McAfee Endpoint Security 10.6.0 - Installation Guide - Linux
COPYRIGHT
Copyright © 2019 McAfee, LLC

TRADEMARK ATTRIBUTIONS
McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
## Contents

1. **Installation overview** ........................................... 5
   - First time installation ........................................ 5
   - Upgrade installation workflow ................................. 6

2. **System requirements** ............................................ 9

3. **Install the software on systems managed with McAfee ePO** ...... 11
   - Check in the packages to the McAfee ePO server .................. 11
   - Check in the package using Software Manager .................... 11
   - Check in the package manually .................................. 12
   - Install the extensions on the McAfee ePO server ................. 12
   - Install the extensions using Software Manager ................... 13
   - Install the extensions manually ................................ 13
   - Install the client software on a managed system using the installation URL .... 13
   - Create an installation URL ..................................... 14
   - Install the software with an installation URL on a managed system ........ 14
   - Deploy the client software from McAfee ePO .................... 15
   - Test the installation .......................................... 15
   - Remove the software from a managed system ..................... 16
   - Remove the software extensions ................................ 16
   - Remove the software from client systems ....................... 16

4. **Install the software on a system managed with McAfee ePO Cloud** .. 19
   - McAfee ePO Cloud components .................................. 19
   - Accessing the McAfee ePO Cloud account ....................... 19
   - Install the client software on managed systems using the installation URL .... 20
   - Create an installation URL ..................................... 20
   - Install the software with an installation URL .................... 20
   - Deploy the client software from McAfee ePO Cloud ............. 21

5. **Install software on standalone Linux systems** .................. 23
   - Install Threat prevention module on standalone systems .......... 23
   - Verify the signature on Ubuntu systems ........................ 23
   - Verify the signature on RPM-based systems ...................... 24
   - Install Threat Prevention module ................................ 24
   - Enable or disable Fanotify and kernel modules .................. 25
   - Install Threat Prevention module using the package management tools .... 26
   - Extract rpm or deb files from the package ....................... 26
   - Install the software from the YUM repository .................... 27
   - Install the software from the Zypper repository ................ 27
   - Install software from the Advanced Packaging Tool (APT) repository ...... 27
   - Install Firewall module on standalone systems .................. 28
   - Install Firewall in prompt mode ................................ 28
   - Install Firewall in silent mode .................................. 28
   - Upgrade the software .......................................... 29
Installation overview

McAfee® Endpoint Security for Linux includes tar.gz files to install or upgrade Threat Prevention (including Access Protection) and Firewall modules on Linux systems.

The McAfee Endpoint Security for Linux includes these modules:

- Threat Prevention (including Access Protection)
- Firewall

The McAfee Endpoint Security Common module is automatically installed with any of the Endpoint Security modules.

Contents

- First time installation
- Upgrade installation workflow

First time installation

When installing the software for the first time, you must install server-side software on the management server, then deploy the client software remotely to managed systems or ask users to install it locally.

1. Check in the product package files to the McAfee ePO server.

2. Manually update your McAfee ePO server with the latest content files required for Endpoint Security.

3. Deploy the client software with default or custom settings to managed systems using the deployment task.

4. Verify that the client software is installed and up to date on all managed systems.
Upgrade installation workflow

Upgrade from a previous version of Endpoint Security for Linux or from a supported legacy product.

1. Confirm that your upgrade path is supported.

2. Check in the product package files and the McAfee Agent package files (if required) to the McAfee ePO server.

3. Upgrade McAfee Agent, if required.

4. Deploy the client software with default or custom settings to managed systems using the deployment task:

5. Verify that the client software is installed and up to date on all managed systems.
Installation overview
Upgrade installation workflow

1. Start your installation.
2. Make sure your product upgrade path is supported.
3. (Optional) Review and prepare custom settings.
4. Upgrade McAfee Agent, if needed.
5. Create a product deployment task.
6. Tasks for first-time installation
   - Additional tasks for upgrade
   - Optional tasks for saving custom settings
7. Verify that product software installed.
8. (Optional) Verify that settings were saved.
9. Done.
System requirements

Systems must meet specific hardware and software specification to install and use the software. Review the requirements before installing or upgrading the software.

Hardware

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>• Intel x86_64 architecture-based processor that supports Intel Extended Memory 64-bit technology (Intel EM64T)</td>
</tr>
<tr>
<td></td>
<td>• AMD x86_64 architecture-based processor with AMD 64-bit technology</td>
</tr>
<tr>
<td>Memory</td>
<td>Minimum: 2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Recommended: 4 GB RAM</td>
</tr>
<tr>
<td>Free disk space</td>
<td>Minimum: 4 GB in the installation directory</td>
</tr>
</tbody>
</table>

Operating systems

For a list of supported distributions for Threat Prevention, see McAfee Knowledge Base KB87073.

