McAfee Endpoint Security 10.7.5 - Threat Prevention Product Guide - Linux

Contents

Product Overview

Overview

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.

Key features

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

Prevention — Avoiding threats

Configure Threat Prevention features to stop intrusions before they gain access to your environment.

- **Viewing managed tasks** — You can view the managed custom tasks from your McAfee ePO server.
- **6010 Engine support** — Pre-packaged with the latest 6010 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 Linux system.
- **Activity logging for on-demand scan** — You can now enable activity logging on-demand scan to track all the files scanned by the on-demand scan task.
- **Policy-Based On-Demand Scan client tasks** — Run a Quick Scan or Full Scan on the Endpoint Security Client from McAfee ePO. Configure the behavior of these scans in the policy settings for an on-demand scan.
- **Profile based scanning** — Allows you to add processes to high risk or low risk profile and configure protection settings accordingly for scanning.
- **Support for McAfee® Global Threat Intelligence™ (McAfee GTI)** — Supports McAfee GTI, a heuristic network lookup for suspicious files when running on-access scanning and on-demand scanning.

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 detections occur.
- **Alerts** — Specify how Threat Prevention notifies you when detections occur, including alerting options and filtering alerts by severity to limit alert traffic.

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

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

- **Support for CPU Throttled On-Demand Scan** — Allows you to configure and control the CPU usage when running on-demand scan task. To use this feature, you must install McAfee® Endpoint Security 10.6.1 or later extensions. For more information about the ePO extension update build numbers, see *McAfee Endpoint Security for Linux installation guide*.
- **Queries, dashboards, and server tasks (McAfee ePO)** — Monitor scanning activity and detections.
- **Log files (McAfee Endpoint Security for Linux Client)** — View a 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.
- **Content repositories** — Reduce network traffic over the enterprise Internet or intranet by moving the content file repository closer to the clients.
- **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, file age, 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 Windows, Linux, and Mac systems.
- **Support for McAfee ePO Cloud** — Support for McAfee ePO Cloud to manage policies for your Linux systems.
- **Enable debug logging from client interface** — Enable debug logging for Threat Prevention using the client interface.
- **Viewing managed tasks** — You can view the managed custom tasks from your McAfee ePO server.
- **Extra.DAT files** — Download and install Extra.DAT files to provide protection from a major virus outbreak.
- **Access Protection** — Allows you to protect files and processes from threats.
- **Migration of Host Intrusion Prevention Linux custom policies** — You can migrate Linux custom policies from Host Intrusion Prevention to Endpoint Security for Linux Threat Prevention.
- **Support for SELinux confinement** — McAfee Endpoint Security for Linux Threat Prevention and Firewall functions appropriately in SELinux policy confined mode.

- **Medium DAT support** — McAfee Endpoint Security for Linux now supports Medium DAT (for content) that reduces the footprint of the product.
- **Container Vulnerability Scanner** — McAfee Endpoint Security for Linux Container Vulnerability Scanner is a command line tool that enables you to identify the vulnerabilities present in your docker images.
- **Log compression support** — McAfee Endpoint Security for Linux Threat Prevention and Firewall now stores these logs in compressed format: `mfetpd`, `mfeoasmgr`, `odsreport`, `mfeespd`, `mfefwd`.
- **Exploit Prevention for Linux** — McAfee Endpoint Security for Linux supports Exploit prevention for Linux in a managed environment. It brings in content support that can automatically define access control policies and settings for processes, files, and directories. By restricting access to specific files and directories, you can protect your systems from vulnerabilities. Content support brings in signatures that can automatically enforce the above policies and can be updated on a regular cadence. The individual signatures can then be managed from ePO and configured to block and report access. For violations, you can either report access violations or disable it.

Note

McAfee Endpoint Security for Linux doesn't support expert rules for Exploit Prevention.

How it protects

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:

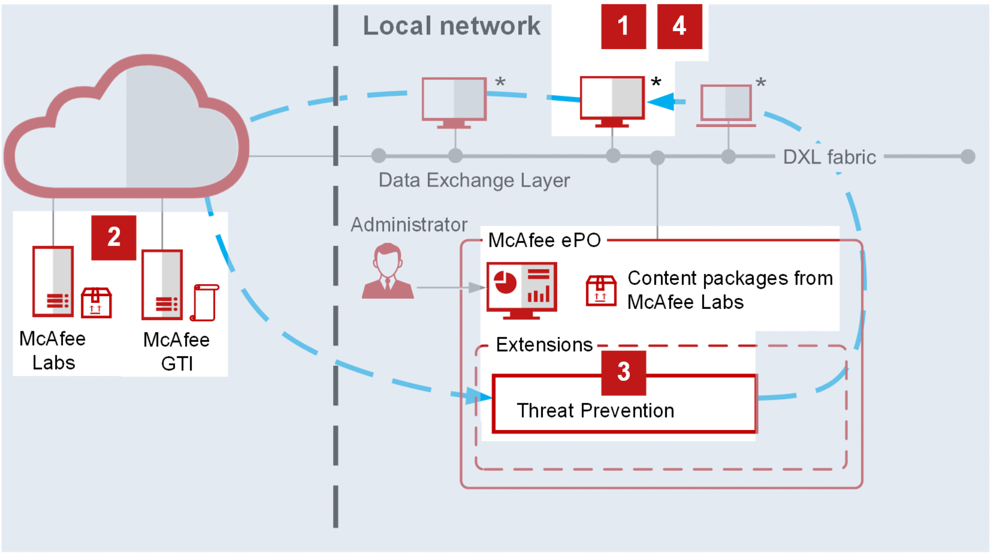
- Performs complex analysis using the malware definition files (DAT) and McAfee GTI
- Decodes the contents of the item you access
- Compares the contents with the known signatures stored in the DAT McAfee GTI to identify malware.

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

The high level work flow of Threat Prevention explained in the following diagram is:

1. Linux endpoints that are protected by Threat Prevention in your network with McAfee GTI enabled.
2. McAfee GTI validates the file and provides file rating.
3. Threat Prevention analyzes the file rating and the action configured in the policy.
4. Threat Prevention takes action on the file according to the configuration.

Threat Prevention process flow



* Client modules: Threat Prevention

Managing Endpoint Security for Linux tasks

mfetpcli command-line Help

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

You can use the mfetpcli 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.

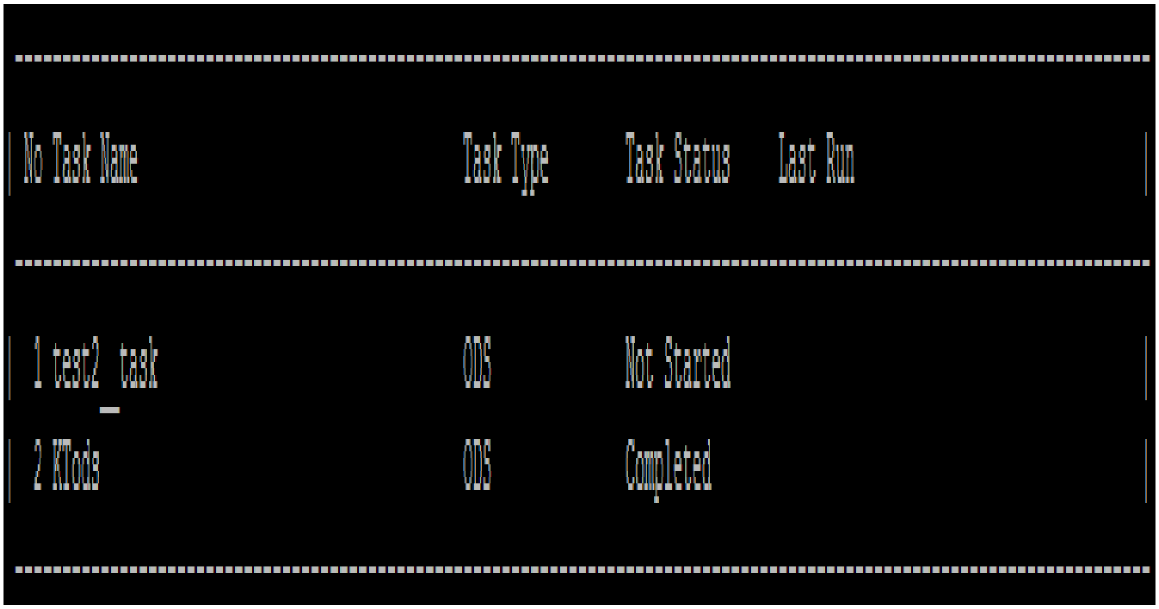
For example, your organization might consider accessing unknown files through websites can expose your systems to threats. To protect your systems from such threats, you can add the browser software Chrome to the High Risk process, and configure settings specifically.

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 mfetpcli 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.



```
------------------------------------------------------------------------------------
| No Task Name                    Task Type    Task Status   Last Run              |
------------------------------------------------------------------------------------
|  1 test2_task                   ODS          Not Started                         |
|  2 KTods                        ODS          Completed                           |
------------------------------------------------------------------------------------
```

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

```
./mfetpcli --runtask --index 2
```

Access the mfetpcli Help

Access the mfetpcli help from the command line to view configurations or to execute tasks. You can also view help from the man page for mfetpcli.

Task

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

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Execute the command.

   ```
   ./mfetpcli --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.

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 a user with administrator rights.
2. Navigate to the directory.

```
cd /opt/McAfee/ens/tp/bin
```

3. Execute the command.

