is deployed to endpoints during upgrades to manage the upgrades, creates the Upgrade Automation log file at this location: %windir%\Temp\McAfeeLogs\EndpointUpgradeAutomation.log

You can specify a new location when you create an Upgrade Automation deployment task or custom installation package.

More than one product component might report entries to the Upgrade Automation log during the upgrade process.

When you do this...	Upgrade Automation log file location is...	Notes
Create a custom package or installer	On the endpoint where you run Package Creator	Package Creator generates the log file.
Deploy a custom package using McAfee ePO	On the endpoint you deploy the upgrade to	Upgrade Automation generates the log file. If you deploy to the same endpoint where you created the custom package, Upgrade Automation appends data to the log file created by Package Creator.
Deploy a custom installer using a third-party tool	On the endpoint you deploy the upgrade to	The installer uses the same product removal and installer logic as Upgrade Automation, and generates a log file with the same name and a similar signature as Upgrade Automation. If you deploy to the same endpoint where you generated the custom installer, the product installer appends

When you do this...	Upgrade Automation log file location is...	Notes
		data to the data it already reported in the log file.

Troubleshooting McAfee Endpoint Security 10.7.x installation issues

Resolve issues that occur when attempting to deploy and install McAfee Endpoint Security 10.7.x on an endpoint.

Installation failures

Resolve these issues that can occur during installation, then attempt the installation again.

If installation fails because...	Do this...
Case-sensitivity is enabled for folders that the installer needs to access.	Disable the case-sensitivity attribute for folders in your source and target installation paths and \Windows\System32\drivers. Required on endpoints running Microsoft Windows 10 October 2018 Update or later.
Client system users don't have permission to access the user temp folder.	Choose one of the following: • Check and update permissions as needed. • Change the folder location temporarily by changing the value for the TEMP and TMP variables to c:\temp, then change them back after installation is complete.
Third-party injectors were detected.	Choose one of the following: • Run McAfee SysPrep to detect and allow trusted third-party software to inject into McAfee processes. • Temporarily remove or disable third-party applications that attempt to inject or hook into the Endpoint Security installation processes.
Installation package size exceeds the maximum size limit in McAfee ePO.	Choose one of the following: • Increase the limit before checking in the package to the McAfee ePO server. • Use Endpoint Security Package Designer to remove unneeded files from the installation package.
Software Catalog (Software Manager on McAfee ePO 5.9.x) is busy checking in required software packages.	Wait until the packages are checked in, then begin installation again. Or, if another task is updating the Software Catalog (Software Manager on McAfee ePO 5.9.x) , you can stop the task.
Root certificates are missing.	Install the latest root certificates, which are required to validate the digital signatures of product files. Missing root certificates can also cause fields not to populate.
Files were left behind by a previous installation of Endpoint Upgrade Assistant.	Remove these files before attempting to install Endpoint Upgrade Assistant again.
The products you removed were reinstalled before Endpoint Upgrade Assistant could install the new versions.	Disable features that detect uninstalled products and reinstall them automatically.

Products don't work as expected

Best practice: For optimal performance and protection, install the same version of the Endpoint Security modules or upgrade all modules to the latest version.

Use these recommendations to resolve unexpected behavior in other products after installing Endpoint Security.

If...	Then...
Third-party applications aren't working correctly after installing Endpoint Security Firewall, and you didn't preconfigure custom Firewall rules.	Enable Adaptive mode to determine whether Firewall is blocking those applications.
Common Event Enabler (CEE)/Common AntiVirus Agent (CAVA) was running with Endpoint Security before the upgrade, and the upgrade occurred without CAVA.	Reinstall Endpoint Security, using the /CAVA command-line option. If you don't use the command-line option when upgrading from a previous version of Endpoint Security with CAVA, the upgrade occurs without CAVA.
The endpoint stops responding (hangs) when memory protection features in McAfee Application Control, McAfee Change Control 8.x or 7.x, and Endpoint Security or Host Intrusion Prevention are running at the same time.	Disable Application Control and Change Control memory protection features, then use the Endpoint Security or Host Intrusion Prevention memory protection features.
You want to check that Real Protect is installed correctly and that endpoints can communicate with the McAfee cloud for detections.	To test Real Protect detection functionality, you can download and run password-protected test files.

Resolving compatibility issues using Firewall Adaptive mode

If third-party applications aren't working correctly after installing Endpoint Security Firewall 10.7.x, and you didn't preconfigure custom Firewall rules, you can enable Adaptive mode to determine whether Firewall is blocking those applications.

