Product Guide

McAfee Endpoint Security for Linux Threat Prevention 10.2.0
Contents

Preface 7
    About this guide .................................. 7
    Audience .................................. 7
    Conventions ................................. 7
    Find product documentation .............................. 8

1 Introduction 9
    How Threat Prevention protects your system .............................. 9
    Product features .................................. 10

2 Installing the software on standalone Linux systems 15
    System requirements ................................ 15
    Verify the signature on RPM-based systems .............................. 16
    Verify the signature on Ubuntu systems ................................ 17
    Install the software on standalone Linux systems ....................... 17
    Install the software using the package management tools ................. 18
    Install the software from the YUM repository .............................. 18
    Install the software from the Zypper repository .............................. 19
    Install the software from the Advanced Packaging Tool (APT) repository ................................ 19
    Upgrading the software .................................. 20
    Supported upgrade scenarios .................................. 20
    Upgrade the software on standalone Linux systems .............................. 20
    View the default settings .................................. 20
    Test the installation .................................. 21
    Uninstall the software from standalone Linux systems ................... 22

3 Managing McAfee Endpoint Security for Linux 23
    isecav command-line Help .................................. 23
    Access the IsecTP Help .................................. 24
    Define risk category for a process .................................. 24
        Add a process to a category .................................. 25
        Change the risk level of a process .................................. 25
        Remove a process from the risk category .................................. 25
    Manage on-access scanning .................................. 26
        Verify the status of the on-access scan .................................. 26
        Enable or disable On-Access Scan .................................. 27
        Configure the On-Access Scan settings for a Standard process type .................................. 27
        Exclude files from the on-access scan .................................. 28
    Manage on-demand scanning .................................. 29
        Create an on-demand scan task .................................. 29
        Run an on-demand scan task .................................. 34
        Check the status of an on-demand scan status .................................. 34
        Delete an on-demand scan task .................................. 35
Protecting your managed Linux systems

4 Installing the software on systems managed with McAfee ePO

System requirements
Check in the package to the McAfee ePO server
Check in the package using Software Manager
Check in the package manually
Install the extensions on the McAfee ePO server
Install the extensions using Software Manager
Install the extensions manually
Install the client software on a managed system using the installation URL
Create an installation URL
Install the software with an installation URL on a managed system
Deploy the client software from McAfee ePO
Test the installation
Migrated policies and their equivalent settings
General policy — Troubleshooting and Advance tab
On-Access Scan policy — General tab
On-Access Scan policy — Detections tab
On-Access Scan policy — Advanced tab
On-Access Scan policy — Actions tab
Remove the software from a managed system
Remove the software extensions
Remove the software from client systems

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

McAfee ePO Cloud components
Accessing the McAfee ePO Cloud account
Install the client software on a managed systems using the installation URL
Create an installation URL
Install the software with an installation URL
Deploy the client software from McAfee ePO Cloud

6 Managing the software with McAfee ePO and McAfee ePO Cloud

Using Endpoint Security extensions as common extensions
Managing policies
Create or modify policies
Assign policies
Common Policy
Configuring client interface access
Configuring debug logging
Activity and event logging
Configure the Common policy
Threat Prevention policy
Configure the On-Access Scan policy
Configure On-Demand Scan policy (Full Scan)
Preface

This guide provides the information you need to work with your McAfee product.

Contents

- About this guide
- Find product documentation

About this guide

This information describes the guide’s target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company’s security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

- *Italic* — Title of a book, chapter, or topic; a new term; emphasis
- **Bold** — Text that is emphasized
- **Monospace** — Commands and other text that the user types; a code sample; a displayed message
- **Narrow Bold** — Words from the product interface like options, menus, buttons, and dialog boxes
- **Hypertext blue** — A link to a topic or to an external website

- **Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
- **Tip:** Best practice information
- **Caution:** Important advice to protect your computer system, software installation, network, business, or data
- **Warning:** Critical advice to prevent bodily harm when using a hardware product
Find product documentation

On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

**Task**

1. Go to the ServicePortal at https://support.mcafee.com and click the Knowledge Center tab.
2. In the Knowledge Base pane under Content Source, click Product Documentation.
3. Select a product and version, then click Search to display a list of documents.
Introduction

McAfee® Endpoint Security for Linux Threat Prevention detects threats and potentially unwanted software, then protects your environment based on settings that you configured.

You can use the software on standalone and managed systems.

- **For standalone systems** — You or your system administrator can install the software and configure settings.
- **For managed systems** — Your system administrator sets up and configures security policies using these servers.
  - McAfee® ePolicy Orchestrator® (McAfee ePO®)
  - McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud)

McAfee Endpoint Security for Linux Threat Prevention is the next version of Anti-malware protection for Linux systems after McAfee® VirusScan® Enterprise for Linux. The shift gear from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux is to provide consistent security for systems irrespective of the operating systems in your environment using one extension. You can use McAfee® Endpoint Security extensions to manage your Windows, Mac, and Linux systems.

Contents
- How Threat Prevention protects your system
- Product features

How Threat Prevention protects your system

Once installed, McAfee Endpoint Security for Linux Threat Prevention starts protecting your Linux systems from threats.

Threat Prevention protects your Linux systems from malware proactively with the predefined actions upon detecting malware and suspicious items.

When enabled, Threat Prevention checks for viruses, trojans, unwanted programs, and other threats by scanning items. The software scans files and folders on local, network-mounted volumes, and removable media whenever you create or access them. You can also run scans on demand.

The software uses the latest anti-malware engine that:
- Performs complex analysis using the malware definition files (DAT)
- Decodes the contents of the item you access
- Compares the contents with the known signatures stored in the DAT files to identify malware.

Use Threat Prevention options to configure actions for on-access scan, on-demand scan, exclude files or paths from scanning, and other settings.
Product features

These features help you prevent, detect, fine tune, and manage the protection configuration for your Linux systems.

Prevention — Avoiding threats

- **Product Update client tasks** — Update the engine and content files automatically from the McAfee download website.
- **5800 Engine support** — Pre-packaged with the latest 5800 engine that provides enhanced detection capabilities.
- **Extra.DAT files** — Download and install Extra.DAT files to provide protection from a major virus outbreak.

Detection — Finding threats

- **On-Access Scan** — Scans files and directories for threats whenever users access them.
- **On-Demand Scan** — Schedules a scan on files and directories at specific times. Each on-demand scan contains its own policy settings. You can also run Full Scan or Quick Scan on a managed system.
- **Policy-Based On-Demand Scan client tasks** — Run a Quick Scan or Full Scan on the client from McAfee ePO. Configure the behavior of these scans in the policy settings for an on-demand scan.

Response — Handling threats

Use product log files, automatic actions, and other notification features to determine the best way to handle detections.

- **Actions** — Configure actions to take when threats are detected.

Tuning — Monitoring, analyzing, and fine-tuning your protection

Monitor and analyze your configuration to improve system performance, and enhance virus protection, if needed. Use these tools and features:

- **Queries, dashboards, and server tasks (McAfee ePO)** — Monitor scanning activity and detections.
- **Log files (McAfee® Endpoint Security for Linux Threat Prevention client)** — View the history of detected items. Analyzing this information might reveal that you must enhance your protection or change the configuration to improve system performance.
- **Scheduled tasks** — Modify client tasks (such as Product Update) and scan times to improve performance by running them during nonpeak times.
- **Scan policies** — Analyze log files or queries and modify policies to increase performance or virus protection, if necessary. For example, you can improve performance by configuring exclusions.
- **Exclusion of files and directories from scanning** — Excludes specific files and directories from on-access scanning and on-demand scanning using criteria such as file type, extension, or wildcards.
- **Option to scan network volumes and compressed files** — Exclude or include mounted network volumes and compressed files from scanning.
- **Option to retain client-side exclusions** — Overwrites or retains the client exclusion list for on-access scanning in a managed environment.
• **Common extensions to manage Windows, Macintosh, and Linux systems** — Use McAfee® Endpoint Security extensions as common extensions to manage policies for your Windows, Macintosh, and Linux systems.

• **Common McAfee ePO Dashboard and queries** — Use the McAfee ePO dashboard to view the status of managed systems.

• **Support for McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud)** — Support for McAfee ePO Cloud to manage policies for your systems.

