McAfee Endpoint Security 10.6.1 - Release Notes - Windows

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® Endpoint Security 10.6.x
- McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.3.1 and later
- McAfee® ePolicy Orchestrator® Cloud (McAfee® ePO™ Cloud)
- McAfee® MVISION ePO

Purpose

This release adds enhancements and fixes problems that were reported in the previous version.

Rating — Critical

Mandatory	**Critical**	High Priority	Recommended

- Critical for all environments.
- Failure to apply a Critical update might result in severe business impact.
- A hotfix for a Severity 1 or Severity 2 issue is considered Critical.

For more information, see KB51560.

What's new

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

Endpoint Security 10.6.1 December release

This release addresses customer-reported issues, memory consumption issues, and product, scanner, and installer stability issues.

For a complete list of current platform, environment, or operating system support, and the build numbers for this release, see KB82761.

The release includes two package types to support these installation paths:

To...	Use this package type
Install Endpoint Security 10.6.1 for the first time.	Endpoint Security 10.6.1 Full Installer
Upgrade from any previous Endpoint Security version.	Endpoint Security 10.6.1 Full Installer
Upgrade from Endpoint Security version 10.6.0.	Endpoint Security 10.6.1 Patch

Installation and upgrade

- **Support for case sensitivity** — On systems running the Microsoft Windows 10 October 2018 Update, verify that the case-sensitivity attribute is disabled for folders where you want to install the product software.

  You can check and change this attribute setting in Windows. Once installed, Endpoint Security protects its product folders against enabling case sensitivity, to ensure that this attribute setting won't prevent future product updates and upgrades.

- **McAfee® MVISION Endpoint uninstall** — The Endpoint Security installer uninstalls McAfee MVISION Endpoint if it's present on the client system before continuing with the installation.
- **Support for Microsoft Windows anti-malware service protection** — Endpoint Security services now start as a Windows-protected service.

Microsoft product support

- Microsoft Windows 10 October 2018 Update
- Microsoft Windows Server 2019

McAfee® Endpoint Security Common

Client interface lockout behavior — Adds the ability to enforce an Endpoint Security Client lockout if the number of failed password attempts exceeds the configured limit. Use the **Enable client interface lockout** setting in the Common **Options** policy in McAfee® ePolicy Orchestrator® (McAfee® ePO™) to configure lockout behavior.

Documentation for this feature will be included in the *McAfee Endpoint Security 10.7.x Common Product Guide* and *McAfee Endpoint Security 10.7.x Common Interface Reference Guide*.

McAfee® Endpoint Security Web Control

Microsoft Edge support — Adds Microsoft Edge as a supported browser.

Resolved issues

This release resolves known issues.

For a list of current known issues, see McAfee Endpoint Security 10.x Known Issues (KB82450).

The resolved issues cover all management platforms.

Table 3-1 Installation and migration

Reference	Resolution
1238934	A blue screen (bugcheck 1a) no longer occurs when installing Endpoint Security.
1241660, 1242888	A blue screen (bugcheck D1) associated with mfeaack.sys no longer occurs.
1241800, 1244858, 1246343, 1247126	A blue screen (bugchecks 133, 1e, and 7f) no longer occurs when upgrading from McAfee® VirusScan® Enterprise to Endpoint Security.
1249888	The SetupEP utility now allows you to enter more than one module name, separated by a comma, when importing policies.
1251931	Mfeesp.exe now starts correctly following an Endpoint Security upgrade.
1252011	A blue screen (bugcheck 3B) associated with mfencbdc.sys no longer occurs when upgrading Endpoint Security.
1258613	The Endpoint Migration Assistant now retains existing assigned Endpoint Security tasks.

Table 3-2 Common

Reference	Resolution
1222359	This release resolves a memory leak with mfencbdc.sys.
1236546	The **McAfee Security Status** dialog box no longer randomly shows Endpoint Security modules as disabled.
1239625	A deadlock that prevented proxy connectivity with McAfee® Client Proxy is now resolved.
1246420	You can no longer use icacls to disable Endpoint Security modules.

Table 3-3 Threat Prevention

Reference	Resolution
1207741	Uploading a file using Rockwell FactoryTalk now takes less time.
1212782	McAfee Profiler now correctly shows processes scanned under high risk and low risk based on the configured Endpoint Security policy.
1224493	When you upgrade to McAfee ePO 5.9, the Exploit Prevention Events query now works correctly.
1228048	A bugcheck 3B associated with the mfehidik.sys driver no longer occurs.