For a list of supported distributions for Firewall, see McAfee Knowledge Base KB91326.

This product cannot be used on 32-bit platforms.

Management platform

• McAfee ePolicy Orchestrator — 5.3.x or later.
• McAfee Agent — 5.6.0 (64-bit) or later.
• McAfee Endpoint Security ePO extension update:
  • Endpoint Security platform extension 10.6.1.1105
  • Endpoint Security Threat Prevention extension 10.6.1.1107
  • Endpoint Security Firewall extension 10.6.1.1088
• McAfee Endpoint Security license extension — 10.6.0 or later.
Install the software on systems managed with McAfee ePO

Install and manage the software on a system that is managed with McAfee ePO. McAfee ePO is an extensible management platform that enables centralized policy management and enforcement of your security products and the systems where they are installed.

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

Contents
- Check in the packages to the McAfee ePO server
- Install the extensions on the McAfee ePO server
- Install the client software on a managed system using the installation URL
- Deploy the client software from McAfee ePO
- Test the installation
- Remove the software from a managed system

Check in the packages to the McAfee ePO server
You can check in the Endpoint Security for Linux packages using the Software Manager or check in the package manually.

Tasks
- Check in the package using Software Manager on page 11
  Check in McAfee Endpoint Security for Linux using the Software Manager.
- Check in the package manually on page 12
  Manually check in the McAfee Endpoint Security for Linux deployment packages to the McAfee ePO Master Repository to manage the software.

Check in the package using Software Manager
Check in McAfee Endpoint Security for Linux using the Software Manager.

Task
1. Log on to the McAfee ePO server as an administrator.
2. From the Software Manager | Product Categories | Software (By Label), Select Endpoint Security | McAfee Endpoint Security for Linux 10.6, select from the right pane, then click Check in All.
For Threat Prevention:
- McAfee ESP KernelModule <version_number> <build_number>
- McAfee Endpoint Security for Linux Threat Prevention <version_number> <build_number>

For Firewall:
- McAfee Endpoint Security for Linux Firewall <version_number> <build_number>

3 On the summary page, accept the McAfee End User License Agreement, then click OK.

Check in the package manually
Manually check in the McAfee Endpoint Security for Linux deployment packages to the McAfee ePO Master Repository to manage the software.

Task
1 Download the .zip file from the McAfee download site to a temporary location on the McAfee ePO server.
2 Log on to the McAfee ePO server as an administrator.
3 Select Menu | Software | Master Repository | Check In Package.
   a For Package type, select Product or Update (ZIP).
   b Click Choose File, select the file, click Choose, then click Next.
   c Select Current as the branch.
4 Click Save.
Repeat this step to check in these packages:
For Threat Prevention:
- McAfeeESP-KernelModule-<version_number>-<build_number>-Release-ePO.zip
- ISecTP-<version_number>-<build_number>-Release-ePO.zip
For Firewall:
- McAfeeFW-<version_number>-<build_number>-Release-ePO.zip

Install the extensions on the McAfee ePO server
Install the extensions on the McAfee ePO server to be able to configure and deploy policies for managed systems.
You must install these extensions in this order to enable the features of the product:
• Endpoint Security for Linux License — Endpoint Security for Linux license extension to view the operating system-specific tag in the policy and task options.
• Endpoint Security Platform — Endpoint Security Common policy extension.
• These product modules as required:
  - Endpoint Security Threat Prevention extension.
  - Endpoint Security Firewall extension.
After installing the extensions, you can install McAfee Endpoint Security Migration Assistant extension to migrate McAfee VirusScan for Linux 1.9 and 2.0.x and McAfee Firewall for Linux 8.0 policies and tasks. For information about installing and using the Endpoint Security Migration Assistant, see McAfee Endpoint Security Migration Guide.

**Tasks**

- *Install the extensions using Software Manager on page 13*
  Install the extensions using the Software Manager.

- *Install the extensions manually on page 13*
  Manually install Endpoint Security extensions on the McAfee ePO server.

**Install the extensions using Software Manager**

Install the extensions using the Software Manager.

**Task**

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

2. Select *Menu, Software*, then click *Software Manager*.

3. From the *Software Manager | Product Categories | Software (By Label)*, select *Endpoint Security | McAfee Endpoint Security for Linux 10.6*, select from the right pane, then click *Check in All*.

**Install the extensions manually**

Manually install Endpoint Security extensions on the McAfee ePO server.