• **Enable debug logging from client system** — Enable debug logging from the client system using the command line.
Protecting your standalone Linux systems

Install the software, analyze and configure the Threat Prevention settings to protect your standalone Linux systems.
Installing the software on standalone Linux systems

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

Contents
- System requirements
- Verify the signature on RPM-based systems
- Verify the signature on Ubuntu systems
- Install the software on standalone Linux systems
- Install the software using the package management tools
- Upgrading the software
- View the default settings
- Test the installation
- Uninstall the software from standalone Linux systems

System requirements

Make sure that your systems meet these requirements for successful installation.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Processors  | • Intel x86_64 architecture-based processor that supports Intel Extended Memory 64-bit technology (Intel EM64T)  
              • AMD x86_64 architecture-based processor with AMD 64-bit technology |
| Memory      | Minimum: 2 GB RAM  
              Recommended: 4 GB RAM                                                 |
## Component Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free disk space</td>
<td>Minimum: 1 GB</td>
</tr>
</tbody>
</table>
| Operating systems (64-bit) | • Operating system 64-bit  
                          |   • SUSE Linux Enterprise Server/Desktop 11.x SP2 and later, and 12.x.       |
|                        |   • Red Hat Enterprise Linux 6.x, and 7.x                                    |
|                        |   • Ubuntu 12.04, 14.04, 15.x, and 16.04.                                   |
|                        |   • Amazon Linux AMI 2014 and later.                                         |
|                        |   • CentOS 6.x and 7.x                                                       |
|                        |   • SUSE and Ubuntu on Amazon Elastic Compute Cloud (Amazon EC2)             |
|                        |   • Red Hat Enterprise Linux 7 on Amazon Elastic Compute Cloud (Amazon EC2)  |
|                        |   • Novell Open Enterprise Server 11 SP1                                    |
|                        |   • Oracle Enterprise Linux 6.x and 7.x both Red Hat and UEK 6.7.            |
|                        |   • Virtual platforms                                                       |
|                        |   • VMware                                                                  |
|                        |   • KVM                                                                     |
|                        |   • Citrix Xen                                                               |
|                        |   • Virtual box                                                             |
|                        |   • Xen                                                                     |
|                        |   • Paravirtual environment — Guest operating system on Xen Hypervisor      |

This product cannot be used on 32-bit platforms.

### 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 root user.
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 ISecESPFileAccess-<version_number>-<build_number>_x86_64.rpm

You get a message similar to ISecESP-<version_number>-<build_number>.x86_64.rpm: rsa sha1 (md5) pgp md5 OK

**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 root user.

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>_64.deb
    dpkg-sig -verify ISecRT-<version_number>.<build_number>_64.deb
    dpkg-sig -verify ISecTP-<version_number>.<build_number>_64.deb
    dpkg-sig -verify ISecESPFileAccess-<version_number>-<build_number>_64.deb

You get a message similar to Processing ISecTP-<version_number>-<build_number>_64.deb...

**Install the software on standalone Linux systems**

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. Log on to the system as root user.
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. Execute the installation script from the directory where you extracted the software.
   ```
   sudo ./install-isectp.sh
   ```
5. Read the [End User License Agreement](#), then type `q` to navigate to the prompt.
6. 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. Later, whenever you need to enable On-Access-Scan, you can enable it using the command-line.

   To install the software with On-Access Scan disabled, execute the command.
   ```
   sudo ./install-isectp.sh oasoff
   ```

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

---

**Install the software 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**

- **Install the software from the YUM repository** on page 18
  Install the software from the repository.
- **Install the software from the Zypper repository** on page 19
  Install the software from the Zypper repository.
- **Install the software from the Advanced Packaging Tool (APT) repository** on page 19
  Install the software from the APT repository.

**Install the software from the YUM repository**

Install the software from the repository.

**Before you begin**

Make sure that the following RPM files are added to your YUM repository.

Task
• Install the software.
  yum install ISecTP

Install the software from the Zypper repository
Install the software from the Zypper repository.

Before you begin
Make sure that the following RPM files are added 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

Task
• Install the software.
  zypper install ISecTP

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

Before you begin
Make sure that the following files are added to your APT repository.
• ISecESP-<version_number>-<build_number>_64.deb
• ISecRT-<version_number>-<build_number>_64.deb
• ISecTP-<version_number>-<build_number>_64.deb
• ISecESPFileAccess-<version_number>-<build_number>_64.deb

Task
• Install the software.
  apt-get install ISecTP
Upgrading the software

You can upgrade the software and migrate your settings from McAfee VirusScan Enterprise for Linux.

Supported upgrade scenarios

McAfee Endpoint Security for Linux Threat Prevention 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.x

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 the supported version before upgrading to McAfee Endpoint Security for Linux Threat Prevention.

Upgrade the software on standalone Linux systems

Upgrade the software from McAfee VirusScan Enterprise for Linux 1.9.2 or 2.x.

Before you begin

Make sure that your system is running a supported version to be able to upgrade.

Task

1. Log on to the system as root user.

2. Download `ISecTP-<version_number>-<build_number>-Release-standalone.tar.gz` to a temporary directory on your computer.

3. Extract the package.

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

4. Run the command from the directory where you downloaded the software.

   ```bash
   ./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.

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 root user.

2. Navigate to the directory.

   ```bash
   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

Test the installation
Test the software 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 root user.
2 Download the EICAR test file.
   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
Uninstall the software from standalone Linux systems

Remove the software from a standalone system using the command line.

**Task**

1. Log on to the system as root user.

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

3. Execute the command.
   
   ```
   ./uninstall-isectp.sh
   ```

4. Type `yes`, when prompted.
Managing McAfee Endpoint Security for Linux

Define or change the software configuration, or view information about the software.

Contents

- isecav command-line Help
- Access the IsecTP Help
- Define risk category for a process
- Manage on-access scanning
- Manage on-demand scanning
- Configure the DAT update schedule
- Configure the Product log settings
- Configure the software to send events to SYSLOG
- Configure the quarantine directory

isecav command-line Help

isecav is a command-line tool to execute tasks, and configure McAfee Endpoint Security for Linux Threat Prevention settings.

You can use the isecav command on standalone and managed systems. For managed systems, the configurations that you set using the command line is overwritten during the policy enforcement.

Before accessing the command-line Help, we recommend that you get familiar with these basic terminologies used in the Help.

Process type

Threat Prevention lets you define single On-Access Scan settings for all processes or different settings for each process type such as Standard, High Risk, and Low Risk.

Process

Threat Prevention determines the risk level based on the process (program) through which you access the file. When you access a file, Threat Prevention identifies the process used to access the file, verifies the risk level defined for that process, then applies the settings that are applicable for the process type. You can define a process as a high risk or low risk. If the process is not defined in either of the category, the process type is set to Standard process. When the process type is set to Use Standard settings for all process, all processes are treated as Standard processes.

For example, your organization might consider accessing unknown files through websites can expose your systems to threats. To protect your systems from such threats, you can add the browser software Chrome to the High Risk process, and configure settings specifically.
You can add, edit, or remove the process to the risk-based process as required using the command line. For more information about adding, changing, or removing the process to process category, see Define settings for a process.

**Index**

Index is a unique number by which isecav identifies a task or process from the list.

When you create multiple on-demand scan tasks, the tasks are listed by its sequence number. You can identify the scan task by its unique number which is called as Index.

```
1 test_task   OOS   Not Started
2 KTods      OOS   Completed
```

For example, this list contains two on-demand scan schedules. To run the task on-demand scan task KTods, from the /opt/isec/ens/threatprevention/bin directory, you must execute the command:

```
./isecav --runtask --index 2
```

---

### Access the IsecTP Help

Access the IsecTP help from the command line to view configurations or to execute tasks.

**Task**

1. Log on to the system as root user.
2. Navigate to the directory.

   `/opt/isec/ens/threatprevention/bin`

3. Execute the command.

   `isecav --help`

---

### Define risk category for a process

You can add processes to a process category, change the risk category for a process, or remove process from the category.

**Tasks**

- **Add a process to a category on page 25**
  Add a process to high risk, low risk, or standard process category from the command line.

- **Change the risk level of a process on page 25**
  Change the risk category of a process from the command-line.

- **Remove a process from the risk category on page 25**
  Remove a process from the risk category when you no longer need them.
**Add a process to a category**
Add a process to high risk, low risk, or standard process category from the command line.

**Task**
1. Log on to the system as root user.
2. Navigate to the directory.
   
   ```
   cd /opt/isecc/ens/threatprevention/bin
   ```
3. Execute the command.
   
   ```
   ./isecav --addprocess --profile_type process_name
   ```

**Example: Add Chrome process to the High Risk category**
Chrome is a browser you use to browse websites. While browsing, you can also save pages or download files that are basically a write operation. While browsing, the browser can also add cookie files to your `/tmp` directory. So, you can add Chrome to the high risk category, and enable the Scan on Write option to scan only write operation happens from the Chrome process.

To add the Chrome browser to the High Risk category, execute the command:

```
./isecav --addprocess --highrisk /usr/bin/google-chrome
```  

**Change the risk level of a process**
Change the risk category of a process from the command-line.

**Task**
1. Log on to the system as root user.
2. Navigate to the directory.
   
   ```
   cd /opt/isecc/ens/threatprevention/bin
   ```
3. Execute the command.
   
   ```
   ./isecav --setprocess --profile_type process_name
   ```

**Example: Change the risk category of Chrome process from high risk to low risk**
To change the Chrome process risk category from High Risk to Low Risk, execute the command:

```
./isecav --setprocess --lowrisk /usr/bin/google-chrome
```  

**Remove a process from the risk category**
Remove a process from the risk category when you no longer need them.

**Task**
1. Log on to the system as root user.
2. Navigate to the directory.
   
   ```
   /opt/isecc/ens/threatprevention/bin
   ```
3. Execute the command.
   
   ```
   ./isecav --delprocess --index <index_number>
   ```
**Example: Remove Chrome from the High Risk category**

To remove Chrome from the High Risk category, you must know the index number of the Chrome process.

1. To list all processes, execute the command 
   
   ```bash
   ./isecav --getoasconfig --processlist
   ```

   According to this list, the index number for Chrome process is 1.