```
./mfetpcli --addprocess --profile_type process_name
```

Note

For Linux, the process name must be the absolute path of the binary getting executed instead of just a 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:

```
./mfetpcli --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 a user with administrator rights.
2. Navigate to the directory.

```
cd /opt/McAfee/ens/tp/bin
```

3. Execute the command.

```
./mfetpcli --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:

```
./mfetpcli --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 a user with administrator rights.
2. Navigate to the directory.

```
cd /opt/McAfee/ens/tp/bin
```

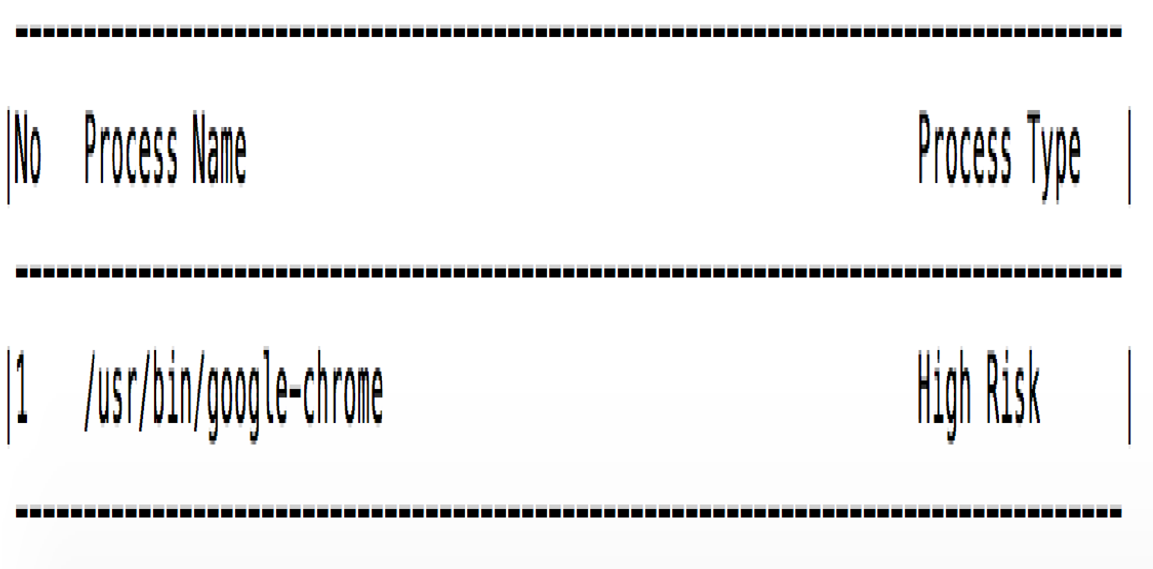
3. Execute the command.

```
./mfetpcli --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 `./mfetpcli --getoasconfig --processlist`.



```
==========================================================================
|No   Process Name                                      Process Type    |
==========================================================================
|1    /usr/bin/google-chrome                            High Risk       |
==========================================================================
```

   According to this list, the index number for Chrome process is 1.
2. Execute the command: `./mfetpcli --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.

Verify the status of the on-access scan

Check whether the on-access scanning is enabled.

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   `cd /opt/McAfee/ens/tp/bin`
3. Get details about the on-access scan task configuration.

   `./mfetpcli --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 a user with administrator rights.
2. Navigate to the /bin directory.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Enable or disable the scan:

   - Enable On-Access Scan: `./mfetpcli --setoasglobalconfig --oas on`
   - Disable On-Access Scan: `./mfetpcli --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 the system as a user with administrator rights.
2. Change directory to the /bin directory.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. View the current settings of the Standard process type.

   ```
   ./mfetpcli --getoasprofileconfig standard
   ```
4. Define the settings for the Standard process type.

   ```
   ./mfetpcli --setoasprofileconfig --profile standard [options]
   ```

Example: Configure the On-Access Scan Settings (Standard process type)

```
./mfetpcli --setoasprofileconfig --profile standard --setmode sor --filetypestoscan 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 the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run a command using this syntax.

   ```
   ./mfetpcli --setoasprofileconfig --profile [standard | highrisk | lowrisk] [exclusion options]
   ```

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

   Note

   > 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 `mfetpcli --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
`--excludepaths`	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 ("").
`--excludefiletype`	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 ("").
`-- excludesubfolder`	Specifies the directory and it's all subdirectories 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 excludes the files in the directory and all its subdirectories.

Using OAS Deferred Scan

For applications with high file I/O usage, there maybe some performance impact when inline scanning mode is used using Fanotify. To resolve this, enable OAS Deferred Scan to make sure read operations are scanned without any impact on the performance.

Note

Deferred scan is applicable only for Fanotify based systems.

When you enable OAS Deferred scan, scan on read is deferred. Be default, McAfee Endpoint Security for Linux only defers Scan on write mode.

You can enable deferred scan using the installer option `sudo ./install-mfetp.sh usedeferredscan` or command line interface option.

Using CPU Throttling for on-access scan

You can enforce OAS CPU throttling only in Fanotify mode when Deferred Scan is in enabled state or scan mode is scan on write. Here, main mfetpd and OAS manager process are throttled.

OAS CPU limit can be set using command line interface or installer option `sudo ./install-mfetp.sh usedeferredscan oascpulimit=value`. The default OAS CPU limit is 100 and on-access scan can be throttled between 50-99.

Note

Setting the value to 100 disables OAS CPU throttling.

Manage on-demand scanning

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

Create an on-demand scan task

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

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run a command using this syntax.

   ```
   ./mfetpcli --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.

Option	Values	Description	Note
`--scanarchive`	`enable` (default) `disable`	Examines the contents of archive (compressed) files, including .jar files. ⚠ **Caution:** Scanning archives is resource-intensive and affects performance.	
`--scanmime`	`enable` `disable` (default)	Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.	
`--scanpups`	`enable` (default) `disable`	Detects, decodes, and scans potentially unwanted programs.	
`--scanunknownprograms`	`enable` (default) `disable`	Detects, decodes, and scans unknown program files.	
`--scanunknownmacros`	`enable` (default) `disable`	Detects, decodes, and scans unknown macro viruses.	
`--scanlocaldrives`	`enable` `disable`	Scans all regular files under locally mounted file systems.	An on-demand task runs a scan on the configured files and directories. So you must set a scan path

Option	Values	Description	Note

`--scanpaths`	Absolute file name, just the name of a file, or Absolute name of the directory, specified according to these guidelines:
	• An Absolute file name and directory name must start with a slash [/].
	• A directory must end with a slash [/].
	• Multiple comma-separated values are allowed.
	• If any values have spaces in between, specify the value in double quotes ("").
		Includes the specified files or directories to the scan.	using one of these options.
			`--scanlocaldrives enable`
			`--scantmpfolders enable`
			`--scannetworkdrives enable`
			`--scanpaths [path]`

`--scantmpfolders`	`enable` `disable`	Scans all files under these directories in the system: /tmp /usr/local/tmp /var/tmp	
`--scannetworkdrives`	`enable` `disable`	Iterates and scans all network mount points on the system. Restricted to NFS and CIFS shares mounted on the system.	

`--scansubfolders`	`enable`
	`disable`
		Iterates through the folders specified.	Only applicable when specified with these options:
			`scanlocaldrives`
			`scanpaths`

Option	Values	Description	Note
			`scantmpfolders` `scannetworkdrives`
`--filetypestoscan`	• `all` (default and recommended) — Scans all files. • `defaultandspecified` — Scans the default files and files with specified extensions. • `onlyspecified` — Scans only files as the user specifies. Mention at least one file type using `addfiletype`.	Specifies which file types to scan.	
`--scanmacros`	`enable` `disable`	Scans for known macro threats in the list of default and specified files.	Only applicable with `filetypestoscan`
`--addfiletype`	Extension name — The file types are specified as extension names and support the wildcard [?]. Duplicate entries are automatically removed.	Adds file types to the default or specified user-defined list.	
`--delfiletype [extension name]`	Extension names — Specify the entry to be deleted.	Deletes file types from the user-defined list of the file.	

Option	Values	Description	Note
`--noextension`	`enable` `disable`	Specifies files to be scanned with no extension.	
`--excludepaths`	Absolute file name, just the name of a file or Absolute name of the directory, specified according to these guidelines: - Wildcards [*, ?] are allowed. - An Absolute file name and directory name must start with a slash [/]. - A directory must end with a slash[/]. - Multiple comma-separated values are allowed. - If any values have spaces in between, specify the values in double quotes ("").	Excludes the specified files or directories from the scan.	
`--excludefiletype`	Extension names, specified according to these guidelines: - Wildcard [?] is allowed. - Multiple comma-separated values are allowed. - If any of the values have spaces in between, specify	Specifies the extensions for exclusion.	

Option	Values	Description	Note
	the value in double quotes ("").		
`--excludepathwithsubfolder`	Excludes the specified directory and it's all sub directories.		Only applicable for directories specified as part of `excludepaths`.
`--usescancache`	`enable` `disable`	Specifies to use the On-Access Scan cache lookup while scanning files for this task.	
`--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.

Option	Values	Description	Note
`--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.
`--gti`	- `enable` — Enables McAfee GTI file rating. - `disable` Disables McAfee GTI file rating. - `sensitivity` Sets the sensitivity level of McAfee GTI file rating.		The sensitivity option is available only when McAfee GTI file rating is enabled for the scan.

Option	Values	Description	Note
`--setmaxcpulimit`	value	The allowed range is 25 to 100. By default, the value is set to 80.	

Example: `./mfetpcli --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 the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run a command using this syntax.

   ```
   ./mfetpcli --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 the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Get details about all on-demand scan tasks.