Table 3-3 Threat Prevention *(continued)*

Reference	Resolution
1228513	Exploit Prevention no longer causes Microsoft Office applications and Internet Explorer to crash.
1229082	Third-party software connections now succeed without a delay.
1230269	The Endpoint Security Client now shows the correct number of files scanned during an on-demand scan.
1230484	The Access Protection activity log now correctly shows the name of the file blocked by the **Running files from common user folders** Access Protection rule.
1233810	When On-Access Scan is enabled, Rockwell Software Logix Designer 30 now takes less time to compile.
1234259	When you disable and re-enable a signature filter in the **Exploit Prevention** policy, the signatures now reappear.
1236052	McAfee-defined rules are now correctly labeled as McAfee-defined rules instead of user-defined rules.
1238673	The Endpoint Security Client no longer crashes when using the **Scan System** option.
1238723	The issue that prevented DAT updates from completing successfully is now resolved.
1240657	A third-party software installation is now successful when McAfee® Endpoint Security Threat Prevention is installed.
1243233	When content files are missing from their installation location, the Exploit Prevention update now succeeds.
1244821	The **Program Compatibility Assistant** dialog box no longer shows a NIPS FireCore Plugin Driver error when installing Threat Prevention.
1245285	The Threat Target file name now appears in the event sent to McAfee ePO and in the Access Protection log.
1246046	On-demand scans now use less CPU.
1247353	The **Doppelganging attacks on processes** Access Protection rule now appears in McAfee ePO. Upgrade the extension only to resolve this issue for previous Endpoint Security client versions.
1248764	Threat Prevention now correctly enforces Access Protection rules.
1249089	Exploit Prevention exclusions now work correctly with signer details as the **Signer** value is now processed as is from the events.
1250085	Mfevtps.exe now uses less CPU.
1250306	This release resolves a memory leak with mfefirek.sys due to packet fragmentation.
1250643	The permission set to view Access Protection subrules now functions correctly.
1254936	Endpoint Security properties, such as Extra.DAT and On-Demand Scan properties, are now displayed correctly in McAfee ePO.
1256356	When the On-Demand Scan option **Scan only when the system is idle** is enabled, the scan no longer randomly resumes when the user is active.
1256656	Special characters are now allowed in the **Signer** field of Exploit Prevention rules.
1256932	Application Protection rules now successfully migrate to Threat Prevention settings using ESConfigTool.
1259768	This release resolves a non-paged pool memory leak when using Cygwin.

Table 3-4 Firewall

Reference	Resolution
1209817	Adaptive mode rules now correctly aggregate and filter on the **Firewall Client Rules** page in McAfee ePO.
1210839	McAfee® Endpoint Security Firewall rules that use IP address ranges no longer block traffic.

Table 3-4 Firewall *(continued)*

Reference	Resolution
1214247	The Firewall policy now takes less time to open regardless of the rules added.
1223229	Firewall rules being saved no longer fail due to java.sql.SQLException: Violation of UNIQUE KEY constraint 'IX_EPOPolicySettings_TenantTypeIDName' errors.
1228817	McAfee ePO now updates policies containing remote networks from the **Firewall Catalog** when the network is changed in the catalog.
1232777	Certain firewall rules no longer block traffic when set to **Disabled**.
1238337	Mfefw.exe now successfully enforces policies that have an improperly formatted signature without consuming excessive amounts of CPU.
1239127	Endpoint Security Firewall now recognizes VirtualBox MAC addresses associated with a hypervisor.
1241115	Changes made to firewall rules now persist when entering subdialogs or making changes to a rule prior to saving it and going back to the Firewall policy view in McAfee ePO.
1245977	Log entries for allowed and blocked traffic are now successfully generated when Network Intrusion Prevention is enabled.
1249305	Firewall Rule queries with a Rule Action filter now return the correct results.
1256757	You can now successfully add IPv6 addresses under trusted networks in a rule.

Table 3-5 Adaptive Threat Protection

Reference	Resolution
1225548	McAfee® Endpoint Security Adaptive Threat Protection (ATP) no longer blocks a file set as **Known Trusted** by Enterprise reputation exception.
1229868	This release resolves a memory leak with mfeatp.exe.
1242894	Sample files are no longer repeatedly submitted to McAfee® Advanced Threat Defense.

Table 3-6 Web Control

Reference	Resolution
1225364	Web Control is now correctly enabled on the system after leaving the corporate network when using the **Disable if a web gateway appliance is detected** setting.
1239725	Mfewc.exe now uses less memory.

Resolved issues in the 10.6.1 November update

This release resolves known issues.

For a list of current known issues, see McAfee Endpoint Security 10.x Known Issues (KB82450).

Table 3-7 Common

Reference	Resolution
1254800	The McAfee system tray icon no longer incorrectly reports that Endpoint Security modules are not responding.
1258035	A mfeesp.exe second-chance exception no longer occurs.