2. Execute the command: 
   
   ```bash
   ./isecav --delprocess --index 1
   ```

---

**Manage on-access scanning**

The on-access scan runs in the background and actively scans your computer system constantly for viruses and other malicious threats. You can set the on-access scan options at the organization or profile level.

**Tasks**

- *Verify the status of the on-access scan on page 26*
  Check whether the on-access scanning is enabled.
- *Enable or disable On-Access Scan on page 27*
  Enable or disable On-Access Scan as required.
- *Configure the On-Access Scan settings for a Standard process type on page 27*
  Configure the On-Access Scan settings for a Standard process from the command-line.
- *Exclude files from the on-access scan on page 28*
  Configure the on-access scan profile to add exclusions.

**Verify the status of the on-access scan**

Check whether the on-access scanning is enabled.

**Task**

1. Log on to your Linux system as root user.
2. Change directory to the /bin folder of the software.
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Get details about the on-access scan task configuration.
   ```bash
   ./isecav --getoasconfig --summary
   ```
4. From the command results, check whether the value for the On-Access Scan is Enabled or Disabled.
Enable or disable On-Access Scan
Enable or disable On-Access Scan as required.

Task
1. Log on to the system as root user.
2. Navigate to the `/bin` directory.
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Enable or disable the scan:
   - Enable On-Access Scan: `./isecav --setoasglobalconfig --oas on`
   - Disable On-Access Scan: `./isecav --setoasglobalconfig --oas off`

Configure the On-Access Scan settings for a Standard process type
Configure the On-Access Scan settings for a Standard process from the command-line.

Task
1. Log on to your Linux system as root user.
2. Change directory to the `/bin` directory.
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. View the current settings of the Standard process type.
   ```bash
   ./isecav --getoasprofileconfig standard
   ```
4. Define the settings for the Standard process type.
   ```bash
   ./isecav --setoasprofileconfig --profile standard [options]
   ```

Example: Configure the On-Access Scan Settings (Standard process type)
```bash
./isecav --setoasprofileconfig --profile standard --setmode sor --filetypestopscan all --onscanerror deny --onscantimeout deny --networkscan enable --scanarchive disable --scanmime enable --scanunknownprograms enable --scanunknownmacros disable --primaryaction clean --secondaryaction delete --primaryactionpup clean --secondaryactionpup delete
```

The command configures the following settings for the Standard process type.

- When to scan — Scan on reading.
- What to scan — All files.
- On Scan error — Deny access to the file.
- On Scan timeout — Deny access to the file.
- Scan Network volumes — Enable.
- Scan Archive files — Disable.
- Scan MIME files — Enable.
- Detect unwanted programs — Enable.
- Detect unknown macros — Disable.
- Threat detection first response — Clean.
- If first response fails — Delete the file.
- Unwanted program first response — Clean.
- If first response fails — Delete.
Exclude files from the on-access scan

Configure the on-access scan profile to add exclusions.

