# McAfee Endpoint Security 10.6.0 - Release Notes

(McAfee ePolicy Orchestrator)

**Contents**



## About this release

This document contains important information about the current release. We recommend that you read the whole document.

We do not support the automatic upgrade of a pre-release software version. To upgrade to a production release of the software, you must first uninstall the pre-release version.

This release was developed for use with:

McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.3.1 and later

### Purpose

This release of McAfee® Endpoint Security contains improvements and fixes, including:

- Enhanced protection against script-based threats
- Additional forensics data on Exploit Prevention events by providing command-line details
- Improved efficacy on offline systems through Real Protect offline scanning support

We recommend that you verify this update in test and pilot groups before mass deployment.

# What's new

The current release of the product includes these enhancements and changes.

## Installation and upgrade enhancements

**Support for Endpoint Upgrade Assistant 2.1** — McAfee® Endpoint Upgrade Assistant adds the ability to upgrade legacy products to Endpoint Security 10.6, and to upgrade Endpoint Security 10.2 or later to version 10.5.3 or later. It also adds the ability to install or upgrade McAfee® Active Response.

## Microsoft product support

- Microsoft Windows 10, version 1803
- Microsoft Windows Server 2016, version 1803

## Common enhancements

For troubleshooting, you can temporarily exclude processes from all Arbitrary Access Control (AAC) rules by configuring a global exclusion policy with the new **Exclusions** setting in McAfee ePO. Use global exclusions only for specific troubleshooting and support purposes.

To avoid security risks, remove a global exclusion immediately after use. Failure to remove a global exclusion leaves your systems vulnerable to malware attacks.

## Threat Prevention enhancements

- Enhances protection against script-based threats by integrating with the Antimalware Scan Interface (AMSI) feature, provided by Microsoft and supported on Windows 10 and Windows Server 2016 systems.

  By default, AMSI integration is in Observe mode. AMSI scanning events report malicious scripts to the server, but no action is taken. Disable Observe mode to actively block these threats.
- Adds command-line parameter details for events triggered by Exploit Prevention rules to distinguish false positives from real attacks.
- Adds the ability to exclude IP addresses from Network IPS.
- Adds the ability to enter full file paths for high-risk and low-risk processes.
- Provides the ability to manage Access Protection settings on Linux systems.
- The **Scan email attachments** option is now called **Detect suspicious email attachments**.
- This release includes the following new Access Protection rules:

| McAfee-defined rule | Description | Default setting | Benefits |
|---|---|---|---|
| Doppelganging attacks on processes | Prevents "Process Doppelgänging" attacks from changing processes. | Report<br>Block | Prevents malware from loading and executing arbitrary code in the context of legitimate or trusted processes. |
| Executing Windows Subsystem for Linux | Prevents an Administrator user from running the Windows Subsystem for Linux (WSL).<br>  This rule was introduced in Endpoint Security 10.5.3, but was missing from the documentation. | Report<br>Block | Prevents malware designed for Linux systems from attacking Windows computers. |

## Firewall enhancements

- Adds the option to specify whether to block or allow traffic by default if the McAfee® Global Threat Intelligence™ (McAfee GTI) ratings server is not available.
- File queries to McAfee GTI are now SHA-256 instead of MD5. Endpoint Security continues to support MD5 for policy configuration and reporting.

## Web Control enhancements

- Adds the ability to run Internet Explorer in extension-off mode with the `-extoff` command-line option.

  Previously, a Self Protection rule blocked Internet Explorer users from using InPrivate browsing and the `-extoff` switch.
- Adds behavior that allows files to be downloaded from blocked sites if the reputation for the file indicates that it isn't malicious.
- Adds support for Firefox version 56 and later and multi-process architecture (E10S).
- File queries to McAfee GTI are now SHA-256 instead of MD5. Endpoint Security continues to support MD5 for policy configuration and reporting.

## Adaptive Threat Protection enhancements

- Adds the ability to control scanning network drives using the new **Scan processes started from network drives** Adaptive Threat Protection setting.

  Previously, Adaptive Threat Protection used the **On network drives** setting from Threat Prevention On-Access Scan.
- Adds a **Product Version (Endpoint Security Adaptive Threat Protection)** property to the Query Builder in McAfee ePO.
- Adds the ability to run client-based Real Protect scanning offline, without requiring connectivity to McAfee GTI or the McAfee® Threat Intelligence Exchange (TIE) server.
- Adds the ability to download Real Protect scanner updates, when available, through content updates. This allows you to keep your protection up to date regardless of what Endpoint Security version you're using.
- Provides the ability to manage Adaptive Threat Protection settings on Mac systems.
- The **Enable Observe mode** option is now disabled by default.
- File queries to McAfee GTI are now SHA-256 instead of MD5. Endpoint Security continues to support MD5 for policy configuration and reporting.
- The Real Protect scanner and Dynamic Application Containment now protect systems against trusted processes that load untrusted DLLs after processes are created.