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

**Task**

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

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

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

   You must install the extensions in this order:
   - Endpoint Security for Linux License — Endpoint Security for Linux license extension to view the operating system-specific tag in the policy and task options.
   - Install these extensions as required:
     - McAfee ESP KernelModule `<version_number>` `<build_number>`
     - Endpoint Security Threat Prevention extension.
     - Endpoint Security Firewall extension.

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

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

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

- **Create an installation URL on page 14**
  Create an installation URL and send it to the users so that they can install McAfee Agent on their managed systems.

- **Install the software with an installation URL on a managed system on page 14**
  The user accesses the URL to install the client software on a managed system.

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

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

1. Log on to the McAfee ePO server as an administrator.
2. Select Menu | Dashboards, then select Getting Started with ePolicy Orchestrator from the drop-down list.
3. On the Product Deployment page, click Start Deployment, define these settings, then click Deploy.
   - System Tree Group
   - McAfee Agent
   - Software and Policies
   - Auto Update
4. On the Initial Product Deployment Summary page, click OK.
   On the Dashboard page, the installation URL appears under Product Deployment section.
5. Email the URL with instructions to install the client software on the system.
   After successful installation, McAfee Agent checks back with the McAfee ePO server for assigned tasks for that system group, then installs the software accordingly.

Install the software with an installation URL on a managed system
The user accesses the URL to install the client software on a managed system.

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

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

1. Open a browser window, paste the installation URL in the address bar, then press Enter.
2. Follow the on-screen instructions.
3. If the installation does not start automatically, click Install.
Deploy the client software from McAfee ePO

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

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

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

**Task**

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. On the **Assigned Client Tasks** tab, click **Actions**, then click **New Client Task Assignment**.
4. Complete these options, then click **Create New Task**:
   a. For product, select **McAfee Agent**.
   b. For task type, select **Product Deployment**.
5. On the **Client Task Catalog** page:
   a. Type a name for the task.
   b. Select **Linux** as the target platform.
   c. In **Products and components**, select the product, select **Install** as the action, then click **Save**.

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

Test the installation

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

**Task**

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

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

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

**Tasks**
- *Remove the software extensions on page 16*
  Remove the extensions from the McAfee ePO server.
- *Remove the software from client systems on page 16*
  Create a client task on the McAfee ePO server to remove McAfee Endpoint Security for Linux from your managed systems.

**Remove the software extensions**
Remove the extensions from the McAfee ePO server.

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

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu | Software | Extensions**.
3. In the left pane, select the extension, then click **Remove**.
4. Select **Force removal, bypassing any checks or errors**, then click **OK**.

**Remove the software from client systems**
Create a client task on the McAfee ePO server to remove McAfee Endpoint Security for Linux from your managed systems.

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

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

8 Select **Force complete policy and task update**, then click **OK**.
Install the software on systems managed with McAfee ePO
Remove the software from a managed system
Install the software on a system managed with McAfee ePO Cloud

Install and manage the software on a system that is managed with McAfee ePO Cloud. McAfee ePO Cloud is an extensible management platform that enables centralized policy management and enforcement of your security products and the systems where they are installed.

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

Contents
- McAfee ePO Cloud components
- Accessing the McAfee ePO Cloud account
- Install the client software on managed systems using the installation URL
- Deploy the client software from McAfee ePO Cloud

McAfee ePO Cloud components
These components make up McAfee ePO Cloud software.

- **McAfee ePO Cloud** — The center of your managed environment. McAfee ePO Cloud delivers security policies and tasks, controls updates, and processes events for all managed systems.

- **McAfee Agent** — A vehicle of information and enforcement between the McAfee ePO Cloud and each managed system. The agent retrieves updates, ensures task implementation, enforces policies, and forwards events for each managed system.

- **Master Repository** — The central location for all McAfee updates and signatures, residing on McAfee ePO Cloud. The Master Repository retrieves user-specified updates and signatures from McAfee.

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

1. The enterprise administrator requests access to use McAfee ePO Cloud.
2. McAfee emails the McAfee ePO Cloud URL and logon information to the enterprise administrator.
3. Log on to the McAfee ePO Cloud server.
Install the client software on managed systems using the installation URL

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

Tasks
• Create an installation URL on page 20
  Create an installation URL to install the software on managed systems.
• Install the software with an installation URL on page 20
  The managed system user can install the software on a local system with an installation URL.

Create an installation URL

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

Task

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

1 Log on to McAfee ePO Cloud as an administrator.
2 Click Menu | Getting Started | Customize.
3 On the Customize Software Installation page, define these settings, then click Done.
   • Group Name — Type a name of the group.
   • Operating System — Select McAfee Agent for Linux.
   • Software and Policies — Select McAfee Endpoint Security software modules as required.
   • Auto Update — Select this option to download updates for the software.