**Task**

1. Log on to your Linux system as root user.
2. Change directory to the /bin folder of the software.
   ```
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Run a command using this syntax.
   ```
   ./isecav --setoasprofileconfig --profile [standard | highrisk | lowrisk] [exclusion options]
   ```

   Specify the profile risk level from which you want to exclude files: standard, highrisk, or lowrisk.

   The high-risk and low-risk process type are enforced only when the `--procsettings` is set to riskbased. If the `--procsettings` value is set to standard, then all processes are defined as standard processes. Run the `isecav --help` command to see the software Help.

   Replace `[exclusion options]` with these options:

   - **Specific when to exclude the files or directories using one of these options.**

     | Option              | Definition                                                                 |
     |---------------------|----------------------------------------------------------------------------|
     | --addexclusionread  | Adds exclusions to the On-Access Scan exclusion list during read operations.|
     | --addexclusionwrite | Adds exclusions to the On-Access Scan exclusion list during write operations.|
     | --addexclusionrw    | Adds exclusions to the On-Access Scan exclusion list during read and write operations.|

   - **Specify the files or directories to exclude using these options.**

     | Option              | Definition                                                                                                                                                                                                 |
     |---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
     | --excludemasks      | Excludes the specified files or directories from the scan. Provide the Absolute file name, just the name of a file, or Absolute name of the directory according to these guidelines:                                                   |
     |                     | • Wildcards [* , ?] are allowed as part of the value.                                                                                                                                                    |
     |                     | • An Absolute file name and directory name must start with a [/].                                                                                                                                 |
     |                     | • A directory must end with a leading slash [/].                                                                                                                                                      |
     |                     | • Multiple comma-separated values are allowed.                                                                                                                                                        |
     |                     | • If any of the values have spaces in between, specify the values in double quotes (" ").                                                                                                         |
     | --excludemask       | Specifies the extensions to exclude. Provide the extension names according to these guidelines:                                                                                                        |
     |                     | • Wildcard [?] is allowed as part of the value.                                                                                                                                                       |
     |                     | • Multiple comma-separated values are allowed.                                                                                                                                                      |
     |                     | • If any of the values have spaces in between, specify the value in double quotes (" ").                                                                                                           |
     | --excludemask       | Specifies the subfolders for the given directory that must be excluded.                                                                                                                             |
     | --excludemask       | Specifies the subfolders for the given directory that must be excluded.                                                                                                                             |
**Example:** --addexclusionread --excludepaths "/home/user1/,/home/user/file1" --excludefiletype "txt,doc,pdf" --excludesubfolder

The command excludes to read these files:
- All files in the `/home/user1/` directory
- `/home/user/file1`
- All .txt, .doc or .pdf file types from any file systems

Also, the `--excludesubfolder` attribute skips the subfolders of the directories mentioned.

### Manage on-demand scanning
Create, configure, schedule, and manage on-demand scan tasks.

**Tasks**
- **Create an on-demand scan task on page 29**
  To configure a scan with your custom settings, create an on-demand task.
- **Run an on-demand scan task on page 34**
  Run an on-demand task that you created.
- **Check the status of an on-demand scan status on page 34**
  Check whether an on-demand scan is enabled.
- **Delete an on-demand scan task on page 35**
  Delete an on-demand scan task when you no longer need it.

### Create an on-demand scan task
To configure a scan with your custom settings, create an on-demand task.

**Task**
1. Log on to your Linux system as root user.
2. Change directory to the `/bin` folder of the software.
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Run a command using this syntax.
   ```bash
   ./isecav --addodstask --name [task name] [additional options]
   ```
   Replace `[task name]` with the name that you want to set. The task name is a mandatory field and must be unique.
   Multiple tasks can be configured with different settings.
   Replace `[additional options]` with the settings that you need.
<table>
<thead>
<tr>
<th>Option</th>
<th>Values</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>--scanarchive</td>
<td>enable (default) disable</td>
<td>Examines the contents of archive (compressed) files, including .jar files.</td>
<td>Scanning archives is resource-intensive and affects performance.</td>
</tr>
<tr>
<td>--scanmime</td>
<td>enable          disable (default)</td>
<td>Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.</td>
<td></td>
</tr>
<tr>
<td>--scanpups</td>
<td>enable (default) disable</td>
<td>Detects, decodes, and scans potentially unwanted programs.</td>
<td></td>
</tr>
<tr>
<td>--scanunknownprograms</td>
<td>enable (default) disable</td>
<td>Detects, decodes, and scans unknown program files.</td>
<td></td>
</tr>
<tr>
<td>--scanunknownmacros</td>
<td>enable (default) disable</td>
<td>Detects, decodes, and scans unknown macro viruses.</td>
<td></td>
</tr>
<tr>
<td>--scanlocaldrives</td>
<td>enable          disable</td>
<td>Scans all regular files under locally mounted file systems.</td>
<td>An on-demand task runs a scan on the configured files and directories. So you must set a scan path using one of these options.</td>
</tr>
<tr>
<td>--scanpaths</td>
<td>Absolute file name, just the name of a file, or Absolute name of the directory, specified according to these guidelines:</td>
<td>Includes the specified files or directories to the scan.</td>
<td>--scanlocaldrives enable --scantmpfolders enable --scannetworkdrives enable --scanpaths [path]</td>
</tr>
<tr>
<td>--scantmpfolders</td>
<td>enable          disable</td>
<td>Scans all files under these directories in the system:</td>
<td>/tmp /usr/local/tmp /var/tmp</td>
</tr>
<tr>
<td>--scannetworkdrives</td>
<td>enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Values</td>
<td>Description</td>
<td>Note</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>--scannetworkdrives</td>
<td>enable/disable</td>
<td>Iterates and scans all network mount points on the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Restricted to NFS and CIFS shares mounted on the system.</td>
<td></td>
</tr>
<tr>
<td>--scansubfolders</td>
<td>enable/disable</td>
<td>Iterates through the folders specified.</td>
<td>Only applicable when specified with these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scanlocaldrives</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scanpaths</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scantmpfolders</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scannetworkdrives</td>
</tr>
<tr>
<td>--filetypestoscan</td>
<td>all</td>
<td>Specifies which file types to scan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>defaultandspecified</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>onyl Specified</td>
<td>Scans only files as the user specifies. Mention at least one file type using addfiletype.</td>
<td></td>
</tr>
<tr>
<td>--scanmacros</td>
<td>enable/disable</td>
<td>Scans for known macro threats in the list of default and specified files.</td>
<td>Only applicable with filetypestoscan</td>
</tr>
<tr>
<td>--addfiletype</td>
<td>Extension name — The file types are specified as extension names and support the wildcard [?]. Duplicate entries are automatically removed.</td>
<td>Adds file types to the default or specified user-defined list.</td>
<td></td>
</tr>
<tr>
<td>--delfiletype [extension name]</td>
<td>Extension names — Specify the entry to be deleted.</td>
<td>Deletes file types from the user-defined list of the file.</td>
<td></td>
</tr>
<tr>
<td>--noextension</td>
<td>enable/disable</td>
<td>Specifies files to be scanned with no extension.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Values</td>
<td>Description</td>
<td>Note</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--excludepaths</td>
<td>Absolute file name, just the name of a file or Absolute name of the directory, specified according to these guidelines:</td>
<td>Excludes the specified files or directories from the scan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wildcards [*], [?] are allowed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An Absolute file name and directory name must start with a slash [/].</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A directory must end with a slash [/].</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multiple comma-separated values are allowed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If any values have spaces in between, specify the values in double quotes (&quot;&quot;&quot;).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--excludefiletype</td>
<td>Extension names, specified according to these guidelines:</td>
<td>Specifies the extensions for exclusion.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wildcard [?] is allowed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multiple comma-separated values are allowed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If any of the values have spaces in between, specify the value in double quotes (&quot;&quot;&quot;).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--excludesubfolder</td>
<td>Excludes subfolders for the directory specified in the exclude path.</td>
<td></td>
<td>Only applicable for directories specified as part of excludepaths.</td>
</tr>
<tr>
<td>--usescancache</td>
<td>enable, disable</td>
<td>Specifies to use the On-Access Scan cache lookup while scanning files for this task.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Values</td>
<td>Description</td>
<td>Note</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| --primaryaction | • continue — No action is taken and the event is logged.  
• clean (default) — Removes the threat from the detected file, if possible. The original file is quarantined by default.  
• delete — Deletes files with potential threats. The original file is quarantined by default. | Sets the primary scan action for threat detection. If the primary action fails, the secondary action is performed. |                                                                    |
| --secondaryaction | • continue — No action is taken and the event is logged.  
• delete (default) — Deletes files with potential threats. The original file is quarantined by default. | This action is performed when primary action fails. | This option is only available when primaryaction is specified as clean.  
For the primary action Delete, the only secondary option valid is Continue. |
| --primaryactionpup | • continue — No action is taken and the event is logged.  
• clean (default) — Removes the threat from the detected file, if possible. The original file is quarantined by default.  
• delete — Deletes files with potential threats. The original file is quarantined by default. | Sets the primary scan action for potentially unwanted programs. If the primary action fails, the secondary action is performed. |                                                                    |