Enabling Adaptive mode allows Endpoint Security Firewall to create client rules automatically, so that necessary applications and websites are not blocked while preserving minimum protection against vulnerabilities.

Adaptive mode analyzes events, then if the activity is considered regular and needed for business, Firewall creates client rules.

By enabling Adaptive mode, you can gather the information you need for tuning your protection settings. You can then convert client rules to server-mandated policies. When tuning is complete, turn off Adaptive mode.

Best practice: To be fully protected by Firewall, turn off Adaptive mode after updating your policies.

You can enable Adaptive mode in these ways:

- From McAfee ePO — In the Firewall Options settings, then apply this policy to the client.
- From Endpoint Security Client — In the Firewall Options settings, do one of these:
    - Click Firewall on the main Endpoint Security status page, then click Advanced and select Adaptive mode.
    - From the Action menu, select Settings, then click Firewall on the Settings page, then click Advanced and select Adaptive mode.

Troubleshooting multiple-product upgrades

Issues when analyzing and preparing deployments

Use this information to resolve issues that occur when using Endpoint Upgrade Assistant to analyze your environment and deploy upgrades to McAfee Endpoint Security 10.7.x.

Issues with analyzing your environment and preparing to upgrade

If you see...	Do this...
Inconsistent product version numbers reported in tables	Refresh the McAfee ePO database, then click Re-Analyze Environment to refresh the page.
Endpoints incorrectly reported as blocked	Refresh the McAfee ePO database, then click Re-Analyze Environment to refresh the page.
The number of endpoints reported by Endpoint Upgrade Assistant doesn't match the number you expect (for example, the number of workstations, servers, or upgrade steps)	Export and download a list of endpoints and their details in CSV format.
Missing software packages highlighted on the Prepare tab	Install the highlighted packages, then click Re-Analyze Environment to refresh the page.
Endpoint Upgrade Assistant takes too long to analyze your environment	Analyze smaller groups of endpoints separately. Select a System Tree group (a subset of endpoints) when you configure an analysis, then configure more analyses with different groups until all endpoints are analyzed.
Outdated information appears in reports	Click Re-analyze Environment, then regenerate the report.
You don't have the required McAfee ePO permissions to analyze your environment	Adjust the permissions.

Issues with deploying upgrades to endpoints

If installation fails because...	Do this...
You don't have the required McAfee ePO permissions to install	Adjust the permissions configured for View and change task settings in the McAfee Agent permission set.
Installation package size exceeds the maximum size limit of 250 MB in McAfee ePO	Choose one of the following: • Increase the limit before checking in the package to the McAfee ePO server. • Use Package Creator to remove unneeded files from the installation package.
Third-party injectors were detected	Download the latest version of McAfee SysPrep from the McAfee Product Downloads site and check it in to each McAfee ePO branch, then deploy the upgrade again. When Upgrade Automation runs on the endpoint, it downloads and runs the updated McAfee SysPrep package.
The product versions or features you want to upgrade aren't supported in Endpoint Upgrade Assistant or Package Creator	Download and install the latest versions from the McAfee Product Downloads site. Use the same version of Endpoint Upgrade Assistant and Package Creator (for example, version 2.6.x of both).
Installation or upgrade was interrupted and requires a restart to continue	Restart the endpoint, then Endpoint Upgrade Assistant automatically resumes the installation or upgrade. When you install or upgrade a McAfee product that includes SysCore while Exploit Prevention is enabled (in Endpoint

If installation fails because...	Do this...
	Security or McAfee Host IPS), Endpoint Upgrade Assistant runs the mfeepmpk_utility.exe utility to detect and replace faulty drivers. If it installs a new driver, the endpoint must be restarted before Endpoint Upgrade Assistant can resume the installation or upgrade. In this case, Endpoint Upgrade Assistant closes and adds this information to the last line of the log file: • Code — `3010` • Message — `EUA_MFEEMPMK_UTIL_REQUIRES_REBOOT`

Issues after deploying upgrades to endpoints

After deploying an Upgrade Automation deployment task to upgrade to McAfee Endpoint Security 10.7.x , use these steps to resolve problems reported in the Upgrade Automation log file on the endpoint. The Upgrade Automation software is deployed with each upgrade to manage the upgrade on the endpoint.

Upgrade Automation updates its log file for each step of the troubleshooting process.