   ```
   ./mfetpcli --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 the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run a command using this syntax.
   ```
   ./mfetpcli --deltask --index [index number]
   ```
   Replace `[index number]` with the index number of the task to delete.

Enabling activity logging for on-demand scan

Enable activity logging for on-demand scan to track all the files scanned by the on-demand scan task.

When activity logging for on-demand scan is enabled, you can track the list of scanned files, timed-out files, and files having errors. If the on-demand scan task is interrupted or stopped before completion, the log file will contain all file details till the on-demand scan is stopped. The log files are available in .zip format at `/var/McAfee/ens/log/tp/odsreport/archive/`

For managed systems, you can configure this feature using the **Endpoint security common** policy extension.

For standalone systems, configure activity logging using the command line.

Configure on-demand scanning activity logging for managed systems

Follow these steps to enable activity logging for on-demand scan in a managed systems.

Task

1. Log on to McAfee ePO as an administrator.
2. Go to **Menu** > **Policy Catalog** > **Endpoint Security Common**.
3. In the **Endpoint Security Common** page, click **Policy Category** > **Options** > **My Default**.
   Click **Show Advanced** on the top left corner of the page.
4. In the **Client Logging** section, enable these options:
   - **Enable activity logging**.
   - Enable log for all scanned files during on-demand scans.
   - **Enable Limit size** (MB) of each of the activity log files and set the log size as 20MB.
5. Navigate to **System Tree**, and click on the **Assigned Policies** tab and in the **Product** section, select **Endpoint Security Common**.
6. Select **Endpoint Security Common** from the Product list, then click **Edit Assignment**.

   In the next page, click **Break inheritance and assign the policy** > **My Default** > **Assigned Policy** and select the **Save** option.
7. In the **System Tree** page, select the system to assign the policy. Click **Wake Up McAfee Agent**, and select **Force complete policy and task update** and select **OK**.
   Endpoint Security Common Policy by default gets enforced on the selected system.

View on-demand scan activity logging status on managed systems

Follow these steps to verify on-demand scan for activity logging on managed systems.

Task

1. Log on to managed systems as an administrator.
2. Navigate to the directory:

   `/opt/McAfee/ens/tp/bin/`
3. Verify the Activity logging for on-demand scan is enabled:

   `/opt/McAfee/ens/tp/bin/mfetpcli`
4. Execute on-demand scan task from Linux client:

   `/mfetpcli --runtask --name quick scan`
5. Verify the completion of on-demand scan task:

   `/mfetpcli --listtasks`
6. Verify on-demand scan activity report:

   `/var/McAfee/ens/log/tp/odsreport/quick\ scan-<timestamp>.zip`

Configure on-demand scanning activity logging for standalone systems

Follow these steps to enable on-demand scan for activity logging for standalone systems.

Task

1. Log on to the system as a user with administrative rights.
2. Navigate to the directory:

   `/opt/McAfee/ens/tp/bin/`
3. Run the command:

   - To enable on-demand scanning task for activity logging:

   `/opt/McAfee/ens/tp/bin/mfetpcli --odsactivitylog enable`

   - To confirm the enabled settings:

   `/opt/McAfee/ens/tp/bin/mfetpcli -showlogsettings`

Disable on-demand scan activity logging

Follow these steps to disable on-demand scan activity logging for standalone systems.

Task

1. Log on to the system as a user with administrative rights.
2. Navigate to the directory:

   `/opt/McAfee/ens/tp/bin/`
3. To disable the on-demand scan activity logging:

   `/opt/McAfee/ens/tp/bin/mfetpcli --odsactivitylog disable`

Set the required product log size

Use this command to set the product log size.

Task

1. Log on to the system as a user with administrative rights.
2. Navigate to the directory:
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run these commands to set the product log size to 20 MB:
   ```
   /opt/McAfee/ens/tp/bin/mfetpcli --setmaxproductlogsize 20
   ```

CPU Throttling for on-demand scan

The CPU Throttling option allows you to limit the CPU usage when you run on-demand scan tasks.

With the defined CPU usage threshold, you can run on-demand scan tasks with other tasks without experiencing performance issue, By configuring this option, you can allocate a specified percentage of CPU cycle for the on-demand scan task, and the remaining percentage of the CPU handles other processes. You can specify the value from 25 to 100. The default value is 80.

This option is supported for the kernel version 2.6.24 or later.

You can verify whether the CPU throttling threshold is applied for the on-demand scan by using the default available tool `top`. When you are using the top's view, you must turn off the irix mode by pressing `Shift + i`. By default, the `irix` mode is always enabled.

For standalone systems, you can define this value when you schedule an on-demand scan using command line. For managed systems, you can select the option from the On-Demand Scan policy.

Protecting Linux endpoints using McAfee GTI

McAfee GTI uses heuristics file reputation to check for suspicious files through on-access scanning and on-demand scanning.

You can enable McAfee GTI protection on standalone systems and systems managed by McAfee ePO or by McAfee ePO Cloud.

When an executable file is accessed by a user, or a manual or automated scan of a workstation or server is performed, files are checked against the McAfee DAT files to determine if they are malicious. If the file does not match a signature or hash in the DAT file, and the file meets proprietary criteria, a query is sent to the cloud to check the file against the McAfee GTI technology database. The McAfee GTI File Reputation service provides an instant reputation score that is interpreted by the Threat Prevention to apply a policy, such as block or quarantine. The result is near real-time protection of your endpoint against new and emerging malware.

Note

The system must have Internet connection to access McAfee GTI.

Sensitivity levels of McAfee GTI

You can configure the sensitivity level that McAfee GTI uses when it determines if a detected sample is malware.

- **verylow** — The detections and risk of false positives are the same as with regular DAT content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of waiting for the next DAT content file update.
- **low** — This setting is the minimum recommendation for systems with a strong security footprint.
- **medium** — Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive.
- **high** — Use this setting for deployment to systems or areas which are regularly infected.
- **veryhigh** — Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. McAfee recommends to use this level for systems that require highest security.

The McAfee GTI sensitivity level is set to **medium** for both on-access scanning and on-demand scanning by default. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections can result in more false positive results.

For more information about McAfee GTI, see KB53735.

Configure McAfee GTI settings for On-Access Scan and On-Demand Scan

Enable or disable McAfee GTI and its sensitive level for on-access scanning and on-demand scanning, and define the sensitivity.

View the McAfee GTI status

View whether McAfee GTI is enabled or disabled for the on-access scan, and its sensitivity level, if enabled.

Task

1. Log on to the system as a user with administrator rights.
2. Navigate to the directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.
   ```
   ./mfetpcli --getoasconfig --summary
   ```

Enable McAfee GTI for On-Access Scan

Enable McAfee GTI for on-access scanning to get file reputation from the McAfee GTI database.

Before you begin

You must have enabled On-Access Scan, and the system you intend to enable McAfee GTI must have Internet connection.

Task

1. Log on to the system as a user with administrator rights.
2. Navigate to the directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```

3. Run the command.
    - To enable McAfee GTI protection: `./mfetpcli --setoasglobalconfig --gti --state enable`

      Note

      When you enable McAfee GTI without specifying the sensitivity level, the default sensitivity level **medium** is applied.

    - To enableMcAfee GTI protection with a sensitivity level: `./mfetpcli --setoasglobalconfig --gti --state enable --sensitivity verylow`

Disable McAfee GTI for On-Access Scan

You can disable the McAfee GTI file reputation check for on-access scanning.

Task

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

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.

   ```
   ./mfetpcli --setoasglobalconfig --gti --state disable
   ```

View the McAfee GTI sensitivity level for On-Access Scan

You can view the sensitivity level defined in McAfee GTI presently for on-access scanning before changing it.

Task

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

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.

   ```
   ./mfetpcli --getoasconfig --summary
   ```

Configure the sensitivity level for McAfee GTI

You can define or change the sensitivity level of McAfee GTI detection.

Task

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

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.

   ```
   ./mfetpcli --setoasglobalconfig --gti --sensitivity high
   ```

   The available parameters are:

- **verylow** — The detections and risk of false positives are the same as with regular DAT content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of waiting for the next DAT content file update.
- **low** — This setting is the minimum recommendation for systems with a strong security footprint.
- **medium** — Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive.
- **high** — Use this setting for deployment to systems or areas which are regularly infected.
- **veryhigh** — Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. McAfee recommends to use this level for systems that require highest security.

Note

These parameters values (`verylow, low, medium, high, and veryhigh`) are case sensitive.

If you already configured the sensitivity level, the latest update replaces the existing sensitivity level. McAfee GTI sensitivity level is set to Medium by default for on-access scanning and on-demand scanning.

Tip

You can also set McAfee GTI state and its sensitivity level using the command `./mfetpcli --setoasglobalconfig --gti --state enable --sensitivity <option>`

Create an on-demand scan with McAfee GTI enabled

Enable McAfee GTI file detection for the scheduled scans wherever required.

Task

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

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.

   ```
   ./mfetpcli --addodstask --name <task_name> --parameter1 <value> --parameter2 <value> --gti --state enable --sensitivity veryhigh
   ```
   The available sensitivity levels are:

   - **verylow** — The detections and risk of false positives are the same as with regular DAT content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of waiting for the next DAT content file update.
   - **low** — This setting is the minimum recommendation for systems with a strong security footprint.
   - **medium** — Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. However, some

detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive.

- **high** — Use this setting for deployment to systems or areas which are regularly infected.
- **veryhigh** — Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. McAfee recommends to use this level for systems that require highest security.

The default sensitivity level for on-demand scanning is **medium**.

Note

> For standalone systems, you can't change the existing on-demand scan settings. For managed systems, you can change the on-demand scan policies for the policy-based on-demand scans such as Full Scan and Quick Scan.

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.

Create a DAT update task

Create a DAT update task from the command-line.

Task

1. Log on to the system as a user with administrator rights.
2. Navigate to the directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Create a DAT update task.
   ```
   ./mfetpcli --addupdatetask --name <task_name> --updatetype --<type_of_update>
   ```
4. View the tasks list to confirm that the DAT update task is created.
   ```
   ./mfetpcli --listtasks
   ```

Example: Create a DAT update task

```
./mfetpcli --addupdate task --name datupdate --updatetype dat
```

When you run the command from the `/opt/McAfee/ens/tp/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 a user with administrator rights.
2. Navigate to the directory.

   `cd /opt/McAfee/ens/tp/bin`
3. View the tasks list to identify the index number of your DAT update task.

   `./mfetpcli --listtasks`
4. Run the DAT update task.

   `./mfetpcli --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.