| --secondaryactionpup | • continue — No action is taken and the event is logged.  
• delete (default) — Deletes files with potential threats. The original file is quarantined by default. | This action is performed when primary action for potentially unwanted programs fails. | This option is only available when primaryaction is specified as clean. |
**Example:** ./isecav --addodstask --name odstask --scanlocaldrives enable

The command adds the on-demand task with task name `odstask`, which scans only the local drives on the system.

**Run an on-demand scan task**
Run an on-demand task that you created.

**Task**
1. Log on to your Linux system as root user.
2. Change directory to the `/bin` folder of the software.
   
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Run a command using this syntax.
   
   ```bash
   ./isecav --runtask --index [index number]
   ```
   Replace `[index number]` with the index number of the task that you want to run. The command does not run if the task is already running.

**Check the status of an on-demand scan status**
Check whether an on-demand scan is enabled.

**Task**
1. Log on to your Linux system as root user.
2. Change directory to the `/bin` folder of the software.
   
   ```bash
   cd /opt/isec/ens/threatprevention/bin
   ```
3. Get details about all on-demand scan tasks.
   
   ```bash
   ./isecav --listtasks
   ```
4. From the command results, check the value for the on-demand scan status.
   - Not Started — The task has not yet started.
   - Running — The task is in-progress.
   - Stopped — The last run was stopped due to user intervention.
   - Aborted — The last run was canceled because of some error.
   - Completed — The last run completed without any errors.
Delete an on-demand scan task
Delete an on-demand scan task when you no longer need it.

**Task**
1. Log on to your Linux system as root user.
2. Change directory to the /bin folder of the software.
   ```bash
cd /opt/isec/ens/threatprevention/bin
   ```
3. Run a command using this syntax.
   ```bash
./isecav --deltask --index [index number]
   ```
   Replace `[index number]` with the index number of the task to delete.

Configure the DAT update schedule
Configure the DAT update task to run immediately, at a scheduled time, or at regular intervals.

You can run the update task at:
- **Daily** — Runs the task daily at the specified time.
- **Weekly** — Runs the task at a specific day of every week. When you specify this option, you must specify the Day of the week option. You can use the comma separator to add multiple days.
- **Monthly** — Runs the task at a specific date of every month. When you specify this option, you must specify the Day of the month option. You can use the comma separator to add multiple dates.
- **Unspecified** — Disables the schedule for a task.
- **Start time** — Runs the task at a specific time. You must use the 24 Hours time format. For example 18:45.

**Tasks**
- *Create a DAT update task on page 35*
  Create a DAT update task from the command-line.
- *Run a DAT update task on page 36*
  Run the DAT update task immediately.
- *Schedule a DAT update task on page 36*
  Run the DAT update task at a specified time or at periodic intervals.

Create a DAT update task
Create a DAT update task from the command-line.

**Task**
1. Log on to the system as root user.
2. Navigate to the directory.
   ```bash
cd /opt/isec/ens/threatprevention/bin
   ```
3. Create a DAT update task.
   ```bash
./isecav --addupdatetask --name <task_name> --updatetype --<type_of_update>
   ```
4. View the tasks list to confirm that the DAT update task is created.
   ```bash
./isecav --listtasks
   ```
Example: Create a DAT update task
./isecav --addupdate task --name datupdate --updatetype dat

When you run the command from the /opt/isec/ens/threatprevention/bin directory, the software creates a DAT update task.

Run a DAT update task
Run the DAT update task immediately.

Task
1 Log on to the system as root user.
2 Navigate to the directory.
   cd /opt/isec/ens/threatprevention/bin
3 View the tasks list to identify the index number of your DAT update task.
   ./isecav --listtasks
4 Run the DAT update task.
   ./isecav --runtask --index <index_number>.

Example to run a DAT update task
If the index number of your DAT update task is 3, you must run the command.
   ./isecav --runtask --index 3

Schedule a DAT update task
Run the DAT update task at a specified time or at periodic intervals.

Before you begin
You must have created a DAT update task.

Task
1 Log on to the system as root user.
2 Navigate to the directory.
   cd /opt/isec/ens/threatprevention/bin
3 View the tasks list to confirm that the DAT update task is created.
   ./isecav --listtasks
4 Schedule the task.
   ./isecav --scheduletask --index <index_number> --daily --starttime <HH:MM>

Example: Schedule a DAT update task to run every day at 12.45
   ./isecav --scheduletask --index 3 --daily --starttime 12:45

When you run the command from the /opt/isec/ens/threatprevention/bin directory, the software runs the DAT update task everyday at 12:45.
Configure the Product log settings

Enable or disable the Product log and define maximum size for the log file.

Product log file stores all events and activity details with time. Enabling the Product log helps you to review the product behavior details, and it is helpful when troubleshooting issues with the product.

Tasks

- Enable or disable the product logging on page 37
  Enable or disable the product logging as required.
- Configure the Product log file size on page 37
  Configure the maximum Product log file size in megabytes.

Enable or disable the product logging

Enable or disable the product logging as required.

Task

1 Log on to the system as root user.

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

3 Run these commands as required.
   - ```
     ./isecav --productlog enable
   ``` — Enables the product log.
   - ```
     ./isecav --productlog disable
   ``` — Disables the product log.

Configure the Product log file size

Configure the maximum Product log file size in megabytes.

Task

1 Log on to the system as root user.

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

3 Run the command.
   ```
   ./isecav --setmaxproductlogsize <Number>
   ```

You can specify the file size between 1 MB and 999 MB. The default value is 10 MB

**Example: Configure the Product log file size to 25 MB**

This command sets the maximum Product log file size to 25 MB.

   ```
   ./isecav --setmaxproductlogsize 25
   ```
Configure the software to send events to SYSLOG

Configure the software to log the information to SYSLOG in addition to storing the information in the product log.

**Task**

1. Log on to your Linux system as root user.
2. Change directory to the `/bin` directory.
   
   `cd /opt/isec/ens/threatprevention/bin`
3. Run the command.
   
   `./isecav --usesyslog enable`

Configure the quarantine directory

Specify the directory where you want to store the quarantined items.

**Task**

1. Log on to your Linux system as root user.
2. Change directory to the `/bin` directory.
   
   `cd /opt/isec/ens/threatprevention/bin`
3. Run the command.
   
   `./isecav --setquarantinefolder /directory_path`
   
   You must specify the absolute path directory.
Protecting your managed Linux systems

Install the McAfee® Endpoint Security extensions and deploy a security strategy to protect your managed Linux systems from threats.

Chapter 4  Installing the software on systems managed with McAfee ePO
Chapter 5  Installing the software on a system managed with McAfee ePO Cloud
Chapter 6  Managing the software with McAfee ePO and McAfee ePO Cloud
Installing the software on systems managed with McAfee ePO

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

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

Contents

- System requirements
- Check in the package 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
- Migrated policies and their equivalent settings
- Remove the software from a managed system

System requirements

Make sure that your system environment meets these requirements and that you have administrator permission.

<table>
<thead>
<tr>
<th>Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Agent</td>
<td>McAfee Agent 5.0.3 and later.</td>
</tr>
<tr>
<td>McAfee ePolicy Orchestrator</td>
<td>5.1.1 and later.</td>
</tr>
</tbody>
</table>

Check in the package to the McAfee ePO server

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

Tasks

- Check in the package using Software Manager on page 42
  Check in McAfee Endpoint Security for Linux using the Software Manager.
- Check in the package manually on page 42
  Manually check in the McAfee Endpoint Security for Linux deployment package to the McAfee ePO Master Repository to manage the software.
Check in the package using Software Manager

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

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 | Software Manager.
3. From the Product Categories list under Software (By Label), select McAfee Endpoint Security for Linux Threat Prevention <version_number> <build_number>, select the package file, then click Check in All.
4. On the summary page, accept the McAfee End User License Agreement, then click OK.

Check in the package manually

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

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

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

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.
- ecn_help — Endpoint Security Common policy Help extension.
After installing the extensions, you can install McAfee Endpoint Security Migration Assistant extension to migrate McAfee VirusScan for Linux 1.9 and 2.x policies and tasks. For information about installing and using the Endpoint Security Migration Assistant, see McAfee Endpoint Security 10.2.0 Migration Guide.

**Tasks**

- *Install the extensions using Software Manager on page 43*
  Install the extensions using the Software Manager.

- *Install the extensions manually on page 43*
  Manually install Endpoint Security extensions on the McAfee ePO server.

**Install the extensions using Software Manager**

Install the extensions using the Software Manager.

**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, then click Software Manager.
3. From the Software Manager | Product Categories | Software (By Label), select Endpoint Security | McAfee Endpoint Security for Linux 10.2, 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**

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

You must install the extensions in this order:

- ENDPL_LIC <version> build_number.zip
- Common.<version>.<build_number>_.(Extension).zip
- Threat_Prevention.<version>.<build_number>.(Extension).zip
- help_ecn_<version>_.zip
- help_etp_<version>_.zip

**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 44**
  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 44**
  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**
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. 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 McAfee Endpoint Security for Linux Threat Prevention <build_number>, select Install as the action, then click Save.

   ![You can add more products by using +.]

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

Test the installation

After deploying the software, verify that the client software is installed and updated correctly on managed systems.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Wait for client systems to report back to the McAfee ePO server (typically after an hour).

2 On the McAfee ePO console, select Menu | Dashboards, then select Endpoint Security: Installation Status for a complete list of managed systems and their installation status.

Migrated policies and their equivalent settings
After migrating policies and settings from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux, you can view the migrated settings in the respective options.

General policy — Troubleshooting and Advance tab
Here is the list of General Policies > Troubleshooting and Advance tab settings migrated from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux Threat Prevention.

Troubleshooting tab

<table>
<thead>
<tr>
<th>In McAfee VirusScan Enterprise for Linux</th>
<th>In McAfee Endpoint Security for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Tab</td>
</tr>
<tr>
<td>General policies</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Advance tab

<table>
<thead>
<tr>
<th>In McAfee VirusScan Enterprise for Linux</th>
<th>In McAfee Endpoint Security for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Tab</td>
</tr>
<tr>
<td>General policies</td>
<td>Advance</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
On-Access Scan policy — General tab

Here is the list of On-Access Scan policy General tab policy settings migrated from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux settings.

<table>
<thead>
<tr>