- In a test environment — Use these steps to ensure Upgrade Automation works correctly.
- In your production environment — Use these steps when an Upgrade Automation task fails.

Task

1. On endpoints, monitor progress in the Agent Monitor, where details about the actions performed by client deployment tasks are logged.
2. Verify that the Endpoint Upgrade Assistant package downloaded McAfee Agent and Endpoint Security. See the table below for more information.
   If McAfee Agent 4.x was installed on the endpoint before upgrading, then FOLDER PATH is C:\ProgramData\McAfee\Common Framework\[Current|Previous|Evaluation]

   If McAfee Agent 5.x was installed on the endpoint before upgrading, then FOLDER PATH is C:\ProgramData\McAfee\Agent\[Current|Previous|Evaluation]

These folders indicate that the download was successful	Product

`<FOLDER PATH>\ENDP_AM_1050`
`<FOLDER PATH>\ENDP_AM_1060`
`<FOLDER PATH>\ENDP_FW_1050`
`<FOLDER PATH>\ENDP_FW_1060`
`<FOLDER PATH>\ENDP_GS_1050`
`<FOLDER PATH>\ENDP_GS_1060`
`<FOLDER PATH>\ENDP_WP_1050`
`<FOLDER PATH>\ENDP_WP_1060`
	Endpoint Security 10.5 or 10.6

`<FOLDER PATH>\EPOAGENT3000`	McAfee Agent 5.0.5 or later
`<FOLDER PATH>\EUA_AUTO1000`	Upgrade Automation package (contains three .exe and two script files)

   Potential remediation step: Make sure the correct versions of McAfee Agent (version 5.0.5 or later) and Endpoint Security (version 10.5.x or 10.6) are checked in to the same branch in McAfee ePO that the Upgrade Automation package was deployed from (for example, Current, Previous, or Evaluation).
3. Verify that there aren't any conflicting products on the endpoint that could stop the Upgrade Automation package from running. Check the logs for this information:

Log entry	Indicates
`All steps completed successfully for product: ENS_HW_Requirements`	Success
`All steps completed successfully for product: ripper_conflict`	Success
`All steps completed successfully for product: ENS_RegistryConflicts`	Success
`All steps completed successfully for product: ENS_MSIConflicts`	Success
`OneBuild progress set to: COPY_FILES_COMPLETE`	Success
`All steps completed successfully for product: ENS1050_Conflicts`	Success
`All steps completed successfully for product: ENSSuccess`	Success

Potential remediation step: Remove conflicting products and redeploy the Upgrade Automation package to the endpoint.

4. Verify that VirusScan Enterprise and Host Intrusion Prevention policies were copied successfully on the endpoint.

Log entry	Indicates
`Step preserve_policy completed successfully for product: VSE 8.8`	Success
`Step preserve_policy failed for product: VSE 8.8`	Failure
`Step preserve_policy completed successfully for product: HIPS 8.0`	Success
`Step preserve_policy failed for product: HIPS 8.0`	Failure

Potential remediation step: If an error occurs while copying policies, it does not stop the installation. After Endpoint Security is installed on the endpoint, it pulls the latest policies from McAfee ePO.

5. Verify that McAfee Agent upgraded successfully.

Log entry	Indicates
`FramePkg.exe -- SUCCESS`	Success
`FramePkg.exe -- FAIL`	Failure

Potential remediation step: Contact Technical Support if the upgrade stops.

6. Verify that Endpoint Security installed successfully.

Log entry	Indicates
`setupCC.exe succeeded`	Success

Log entry	Indicates
`setupCC.exe --FAIL`	Failure
`setupTP.exe succeeded`	Success
`setupTP.exe --FAIL`	Failure

Potential remediation steps:

- If Endpoint Upgrade Assistant closes, and reports the code 3010 and the message `EUA_MFEEMPMK_UTIL_REQUIRES_REBOOT` in the last line of the log file, the McAfee Exploit Prevention driver was upgraded on the endpoint. Restart the endpoint, then Endpoint Upgrade Assistant automatically resumes installing Endpoint Security.
- Contact Technical Support if the installation stops.

7. Verify that Upgrade Automation finished successfully.

Log entry	Indicates
`All steps completed successfully for product: ENSSuccess`	Success
`OneBuild exit code is 0`	Success

Reporting events in System Custom Property fields for McAfee Endpoint Security 10.7.x upgrades

When deploying McAfee Endpoint Security 10.7.x upgrades, Endpoint Upgrade Assistant provides the ability to monitor some endpoint events by using command-line options. This allows you to know when specific events occur and respond to them, if needed. For example, you can check when it's time to restart the endpoint after upgrading McAfee DLP.

