Release Notes

McAfee Endpoint Security 10.6.1

July Update

For use with ePolicy Orchestrator

Contents

Rating

The rating defines the urgency for installing this update.

Rating – Mandatory

Mandatory	Critical	High Priority	Recommended

- Required for all environments.
- Failure to apply Mandatory updates might result in a security breach.
- Mandatory patches and hotfixes resolve vulnerabilities that might affect product functionality and compromise security.
- You must apply these updates to maintain a viable and supported product.

For more information, see KB51560.

What's new in the July 10.6.1 release

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

New features

Support for case sensitivity — On systems running Microsoft Windows 10 version 1903, the software can be installed on a folder with Case Sensitivity enabled.

The release includes a full installer package and can be used to install McAfee® Endpoint Security 10.6.1 for the first time or upgrade from any previous Endpoint Security version.

This release includes the following build numbers:

Component	Version
Endpoint Security Platform	10.6.1.1555.3
Endpoint Security Platform extension	10.6.1.1201.1
Endpoint Security Threat Prevention	10.6.1.1638.1
Endpoint Security Threat Prevention extension	10.6.1.1222.1
Endpoint Security Firewall	10.6.1.1324.2
Endpoint Security Firewall extension	10.6.1.1181.1
Endpoint Security Web Control	10.6.1.1401.3
Endpoint Security Web Control extension	10.6.1.1177.1
Endpoint Security Adaptive Threat Protection	10.6.1.1398.1
Endpoint Security Adaptive Threat Protection extension	10.6.1.1183.1
Endpoint Security Migration Assistant extension	10.6.1.1030.1

This release extends support to additional platforms, environments, or operating systems.

- Microsoft Windows 10 version 1903 (May 2019 Update)

Resolved issues in the July 10.6.1 release

This release resolves known issues from the previous releases of the product.

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

Installation

Component	Reference	Resolution
Installation	1262173	When upgrading to Endpoint Security 10.6.1, failure to access the Logcfg folder causes an installation failure. This release resolves the issue.
User Interface	1265911	Endpoint Security now displays the correct version information in Add or Remove Programs.
Installation	1267001	Systems no longer prompt for a restart while upgrading to Endpoint Security 10.6.1.
Installation	1268188	The upgrade from Endpoint Security 10.5.3 to 10.6.1 is now successful.

Threat Prevention

Component	Reference	Resolution
Feature Fix	1239384	On-demand scan scheduled tasks now function properly even when a system resumes after a restart.
User Interface	1256743	The correct number of files scanned during a right-click on-demand scan are now displayed in the Endpoint Security Client.
Feature Fix	1260820	The Threat Target file name now appears correctly in the event sent to McAfee® ePolicy Orchestrator® (McAfee® ePO™) and the Access Protection log.
Installation	1260865	Systems no longer prompt for a restart while upgrading to Endpoint Security 10.5.5.
Performance	1263328	Exploit Prevention injection no longer interferes with large memory allocations in 32-bit applications.
Installation	1264682	Installations of McAfee® VirusScan® Enterprise from a shared location that is protected by McAfee Endpoint Security are now successful.
Installation	1265275 1267001	This release resolves issues that would cause Endpoint Security to continually prompt for a system restart to complete the upgrade.
Installation	1265488	McAfee® Endpoint Security Threat Prevention and McAfee® Endpoint Security Adaptive Threat Protection (ATP) fail to upgrade to 10.6.1 Dec update from 10.5.4. This release resolved the issue.
Feature Fix	1266694	The **Source description** field with 256-characters limitation is now increased to 500 characters.
Feature Fix	1266885	This release resolves a bug check 50, PAGE_FAULT_IN_NONPAGED_AREA issue, involving the mfeepmpk.sys driver when a shell script is run in Windows Subsystem for Linux.
User Interface	1268965	McAfee Endpoint Security Threat Events now correctly display the

		Detecting product version.
Performance	1269553	This release resolves the memory leak issues reported in the mfetp process.
Performance	1275238 1274791	This release resolves a blue screen issue (bug check 0x19) that occurred randomly after accessing a network resource when **Exploit Prevention** is enabled.

Firewall

Component	Reference	Resolution
Interoperability	1260136	Citrix NetScaler EPA scans now succeed, and German operating systems can now connect to VPN.
User Interface	1271914	Scroll bars now appear on Firewall Client Rules if aggregation is enabled.

Adaptive Threat Protection

Component	Reference	Resolution
Feature Fix	1272579	This release resolves the issue where Dynamic Application Containment events failed to parse to the McAfee ePO database, when events contained an invalid UTC time stamp.
Feature Fix	1244154	Corruption of an existing ATP.XML leads to loss of McAfee® Endpoint Security Adaptive Threat Protection (ATP) functionality. This release introduces a mechanism to re-create the XML during the standard McAfee Agent policy enforcement, when the existing XML is corrupted.
Feature Fix	1270240	The McAfee® Advanced Threat Defense sample submissions to McAfee® Threat Intelligence Exchange (TIE) occurred two times. This release resolves the issue.
Performance	1271523	This release resolves the memory leak issues reported in the mfeatp process.

Copyright © 2019 McAfee, LLC
McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC, or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.