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

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

   On the right side pane under Getting Started, the URL that you created appears.
6 Email the URL with installation instructions to the system user.

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

Install the software with an installation URL

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

Before you begin
• Make sure that your system meets the hardware and software requirements.
• You must have an installation URL that you created or received from your administrator.
Task
For details about product features, usage, and best practices, click ? or Help.

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

Deploy the client software from McAfee ePO Cloud
Deploy the client software to systems in your network that are managed.

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

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

You need to run this task to install Threat Prevention and Firewall separately.
Install the software on a system managed with McAfee ePO Cloud
Deploy the client software from McAfee ePO Cloud
Install software on standalone Linux systems

Install the software on RPM-based and Ubuntu-based standalone systems.

Contents
- Install Threat prevention module on standalone systems
- Install Threat Prevention module using the package management tools
- Install Firewall module on standalone systems
- Upgrade the software
- Test the installation
- View the default settings
- Uninstall the software from standalone systems

Install Threat prevention module on standalone systems

You can install Endpoint Security for Linux Threat Prevention module in one of this method.

Tasks
- Verify the signature on Ubuntu systems on page 23
  Update the GPG in the Ubuntu database, and verify the authenticity of the software.
- Verify the signature on RPM-based systems on page 24
  Before installing the software, verify the software authenticity by validating the signature.
- Install Threat Prevention module on page 24
  Use the command line to install the software on RPM-based and Ubuntu-based systems.
- Enable or disable Fanotify and kernel modules on page 25
  After installation, you can switch from Fanotify to kernel and conversely.

Verify the signature on Ubuntu systems

Update the GPG in the Ubuntu database, and verify the authenticity of the software.

Task
1. Log on to the system as a user with administrator rights.
2. Locate the public key (GPG) from the software download site.
3  Import the public key.
   gpg --import <Public Key>

4  Verify the signature.
   dpkg-sig -verify ISecESP-<version_number>-<build_number>.deb
   dpkg-sig -verify ISecRt-<version_number>.<build_number>.deb
   dpkg-sig -verify ISecTP-<version_number>.<build_number>.deb
   dpkg-sig -verify ISecESPFFileAccess-<version_number>-<build_number>.deb
   dpkg-sig -verify ISecESPAac-<version_number>-<build_number>.deb

   You get a message similar to Processing ISecTP-<version_number>-<build_number>.deb...
   GOODSIG _gpgbuilder 284E8BE753AE45DFF8D82748DDDF2F4CE732A79A 1414371553

**Verify the signature on RPM-based systems**

Before installing the software, verify the software authenticity by validating the signature.

**Task**

1  Log on to the system as a user with administrator rights.

2  Locate the public key (GPG) from the software download site.

3  Import your public key to your RPM DB using this command.
   rpm --import <Public_Key_Name>

   If you don't import the public key using this command, you will get the following warning message during the installation.
   /tmp/tmp.FdcQqEpF3i/ISecTP-<version_number>-<build_number>.x86_64.rpm: Header V4 RSA/SHA1 Signature, key ID <key_number>: NOKEY

4  Verify the signature.
   rpm -K ISecESP-<version_number>-<build_number>_x86_64.rpm
   rpm -K ISecRt-<version_number>-<build_number>_x86_64.rpm
   rpm -K ISecTP-<version_number>-<build_number>_x86_64.rpm
   rpm -K ISecESPFFileAccess-<version_number>-<build_number>_x86_64.rpm
   rpm -K ISecESPAac-<version_number>-<build_number>-<build_number>.x86_64.rpm

   You get a message similar to ISecESP-<version_number>-<build_number>_x86_64.rpm: rsa sha1

**Install Threat Prevention module**

Use the command line to install the software on RPM-based and Ubuntu-based systems.

---

**Before you begin**

You must have installed the McAfee Agent software on the system you intend to install the software. For information about installing the software, see the product guide of your version of McAfee Agent.

Uninstall competitor's software from the system. McAfee Endpoint Security for Linux doesn't support the co-existence of competitor's software in the system.
Task
1  Download the package IsecTP-<version_number>-<build_number>-release-standalone.tar.gz from the McAfee Software Download site using your McAfee Grant Number to a temporary directory of your system.

2  Log on to the system as a user with administrator rights.

3  Download ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz to a temporary directory on your system.

4  Extract the package.

   tar -zxvf ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz

5  Execute the installation script from the directory where you extracted the software.

   sudo ./install-isectp.sh

6  Read the End User License Agreement, then type q to navigate to the prompt.

7  Type accept, then press Enter.

   ! McAfee Endpoint Security for Linux does not support using the nails.options file.