Events are reported in one of the four Custom fields that appear on the System Properties tab of the McAfee ePO System Details page.

To enable this feature, create an Upgrade Automation deployment task in McAfee ePO and specify this command-line option:

`--tag[=1-4]`

where 1–4 specifies one of four Custom fields.

For example, `--tag=3` reports endpoint events in the Custom 3 field, and `--tag` or `--tag=1` reports in the Custom 1 field.

Supported events for Custom fields

Not all upgrade workflows use all the supported event properties. Endpoint Upgrade Assistant reports these properties:

Property	Description
EUA_CLIENT_EXECUTION_STARTED	Endpoint upgrade has started.
EUA_REBOOT_REQUIRED ENS_INSTALL_PENDING	Restart the endpoint.
EUA_ENDPOINT_REBOOTED ENS_INSTALLING	• Endpoint has been restarted. • Endpoint Security is installing.
EUA_EXECUTION_COMPLETE	• Deployment task is completed. • Check the status of the deployment task on the Deploy & Track tab.
EUA_EXECUTION_COMPLETE REBOOT_REQUIRED DLP_UPGRADED	• Deployment task is completed. • Check the status of the deployment task on the Deploy & Track tab. • Restart the endpoint to enable McAfee DLP.

These are some general guidelines for using the Custom fields:

- Endpoint Upgrade Assistant doesn't remove or change the value displayed. For example, if you restart an endpoint, the REBOOT_REQUIRED value doesn't change.
- The value in the Custom field isn't updated or removed until it is overwritten by another task on the endpoint.
- If a Custom field is being used by another application for another purpose, reporting for Endpoint Upgrade Assistant might be affected.
- The `--tag` option is not related to tagging endpoints for updates in the System Tree.

Refresh the McAfee ePO 5.10.x–5.9.x database

To analyze the products installed on endpoints, Endpoint Upgrade Assistant queries the McAfee ePO 5.10.x or 5.9.x database. Refreshing the information in the database ensures that all products installed on the endpoints in your environment are reported correctly.

When the version information for McAfee products on one or more endpoints is not correctly captured in the database, those endpoints are blocked from upgrades. In some cases, endpoints might report blank or incorrectly formatted version information. You can often resolve issues reported in Endpoint Upgrade Assistant by sending endpoints an agent wake-up call that asks for full properties.

Task

1. From the Overview tab, select Export System and Product Details to export details about these endpoints in CSV format.
   Use this information to identify and resolve issues with each endpoint.
2. Create a McAfee ePO task to update the client properties for these specific endpoints.
   This refreshes the information in the McAfee ePO database.

Remove files after a failed installation of Endpoint Upgrade Assistant

If Endpoint Upgrade Assistant fails to completely install, you need to manually remove the components that were installed before attempting to install it again.

Before you begin

Examine the Orion logs to determine why the installation failed. If McAfee ePO is installed in the default location, the logs are located under C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\Logs.

Task

1. Remove the extension .xml from C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\conf\Catalina\localhost \UpgradeAssistant.XML.
2. Remove the extensions directory from C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\extensions\installed \EndpointUpgradeAssistant.
3. Remove the OrionExtensions entry from the McAfee ePO database table.
   Run the following SQL query:

   ```
   DELETE FROM dbo.OrionExtensions WHERE Name = 'EndpointUpgradeAssistant'
   ```

4. *(Optional)* Restart the McAfee ePO server only if you can't execute the first two steps (for example, if the files are locked).

Reporting an issue to McAfee Support

When reporting an issue to McAfee Support, it is important to collect and send all the required information.

Collecting product data to send to McAfee

You need to use the MER (Minimum Escalation Requirements) tool to collect required McAfee data from Endpoint Security and other McAfee products on your endpoint, such as:

- Registry details
- File version details
- Files
- Event logs
- Process details

Technical Support uses this data to analyze and resolve your problem.