<th>In McAfee VirusScan Enterprise for Linux</th>
<th>In McAfee Endpoint Security for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Tab</td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On-Access Scan policy — Detections tab

Here is the list of On-Access Scan policy Detections tab settings migrated from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux.

<table>
<thead>
<tr>
<th>In McAfee VirusScan Enterprise for Linux</th>
<th>In McAfee Endpoint Security for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Tab</td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Detections</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Detections</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Detections</td>
</tr>
</tbody>
</table>
## On-Access Scan policy — Advanced tab

Here is the list of On-Access Scan policy Advanced tab settings migrated from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux.

<table>
<thead>
<tr>
<th>In McAfee VirusScan Enterprise for Linux</th>
<th>In McAfee Endpoint Security for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Tab</td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Advanced</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Advanced</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Advanced</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## On-Access Scan policy — Actions tab

Here is the list of On-Access Scan policy Actions tab settings migrated from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux.

<table>
<thead>
<tr>
<th>In McAfee VirusScan Enterprise for Linux</th>
<th>In McAfee Endpoint Security for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Tab</td>
</tr>
<tr>
<td>On-Access Scanning policy</td>
<td>Actions</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>In McAfee VirusScan Enterprise for Linux</td>
<td>In McAfee Endpoint Security for Linux</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>If the above action fails</strong></td>
<td><strong>Process settings &gt; Actions &gt; If the first response fails</strong></td>
</tr>
<tr>
<td>No secondary options available for this action</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Deny access to infected files and continue</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Move infected files to the quarantine directory (configured in General tab)</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Delete infected files automatically</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Rename infected files automatically</td>
<td>On-Access Scan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When Programs &amp; Jokes are found</th>
<th><strong>Process settings &gt; Actions &gt; Threat detection first response</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access to infected files and continue</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Move infected files to the quarantine directory (configured in General tab)</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Delete infected files automatically</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Rename infected files automatically</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Clean infected files automatically</td>
<td>On-Access Scan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>If the above action fails</strong></th>
<th><strong>Process settings &gt; Actions &gt; If the first response fails</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>No secondary options available for this action</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Deny access to infected files and continue</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Move infected files to the quarantine directory (configured in General tab)</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Delete infected files automatically</td>
<td>On-Access Scan</td>
</tr>
<tr>
<td>Rename infected files automatically</td>
<td>On-Access Scan</td>
</tr>
</tbody>
</table>
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 50
  Remove the extensions from the McAfee ePO server.
- Remove the software from client systems on page 50
  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.
Installing the software on systems managed with McAfee ePO
Remove the software from a managed system
Installing the software on a system managed with McAfee ePO Cloud

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

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

Contents

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

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

Tasks

- Create an installation URL on page 54
  Create an installation URL to install the software on managed systems.
- Install the software with an installation URL on page 54
  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
Installing the software on a system managed with McAfee ePO Cloud
Deploy the client software from McAfee ePO Cloud
Managing the software with McAfee ePO and McAfee ePO Cloud

Integrate and manage McAfee Endpoint Security for Linux using the McAfee ePO or McAfee ePO Cloud platform.

The primary differences in managing policies in two environments are:

- McAfee ePO — Organizations maintain a McAfee ePO server in their premises. Administrators check in and install the software on the server, create policy settings, and enforce them on multiple managed systems using deployment tasks.

- McAfee ePO Cloud — McAfee or the service provider maintains the McAfee ePO server, including checking in and installing the software. After setting up the cloud account from McAfee or another service provider, local administrators create policies and enforce them on managed systems using deployment tasks.

For instructions about setting up and using McAfee ePO and McAfee Agent, see the product guide for your version of the product.

Contents

- Using Endpoint Security extensions as common extensions
- Managing policies
- Common Policy
- Threat Prevention policy
- Queries and reports

Using Endpoint Security extensions as common extensions

Use the latest Endpoint Security extensions as common extensions to manage Threat Prevention policies and tasks on your Microsoft Windows, Macintosh, and Linux systems.

You can use Endpoint Security extensions to configure and deploy policies for your Windows, Macintosh and Linux systems. On each policy page, a tag indicates that the option applies only to specific operating systems. For example:

- **Windows only** — Applies only to Windows-based systems.
- **Linux only** — Applies only to Linux-based systems.
- **Windows and Mac only** — Applies only to Windows and Macintosh-based systems.
- **Windows and Linux only** — Applies only to Windows and Linux-based systems.

The policy options without tags are applicable to Windows, Mac, and Linux systems.

To view these tags in the policy and task options, you must have installed the licensing extension on your McAfee ePO server.
Managing the software with McAfee ePO and McAfee ePO Cloud

Managing policies

McAfee Endpoint Security for Linux policies provide options to configure features, feature administration, and to log details on managed systems. You can find these policies on the Policy Catalog page under Product:

- Endpoint Security Threat Prevention
- Endpoint Security Common

Configure these policies with your preferences, then assign them to groups of the managed systems. For generic information about policies, see the product guide for your version of McAfee ePO.

Create or modify policies

You can create and edit policies for a specific group in the System Tree.

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 From the Policy Catalog, select a Product and Category.
3 Perform these steps to create or modify a policy.

<table>
<thead>
<tr>
<th>To create a policy</th>
<th>To modify a policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Click New Policy.</td>
<td>1 Click the policy you want to modify.</td>
</tr>
<tr>
<td>2 Type the Policy Name.</td>
<td>2 Modify the settings.</td>
</tr>
<tr>
<td>3 Click OK.</td>
<td></td>
</tr>
<tr>
<td>4 Configure the settings.</td>
<td></td>
</tr>
<tr>
<td>4 Click Save.</td>
<td></td>
</tr>
</tbody>
</table>

Assign policies

After you create or modify policies, assign them to the systems or groups that are managed by McAfee ePO.

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 Navigate to System Tree, select a group or systems, then click the Assigned Policies tab.
3 Select a product from the product list, select a policy, then click Edit Assignment.
4 Select the policy to assign, select appropriate inheritance options, then click Save.
Common Policy

Use the Common Policy options to configure protection settings for your managed systems. Configure settings in the Common Policy to:
• Configure preferences for debug logging.
• Configure event logging preferences.
• Specify log files location.
• Configure product activity logging.
• Configure the size of activity logging file size.

Configuring client interface access

Classify your user group and determine the required access level for them. The Endpoint Security Common policy provides:
• Full access — Allows the managed system user to view or change all feature settings using the local system password credentials. You can provide Full access to users for whom you don’t want to restrict any action.

If the managed system user changes the protection settings locally, the subsequent policy enforcement overrides the changes.

Configuring debug logging

Administrators can enable or disable debug logging for the installed modules. When you enable debug logging for a module, events are logged for all components of the module.

For example, if you enable debug logging for Threat Prevention, events are logged for on-access scanning, and on-demand scanning at user level and at the kext level.

Activity and event logging

The Activity Log and Events Log record details of all Threat Prevention activities. Event Log sends all events that were recorded on the client to McAfee ePO.

Activity log

Activity log records all McAfee Endpoint Security for Linux Threat Prevention activities. You can define the log file size between 1 MB and 999 MB. The default is 10 MB. When the file size exceeds the limit, the current file is backed up and a new log file is created. The software retains the last 5 versions of the log files.

Event log

When enabled, all events are recorded to the Event Log on the McAfee Endpoint Security for Linux client, and sent to McAfee ePO. You can also send all events to the Event Log on the client syslog on Linux clients. The location of syslog is configurable on Linux systems.

Configure the Common policy

Configure the Common policy settings to define the log settings.
**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. From the Policy Catalog, select Endpoint Security Common as the product, then Options as the category.
3. Click New Policy, type a name for the policy, then click OK.
4. On the Policy Catalog page, click Show Advanced, then define these options:

<table>
<thead>
<tr>
<th>In this section...</th>
<th>In this category...</th>
<th>Configure...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Interface Mode</td>
<td>Activity Logging</td>
<td>• Full access — Allows the managed system user to view or change all feature settings using the local system password credentials.</td>
</tr>
</tbody>
</table>

- **Client logging**
  - **Activity Logging**
    - **Enable activity logging** — Enables logging of all McAfee Endpoint Security for Linux activity.
    - **Limit size (MB) of each of the activity log files** — Limits the log file size between 1 MB and 999 MB. The default is 10 MB. When the file size exceeds the limit, the current file is backed up and a new log file is created. The software retains the last 5 versions of the log files.

- **Debug Logging**
  - **Enable for Threat Prevention** — Enables debug logging for Threat Prevention. You can find the logs at:
    /opt/ise/ens/threatprevention/var/

- **Event Logging**
  - **Enable for Threat Prevention** — Enables debug logging for Threat Prevention. You can find the logs at:
    /opt/ise/ens/threatprevention/var/.
  - **Send events to McAfee ePO** — Sends all events logged to the Event Log on the client to McAfee ePO.
  - **Log events to Windows Event Log or syslog** — Sends all events to the McAfee Endpoint Security for Linux client syslog. The location of syslog is configurable on Linux systems.

5. Click Save.

6. In the System Tree, select the systems or groups.

7. In the right pane, click the Group Details tab, then click Wake Up Agents.

8. In Force policy update, select Force complete policy and task update, then click OK.

---

**Threat Prevention policy**

Threat Prevention checks for malware and other threats by scanning items on your managed systems. Use Endpoint Security Threat Prevention policy to configure scanning settings for your managed systems.