   When you install the software using the installation script install-isectp.sh, the On-Access Scan option is enabled by default.

   To install the software with On-Access Scan disabled, execute the command.

   sudo ./install-isectp.sh oasoff from the directory where you extracted the software.

   For information about enabling the On-Access Scan using the command line, see Enable or Disable On-Access Scanning or the manpage help.

Enable or disable Fanotify and kernel modules

After installation, you can switch from Fanotify to kernel and conversely.

Task
1  Log on to the system as a user with administrator rights.

2  Run these commands as required:

   • To switch from kernel modules to Fanotify - /isecav --usefanotify

   • To switch from Fanotify to kernel modules - /isecav --usekernelmodule

3  Restart the IsecTP service.

   service isectpd restart

   For RedHat Enterprise Linux 7.x and CentOS 7.x systems, the kernel module is enabled by default. For Ubuntu, SUSE, and Oracle Enterprise Limited, Fanotify is enabled by default.
Install Threat Prevention module using the package management tools

Install the software using the Yellowdog Updater Modified (YUM), Advanced Packaging Tool (APT), and Zypper package management tool.

When you install McAfee Endpoint Security for Linux Threat Prevention from the YUM, APT, and Zypper repositories, the On-Access Scan is disabled by default. To enable On-Access Scan after installation, use the command-line. For information about enabling the On-Access Scan using the command line, see Enable or Disable On-Access Scanning or the manpage help.

Tasks

- Extract rpm or deb files from the package on page 26
  Extract rpm and deb files from the Endpoint Security for Linux package.
- Install the software from the YUM repository on page 27
  Install Threat Prevention and Firewall from the YUM repository.
- Install the software from the Zypper repository on page 27
  Install Threat Prevention and Firewall from the Zypper repository.
- Install software from the Advanced Packaging Tool (APT) repository on page 27
  Install Threat Prevention and Firewall software from the APT repository.

Extract rpm or deb files from the package

Extract rpm and deb files from the Endpoint Security for Linux package.

Task

1. Download the Threat Prevention package
   ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz

2. Run these commands:
   - Extract tar -zxvf ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz
   - Extract tar -zxvf ISecTP-<version_number>-<build_number>-standalone.linux.tar.gz
   - Extract tar -zxvf McAfeeESP-Basic-<version_number>-<build_number>-Full.linux.tar.gz
   - Extract tar -zxvf McAfeeESP-KernelModule-<version_number>-<build_number>-Full.linux.tar.gz

3. Download the Firewall package
   McAfeeFW-<version_number>-<build_number>-Release-standalone.tar.gz

4. Run these commands:
   - tar -zxvf McAfeeFW-<version_number>-<build_number>-Release-standalone.tar.gz
   - tar -zxvf McAfeeFW-<version_number>-<build_number>-standalone.linux.tar.gz

To use Threat Prevention, download only the Threat Prevention package, or to use Firewall, download only the Firewall package.
Install the software from the **YUM** repository

Install Threat Prevention and Firewall from the YUM repository.

**Task**

1. Add these RPM files to your YUM repository.
   - ISecESP-<version_number>-<build_number>_x86_64.rpm
   - ISecRt-<version_number>-<build_number>_x86_64.rpm
   - ISecTP-<version_number>-<build_number>_x86_64.rpm
   - ISecESPFileAccess-<version_number>-<build_number>_x86_64.rpm
   - ISecESPAac-<version_number>-<build_number>_x86_64.rpm
   - McAfeeFW-<version_number>-<build_number>_x86_64.rpm

2. Install the software.
   - **Threat Prevention:** yum install ISecTP
   - **Firewall:** yum install McAfeeFW

Install the software from the **Zypper** repository

Install Threat Prevention and Firewall from the Zypper repository.

**Task**

1. Add these files to your Zypper repository.
   - ISecESP-<version_number>-<build_number>_x86_64.rpm
   - ISecRt-<version_number>-<build_number>_x86_64.rpm
   - ISecTP-<version_number>-<build_number>_x86_64.rpm
   - ISecESPFileAccess-<version_number>-<build_number>_x86_64.rpm
   - ISecESPAac-<version_number>-<build_number>_x86_64.rpm
   - McAfeeFW-<version_number>-<build_number>_x86_64.rpm

2. Install the software.
   - **Threat Prevention:** zypper install ISecTP
   - **Firewall:** zypper install McAfeeFW

Install software from the **Advanced Packaging Tool (APT)** repository

Install Threat Prevention and Firewall software from the APT repository.