## Documentation available at docs.mcafee.com

You can now access the latest documentation for McAfee Business Products online at docs.mcafee.com. This new portal collects all documentation for products released since mid-2016 and will be the ongoing library for Business Product Documentation.

- Search — Search across all guides for McAfee Business Products. Quickly narrow results with category filters (product, version, guide type).
- All device access — Access the site from any device (mobile, tablet, desktop, etc.).
- Always up to date — Know that you are always reading the most current version of a document.

- PDFs available — Save as much of a guide as you need in PDF format, whether a single page, a section of pages, or an entire guide.
- Share with colleagues — Easily share links to individual topic pages.

### McAfee product support

This release adds support for McAfee® Endpoint Security for Servers. Endpoint Security for Servers monitors and controls the load of hypervisors for Virtual Desktop Infrastructure (VDI) and virtual servers. It works with Threat Prevention to minimize the performance impact of resource-intensive tasks like on-demand scan.

## Resolved issues

The current release of the product resolves these issues. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

### Installation

| Reference | Resolution |
|---|---|
| 1203657 | Endpoint Security now deletes the plug-in keys of previous Endpoint Security versions during an upgrade so that previous versions don't appear in McAfee ePO properties. |
| 1230704 | The installation package version in the **Master Repository** now matches the version reported by the client, so product deployments show as complete. |

### Migration

| Reference | Resolution |
|---|---|
| 1209113 | Environments with large McAfee® Host Intrusion Prevention DNS Blocking policies now successfully migrate to Endpoint Security on McAfee ePO 5.9. |
| 1214578 | The Export Table functionality for previewing policy migration now correctly exports the table contents. |
| 1216105 | User-based policy migration now ignores errors from user account validation. |
| 1220975 | The Endpoint Security Migration server task now correctly calculates the percent complete. |
| 1222085 | McAfee® VirusScan® Enterprise Access Protection policies with these types of rules now successfully migrate to Endpoint Security:<br>• Include process list contains double quotes.<br>• Exclude process list does not contain double quotes. |

### Common

| Reference | Resolution |
|---|---|
| 1193471 | When a domain controller is installed on the McAfee ePO server, the rule compiler now works with a list of users based on the user profiles instead of the entire list of users. This prevents Endpoint Security from hanging during startup. |
| 1201828 | The mfeesp.exe process no longer crashes if the encrypted McAfee GTI password is missing from the GTIBL.xml file. |
| 1213541 | Microsoft Windows 10 no longer crashes when calculating the hash of files larger than 4 GB. |
| 1213665 | Starting Endpoint Security services no longer prevents the successful start of services from other vendors. |

| Reference | Resolution |
|---|---|
| 1218889 | This release resolves a system hang that might occur when Endpoint Security is installed with third-party filter drivers. |
| 1228855 | Endpoint Security module events are no longer truncated if the local host name is longer than 15 characters. |
| 1229081 | The "Failed to finalize reputation for file error" text that appears in the EndpointSecurityPlatform_Errors.log for error code 0xc030002f now says, "Reputation already finalized." |
| 1230235 | After upgrading, the Self Protection and Access Protection activity logs now show the correct information. Also, the language in activity logs now matches the client system language when **Activity logging language** is set to **Automatic**. |
| 1231623 | The code to automatically uninstall the Endpoint Security Platform after all modules have been uninstalled now verifies that there are no Endpoint Security modules remaining on the system before removing the Endpoint Security Platform. |
| 1234006 | The EndpointSecurityPlatform_Errors.log no longer incorrectly reports the failure to drop a non-existent database trigger as an error. Now, an error message is logged only if an actual database error occurs while dropping the trigger. Also, the log text now includes a detailed description of any database errors. |