Table 3-8 Threat Prevention

Reference	Resolution
1228513	Microsoft Office applications no longer crash when migrating from McAfee VirusScan Enterprise to Endpoint Security.
1237955	The **Signer** field in Access Protection now supports more characters.

Table 3-8 Threat Prevention *(continued)*

Reference	Resolution
1239608	Mfetp.exe CPU usage no longer spikes when enforcing policies.
1240144	The right-click **Scan for threats** option now correctly appears in the same language as the operating system.
1245285	The Threat Target file name now correctly appears in the event sent to McAfee ePO and the Access Protection log.
1246900	McAfee ePO and the Endpoint Security Client now validate paths for on-access scan exclusions.
1247845	The Anti-Malware Engine's memory is now protected to prevent corruption from third-party products that could lead to false positives and incorrect conviction of clean files.
1250713	The malware detection pop-up message is now consistent for on-access scans.
1251396	Exploit Prevention no longer causes Microsoft Windows script engines to hang.
1256801	When the path for an on-access scan exclusion is missing a slash (/) character, the high risk and low risk exclusion list on the client system is no longer blank, and policy enforcement of valid exclusions now functions correctly.

Table 3-9 Adaptive Threat Protection

Reference	Resolution
1238355	The file type **Unknown** is now spelled correctly in ATP events.
1249372	ATP now honors on-access scan exclusions regardless of DLL injection into the excluded process, so the process is no longer monitored by Dynamic Application Containment or Real Protect.
1251575	A memory leakage of mfeatp.exe no longer occurs.
1257207	The **Signer** field in Dynamic Application Containment now supports more characters.

Resolved issues in the 10.6.1 December update

This release resolves known issues.

For a list of current known issues, see McAfee Endpoint Security 10.x Known Issues (KB82450).

Table 3-10 Migration

Reference	Resolution
1258613	The Endpoint Migration Assistant now retains existing assigned Endpoint Security tasks.

Table 3-11 Threat Prevention

Reference	Resolution
1238723	The issue that prevented DAT updates from completing successfully is now resolved.
1245285	The Threat Target file name now appears in the event sent to McAfee ePO and in the Access Protection log.
1249089	Exploit Prevention exclusions now work correctly with signer details as the **Signer** value is now processed as is from the events.
1250643	The permission set to view Access Protection subrules now functions correctly.
1254936	Endpoint Security properties, such as Extra.DAT and On-Demand Scan properties, are now displayed correctly in McAfee ePO.
1256356	When the On-Demand Scan option **Scan only when the system is idle** is enabled, the scan no longer randomly resumes when the user is active.
1256656	Special characters are now allowed in the **Signer** field of Exploit Prevention rules.

Table 3-11 Threat Prevention *(continued)*

Reference	Resolution
1256932	Application Protection rules now successfully migrate to Threat Prevention settings using ESConfigTool.
1259768	This release resolves a non-paged pool memory leak when using Cygwin.

Table 3-12 Firewall

Reference	Resolution
1228817	McAfee ePO now updates policies containing remote networks from the **Firewall Catalog** when the network is changed in the catalog.
1256757	You can now successfully add IPv6 addresses under trusted networks in a rule.

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 for all management types.

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

A utility, mfeepmpk_utility.exe, is included in this installation package to resolve an issue with a faulty Exploit Prevention driver. The utility automatically detects if the endpoint system has the faulty driver and might prompt you to perform a one-time restart during your installation or upgrade to resolve the issue. For more information, see KB90301.

Upgrade support

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

Endpoint Security content files

You must manually update your McAfee ePO server with the latest AMCore, ATP, and Exploit Prevention content files required for Endpoint Security.

AMCore content packages include ATP content. McAfee releases new ATP content files every month. For information about the latest ATP content, see the McAfee TIE and ATP Security Content Release Notes.

For information about the latest Exploit Prevention content, see the McAfee Exploit Prevention Security Content Release Notes.

Management software

- McAfee ePO 5.3.1 and later
- McAfee ePO Cloud

  For the latest Endpoint Security management entitlement and license information, see KB87057.
- McAfee MVISION ePO

- McAfee Agent 5.0.5, minimum for Microsoft Windows 10 October 2018 Update
- McAfee Agent 5.0.2, minimum for all other Microsoft Windows versions
- McAfee Agent 5.5.1 (build 342) and later (recommended)

  For systems running an earlier version of McAfee Agent:

  - On systems managed by McAfee ePO, upgrade McAfee Agent manually before deployment.
  - On systems managed by McAfee ePO Cloud, no action is required. The new agent is installed automatically on managed systems from the McAfee ePO Cloud installation URL sent to users.
  - On unmanaged systems, no action is required to upgrade version 4.0 and later. For earlier versions, upgrade McAfee Agent manually.

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.

0-00