```
./mfetpcli --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 a user with administrator rights.
2. Navigate to the directory.

   `cd /opt/McAfee/ens/tp/bin`
3. View the tasks list to confirm that the DAT update task is created.

   `./mfetpcli --listtasks`
4. Schedule the task.

   `./mfetpcli --scheduletask --index <index_number> --daily --starttime <HH:MM>`

Example: Schedule a DAT update task to run every day at 12.45

```
./mfetpcli --scheduletask --index 3 --daily --starttime 12:45
```

When you run the command from the `/opt/McAfee/ens/tp/bin` directory, the software runs the DAT update task everyday at 12:45.

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 the system as a user with administrator rights.
2. Change directory to the /bin directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.
   ```
   ./mfetpcli --usesyslog enable
   ```

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.

Enable or disable the product logging

Enable or disable the product logging as required.

Task

1. Log on to the system as a user with administrator rights.
2. Navigate to the directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run these commands as required.
   - `./mfetpcli --productlog enable` — Enables the product log.
   - `./mfetpcli --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 a user with administrator rights.
2. Navigate to the directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.
   ```
   ./mfetpcli --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.

```
./mfetpcli --setmaxproductlogsize 25
```

Configure the quarantine directory

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

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command.
   ```
   ./mfetpcli --setquarantinefolder /directory_path/
   ```
   You must specify the absolute path directory.

   Note

   You can't configure the existing directories to quarantine the detections. You should specify a new directory name.

   For example,./mfetpcli --setquarantinefolder /root/ensl_quarantinedir/
   The default quarantine directory for standalone systems is /Quarantine. For systems managed by McAfee ePO, you can use the Common Policy to configure the quarantine directory. The default directory configured in the Common Policy is /quarantine/.

Access Protection

Access Protection allows you to define access control policies and settings for processes, files, and directories. By restricting access to specific files and directories, you can protect your systems from vulnerabilities.

You can create Access Protection rules, edit the rule settings, or delete the rules from the command line. You can also enable, disable, or change the McAfee ePO default rules. But you can't delete these rules. For each rule, you can define the action as **Report**, **Block**, or **Block** and **Report**. Access Protection also allows global exclusion to exclude processes that are critical for business criticality.

For managed systems, the policies that you configure on client systems are overridden by the Access Protection policies from McAfee ePO during the policy enforcement. There are no McAfee default rules defined for standalone systems.

Enable Access Protection

Use Access Protection commands to protect your standalone systems from external attacks. Enable, disable, or view the status of Access Protection using mfetpcli commands.

Task

1. Log on to the system as a user with administrator rights.
2. Change the directory to the Threat Prevention bin directory.
   ```
   cd /opt/McAfee/ens/tp/bin
   ```

3. To enable Access Protection, run:

   ```
   ./mfetpcli --setapstatus enable
   ```

   Note

   > To disable Access Protection, run:
   > `./mfetpcli --setapstatus disable`

View the status of Access Protection

Print the status of Access Protection, whether it is enabled or disabled.

Task

1. Log on to the system as a user with administrator rights.
2. Change the directory to the Threat Prevention bin directory.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command:

   ```
   ./mfetpcli --getapstatus
   ```

Access Protection rules

Access Protection rules are conditions that you can set to block, report, exclude, or include files, users, or processes to protect your managed or standalone systems. You can create custom rules for Access Protection and change the parameters as required.

Create Access Protection rules

You can create Access Protection rules, edit the rule settings, or delete the rules from the command line.

Task

1. Log on to the system as a user with administrator rights.
2. Change the directory to the`/bin` directory.

   ```
   cd /opt/McAfee/ens/tp/bin
   ```
3. Run the command:

   ```
   ./mfetpcli --createaprule --rulename [value] --block [enable |disable] --report [enable |disable] --
   subrulename [value] --subruletype [file | process] --operations [value(s)] --includetargetfile [file1,
   file2...]
   ```

Example: Create a rule to block create file operation

```
./mfetpcli --createaprule --rulename test1 --block enable --report enable --subrulename stest1 --subruletype
file --operations create --includetargetfile /tmp/testfile1
```

When you run the command from the `/opt/McAfee/ens/tp/bin` directory, a rule `test1` with a subrule `stest1` is created that blocks the user from creating a file or directory with the name `testfile1` in the `/tmp` directory.

Commands specific to Access Protection rules

When you create a rule, use parameters to block enable/disable, to apply the rule to specific users, files, or processes. You can also use parameters to report the number of tries made to access the rule-enabled files. You can also edit any rule using rule index. The `getallaprules` command lists all access protection rules with rule index created for a system.

Access Protection parameters to create rules

Options	Description
`--rulename [value]`	This command is used to name the Access Protection custom rule. Here, `value` can be alphanumeric and can take a maximum of 256 characters. Each custom rule name must be unique. When creating a rule, this parameter is mandatory.
`--block [enable | disable]`	This command is used to enable or disable blocking of access attempts defined in the rule. This parameter is mandatory. The parameter to enable or disable the `block` command:`--block [enable | disable]` **Note:** When creating a rule, both `--block` or `--report` parameters are mandatory. A rule is disabled when both `--block` and `-report` are disabled. If both rules exist, then `block` is given the higher precedence.
`--report [enable | disable]`	This command is used to enable or disable reporting of access tries. This parameter is mandatory. **Note:** When creating a rule, both `--block` or `--report` parameters are mandatory. A rule is disabled when both `--block` and `-report` are disabled. If both rules exist, then `block` is given the higher precedence.
	This is an optional parameter and specifies the applicable process that triggers the rule if there is

Options	Description
• `--includeprocess [name1:file1, name2:file2,…]` • `--excludeprocess [name1:file1, name2:file2,…]`	a subrule violation. You can identify a process with a name and a file. File can be either the file name or path. Wildcards [*, ?, and **] and comma-separated values are also accepted. **Note:** When `--includeprocess` and `--excludeprocess` are not specified, the rule becomes applicable to all processes. When the same process is mentioned in `--includeprocess` and `--excludeprocess`, then `--excludeprocess` takes higher precedence.
• `--includeusers [user1, user2,…]` • `--excludeusers [user1, user2,…]`	`--includeusers` triggers the rule for the specified users when there is a violation, whereas `--excludeusers` does not trigger the rule even when there is a rule violation. These parameters are optional and can accept comma-separated values. Local and Domain users are supported. **Note:** When `--includeusers` and `--excludeusers` are not specified, the rule becomes applicable to all users. When the same user is mentioned in `--includeusers` and `--excludeusers` then `--excludeusers` takes higher precedence.

Access Protection subrules

Access Protection subrules are conditions that are specified for a rule. Subrules are rules where you can specify the operation and target.

A rule must have at least one sub rule. You can create only one subrule while creating a rule. To add more subrules to a rule, you can use `--editaprule`. Subrule types can be set as file or process. Depending on the subrule type, you can specify the operations for the subrule.

Subrule parameters

Edit a custom Access Protection rule identified by `ruleindex`.

Parameters to create and edit subrules

Command	Description
`--addsubrule`	This command is used to add subrules to a rule.
`--editaprule [ruleindex]`	Edits a custom Access protection rule identified by `ruleindex`.

Parameters to manage subrules

Command	Description
`--subrulename [value]`	This command is used to name the subrule that is added to the rule. The subrule name must be unique within a rule. This parameter is mandatory.
`--subruletype [file | process]`	This command is used to set the type of subrule. The type can be file or process. This parameter is mandatory.
`--operations [value(s)]`	This command is used to specify the operations associated with the subrule. Operations can vary based on the type of the subrule. Possible values for file subrule — create, delete, execute, change permission, read, rename, write, change owner, symlink, and hardlink. Possible values for process subrule — terminate and run. This parameter is mandatory. Single or comma-separated values are allowed.

Access Protection subrule targets

Targets are files or processes on which a subrule action is applied.

Depending on the `--subruletype`, the targets can differ. A subrule must have at least one target.

Multiple targets can be added at the same time for a subrule.

When `--subruletype` is `file`, the following target parameters can be used.

Commands for subrule target file

Command	Description
`--includetargetfile [file1, file2…]`	Specifies the target files that are included in a file subrule. The values for `file` can be file, name, or path. Wildcards [*, ?, and **] and comma-separated values are also allowed.
`--includetargetdstfile [file1, file2…]`	Specifies the destination file or paths that are included in a file subrule. The target operations available for a file subrule are **Rename**, **Hardlink**, or **Symlink**. Wildcards [*, ?, and **] and comma-separated values are also allowed.
`--excludetargetfile [file1, file2…]`	Specifies the target files that are excluded when defining the subrule target based on either the file, name, or path. Wildcards [*, ?, and **] and comma-separated values are also allowed.
`--excludetargetdstfile [file1, file2…]`	Specifies the target destination file or paths that are excluded for a file subrule. The target operations available for a file subrule are **Rename**, **Hardlink**, or **Symlink**. Wildcards [*, ?, and **] and comma-separated values are also allowed.

Subrule targets when the subrule type is process:

Commands for subrule target process

Command	Description
`--includetargetprocess [name1:file1, name2:file2,…]`	Specifies the target process that is included when applying the subrule. The target process has a name

Command	Description
	and a file. The value for `file` can be either the file name or path. Wildcards [*, ?, and **] and comma-separated values are also allowed.
`--excludetargetprocess [name1:file1, name2:file2,…]`	Specifies the target process that must be excluded when applying the subrule. The target process has a name and a file. The value for `file` can be either the file name or path. Wildcards [*, ?, and **] and comma-separated values are also allowed.

Access Protection global exclusions

Processes in the global exclusions list are excluded from rules.

Exclusions are useful when you want to exclude system-specific files or processes to run as configured.

Command	Description
`--setapexclusions [name1:processfile1, name2:processfile2,…]`	Excludes the specified processes, identified by a name and file, for all Access Protection rules. `processfile` can either be the file name or path. Wildcards [*, ?, and **] and comma-separated values are allowed. **Note:** Adding a [*] in this setting ensures that all processes are excluded.
`--getapexclusions`	Prints the processes that are excluded for all rules.

Add Access Protection global exclusions

Exclude processes from triggering a rule when there is a violation.

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the bin directory.