### Configure the On-Access Scan policy

Create an on-access policy to enable or disable on-access scan, define scanning time limit for each file, and to define exclusions.

**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. From the Policy Catalog, select Endpoint Security Threat Prevention as the product, then select On-Access Scan as the category.
3. Click New Policy, type a name for the policy, then click OK.
4. Click the policy that you created, click Show Advanced.
5. In the On-Access Scan section, define these settings.

<table>
<thead>
<tr>
<th>In...</th>
<th>Configure...</th>
</tr>
</thead>
</table>
| On-Access Scan | - Enable On-Access Scan — Enables or disables on-access scanning on managed systems.  
- Specify maximum number of seconds for each file scan — Specify the scan timeout value to scan each item. If you deselect this option, the value is set to 45 seconds. |
| Process Settings | Depending on the process or program through which a file is accessed, Threat Prevention categorizes the risk level as high risk process and low risk process. If the process doesn't fall under these categories, it is considered as standard process.  
- Use Standard settings for all processes — Applies standard settings when performing on-access scanning.  
- Configure different settings for High Risk and Low Risk processes — Applies different scanning settings for each process type that you identify. You can add, edit, or remove process and its type as required. |
<table>
<thead>
<tr>
<th>In...</th>
<th>Configure...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the <strong>Standard High Risk Low Risk</strong> process type:</td>
<td></td>
</tr>
<tr>
<td>• In <strong>When to scan:</strong></td>
<td></td>
</tr>
<tr>
<td>• When writing to disk — Scans files when they are written to.</td>
<td></td>
</tr>
<tr>
<td>• When reading from disk — Scans all files when they are read.</td>
<td></td>
</tr>
<tr>
<td>• Let McAfee decide — Scans files when written to or read.</td>
<td></td>
</tr>
<tr>
<td>• Do not scan when reading from or writing to disk — Doesn't scan files when reading from or writing operation. This is applicable only to Low Risk process.</td>
<td></td>
</tr>
<tr>
<td>• In <strong>What to scan:</strong></td>
<td></td>
</tr>
<tr>
<td>• All files — Scans files with any extension.</td>
<td></td>
</tr>
<tr>
<td>• Default and specified file types — Scans files with extensions defined in the software, and the extensions you specify.</td>
<td></td>
</tr>
<tr>
<td>For the list of default files that are scanned when Default and Specified file types option is selected, see McAfee KnowledgeBase article <a href="https://www.mcafee.com">KB79626</a>.</td>
<td></td>
</tr>
<tr>
<td>• Scan for Macros — Enables scanning for macros in all files.</td>
<td></td>
</tr>
<tr>
<td>• Specified file types only — Scans only files with extensions that you specify, and optionally, files with no extension.</td>
<td></td>
</tr>
<tr>
<td>• On network drives — Scans files in mounted-network volumes.</td>
<td></td>
</tr>
<tr>
<td>• Compressed archive files — Scans the contents of compressed archive files.</td>
<td></td>
</tr>
<tr>
<td>![Alert] Scanning compressed archive files requires additional time.</td>
<td></td>
</tr>
<tr>
<td>• Compressed MIME-encoded files — Scans Multipurpose Internet Mail Exchange email messages.</td>
<td></td>
</tr>
<tr>
<td>• In <strong>Additional scan options:</strong></td>
<td></td>
</tr>
<tr>
<td>• Detect unwanted programs — Enables the scanner to detect potentially unwanted programs.</td>
<td></td>
</tr>
<tr>
<td>• Detect unknown program threats — Enables the scanner to detect unknown programs.</td>
<td></td>
</tr>
<tr>
<td>• Detect unknown macro threats — Enables the scanner to detect unknown macro threats.</td>
<td></td>
</tr>
<tr>
<td>In **Actions</td>
<td>Threat detection first response:**</td>
</tr>
<tr>
<td>• Deny access to files — Prevents users from accessing any files with potential threats.</td>
<td></td>
</tr>
<tr>
<td>• Delete files — Deletes files that contain malware.</td>
<td></td>
</tr>
<tr>
<td>• Clean files — Removes threats from the detected file.</td>
<td></td>
</tr>
<tr>
<td>You can also configure a secondary response using the <strong>If first response fails</strong> option, in case the primary response is unsuccessful.</td>
<td></td>
</tr>
<tr>
<td>In <strong>Unwanted program first response:</strong></td>
<td></td>
</tr>
<tr>
<td>• Clean files — Removes the threat from the detected file.</td>
<td></td>
</tr>
<tr>
<td>• Delete files — Deletes the file that contains threats.</td>
<td></td>
</tr>
<tr>
<td>• Deny access to files — Prevents users from accessing files with potential threats.</td>
<td></td>
</tr>
<tr>
<td>• Allow access to files — Allows users to access the detected file.</td>
<td></td>
</tr>
<tr>
<td>• Scan Timeout response — Action to take when scanning timeout for a file.</td>
<td></td>
</tr>
<tr>
<td>• Scan Error Response — Action to take when scan fails with error.</td>
<td></td>
</tr>
</tbody>
</table>
In... Configure...

You can also configure a secondary response using the **If first response fails** option, in case the primary response is unsuccessful.

In the **Exclusions** section, click:

- **Add** — To add files to the exclusion list.
- **Edit** — To edit the exclusion settings.
- **Delete** — To remove the selected item from the exclusion list.
- **Clear All** — To remove all items from the exclusion list.

Enable **Overwrite exclusions configured on the client** to overwrite the exclusions list created by the managed system user.

For more information about configuring exclusions, see *Exclude files or directories from scanning*.

6 Click **Save**.

**Configure On-Demand Scan policy (Full Scan)**

Configure On-Demand Full Scan policy settings for your managed system.

**Task**

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

1 Log on to McAfee ePO as an administrator.

2 From the **Policy Catalog**, select **Endpoint Security Threat Prevention** as the product, then select **On-Demand Scan** as the category.

3 Click **New Policy**, type a name for the policy, then click **OK**.

4 Click the policy that you created, click the **Full Scan** tab, then define these settings.

<table>
<thead>
<tr>
<th>In...</th>
<th>Configure...</th>
</tr>
</thead>
</table>
| **What to Scan** | • **Compressed MIME-encoded files** — Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.  
  • **Compressed archive files** — Scans the contents of compressed archive files.  
  **(i)** Scanning compressed archive files requires additional time. |
| **Additional Scan Options** | • **Detect unwanted programs** — Enables the scanner to detect potentially unwanted programs.  
  • **Detect unknown program threats** — Detects files that contain code resembling malware.  
  • **Detect unknown macro threats** — Detects unknown macro threats. |
<table>
<thead>
<tr>
<th>In...</th>
<th>Configure...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Locations</strong></td>
<td></td>
</tr>
</tbody>
</table>
  - **Scan subfolders** — Examines all subfolders in the specified volumes when any of these options are selected.  
  - **Home folder** — Scans the Home directory.  
  - **Temp folder** — Directories with the name `/var/tmp` and `/tmp` are scanned.  
  - **User profile folder** — Scans the user profile directory.  
  - **File or folder** — Scans only the Linux-specific path.  
  - **All local drives** — Any mounted file system that is not a specified file system or a network file system.  
  - **All fixed drives** — Scans all fixed drives.  
  - **All mapped drives** — Any mounted file system type of NFS, CIFS, or SMBFS is considered as a mapped drive. When you select this option, all such file systems are scanned.  
  
  You can add locations by clicking `+`. Click `−` to remove the locations from scanning. |

| **File Types to Scan** |  
  - **All files** — Scans all files regardless of extension.  
  
  McAfee strongly recommends that you enable All files to make sure that no malware threat resides in your managed systems.  
  - **Default and specified file types** — Scans files with extensions defined in the software and extensions you specify.  
    For the list of default files that are scanned when Default and Specified file types option is selected, see McAfee KnowledgeBase article [KB79626](#).  
  - **Scan for macros** — Enables scanning for macros in all files.  
  - **Specified file types only** — Scans only files with extensions that you specify. Select Include files with no extension to scan files that contain no extension. |

| **Exclusions** |  
  In the Exclusions section, click:  
  - **Add** — To add files to the exclusion list.  
  - **Edit** — To edit the exclusion settings.  
  - **Delete** — To remove the selected item from the exclusion list.  
  - **Clear All** — To remove all items from the exclusion list.  
  
  For more information about configuring exclusions, see Exclude files or directories from scanning. |
<table>
<thead>
<tr>
<th>In...</th>
<th>Configure...</th>
</tr>
</thead>
</table>
| **Actions** | **In Threat detection first response:**  
- **Continue scanning** — Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.  
- **Clean files** — Removes the threat from the detected file.  
- **Delete files** — Delete the file that contains malware.  
You can also configure a secondary response using the **If first response fails** option, in case the primary response is unsuccessful.  
For Linux, when the action is set to **Deny**, on detection, the actual file write operation is not stopped. However, the subsequent action is denied.  
**In Unwanted program first response:**  
- **Continue scanning** — Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.  
- **Clean files** — Removes the threat from the detected file.  
- **Delete files** — Delete the file that contains malware.  
You can also configure a secondary response using the **If first response fails** option, in case the primary response is unsuccessful.  
If all actions fail, the fallback action is deny access. |
| **Performance** | **Use the scan cache** — Enables the scanner to use the existing clean scan results.  
- **Specify maximum number of seconds for each file scan** — Limits each file scan to the specified number of seconds. The default value is 45 seconds, and this option is enabled by default. If a scan exceeds the time limit, the scan stops cleanly and logs a message.  
- **Specify maximum number of threads allowed** — Limits the number of on-demand scan threads that can run simultaneously. |

5 Click **Save**.

For scheduling the task, see the product guide for your version of McAfee ePO.

**McAfee Endpoint Security for Linux does not support the Right-Click Scan option.**

**Configure an On-Demand Scan policy (Quick Scan)**

Configure an On-Demand Quick Scan policy settings for 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 From the **Policy Catalog**, select **Endpoint Security Threat Prevention** as the product, then select **On-Demand Scan** as the category.

3 Click **New Policy**, type a name for the policy, then click **OK**.

4 Click the policy that you created, click the **Quick Scan** tab, then define these settings.
<table>
<thead>
<tr>
<th>In...</th>
<th>Configure...</th>
</tr>
</thead>
</table>
| **What to Scan** | - Compressed MIME-encoded files — Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.  
- Compressed archive files — Scans the contents of compressed archive files.  

⚠️ Scanning compressed archive files requires additional time. |
| **Additional Scan Locations** | - Detect unwanted programs — Detects unwanted programs.  
- Detect unknown program threats — Detects files that contain code resembling malware.  
- Detect unknown macro threats — Detects unknown macro threats. |
| **Scan Locations** | - Scan subfolders — Examines all subfolders in the specified volumes when any of these options are selected.  
  - Home folder  
  - Temp folder  
  - File or folder  
  - All mapped drives  

Select the directory from the Specify locations drop-down list. You can add directories by clicking ➕. Click ➭ to remove the directory from scanning. |
| **File Types to Scan** | - All files — Scans all files regardless of extension.  

⚠️ **Best Practice:** Enable All files to make sure that no malware threat resides in your managed system.  
- Default and specified file types — Scans files with extensions defined in the software and extensions you specify.  
  
  For the list of default files that are scanned when Default and Specified file types option is selected, see McAfee KnowledgeBase article KB79626.  
- Scan for macros — Enables scanning for macros in all files.  
- Specified file types only — Scans only files with extensions that you specify. Select All files with no extension to scan files that contains no extension. |
| **Exclusions** | In the Exclusions section, click  
- Add — To add files to the exclusion list.  
- Edit — To edit the exclusion settings.  
- Delete — To remove the selected item from the exclusion list.  