**Task**

1. Add these files to your APT repository.
   - ISecESP-<version_number>-<build_number>.deb
   - ISecRt-<version_number>-<build_number>.deb
   - ISecTP-<version_number>-<build_number>.deb
   - ISecESPFileAccess-<version_number>-<build_number>.deb

Install software on standalone Linux systems

Install Threat Prevention module using the package management tools
Install software on standalone Linux systems
Install Firewall module on standalone systems

- ISecESPAac-<version_number>-<build-number>.deb
- McAfeeFW-<version_number>-<build-number>.deb

2 Install the software.
- Threat Prevention: `apt-get install isectp`
- Firewall: `apt-get install mcafeefw`

---

Install Firewall module on standalone systems

Install Endpoint Security for Linux Firewall module in silent mode or prompt mode. The default option is prompt mode.

**Tasks**
- **Install Firewall in prompt mode on page 28**
  Install Endpoint Security for Linux Firewall in prompt mode where your inputs are required during the installation.
- **Install Firewall in silent mode on page 28**
  Install Endpoint Security for Linux Firewall with a non-interactive process, where the firewall is installed and enabled automatically.

---

Install Firewall in prompt mode

Install Endpoint Security for Linux Firewall in prompt mode where your inputs are required during the installation.

**Task**
1. Log on to the system as a user with administrator rights.
2. Execute the installation script from the directory where you extracted the software:
   ```bash
   sudo ./install-mfw.sh prompt
   ```
3. When the **End-User License Agreement** appears, type `accept`, then press **Enter**.

Endpoint Security for Linux Firewall is installed in prompt mode.

---

Install Firewall in silent mode

Install Endpoint Security for Linux Firewall with a non-interactive process, where the firewall is installed and enabled automatically.

**Task**
1. Log on to the system as a user with administrator rights.
2. Execute the installation script from the directory where you extracted the software:
   ```bash
   sudo ./install-mfw.sh silent
   ```

Endpoint Security for Linux Firewall is installed in silent mode.

When the installation is complete, the software starts protecting your Linux system immediately. Any existing network connections that are running on your system are disconnected. You must re-establish those connections.
Upgrade the software

You can upgrade the software and migrate your settings from McAfee VirusScan Enterprise for Linux 1.9.2 or 2.0.x, or Endpoint Security for Linux Threat Prevention 10.2.x or 10.5.x, or McAfee Firewall of Linux 8.0.x.

Supported upgrade scenarios

McAfee Endpoint Security for Linux supports upgrading the software and migrating your scan settings from a previously installed version of the software.

You can upgrade the software from:

- McAfee VirusScan Enterprise for Linux 1.9.2
- McAfee VirusScan Enterprise for Linux 2.0.x
- McAfee Endpoint Security for Linux Threat Prevention 10.2.x and 10.5.x
- McAfee® Firewall for Linux 8.0.x

If you installed the McAfee VirusScan Enterprise for Linux 1.9.2 or 2.0.x or McAfee VirusScan Enterprise for Linux 10.2.x or 10.5.x, and McAfee Firewall for Linux 8.0.x, on your system, you must download and extract both McAfee Endpoint Security for Linux Threat Prevention and Firewall packages to the same directory on your system.

Make sure that you upgrade the software in these combinations.

<table>
<thead>
<tr>
<th>If you already installed</th>
<th>Upgrade to</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee VirusScan Enterprise for Linux 1.9.2 or 2.0.x</td>
<td>McAfee Endpoint Security for Linux Threat Prevention 10.6.0</td>
</tr>
<tr>
<td>McAfee Endpoint Security for Linux Threat Prevention 10.2.x or 10.5.x</td>
<td>McAfee Endpoint Security for Linux Threat Prevention 10.6.0</td>
</tr>
<tr>
<td>McAfee VirusScan Enterprise for Linux 1.9.2 or 2.0.x and McAfee Firewall for Linux 8.0.x</td>
<td>You must run the McAfee Endpoint Security for Linux Threat Prevention installation script to upgrade the software. It also upgrades your McAfee Firewall for Linux to McAfee Endpoint Security for Linux Firewall automatically.</td>
</tr>
<tr>
<td>McAfee Endpoint Security for Linux 10.2.x or 10.5.x and McAfee Firewall for Linux 8.0.x</td>
<td>You must run the McAfee Endpoint Security for Linux Threat Prevention installation script to upgrade the software. It also upgrades your McAfee Firewall for Linux to McAfee Endpoint Security for Linux Firewall automatically.</td>
</tr>
<tr>
<td>McAfee Firewall for Linux 8.0.x</td>
<td>McAfee Endpoint Security for Linux Firewall 10.6.0</td>
</tr>
</tbody>
</table>

For managed systems, when upgrading the software, you must check in all three packages (ESPkernel package, Threat Prevention, and Firewall package) in the same branch. Then, create and run a deployment task for Threat Prevention.