```
cd /opt/McAfee/ens/tp/bin
```

3. To add the exclusion:

```
./mfetpcli --setapexclusions [name1:processfile1, name2: processfile2,…]
```

4. To view the list of exclusions:

```
./mfetpcli --getapexclusions
```

5. To remove the process from the exclusion:

```
./mfetpcli --deleteapexclusions [name1:processfile1, name2: processfile2,…]
```

Other Access Protection commands

You can view all Access Protection rules and their configuration details.

Commands to manage Access Protection rules

Commands	Description
`--getallaprules`	Prints all the Access Protection rules (irrespective of whether the rules are enabled or disabled). Information displayed includes rule index, rule name, actions, and origin (McAfee-defined or User-defined). To view all Access protection rules, run:`./mfetpcli --getallaprules`
`--getapruleconfig [ruleindex]`	Prints the details of the Access Protection rule identified by `ruleindex`. Information displayed includes actions, processes/users to which the rule applies, subrule and their associated targets. To print the Access Protection rules, run: `./mfetpcli --getapruleconfig [ruleindex]`
`--deleteaprule [ruleindex]`	To delete the Access Protection rule identified by `ruleindex`. Rule name cannot be used when deleting rules. **Note:** McAfee-defined rules cannot be deleted. To delete an Access Protection rule, run: `./mfetpcli --deleteaprule [ruleindex]`

Exploit Prevention

McAfee Endpoint Security for Linux supports Exploit prevention for Linux in a managed environment.

It brings in content support that can automatically define access control policies and settings for processes, files, and directories. By restricting access to specific files and directories, you can protect your systems from vulnerabilities. Content support brings in signatures that can automatically enforce the above policies and can be updated on a regular cadence. The individual signatures can then be managed from ePO and configured to block and report access.

For violations, you can either enable or disable reporting.

Note

Exploit Prevention is not supported in standalone systems.

Note

McAfee Endpoint Security for Linux doesn't support expert rules for Exploit Prevention.

Configure Exploit Prevention

Configure Exploit Prevention policy in your system.

Before you begin

- You must have installed McAfee Endpoint Security Threat Prevention extension 10.7.0.840 or above for Exploit prevention to work in your environment.
- Check-in Endpoint Security Exploit prevention Linux content.

Note

If you first check in Endpoint Security Exploit prevention Linux content and then install McAfee Endpoint Security Threat Prevention extension, the exploit prevention signatures doesn't reflect in the policy.

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   ```
   /opt/McAfee/ens/tp/bin
   ```

3. On a managed system, to enable Exploit Prevention, run:

   ```
   ./mfetpcli --setepstatus enable
   ```

Note

To disable Exploit Prevention, run:

```
./mfetpcli --setepstatus disable
```

Enable Exploit Prevention Policies from McAfee ePO

You can enable Exploit Prevention policies from McAfee ePO.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Secuity Threat Prevention** from the **Product** list.
3. Select **Category** as **Exploit Prevention**.
4. Open the policy and click **Enable Exploit Prevention**.

   Note

   You can enable or disable Exploit Prevention policies using this option.

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

View the status of Exploit Prevention

Print the status of Exploit Prevention, whether it is enabled or disabled.

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

   ```
   /opt/McAfee/ens/tp/bin
   ```

3. Run the command:

   ```
   ./mfetpcli --getepstatus
   ```

View Exploit Prevention status from McAfee ePO

You can check the status of Exploit Prevention using McAfee ePO.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, select the system.
3. In the**Products** section, select **Endpoint Security Threat Prevention**.
4. Check the **Exploit Prevention** section to view the status of Exploit Prevention.

Checking the status of content update task

You can configure content update task on client system.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, select the systems or groups for which you assigned the task.
3. To update the content on your system, click **Agent** | **Run Client Task Now**.
4. Complete these options, then click **Create New Task**:
    a. For product, select **McAfee Agent**.
    b. For task type, select **Product Update**.
5. On the **Selected Package** catalog, select **Endpoint Security Exploit Prevention Linux Content** and click on **Run Task Now**.

Check the status of content update

You can view the status of content available on your system.

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.

```
/opt/McAfee/ens/tp/bin
```

3. Run the command:

```
./mfetpcli --version
```

Checking content update status from McAfee ePO

You can view content update status from McAfee ePO.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, select the system.
3. In the **Products** section, select **Endpoint Security Threat Prevention**.
4. Check **Exploit Prevention content version** section

Queries & Reports

Run Queries & Reports to check Exploit Prevention content and compliance status.

- Log on to the McAfee ePO server as an administrator.
- Click on **Queries & Reports**, and type Exploit in the **Quick find** tab.
- Select **Endpoint Security Threat Prevent: Exploit Prevention Content Status**, and click **Run** to view the content status of the machines.
- Select **Endpoint Security Threat Prevent: Exploit Prevention Content Compliance Status**, and click **Run** to check the compliance status of systems.

Configuring Exploit Prevention Exclusions

You can check exclusions policies for Exploit Prevention.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Policy** | **Policy Catalog**, then select **Endpoint Secuity Threat Prevention** from the **Product** list.
3. From the **Category** list, select **Exploit Prevention**.
4. Click the name of an editable policy.
5. Click on **Add** and select **Linux File - Process** from the **Exclusion Type** drop-down list.
6. In the **Properties** section, add **Name** and **File name and path**.
7. Click **Save**.
8. In the right pane, select **Group Details**, then click **Wake Up Agents**.

Checking list of exclusions

Check list of exclusions available in Exploit Prevention policy.

Task

1. Log on to the system as a user with administrator rights.
2. Change directory to the /bin folder of the software.
   ```
   /opt/McAfee/ens/tp/bin
   ```
3. Run the command:
   ```
   /mfetpcli --getepexclusions
   ```

Supported Exploit Prevention commands

You can view all Exploit Prevention policies and their configuration details.

Command	Description	Comments
--version	Prints the Exploit prevention content version. To view Exploit prevention content version, run: `./mfetpcli --version`	Content version carries major version and build number. Build number is 5 digit number
--getallepsignatures	Prints signature ID, signature name, CVE details, block status , report status, and type of signature.	If signature is associated with any CVE, then the CVE ID will be printed in the output.
--getepstatus	Prints the status of exploit prevention.	

Command	Description	Comments
	To view the status of Exploit prevention, run: `./mfetpcli --getepstatus`	

--setepstatus	Allows user to enable or disable exploit prevention feature.
	To enable or disable Exploit prevention, run:
	`./mfetpcli --setepstatus enable/disable`
	To view the status of Exploit prevention, run:
	`./mfetpcli --getepstatus`
		Note: Exploit Prevention is not supported on unmanaged system. So, you cannot enable exploit prevention from CLI in unmanaged mode.

--getepexclusions	Allows user to add exclusion files. To check the list of exclusions, run: `/mfetpcli --getepexclusions`	

Filters

McAfee Endpoint Security for Linux supports Files and Processes filters.

You can apply filters for **Severity**, **Status**, **Origin**, and **Operating System**.

Check if an event is reported back to McAfee ePO

Follow these steps to check if an event is reported back to McAfee ePO.

Task

1. Log on to the system as a user with administrator rights.
2. Navigate to **System Tree**, and select the system.
3. Click **Threat Events**.

   Event is reported back to McAfee ePO. Click on the **Event ID** to get more details of the event.

Note

Event gets generated when the **Report** status is enabled for signature.

Exploit Prevention in standalone mode

In standalone mode, you cannot enable Exploit Prevention using the CLI option.

Skipping loading of certain signatures

Exploit prevention skips loading of signatures when policy rule ID is not part of any rule in content.

Exploit prevention content carries signatures definitions, these signatures can be conditional based signatures. For example, certain signatures are valid for few versions of product.

During policy enforcement when the rule ID in the policy does not match with the rule ID present in the content, then the rule will not be enforced to the kernel.

Supporting Security Enhanced Linux (SELinux) confinement

McAfee Endpoint Security for Linux Threat Prevention and Firewall now functions appropriately in SELinux policy confined mode.

SELinux is a kernel security module that allows enforcement of access controls that are loaded at the start of a system. You can use SELinux to confine programs and services as well as access to files, network, IPC, and other processes.

SELinux RPM provides SELinux policies to confine any service installed by McAfee McAfee Endpoint Security for Linux. When you install McAfee Endpoint Security for Linux along with McAfee Endpoint Security for Linux SELinux RPM, the McAfee Endpoint Security for Linux processes run in SELinux confinement. When installed, the SELinux modules create contexts for McAfee Endpoint Security for Linux processes, binaries, configuration files, log files, etc.

Supporting Medium DAT

McAfee Endpoint Security for Linux now supports Medium DAT (for content) that reduces the on-disk footprint of the product.

The advantages of Medium DATs is that it has all the capabilities of AVV DATs and occupies lesser space and memory, in addition to being faster and lighter than AVV DATs. The McAfee Endpoint Security for Linux package is bundled with a minimal DAT with version 999 that makes the deployment package smaller in size.