Required information

Provide this information to McAfee when reporting an issue:

- Data collected by MER
- Brief description of the issue — If possible, provide the steps required to reproduce the issue.
- Screen shots
- McAfee ePO server logs from the time when the issue occurred
- Approximate number of endpoints running in your environment
- Version numbers for:
    - McAfee ePO
    - Endpoint Security product modules
- If you upgraded using Endpoint Upgrade Assistant:
    - Version of the Endpoint Upgrade Assistant product extension
    - An export of the endpoint's system and product details, if relevant

Export system and product information

Search, sort, filter, and validate results from Endpoint Upgrade Assistant by downloading the information for a selected category in comma-separated values (CSV) format. Send this information to McAfee support when reporting an issue with Endpoint Upgrade Assistant, or use it to troubleshoot issues, identify the endpoints required for upgrades, and resolve differences between the reported and expected status of endpoints.

Task

1. From the Overview tab, in the Environment Overview table, click Export System and Product Details.
2. Import this data into Microsoft Excel, then sort and filter as needed to identify the endpoints outside your expected groupings.

Remove the Endpoint Security 10.7.x software

Using a new McAfee ePO deployment task

To remove McAfee Endpoint Security 10.7.x from a group of McAfee ePO or MVISION ePO endpoints, you can schedule a new deployment task in McAfee ePO 5.10.x or 5.9.x .

This might be useful for testing or before reinstalling the client software.

Caution: Reinstall the client software as soon as possible. When it is uninstalled, the endpoint is not protected against threats.

Best practice: Duplicate the task you used to install the product, then change the Action to Remove.

Task

1. From McAfee ePO, select Menu → Software → Product Deployment.
2. On the Product Deployment page, click New Deployment.
3. On the New Deployment page:
   a. Enter a name for the task.
   b. Select each module you want to remove from the Package drop-down list, clicking + each time you want to select another one.
      Endpoint Security Platform, also called the Common module, is removed automatically with the last module.
   c. Change the Action to Remove.
   d. Select the endpoints to remove the product from.
   e. Configure any other settings, then click Save at the top of the page.
      The Product Deployment page opens with your new project added to the list of deployments. Also, a client task is automatically created with the settings.

Results

To verify that the client software was removed from the selected endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that the software was removed from the correct number of endpoints.

Using your original McAfee ePO deployment task

If you've saved the McAfee ePO 5.10.x or 5.9.x deployment task that you used to install McAfee Endpoint Security 10.7.x, you can use it to remove the product from a group of McAfee ePO or MVISION ePO endpoints.

Before you begin

- You must know the group name of the endpoints where the product software is installed to use the uninstall feature in Product Deployment.
- If there are any endpoints you don't want to uninstall the product software from, move them to a different group before starting this process.

This product software uninstallation process uses the product deployment task created during your initial software installation. When the uninstallation task is complete, all endpoints in the System Tree group specified at installation have all product software removed.

Task

1. McAfee ePO, select Menu → Software → Product Deployment.
2. From Advanced Options, select Advanced Product Deployment.
3. In the System Tree list, select the deployment task that you used to initially create the installation URL.
4. With the product deployment task selected, in the Action list, click Remove.
5. Click OK.
   The configured product software is removed from all endpoints in the selected System Tree group. When the removal is finished, the message Uninstall Successful appears with the number of updated endpoints shown in parentheses.

Results

To verify that the client software was removed from the selected endpoints, select Menu → Reporting → Dashboards, then select Endpoint Security: Installation Status. Check that the software was removed from the correct number of endpoints.

Using the Windows Control Panel

You can remove McAfee Endpoint Security 10.7.x by using the Windows Control Panel on the endpoint. You might do this for testing or before reinstalling the product on a single endpoint.

Caution: Reinstall the client software as soon as possible. When it is uninstalled, the endpoint is not protected against threats.

Task

1. On the endpoint, open the Windows Control Panel, then go to the Uninstall Programs screen.
2. From the list of programs, select each installed product module, then click Uninstall.
   - McAfee Endpoint Security Adaptive Threat Protection — Must be uninstalled before uninstalling Threat Prevention.
   - McAfee Endpoint Security Firewall
   - McAfee Endpoint Security Threat Prevention
   - McAfee Endpoint Security Web Control

   Endpoint Security Platform (Common module) is uninstalled automatically with the last product module. You can't uninstall it while other product modules are installed.
3. If prompted, enter a password.
   By default, no password is required.
4. Wait for the installer to report that it has removed the support components. If you do not see a notification, check the Event Log to verify that Endpoint Security Platform was removed successfully.
5. If no other McAfee products are installed, select McAfee Agent in the Uninstall Programs screen of the Windows Control Panel, then click Uninstall.

COPYRIGHT

McAfee
Together is power.