You can also migrate policies from McAfee Firewall for Linux 8.0.x to using Endpoint Migration Assistant then upgrade it.

When you upgrade the software, the anti-malware preferences are migrated to the Threat Prevention settings.

If you installed an unsupported version, upgrade the software to a supported version before upgrading to McAfee Endpoint Security for Linux Threat Prevention.
Upgrade Threat Prevention on standalone Linux systems

Upgrade the software from McAfee VirusScan Enterprise for Linux 1.9.2 or 2.0.x or McAfee Endpoint Security for Linux Threat Prevention 10.2.x or 10.5.x.

Before you begin
Make sure that your system is running with a supported version that you can upgrade.

Task
1. Log on to the system as a user with administrator rights.
2. Download ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz to a temporary directory on your computer.
3. Extract the package.
   ```
   tar -zxvf ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz
   ```
4. Run the command from the directory where you downloaded the software.
   ```
   ./install-isectp.sh
   ```

To upgrade the software from the previous versions, you must use the ./install-isectp.sh script. After you upgrade from McAfee VirusScan Enterprise for Linux 1.9.2, you must restart the system.

Upgrade Host Intrusion Prevention to Endpoint Security for Linux Threat Prevention

Upgrade Linux systems running Host Intrusion Prevention version 8.0 patch 10 or later to Endpoint Security for Linux Threat Prevention 10.6.0.

When upgrading systems running with Endpoint Security for Linux 10.2.x, where Host Intrusion Prevention software is already installed, Endpoint Security for Linux Threat Prevention 10.6.0 gets installed with Access Protection. Here, Host Intrusion Prevention is uninstalled during the upgrade.

Task
1. Log on to the system as a user with administrator rights.
2. Download ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz to a temporary directory on your computer.
3. Extract the package.
   ```
   tar -zxvf ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz
   ```
4. Run the command from the directory where you downloaded the software.
   ```
   ./install-isectp.sh
   ```

After you upgrade to Endpoint Security for Linux Threat Prevention 10.6.0 on systems where Host Intrusion Prevention already installed, you must restart the system.

Upgrade McAfee Firewall for Linux to Endpoint Security for Linux Firewall

Upgrade Linux systems running McAfee Firewall for Linux 8.0.x to Endpoint Security for Linux Firewall 10.6.0.

When upgrading systems running with McAfee Firewall for Linux 8.0.x, Endpoint Security for Linux Firewall 10.6.0 is installed and McAfee Firewall for Linux is uninstalled during the upgrade.
Task
1. Log on to the system as a user with administrator rights.
2. Download McAfeeFW-<version_number>-<build_number>-Release-standalone.tar.gz to a temporary directory on your computer.
3. Extract the package:
   `tar -zxvf McAfeeFW-<version_number>-<build_number>-Release-standalone.tar.gz`
4. Run the command from the directory where you downloaded the software:
   `./install-mfw.sh`

Endpoint Security for Linux Firewall is installed and the existing Firewall rules are migrated automatically.

Upgrade software using repositories (YUM, zypper, or apt-get)
Upgrade the software using the YUM, zypper, or apt-get repositories.

Before you begin
Before you upgrade, see the supported upgrade combination table in the supported upgrade scenario section.

Task
1. Copy all rpm or deb files.
2. Stop all Threat Prevention and Firewall services.
   `/opt/McAfee/mfw/bin/mfefirewallControl.sh stop`
   `/opt/isec/ens/threatprevention/bin/isectpdControl.sh stop`
   `/opt/isec/ens/esp/bin/isecespdControl.sh stop`
3. Run the upgrade command:
   YUM repository:
   `yum install ISecTP McAfeeFW`
   zypper:
   `zypper install ISecTP McAfeeFW`
   apt-get:
   `apt-get install isectp mcafeefw`
4. Start all Threat Prevention and Firewall services.
   `/opt/isec/ens/esp/bin/isecespdControl.sh start`
   `/opt/isec/ens/threatprevention/bin/isectpdControl.sh start`
   `/opt/McAfee/mfw/bin/mfefirewallControl.sh start`

Test the installation

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

Tasks
- Test Threat Prevention installation on page 32
  Test Threat Prevention to make sure that it is installed properly and can protect your system.
- Test Access Protection installation on page 32
  Test the software to make sure that Access Protection is enabled and can protect your system.
Test Threat Prevention installation

Test Threat Prevention to make sure that it is installed properly and can protect your system.