Note

On fresh installation, McAfee recommends updating the minimal DAT to the latest version of medium DAT. Since the minimal DAT version is used to reduce the product footprint, you must update the DAT to the latest version immediately after installation to protect your systems from malware threats.

Identifying vulnerabilities in docker images using McAfee Endpoint Security for Linux Container Vulnerability Scanner

McAfee Endpoint Security for Linux Container Vulnerability Scanner is a command line tool that enables you to identify the vulnerabilities present in your docker images.

You can use this tool to list images in a docker private registry or docker hub. This tool also enables you to filter the scan results by severity level and store results in a file either in table or JSON format.

Supported platforms

McAfee Endpoint Security for Linux Container Vulnerability Scanner currently supports these operating systems:

- Ubuntu 16.04 LTS, 18.04 LTS, and 20.04
- RedHat 6.x, 7.x, and 8.2

You can use McAfee Endpoint Security for Linux Container Vulnerability Scanner in these registries:

- Docker hub
- Private registry with basic authentication

Configure McAfee Endpoint Security for Linux Container Vulnerability Scanner

Before you begin

You must have McAfee Agent 5.6.4.110 or later installed and running on your system. For private registry setups that support https, you must store the self-signed TLS certificate in your cert store for appropriate functioning of Container Vulnerability Scanner.

To configure McAfee Endpoint Security for Linux Container Vulnerability Scanner, you must first enter your registry credentials in the config yaml file. The registry credentials must include the name of the registry, URL, and the username with which you are trying to access the registry. For docker hub registry image, the registry name is fixed as DockerHub. There can be only one DockerHub. For private registry, you can have a username of your choice.

Follow these steps to configure McAfee Endpoint Security for Linux Container Vulnerability Scanner on your system.

Task

1. Create a config file:
   `$HOME/.mfecvs.yaml`

   You can also change the location of the yaml using –config flag with the intended commands. For a sample on how to write the yaml file, please refer to `.mfecvs.yaml.sample` shipped along with the product.

   ```
   ./mfecvs --config "/path/to/file" list
   ```

2. Use the help command to know the correct usage of a particular command. The help commands also enables you to get to the man page.

   Few examples of help commands include`./mfecvs help`, `./mfecvs help list`, and `/mfecvs help scan`.

These commands enables you to output a manpage that describes the usage details of the command.

3. To list an image in the registry for both private docker registries and docker hub, navigate to:

   ```
   ./mfecvs help list
   ```

   [Private Registry]

   ```
   mfecvs list --registry "YourPrivateRegistryName"
   ```

   [Docker Hub]

   Note

   > If registry flag is not set, then the default registry is assumed to be docker hub.

   ```
   mfecvs list -r "DockerHub"
   ```

   or

   ```
   mfecvs list
   ```

   Flags that can be used with the list command:

   Flags:

-h,	--help	help for list
-p,	--password string	Specify the password for the registry
-r,	--registry string	Specify the name of the registry to look for images. Default is docker hub

   Global Flags:

--config string	config file (default is $HOME/.mfecvs.yaml)

4. On entering the password, Container Vulnerability Scanner fetches all the images present in your registry.

Perform image scanning with McAfee Endpoint Security for Linux Container Vulnerability Scanner

Follow these steps to scan docker hub and private registry images using McAfee Endpoint Security for Linux Container Vulnerability Scanner.

Before you begin

You must have McAfee Agent 5.6.4.110 or later installed and running on your system. For private registry setups that support https, you must store the self-signed TLS certificate in your cert store for appropriate functioning of Container Vulnerability Scanner.

Important

> To get the CVE information, the McAfee CVS scanner must have access to https://www.myshn.net/.

Task

1. Navigate to the location of mfecvs binary:

   ```
   cd $HOME/some/path/CVS
   ```

2. To start scanning:

   ```
   ./mfecvs help scan
   ```

   This command helps you to get the vulnerabilities information for a particular $image:$tag

   [Private Registry]

   ```
   mfecvs scan -r "Docker Private Registry" -i ubuntu:latest -f json -o output.json
   ```

   [Docker Hub]

   Note

   > If registry flag is not set, then the default registry is assumed to be DockerHub.

   ```
   mfecvs scan -i ubuntu:latest --format table --output Vulnerability.txt --severity High
   ```

   Flags that can be used with the list command:

   Flags:

-f	--format string	Specify the format to get the output. Valid options are table and json. Eg: --format table (default "table")

-h	--help	help for scan
-i	--image string	Specify the imagename to scan. Eg: --image ubuntu:latest
-o	--output string	Specify the output file. Eg: --output vulnerabilities.json
-p	--password string	Specify the password for the registry
-r	--registry string	Specify the name of the registry to look for images. Default is docker hub.
-s	--severity string	Specify the minimum severity to output. Valid options are Default, High, Medium, Low, and Unknown. Eg: --severity High (default "High")

Global Flags:

--config string	config file (default is $HOME/.mfecvs.yaml)

Classify your scan using these flags as required.

3. On entering your password, the Container Vulnerability Scanner displays the results mentioning the severity level of each package.

Managing the software using McAfee ePO and McAfee ePO Cloud

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.

Note

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

To create or apply Access Protection rules for Linux systems, select the option **Linux** in the **Policy Catalog** page.

For the list of features supported for each operating system, see McAfee KnowledgeBase article KB84410.

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**.

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

Task

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.

To create a policy	To modify a policy
1. Click **New Policy**. 2. Type the **Policy Name**. 3. Click **OK**. 4. Configure the settings.	a. Click the policy you want to modify. b. Modify the settings.

4. Click **Save**.

Assign policies

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

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

Task

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.

Tip

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.

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 Endpoint Security for Linux Threat Prevention activities.

These log files sizes are monitored against the defined file size threshold in the product. If the file size exceeds the threshold, the log file is archived to the log archive directory through log rotation. You can define the log file size between 1 MB and 999 MB. The default size is 10 MB.

Log rotation happens on 2 scenarios:

- When the log file size reaches the defined threshold.
- When the mfetpd (product) services are restarted.

In addition to these 2 scenarios, log rotation also happens:

- When the product is shut down normally.
- If the product is stopped under abnormal circumstances, log rotation does not happen.
- When you start the product after the abnormal process termination, logs are appended to the older log file. But if the older log file size is greater than the threshold, the log file rotation happens first. The product then starts writing to a fresh log file.
- Log rotation also happens in real time when the product's active log size exceeds the defined threshold.

Every time a log file is rotated, it also checks the log archive directory size. If the directory size exceeds the threshold, it deletes the oldest file.

Note

The threshold of the log archive directory is same as the limit defined in the product. For example, if the product uses the default limit of 10 MB, the log archive directory threshold is also 10 MB.

These thresholds are also applied to each log archive-related directory (such as mfeoasmgr, mfescanfactory, or mfeodscollector) in the following directories:

- /var/McAfee/ens/log/tp
- /var/McAfee/ens/log/esp

The archived logs are automatically deleted when the total size of the log archive directory exceeds the threshold (default limit * 5 times).

Each process of Endpoint Security for Linux Threat Prevention has its own dedicated archive log directory. If one of these directories exceeds the threshold (default limit * 5 times), the software deletes the oldest log file in that directory.

The oldest log file is the file that contains the smallest number in its secondary name. After deleting the oldest log file, the process again checks the log archive directory size. If the directory size is still greater than the threshold, the software again deletes the oldest log file from the existing files. This cycle continues until the directory size becomes lesser than the threshold value (default limit * 5 times).

For example, the log files names in the log archive directory are mfetpd.log, mfetpd.log00000, mfetpd.log00001, mfetpd.log0000.

mfetpd.log is the oldest log file in the Active Directory. mfetpd.log00000 is the next older file, then the next older file is mfetpd.log00001. But, when log rotation deletes the oldest log file mfetpd.log, it no longer appears in the archive directory, and the mfetpd.log00000 becomes the oldest log file. If mfetpd.log and mfetpd.log00000 are deleted, mfetpd.log00001 becomes the oldest log file.

If any process is never started or never executed (for example On-demand scan is never used), then its log file and log archive directory's size or age does not change.

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.

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

Task

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:

In this section...	In this category...	Configure...
Client Interface Mode		• **Full access** — Allows the managed system user to view or change all feature settings using the local system password credentials.
Client logging	**Activity 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: `/var/McAfee/ens/log/tp/` **Event Logging** • **Enable for Threat Prevention** — Enables debug logging for Threat Prevention. You can find the logs at: `/var/McAfee/ens/log/tp/` • **Send events to McAfee ePO** — Sends all events logged to

In this section...	In this category...	Configure...
		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.
Proxy Settings		- **No proxy server** — Threat Prevention directly sends the request to the McAfee GTI server. For managed systems, this is the default option selected in the McAfee ePO Common Policy settings. For standalone systems, the software always works in this mode. - **Use system proxy settings** — Threat Prevention uses the proxy server settings configured in the managed Linux system. You must configure the managed Linux system with the proxy server settings, then enforce the policy from McAfee ePO. Use the **Enable HTTP proxy authentication** option when the credentials of the proxy server are not defined in the managed Linux systems. - **Configure proxy server** — Threat Prevention uses the proxy server settings such as IP address and credentials in the Common Policy.

In this section...	In this category...	Configure...
		▫ **HTTP address (must be DNS, IPv4, or IPv6)** — Specifies the IP address of the proxy server. For IPv6, you must specify the IP address in square bracket. For example, `http://[xxxx:xxxx:xxxx:x::xx]:<port-number>`. ▫ **Port** — Specifies the port number. The default port number is 3128. ▫ **Exclude these addresses** — Excludes the addresses specified in this list. ▫ **Enable proxy authentications** — Enables proxy authentications for your managed Linux systems. ▫ **User name** — Specifies the user. ▫ **Password** — Specifies the password. ▫ **Confirm Password** — Confirms the password.

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**.