## Threat Prevention

| Reference | Resolution |
|---|---|
| 1204964 | Internet browsers no longer hang due to invalid file paths for exclusions. This fix applies to exclusions in the Access Protection, Exploit Prevention, Dynamic Application Containment, and Self Protection interfaces. |
| 1205901 | The **Detect suspicious email attachments** setting, previously called **Scan email attachments**, now honors exclusions specified under **Exclusion by Detection Name**. |
| 1208784 | The Endpoint Security installation no longer resets the Quarantine directory to the default directory when AMCore is upgraded. |
| 1211627 | Saving an Access Protection policy now takes less time. |
| 1212209 | Endpoint Security now reports the second status of a **Clean** action as "successful" on both the Endpoint Security Client and McAfee ePO if the first status is "delete pending." |
| 1213197 | On-Access Scan policy settings now correctly apply empty high-risk and low-risk process lists. |
| 1214409 | Local computers no longer hang when On-Access Scan is enabled and an RDP session is established. |
| 1216350 | McAfee ePO now correctly synchronizes edited rules with a second McAfee ePO server. |
| 1216575 | Policy settings in McAfee ePO now allow you to enter full path process exclusions. |
| 1218165 | This release improves scan engine and file I/O handling to increase performance during local file copy operations. |
| 1218572 | Access Protection is now disabled on the client system if it's disabled in McAfee ePO policy settings. |
| 1219673 | Exploit Prevention rule 6015 no longer reports events when it's disabled, and the text strings of digital signatures are now normalized so that exclusions work correctly. |
| 1220432 | A bugcheck 133 no longer randomly occurs on systems with high network use. See KB89771 for more information. |
| 1221244 | You can now enter full file paths for high-risk and low-risk processes. |
| 1221247 | A crash no longer occurs when On-Demand Scan client tasks are changed while a running on-demand scan is ending. |
| 1224709 | A bugcheck 135 associated with the mfencbdc.sys driver no longer occurs. |

| Reference | Resolution |
|---|---|
| 1226318 | Network traffic no longer causes a blue screen when Endpoint Security is installed on a system that is also running Panda Security software. |
| 1230279 | Pool allocations made by mfehidk.sys, the registered anti-malware driver used by Endpoint Security, were leaking memory during each process creation done under the Windows Subsystem for Linux. This release resolves this issue. |
| 1231037 | The on-demand scanner no longer becomes unresponsive, leading to incomplete scans. Threat Prevention now successfully reports properties, such as the AMCore content version, back to McAfee Agent. |
| 1231176 | The **Safety Pulse** setting is no longer dependent on the **McAfee GTI feedback** setting. |

## Firewall

| Reference | Resolution |
|---|---|
| 1181041 | Connection isolation in Location Aware Groups now successfully works with local networks. |
| 1188093 | Websites now take less time to load. |
| 1197596 | Location Aware Groups with local networks now work correctly. |
| 1203899 | Pointmgr.exe, a third-party application, now works correctly when Firewall is enabled. |
| 1207770 | Network connectivity now successfully continues when switching from Wi-Fi to a docked LAN network. |
| 1208966 | VPN connections no longer intermittently disconnect when Location Aware Groups are used with the DNS server. |
| 1212178 | Adaptive mode rules now include all signer details and file description information. |
| 1215721 | Only one instance of a location now appears in the **Firewall Catalog**, regardless of how many groups contain the location. |
| 1216361 | Firewall now allows exclusion-specific IP addresses from McAfee GTI lookups, but still includes the IP addresses to process against Firewall rules. |
| 1217352 | The **Allow bridged traffic** setting now works correctly. |
| 1217942 | Location Aware Groups now work correctly when the system is connected to both wired and wireless networks. |
| 1219285 | Firewall events are now correctly parsed by McAfee ePO. |
| 1221732 | Log entries and events for blocked traffic are now successfully generated when Network Intrusion Prevention is enabled. |
| 1221865 | Inbound McAfee GTI high-risk connections now correctly override McAfee GTI rating blocks when the remote IP address is a trusted network. |
| 1221887 | Access to certain firewall rule data structures is now serialized, preventing potential crashes in mfefw.exe. |
| 1226709 | The Defined Networks list is now sorted by IP address. |
| 1226742 | When Firewall tests whether the McAfee ePO server is reachable, the test now looks at all Agent Handlers in the list, instead of only the first one. Previously, if the first Agent Handler was offline, the reachability test failed. |
| 1229607 | The McAfee ePO reachability test now succeeds in cases where the number of Agent Handlers previously exceeded a limited buffer size. |