- Clear All — To remove all items from the exclusion list.  

For more information on configuring exclusions, see Exclude files or directories from scanning. |
In Threat detection first response:

- **Continue scanning** — Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.
- **Clean files** — Removes the threat from the detected file.
- **Delete files** — Deletes the file that contains malware.

You can also configure a secondary response using the **If first response fails** option, in case the primary response is unsuccessful.

In Unwanted program first response:

- **Continue scanning** — Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.
- **Clean files** — Removes the threat from the detected file.
- **Delete files** — Deletes the file that contains malware.

You can also configure a secondary response using the **If first response fails** option, in case the primary response is unsuccessful.

In Performance:

- **Use the scan cache** — Enables the scanner to use the existing clean scan results.
- **Specify maximum number of seconds for each file scan** — Limits each file scan to the specified number of seconds. The default value is 45 seconds, and this option is enabled by default. If a scan exceeds the time limit, the scan stops cleanly and logs a message.
- **Specify maximum number of threads allowed** — Limits the number of on-demand scan threads that can run simultaneously.

5 Click **Save**.

For scheduling the task, see the product guide of your version of McAfee ePO.

McAfee Endpoint Security for Linux does not support the **Right-Click Scan** option.

**Exclude files or directories from scanning**

Exclude files or directories from on-access scanning and on-demand scanning.

**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 From the **Policy Catalog**, select **Endpoint Security Threat Prevention** as the product, then select **On-Access Scan** or **On-Demand Scan** as required.

3 Click the policy, then click **Show Advanced**.

   If you haven't created a policy, click **New Policy**, type a name for the policy, then click **OK**.

4 In the **Exclusion** area under **Process Settings**, click **Add** and define these settings as required, then click **Save**.
### Schedule a full or quick scan on managed systems

Schedule an on-demand scan to detect malware threats in the managed system.

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

3. Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**.
   a. For **Product**, select **Endpoint Security Threat Prevention**.
   b. For **Task Type**, select **Policy Based On-Demand Scan**, select the task from the **Task Name** list, then click **Next**.

4. Define these parameters, then click **Next**.
   - **Schedule status**
   - **Schedule type**
   - **Effective period**
   - **Start time**
   - **Task runs according to**
   - **Options**

McAfee Endpoint Security for Linux Threat Prevention supports only the **Daily**, **Weekly**, **Monthly**, **Once**, and **Run Immediately** options.

5. In the **Summary** page, click **Save**.

6. In the **System Tree**, select the systems or groups where you assigned the task.

7. In the right pane, click the **Group Details** tab, then click **Wake Up Agents**.

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

### Schedule a custom on-demand scan

Schedule a custom on-demand scan for 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 | Client Task Catalog.

3 In Client Task Types, expand Endpoint Security Threat Prevention, select Custom On-Demand Scan, then click New Task.

4 Select Custom On-Demand Scan from the Task Type drop-down list.

5 Define these settings, then click Save.
   - Name
   - Description
   - Scan Options
   - Scan Locations
   - File Types to Scan
   - Exclusions
   - Actions
   - Scheduled scan options

6 On the Client Task Catalog page, select the custom scan that you created, click Assign, select a group to assign the task, then click OK.

7 Configure the settings on each of these pages, then click Next.
   - Select Task
   - Schedule

8 Review your settings on the Summary page, then click Save.

**Configure the location for the quarantined items**
Configure the location to store the quarantined items on your managed system.

**Task**

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

2 From the Policy Catalog, select Endpoint Security Threat Prevention as the product, then select Options as the category.

3 In Quarantine Manager, select the directory from the Quarantine folder drop-down. The default location is quarantine.

4 Click Save.

**Schedule the DAT update**
Schedule an update to keep the content files and engine up to date.

**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 On the **Assigned Client Tasks** tab, click **Actions**, then select **New Client Task Assignment**.
   a For product, select **McAfee Agent**.
   b For task type, select **Product Update**.
   c Click **Create New Task** to open the **Client Task Catalog**.
   d Type a name for the task, select **Linux Engine** and **DAT** in **Signatures and engines** from **Package types**, then click **Save**.
      The task is listed under **Task Name**.
   e Select the task, then click **Next**.

4 On the **Schedule** page, define the schedule for the task.
   a In the **System Tree**, select the systems or groups where you want to assign the task.
   b Set these values, then click **Next**.
      • **Schedule status**
      • **Schedule type**
      • **Effective period**
      • **Start time**
      • **Task runs according to**
      • **Options**

McAfee Endpoint Security for Linux Threat Prevention supports only the **Daily**, **Weekly**, **Monthly**, **Once**, and **Run Immediately** options.

5 On the **Summary** page, click **Save**.

6 In the right pane, select **Group Details**, then click **Wake Up Agents**.

7 In **Force policy update**, select **Force complete policy and task update**, then click **OK**.

---

**Queries and reports**

Run predefined queries to generate reports, or modify queries to generate custom reports.

**Queries for Threat Prevention**

Here is the list of queries that you can view or customize for Threat Prevention.

<table>
<thead>
<tr>
<th>Query...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Security Threat Prevention: Hotfixes Installed</strong></td>
<td>The hotfixes installed for the software.</td>
</tr>
<tr>
<td><strong>Endpoint Security Threat Prevention: On-Access Scan Compliance Status</strong></td>
<td>This is the On-Access Scan compliance status.</td>
</tr>
<tr>
<td><strong>Endpoint Security Threat Prevention: Duration of Completed Full Scans in the Last 7 Days</strong></td>
<td>The duration of the completed Full Scan in the last seven days.</td>
</tr>
<tr>
<td><strong>Endpoint Security Threat Prevention: Systems Not Completed a Full Scan in the Last 7 Days</strong></td>
<td>The number of systems that have not completed a Full Scan in the last seven days but within the last month.</td>
</tr>
<tr>
<td><strong>Endpoint Security Threat Prevention: Systems Not Completed a Full Scan in the Last Month</strong></td>
<td>The number of systems that have not completed a Full Scan in the last month.</td>
</tr>
<tr>
<td><strong>Endpoint Security Threat Prevention: Duration of Completed Quick Scans in the Last 7 Days</strong></td>
<td>The duration of the completed Quick Scan in the last seven days.</td>
</tr>
</tbody>
</table>
### Endpoint Security Threat Prevention: Detection Response Summary
The number of threats where an action was taken (Clean, or Delete), versus the number threats where no action was taken, in the last three months.

### Endpoint Security Threat Prevention: Threats Detected Over the Previous 2 Quarters
The threats detected in the previous two quarters.

### Endpoint Security Threat Prevention: Threat Count by Severity
The number of events (slice counts) and event severities (slices) that occurred in the last three months.

### Endpoint Security Threat Prevention: Top 10 Detected Threats
The top 10 detected items in the last three months.

### Endpoint Security Threat Prevention: Top 10 Threat Sources
The top 10 computers that are the source for a threat in the last three months.

### Endpoint Security Threat Prevention: Top 10 Computers with the Most Detections
The 10 ten computers with the most detections in the last three months.

### Endpoint Security Threat Prevention: Top 10 Threats Per Threat Category
The top 10 threats per threat category in the last three months, grouped by threat category then by threat name.

### Endpoint Security Threat Prevention: Top 10 Users with the Most Detections
The top 10 users with the most detections in the last three months.

### Other queries
Run these queries to generate reports, or modify them to generate custom reports.

<table>
<thead>
<tr>
<th>Query..</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security: Top Infected Users in the Last 7 Days</td>
<td>The list of top infected users in the last seven days.</td>
</tr>
<tr>
<td>Endpoint Security: Primary Vectors of Attack in the Last 7 Days</td>
<td>The list of Primary Vectors of Attack in the last seven days.</td>
</tr>
<tr>
<td>Endpoint Security: Top Threats in the Last 48 Hours</td>
<td>The list of top threats in the last 48 hours.</td>
</tr>
<tr>
<td>Endpoint Security: Threats Detected in the Last 24 Hours</td>
<td>The number of threat events generated in the last 24 hours.</td>
</tr>
<tr>
<td>Endpoint Security: Threats Detected in the Last 7 Days</td>
<td>The number of threat events generated in the last seven days.</td>
</tr>
<tr>
<td>Endpoint Security: Summary of Threats Detected in the Last 24 Hours</td>
<td>The summary of threats detected in the last 24 hours.</td>
</tr>
<tr>
<td>Endpoint Security: Summary of Threats Detected in the Last 7 Days</td>
<td>The summary of threats detected in the last seven days.</td>
</tr>
<tr>
<td>Endpoint Security: Currently Enabled Technology</td>
<td>The list of technology that are currently enabled on each managed system.</td>
</tr>
<tr>
<td>Endpoint Security: Policy Compliance by Computer Name</td>
<td>Two lists of computers which do and do not have the latest policy applied.</td>
</tr>
<tr>
<td>Endpoint Security: Policy Compliance by Policy Name</td>
<td>A Boolean pie chart showing that policies have and have not been updated on the client system.</td>
</tr>
<tr>
<td>Endpoint Security Platform: Hotfixes Installed</td>
<td>The list of hotfixes installed for the software.</td>
</tr>
<tr>
<td>Endpoint Security: Installation Status Report</td>
<td>The stacked bar chart of multiple modules and their installation status.</td>
</tr>
</tbody>
</table>
**Index**

**A**
- about this guide 7
- APT repository
  - installing the software 19
  - setting up repository 19

**C**
- check-in package, ePolicy Orchestrator
  - checking in package 42
- client software
  - configuring access 59
  - installation 54
  - installing using url 44
  - installing with URL 54
  - preventing uninstallation 59
- client software access
  - full access 59
  - locking client interface 59
  - standard access 59
- command-line
  - configuring on-access scan 27
- configuration
  - enabling debug logging 59
- configuring
  - quarantine directory 69
- content files update, ePolicy Orchestrator
  - scheduling 69
- conventions and icons used in this guide 7
- creation
  - installation url 54

**D**
- DAT
  - scheduling the update 36
  - Updating the DAT 36
- DAT update
  - creating a task 35
- DAT update, ePolicy Orchestrator
  - scheduling 69
- Default settings, viewing 20
- deployment, ePolicy Orchestrator 45
- documentation
  - audience for this guide 7
- documentation (continued)
  - product-specific, finding 8
  - typographical conventions and icons 7

**E**
- enabling
  - on-access-scan 27

**I**
- installation
  - client software 43, 44, 54
  - extensions 42
  - RPM systems 17
  - Ubuntu systems 17
  - using APT repository 19
  - using software manager 43
  - using url 44
  - using URL 54
  - using urls 43
- installation URLs
  - McAfee ePO cloud 54

**M**
- McAfee ServicePortal, accessing 8

**O**
- on-demand scan
  - scheduling custom scans 68
  - scheduling from ePolicy Orchestrator 68

**P**
- package
  - checking in 41, 42
- packages
  - checking in 42
- policies
  - assign 58
  - create 58
  - management 58
  - modify 58
- process
  - defining risk level 24
product
  enabling log 37
product log
  configuring file size 37

R
removal of software 50
removal of software extension 50
requirements
  managed systems 41
  management server 41
risk category
  changing process 25
  removing process 25

S
scan
  scheduling custom scans 68
ServicePortal, finding product documentation 8

signature
  verifying software 17
software
  verifying signature 17
standalone
  upgrading software 20
syslog
  configuring software 38

T
technical support, finding product information 8

U
uninstallation
  RPM-based systems 22
  Ubuntu-based systems 22
urls
  installing client software 43