Using proxy settings for McAfee GTI and DAT update

For managed systems, you can enable proxy server settings to retrieve McAfee GTI reputation and update DAT for Threat Prevention. You can specify proxy server options in the Common policy settings.

Using the Common Policy settings, you can enable, disable, or configure the proxy settings for McAfee GTI. Once you configure the proxy settings, the McAfee GTI queries are sent to McAfee GTI through the proxy servers you configured. The software supports these proxy settings mechanisms:

- With authentication
- No authentication
- Kerberos authentication

For the systems managed by McAfee ePO, you can use the **Use System Proxy** option in the Common policy, and configure the script changes in the managed Linux endpoint's deamon process according to your environment. Once configured, the file ratings are derived from McAfee GTI through the proxy server.

McAfee GTI proxy is not supported on standalone Linux systems. You can't configure proxy settings for McAfee GTI proxy using the command line on standalone Linux systems. But, you can configure the deamon process to get McAfee GTI through the proxy server. For more information about configuring the deamon process for your environment, see *Configure system proxy authentication on managed Linux endpoints*.

For DAT update, the proxy in standalone machines can be set using this command-line:

```
/opt/McAfee/ens/tp/bin/mfetpcli --addproxy --type http --url "http://sampleproxy.url" --port 5678 --username
"username" --password "password"
```

The Common Policy proxy settings provide three options:

- **No proxy server** — Threat Prevention directly sends the request to the McAfee GTI server. For managed systems, this is the default option selected in the Common Policy settings. For standalone systems, the software always works in this mode.
- **User system proxy settings** — Threat Prevention uses the proxy server settings configured in the managed Linux system. You must configure the managed Linux system with the proxy server settings, then enforce the policy from McAfee ePO. Use the **Enable HTTP proxy authentication** option when the credentials of the proxy server are not defined in the managed Linux system.
- **Configure proxy server** — Threat Prevention uses the proxy server settings such as IP address and credentials you define in the Common Policy.
  - **HTTP address (must be DNS, IPv4, or IPv6)** — Specifies the IP address of the proxy server.

    Important

    > When you specify the IPv6 address, you must specify it with square brackets. For example, `http://[0000:0000:0000:0::00]: <port_number>`. Otherwise, the IPv6 doesn’t work.

  - **Port** — Specifies the port number. The default port number is 3128.
  - **Exclude these addresses** — Excludes the addresses specified in this list.
  - **Enable proxy authentications** — Enables proxy authentications for your managed Linux systems.
  - **User name** — Specifies the user name.
  - **Password** — Specifies the password.
  - **Confirm Password** — Confirms the password.

Configure system proxy authentication on managed Linux endpoints

In System Proxy Settings, the software supports only the basic proxy authentication.

You can configure the authentication in the daemon process (mfetpd) by defining the environment `http_proxy` or `https_proxy` as a variable.

For example:

- `http_proxy="http://username:usernamepassword@sampleproxy.url:5678`
- `https_proxy="https://username:usernamepassword@sampleproxy.url:5678`

Define these environment variables in the deamon process's init script. The configuration process varies according to the distribution you are using in your environment. The software supports these 3 types of init systems:

- Systemd
- SysVInit
- Upstart

Configure the proxy authentication for systemd based systems

Navigate to the respective directory and configure the environment variable and its value.

Task

1. Navigate to the directory and open the file.

   `/lib/systemd/system/mfetpd.service`
2. In **Service section**, add an entry.

   `<environment variable>=<user's proxy settings>`

   For example: `http_proxy="http://username:usernamepassword@sampleproxy.url:5678"`
3. Reload the mfetpd service.

   `systemctl daemon-reload`

Configure the proxy authentication for SysVInit systems

Navigate to the respective directory and configure the environment variable and its value, and export it.

Task

1. Navigate to the directory and open the file.

   `cd /etc/init.d/mfetpd`
2. Define the environment variable in the mfetpd configuration file.

   `<environment variable>=<user's proxy settings>`

   `export <environment variable>`

   For example:

   ```
   http_proxy="http://username:usernamepassword@sampleproxy.url:5678"
   export http_proxy
   ```

3. Restart the mfetpd service.

   `service mfetpd restart`

Configure the proxy authentication for Upstart based systems

Navigate to the respective directory, create the configuration file, and define the environment variable.

Task

1. Navigate to the file.

   `/etc/init/mfetpd.conf`
2. Create a configuration file <proxyConfigFileName> in the `/etc/default` directory.
3. Declare and export the environment variable of proxy in the <proxyConfigFileName> file.

   ```
   env
   http_proxy="http://username:usernamepassword@sampleproxy.url:5678"
   export http_proxy
   ```
4. Save the <proxyConfigFileName> file, and make sure that the file has execute permission.
5. Navigate to the file `/etc/init/mfetpd.conf`
6. In the script section of upstart file, add this command to allow your environment variables to be set for that process.

   `./etc/default/<proxyConfigFileName>`

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.

Product	Category	Available options
Endpoint Security Threat Prevention	On-Access Scan	• Enable or disable on-access scanning on managed systems. • Specify time limit to scan each file. • Specify when to scan files. • Scan specific types of files. • Define actions for detected items and unwanted programs. • Exclude files and directories.
	On-Demand Scan	• Run full scan and quick scan on managed systems. • Scan specific directories and their subdirectories.

Product	Category	Available options
		- Scan specific types of files. - Define actions for detected items and unwanted programs. - Exclude files and directories from scanning.

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.

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

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 **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.

In...	Configure...
On-Access Scan	- **Enable On-Access Scan** — Enables or disables on-access scanning on managed system. - **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.
McAfee GTI	- **Enable McAfee GTI** — Enables McAfee GTI, a heuristic network look up for suspicious files. Select the **Sensitivity level** as required: - **Very low** — The detections and risk of false positives are the same as with regular DAT content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of waiting for the next DAT content file update.

In...	Configure...
	• **Low** — This setting is the minimum recommendation for systems with a strong security footprint. • **Medium** — Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive. • **High** — Use this setting for deployment to systems or areas which are regularly infected. • **Very high** — Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. McAfee recommends to use this level for systems that require highest security.
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. In the **Standard High Risk Low Risk** process type: • In **When to scan**: ▫ **When writing to disk** — Scans files when they are written to. ▫ **When reading from disk** — Scans all files when they are read.

In...	Configure...
	▫ **Let McAfee decide** — Scans files when written to or read. • **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. • In **What to scan**: ▫ **All files** — Scans files with any extension. ▫ **Default and specified file types** — Scans files with extensions defined in the software, and the extensions you specify. For the list of default files that are scanned when Default and Specified file types option is selected, see McAfee Knowledge Base article KB79626. ▫ **Scan for Macros** — Enables scanning for macros in all files. ▫ **Specified file types only** — Scans only files with extensions that you specify, and optionally, files with no extension. • **On network drives** — Scans files in mounted-network volumes. • **Compressed archive files** — Scans the contents of compressed archive files. **Caution:** Scanning compressed archive files requires additional time. • **Compressed MIME-encoded files** — Scans Multipurpose Internet Mail Exchange email messages. • In **Additional scan options**: ▫ **Detect unwanted programs** — Enables the scanner to detect potentially unwanted programs. • **Detect unknown program threats** — Enables the scanner to detect unknown programs. • **Detect unknown macro threats** — Enables the scanner to detect unknown macro threats.

In...	Configure...
	In **Actions** → **Threat detection first response**: • **Deny access to files** — Prevents users from accessing any files with potential threats. • **Delete files** — Deletes files that contain malware. • **Clean files** — Removes threats from the detected file. 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**: • **Clean files** — Removes the threat from the detected file. • **Delete files** — Deletes the file that contains threats. • **Deny access to files** — Prevents users from accessing files with potential threats. • **Allow access to files** — Allows users to access the detected file. • **Scan Timeout response** — Action to take when scanning timeout for a file. • **Scan Error Response** — Action to take when scan fails with error. 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.

In...	Configure...
	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.

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

Task

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.

In...	Configure...
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. **Note:** 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.

In...	Configure...
Scan Locations	• **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. **Note:** 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.

In...	Configure...
	• **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.
McAfee GTI	• **Enable McAfee GTI** — Enables McAfee GTI, a heuristic network look up for suspicious files. Select the **Sensitivity level** as required: • **Very low** — The detections and risk of false positives are the same as with regular DAT content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of waiting for the next DAT content file update. • **Low** — This setting is the minimum recommendation for systems with a strong security footprint. • **Medium** — Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive. • **High** — Use this setting for deployment to systems or areas which are regularly infected. • **Very high** — Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. McAfee recommends to use this level for systems that require highest security.
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.

In...	Configure...
	• **Clear All** — To remove all items from the exclusion list. For more information about configuring exclusions, see *Exclude files or directories from scanning*.
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

In...	Configure...
	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. • **Limit maximum CPU usage (Available only when Scan anytime is selected)** — Limit the CPU usage when you run on-demand scan tasks. The default value is 80. You can specify the value 25 to 100.

5. Click **Save**.
   For scheduling the task, see the product guide for your version of McAfee ePO.

Note

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.

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

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 **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.

In...	Configure...
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.

In...	Configure...
	⚠ **Caution:** 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. **Tip: 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.

In...	Configure...
	• **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.
McAfee GTI	• **Enable McAfee GTI** — Enables McAfee GTI, a heuristic network check for suspicious files.
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*.
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** — 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.

In...	Configure...
	• **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.
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.

Note

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.

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

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 **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**.

In...	Configure...
What to exclude	• **Pattern (can include wildcards * or ?)** — Specifies the file pattern to exclude. For example, to exclude all files in the desktop from scanning, specify the path as `/Users/user/Desktop/*` • **Also exclude subfolders** — Excludes files and directories from the specified location. • **File type (can include wildcard ?)** — Excludes files that contain the extension. Select **Overwrite exclusions configured on the client** (On-Access Scan only) to overwrite the client exclusion list.
When to exclude	• **On read** — (On-Access Scan only) Excludes from scanning when the file is accessed. • **On write** — (On-Access Scan only) Excludes from scanning when the file is changed.