### Adaptive Threat Protection

| Reference | Resolution |
|---|---|
| 1195161 | Adaptive Threat Protection now correctly checks the TIE server for reputation information. |
| 1197643 | File reputation changes are now applied locally and reputation attributes are now correctly refreshed after a reputation change. |
| 1204453 | The **View installed updates** section in **Programs and Features** now shows the Adaptive Threat Protection hotfix name as **McAfee Endpoint Security Adaptive Threat Protection** instead of **Display Name**. |
| 1214522 | The Real Protect proxy no longer tries to connect to google.com to validate Internet connectivity. |
| 1224492 | The mfeesp.exe service no longer crashes due to incorrect Adaptive Threat Protection event dates, and Adaptive Threat Protection now uses the correct date for events. |
| 1224673 | The **Product Version (Endpoint Security Adaptive Threat Protection)** column is now displayed in the McAfee ePO Query Builder. |
| 1228240 | When Adaptive Threat Protection is in Observe mode, Dynamic Application Containment events no longer generate if processes/paths are excluded by a Dynamic Application Containment exclusion. |
| 1229328 | The Windows Subsystem for Linux is now trusted by Adaptive Threat Protection so commands from the subsystem are trusted and not sent for further reputation check. |
| 1230262 | Mfeatp.exe CPU usage no longer spikes when an Extra.DAT file is present. |
| 1233360 | A memory leak in mfeatp.exe no longer occurs. |

### Web Control

| Reference | Resolution |
|---|---|
| 1216383 | Web Control now works correctly with Firefox version 56 and later. |

# Installation information

Use this information while installing Endpoint Security.

**Best practice:** Restart the client system after installing this release of the product.

## Requirements

This release installs Endpoint Security on Windows systems that are managed by McAfee ePO.

For a complete list of current system requirements, see KB82761.

### Upgrade support

The Endpoint Security modules support upgrading from the previously released minor version only. For optimal performance and protection, we recommend that you upgrade all Endpoint Security modules to the same version.

### Important information about Exploit Prevention

The Endpoint Security 10.6 installation package includes the McAfee Exploit Prevention Content 10.6.0.8330. This content version adds support for the new digital signatures used by Endpoint Security 10.6. The installation updates the content on systems running Endpoint Security with previous versions of the content.

### Management software

- McAfee ePO 5.3.1 and later
- McAfee Agent 5.0 Patch 2 (5.0.2.333) (minimum)

  McAfee Agent 5.5.0 or later (recommended)

  For systems running an earlier version of McAfee Agent:

  - On systems managed by McAfee ePO, upgrade McAfee Agent manually before deployment.

### Supported legacy products (required for migration only)

Migration supports all patch levels for these legacy products.

- McAfee® VirusScan® Enterprise 8.8
- McAfee® Host Intrusion Prevention 8.0
- McAfee® SiteAdvisor® Enterprise 3.5
- McAfee® Endpoint Protection for Mac 2.3 or McAfee® VirusScan for Mac 9.8

### Products and platforms no longer supported

- McAfee Agent 5.0.2.132 and earlier
- Windows Server 2008
- Windows Vista Service Pack 2 (SP2)

## Installation and upgrade tools

McAfee ePO provides tools to assist with installing and upgrading Endpoint Security. You can download and install these tools from the Software Manager.

- **Endpoint Security Package Designer** — Creates a single, custom Endpoint Security installation package that includes post-release hotfix packages. The custom installation package is larger than the standard installation package, but ensures that hotfix releases are applied during installation, instead of waiting for an update task to retrieve the hotfix files from the McAfee ePO repository. You can also include preconfigured, custom policies in the custom package.
- **Endpoint Migration Assistant** — Migrates custom policy settings when you upgrade legacy products to Endpoint Security. You can migrate all your settings automatically, or select settings to migrate manually and configure them before migration if needed.
- **Endpoint Upgrade Assistant** — Simplifies and automates the tasks required to upgrade environments to Endpoint Security. Endpoint Upgrade Assistant supports upgrades from legacy products or from earlier versions of Endpoint Security. This tool analyzes managed systems, detects the supported McAfee products that are installed, and determines the minimum requirements for upgrading.

  You can use Endpoint Upgrade Assistant to determine which systems are ready for automatic upgrades, then upgrade them with a single deployment task. You can also plan, deploy, and track manual upgrades throughout your environment.
- **Endpoint Package Creator** — With Endpoint Upgrade Assistant, creates an installation package for use with third-party deployment solutions.

# Known issues

For a list of known issues in this product release, see KB82450.

# Getting product information by email

The Support Notification Service (SNS) delivers valuable product news, alerts, and best practices to help you increase the functionality and protection capabilities of your McAfee products.

To receive SNS email notices, go to the SNS Subscription Center at https://sns.secure.mcafee.com/signup_login to register and select your product information options.

# Where to find product documentation

Go to docs.mcafee.com to find the product documentation for this product.

Go to support.mcafee.com to find supporting content on released products, including technical articles.

## Additional Endpoint Security information

For more information about working with Endpoint Security, go to the Endpoint Security Expert Center.

To view the latest recommendations for installing and managing Endpoint Security, see Recommendations for Endpoint Security.

To view frequently asked questions about Endpoint Security, including installation information, configuration best practices, troubleshooting tips, and more, see KB86704.