Before you begin
You must have enabled the On-Access Scan protection.

Access the EICAR standard anti-virus test file to test the Threat Prevention feature. This file is the combined effort by anti-virus vendors to implement one standard that customers can use to validate the anti-virus software.

Task
1. Log on to the system as a user with administrator rights.
2. Download the EICAR test file.
   ```bash
   wget www.eicar.org/download/eicar.com.txt
   ```
3. Verify the detection in the log file.
   The default location of the log file is `/opt/isec/ens/threatprevention/var/isecoasmgr.log`

Test Access Protection installation

Test the software to make sure that Access Protection is enabled and can protect your system.

Task
1. Log on to the system as a user with administrator rights.
2. Change the directory to the Threat Prevention bin directory.
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Run the command:
   ```bash
   ./isecav --getapstatus
   ```
   If Access Protection status is **Enabled**, verify whether Access Protection is working.
   To verify whether Access Protection is working, create a rule to block a file `/tmp/testfile1`.
   ```bash
   ./isecav --createaprule --rulename test1 --block enable --report enable --subrulename stest1 --subruletype file --operation create --includetargetfile /tmp/testfile1
   ```
   When you run the command from the `/opt/isec/ens/threatprevention/bin` directory, a rule test1 with a subrule stest1 is created that blocks the user from creating a file or directory with the name testfile1 in the /tmp directory.

4. Run the command: `touch /tmp/testfile1`
   The following message is displayed: `cannot touch '/tmp/testfile1': Permission denied`

For more information about Access Protection commands, see the *McAfee Endpoint Security for Linux product guide*. 
View the default settings

After installing the software, view the default settings and fine tune them for your business requirements.

Task

1. Log on to the system as a user with administrator rights.

2. Navigate to the directory.
   
   cd /opt/isec/ens/threatprevention/bin

3. Execute these commands.
   
   • View the product version.
     ./isecav --version

   • View On-Access Scan status and settings.
     ./isecav --getoasconfig --summary

   • View the default settings of standard process type.
     ./isecav --getoasprofileconfig standard

   • View the default settings of the high risk process type.
     ./isecav --getoasprofileconfig highrisk

   • View the default settings of the low risk process type.
     ./isecav --getoasprofileconfig lowrisk

   • View the processes that are configured for high risk and low risk process type.
     ./isecav --getoasconfig --processlist

   • View the files added to the exclusion list for standard process type.
     ./isecav --getoasconfig --exclusionlist --profile standard

   • View the files added to the exclusion list for high risk process type.
     ./isecav --getoasconfig --exclusionlist --profile highrisk

   • View the files added to the exclusion list for low risk process type.
     ./isecav --getoasconfig --exclusionlist --profile lowrisk

   • View the list of default tasks.
     ./isecav --listtasks

   • Enable Access Protection
     ./isecav --setapstatus [enable]

Uninstall the software from standalone systems

Uninstall Endpoint Security for Linux modules (Threat Prevention or Firewall) from the standalone systems.

Tasks

• Uninstall Threat Prevention from standalone systems on page 34
  Remove the software from a standalone system using the command line.

• Uninstall Firewall from standalone systems on page 34
  Uninstall Firewall module from a standalone Linux system using a command-based script.
Uninstall Threat Prevention from standalone systems
Remove the software from a standalone system using the command line.

**Task**
1. Log on to the system as a user with administrator rights.
2. Navigate to the directory.
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Execute the command.
   ```bash
   ./uninstall-isectp.sh
   ```
4. Type `yes`, when prompted.

Uninstall Firewall from standalone systems
Uninstall Firewall module from a standalone Linux system using a command-based script.

**Task**
1. Log on to the system as a user with administrator rights.
2. Navigate to the directory:
   ```bash
   /opt/McAfee/mfw/bin
   ```
3. Run this command:
   ```bash
   sudo ./uninstallmfw.sh
   ```
   You can uninstall Endpoint Security for Linux Firewall in prompt mode or silent mode by using the respective option in the command.
Index

C
check-in package, ePolicy Orchestrator checking in package 12
client software
  installation 20
  installing using url 14
  installing with URL 20
creation
  installation url 20

D
Default settings, viewing 33
deployment, ePolicy Orchestrator 15

I
installation
  client software 13, 14, 20
  extensions 12
  using url 14
  using URL 20
  using urls 13
installation URLs
  McAfee ePO cloud 20

P
package
  checking in 11
packages
  checking in 12

R
removal of software 16
removal of software extension 16

S
signature
  verifying software 23
software
  verifying signature 23
standalone
  upgrading software 30

U
urls
  installing client software 13