Schedule a full or quick scan on managed systems

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

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

Task

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.

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

Task

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**
    - **McAfee GTI**
    - **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.

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

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** | **Systems** | **System Tree**, then select a group or systems.
3. On the **Assigned Client Tasks** tab, click **Actions**, then select **New Client Task Assignment**.
    1. For product, select **McAfee Agent**.
    2. For task type, select **Product Update**.
    3. Click **Create New Task** to open the **Client Task Catalog**.
    4. 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**.
    5. Select the task, then click **Next**.
4. On the **Schedule** page, define the schedule for the task.
    1. In the **System Tree**, select the systems or groups where you want to assign the task.
    2. 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**.

Restore the quarantined items

Restore the quarantined items from the managed Linux endpoints for sending it for further analysis.

Task

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 **Restore from Quarantine**, click **New Task**, then select **Restore from Quarantine** from the Task Types.
4. In the **Client Task Catalog** page, define these settings:
    - **Task name** — Specifies the name of the task.
    - **Description** — Specifies the purpose of the task and its other references.

- **Items to Restore** — Specifies the exact detection name of the item to restore.

5. Review the settings, then click **Save**.
   For information about restoring the quarantined items on a standalone system, see McAfee Knowledge Base article KB88067.

Using proxy settings

You can use proxy servers for product update, DAT update, and McAfee GTI look up

All communications between the managed Linux endpoints and McAfee ePO happens through McAfee Agent. When McAfee Agent is configured with proxy, the McAfee ePO communication also happens through that proxy. For product update and DAT update, you can use the proxy settings in the McAfee Agent repository policy. In the Proxy tab, you can specify proxy for http and FTP.

Proxy for product update and DAT update

For Product update and DAT update, you can use the system proxy settings.

For product update and DAT update through proxy, you can use the proxy settings in the McAfee Agent repository policy. You can also specify the proxy for http and FTP. For standalone environment, you have command-line option to configure the proxy settings.

McAfee GTI Proxy

You can configure proxy for McAfee GTI using the system proxy settings in McAfee ePO server settings. The communication between Endpoint Security for Linux and McAfee GTI happens through the http protocol. You can also use the Common Policy settings, to enable, disable, or configure the proxy settings for McAfee GTI. Once you configure the proxy settings, the McAfee GTI queries are sent to McAfee GTI through the proxy servers you configured. The software supports these proxy settings:

- With authentication
- No authentication
- Kerberos authentication

Queries and reports

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

Configure Access Protection rules

Change the behavior of McAfee-defined rules or create custom rules to protect your managed access points.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Product** list.
2. From the **Category** list, select **Access Protection**.
3. Click the name of an editable policy.
4. Click **Show Advanced**.

5. Select the platform as Linux.
6. Change a McAfee-defined rule: In the **Rules** section, select the rule, then click **Edit**.
   a. On the **Rule** page, configure rule options.
   b. In the **Executables** section, click **Add**, configure executable properties, then click **Save** twice to save the rule.
7. Create a custom rule: In the **Rules** section, click **Add**.
   a. On the **Rule** page, configure the settings.
   b. In the **Executables** section, click **Add**, configure executable properties, then click **Save**.

      An empty **Executables** table indicates that the rule applies to all executables.

   c. In the **User Names** section, click **Add**, configure user name properties, then click **Save**.
      An empty **User Names** table indicates that the rule applies to all users.
   d. In the **Subrules** section, click **Add**, then configure subrule properties.

      Tip

      Best practice: To avoid impacting performance, don't select the **Read** operation.

   e. In the **Targets** section, click **Add**, configure target information, then click **Save** three times.
8. Specify the behavior of the rule: In the **Rules** section, select **Block**, **Report**, or both for the rule.
   - To select or deselect all rules under **Block** or **Report**, click **Block All** or **Report All**.
   - To disable the rule, deselect both **Block** and **Report**.
9. Click **Save**.

Migrating policies from Host Intrusion Prevention

You can migrate custom policies and Linux rules from Host Intrusion Prevention version 8 with patch 10 and later so that you can continue to apply the same rules to your managed systems from Endpoint Security for Linux Threat Prevention.

Custom policies from Host Intrusion Prevention are migrated to Access Protection in Endpoint Security for Linux. You can use the automatic or the manual mode for migrating the custom policies. For migrating custom policies from Host Intrusion Prevention to Endpoint Security for Linux Threat Prevention, you must upgrade Endpoint Security for Linux Threat Prevention to 10.5, then migrate the policies.

The custom policies created using the Host Intrusion Prevention **General** → **Category** → **Trusted Applications** and Host Intrusion Prevention **IPS** → **Category** → **IPS Rules/IPS Protection** can be migrated to Endpoint Security for Linux Access Protection.

The policies created in Host Intrusion Prevention **General (Trusted Applications)** can be migrated only in the automatic mode. The policies in Host Intrusion Prevention **IPS** (IPS Rules and IPS Protection) can be migrated using both automatic and manual modes.

Note

Host Intrusion Prevention **General** → **Trusted Applications** can be migrated only when the **Mark trusted for IPS (All platforms)** option is enabled while creating the policy.

How the migration works

Use the Endpoint Migration Assistant to migrate product settings where a supported legacy version of a product module is installed.

1. Install the Migration Assistant extension on the McAfee ePO server.
2. Open the Migration Assistant, select an automatic or manual path, then follow the instructions on the screen.

    - **Automatic migration** — Migrates supported legacy settings for all supported Windows products installed on your managed systems or only the systems in one group. Optionally migrates all supported settings for supported Mac and Linux products. Retains assignments.
    - **Manual migration** — Lets you select the settings to migrate, then edit the policies if needed. Does not retain assignments.

Migrate policies manually

Manually migrate selected policies for the supported products you have installed on Linux systems. Use manual migration to migrate selected policies, client tasks, or the Host IPS Catalog for your legacy products. The Endpoint Migration Assistant lets you select specific objects to migrate and edit the policies if needed. Manual migration does not retain assignments for migrated objects.

Before you begin

- Install the **Endpoint Migration Assistant** extension on the McAfee ePO server.
- Do not allow others to make changes to the objects you are migrating until migration is complete.

The custom policies created in Host Intrusion Prevention: IPS categories can be migrated to Endpoint Security for Linux.

Task

1. Log on to McAfee ePO server as an administrator.
2. Select **Menu** → **Policy** → **Endpoint Migration Assistant**.
3. Select the migration mode as manual.
4. For manual migration, select objects to migrate as **Policies**.
5. For **Objects to Migrate**, select **Policies**, then click **Next**. Only the objects that you have permission to view are listed.
6. Under **Available Policies** in the left pane, select policy categories for your products. The legacy policies within those categories are listed on the right side of the screen.
    a. If a category contains multiple policies, select the name of the policy to migrate from the drop-down list that appears next to the category name.
    b. If settings in a selected policy are merging with policies from other categories, the Migration Assistant displays the other categories. For each of these categories:

        - Select the name of the policy to migrate.

- If you don't want to migrate settings in that category now, select **None**. If you select **None** for all the merging categories, no new policy is created for these categories.

7. Click **Next**.
   The Migration Assistant displays the source policies on the left side of the screen. At the top of the screen, you see tabs for each Endpoint Security policy to be created. Each tab gives a preview of the new policies created when the selected source policies are migrated. The left pane shows the selected source policies.
8. Click **Next** to start the manual migration wizard.
9. On the open tab, type a name for the policy, type notes to describe it, and configure its options, then click **Next** to proceed to the next tab. Repeat this step until you have configured all the selected policies, then click **Next**.
10. Review the summary of changes, then click **Save** to create the new policies and add them to the Policy Catalog.
11. Select whether to migrate more objects.
    - **Yes** — Displays the screen where you can select additional objects to migrate.
    - **No** — Displays the first screen with default settings.

Migrate policies automatically

Custom policies created in Host Intrusion Prevention can be migrated automatically or manually using the Endpoint Migration Assistant. Currently, the custom policies created for Host Intrusion Prevention: IPS can be migrated automatically and manually. You must apply the policy to an entire system tree or a single group in the system tree before you migrate your policies in the automatic mode.

Before you begin

Make sure that **Endpoint Migration Assistant** extension is installed in the McAfee ePO.

Task

1. Log on to McAfee ePO server as an administrator.
2. Select **Menu** → **Policy** → **Endpoint Migration Assistant**.
3. Select the migration mode as automatic.
4. For manual migration, select objects to migrate as **Policies**.
5. For automatic migration, select the system to be migrated, click **Next**. You can select the entire System Tree or a single group in the system tree.
6. Click **Next** to generate a preview of the new Endpoint Security policies.
   A progress bar appears and lets you know how many policies are being included in the preview.
7. Review the new policies.
   a. Under **New Categories** in the left pane, select a category, then preview the new policies for that category in the right pane.
   b. (Optional) For every new policy that is created under Endpoint Security, click **Rename and Edit Notes** to rename the policy or edit the policy notes, if needed.
8. Click **Save** to run a server task to complete the migration.

Results

The Migration Assistant runs a server task in the background to migrate your policies. You can check its status in the Server Task Log. You must wait for the server task to complete before starting another migration session.

Verify migrated policies

Check that objects were migrated successfully before deploying Endpoint Security for Linux to managed systems.

Before you begin

Make sure that you have used the Endpoint Migration Assistant to manually migrate legacy product settings to Endpoint Security.

Task

1. In McAfee ePO, select **Menu** → **Policy** → **Policy Catalog**.
2. Select each product module, then check that the migrated policies were created.

COPYRIGHT