Release Notes

McAfee Endpoint Security 10.7.0

September 2020 Update

For use with ePolicy Orchestrator

Contents

Rating

The rating defines the urgency for installing this update.

Rating – Critical

Mandatory	**Critical**	High Priority	Recommended

Critical

- 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 in the 10.7.0 September Update release

This update includes fixes and resolutions for several issues, as well as cumulative fixes from the previous monthly updates.

New Platform Support

This release is a candidate for same-day support of the upcoming Microsoft 20H2 release for workstations and servers. The provided packages can be used to install McAfee® Endpoint Security 10.7.0 for the first time or to upgrade from any previous Endpoint Security version in preparation for OS upgrade.

Configuration Option Enhancements

The following policy settings are now available as configuration options:

Ability to set Threat Prevention On-Access Scanner to Observe mode

In the *Threat Prevention On-Access Scan* policy, users can now select "*Allow access to file*" from the drop-down menu for the Threat Prevention On-Access first response action. This will place the scanner into Observe mode, which can be useful when performing investigative test scenarios, such as those conducted during MITRE or Purple Team testing.

Note: By selecting this option, On-Access Scanner will alert and send detection events for the purpose of observation, but will **not** take remediation actions against detected threats. It is recommended that this setting be used only in controlled testing scenarios and is not advised for extended use.

Option to override Unverified URL categorization in Web Control

In the *Web Control Options* policy users now have a checkbox option *Allow Green-rated file downloads from not yet verified URL* to allow browsers to download a file with green rating from a URL with unverified categorization. For this option to appear, the Action enforcement setting for *Apply this action to sites not yet verified by McAfee GTI* must be set to *Block*. This option is currently only available for enforcement to the Google Chrome browser.

Option to disable Adaptive Threat Protection Story Graph feature

In the *Adaptive Threat Protection Options* policy, there is now a checkbox option to enable or disable the Story Graph feature. Story Graph is enabled by default.

Additional Access Protection rule

Users now have the option to prevent modification of the Endpoint Security logs folder via a new Access Protection rule *Protect Endpoint Security logs folder*. This rule is disabled by default. For more information regarding the considerations necessary if using the rule, and best practices for if a custom log folder is configured, refer to the *Configuring Threat Prevention* chapter of the *McAfee Endpoint Security Product Guide.*

Configuration of Credential Theft Protection

As was also provided in the July Update, this release provides proactive policy configuration options for a functionality that will be provided in a coming Real Protect content release. Credential Theft Protection provides additional protection against LSASS attacks. The default configuration of Credential Theft Protection is enabled with Observe mode disabled.

McAfee will send out advanced SNS Notification regarding the release date of the Real Protect content version that will enable this capability on systems with Adaptive Threat Protection 10.7.0.2059 (July Update 2020) and later. For information regarding how to subscribe to SNS Notifications, please see KB67828.

Additional Information

Note: If Endpoint Security 10.7.0 September Update is installed on unpatched Microsoft Windows 7 or Server 2008 R2 for Microsoft KB4474419 then a notification prompt appears notifying that the installation is not SHA1 signed.

This will occur regardless of installation method used. This is because Microsoft has fully deprecated SHA1 signing in their switch from dual signing with SHA1/SHA2 to SHA2 only.

This does not affect Endpoint Security 10.7.0 September Update's ability to successfully install.

The pop-up will not be experienced on Windows 7 SP1 or Server 2008 R2 SP1 and above. In order to avoid this scenario, McAfee recommends that you apply the necessary Windows patches.

This release includes the following build numbers:

Component	Version
Endpoint Security Platform	10.7.0.2000
Endpoint Security Platform extension	10.7.0.697
Endpoint Security Threat Prevention	10.7.0.2067
Endpoint Security Threat Prevention extension	10.7.0.755
Endpoint Security Firewall	10.7.0.1433
Endpoint Security Firewall extension	10.7.0.684
Endpoint Security Web Control	10.7.0.1740
Endpoint Security Web Control extension	10.7.0.750
Endpoint Security Adaptive Threat Protection	10.7.0.2329
Endpoint Security Adaptive Threat Protection extension	10.7.0.705
Endpoint Security Threat Detection Reporting extension	1.0.0.522

For more details about the product versions listed in Control Panel, see KB92355.

Resolved issues in the 10.7.0 September Update release

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

Platform

Component	Reference	Resolution
Interoperability	ENSW-102203	Resolves an issue where McAfee® Endpoint Security Web Control hooking into Microsoft Project caused it to hang on startup with previous versions of McAfee Endpoint Security 10.7.
Feature Fix	ENSW-102065	Resolves an issue where on opening Windows Explorer the MSI self-repair mechanism starts due to missing Endpoint Security swidtag file.

Threat Prevention

Component	Reference	Resolution
Performance	ENSW-105718	Resolves an issue where compile-time takes more time on Jenkins server with McAfee Endpoint Security installed.
Feature Fix	ENSW-103106	Umlaut characters are now allowed to be used under the 'Username' section of Custom Access Protection rules.
Feature Fix	ENSW-101683	Resolves an issue where AMCore compliance query displays systems with AMCore Content Date older than 7 days as compliant.
Feature fix	ENSW-101681	Resolves an issue where On Access scan policies that contains custom exclusions (\\.\ and \\?\) fails to apply on the system.
Feature Fix	ENSW-101680	Resolves an issue where Endpoint Security records disconnected usernames on threat events on Windows server machines.
Interoperability	ENSW-101381	Resolves an issue where Microsoft Outlook crashes randomly when McAfee Endpoint Security is present on the system with Exploit prevention enabled.
Feature Fix	ENSW-97673	Resolves an issue where Scriptscan settings (enable/disable) does not reflect correctly after the system reboot.

Adaptive Threat Protection

Component	Reference	Resolution
Feature Fix	ENSW-103322	Resolves an issue where trusted applications are being contained because the JCM cache does not persists after the McAfee® Endpoint Security Adaptive Threat Protection (ATP) shutdown.
Feature Fix	ENSW-104809	Resolves an issue where trusted applications are being contained because the JCM cache does not persist after content update.

Firewall

Component	Reference	Resolution
Feature Fix	ENSW-99854/	Resolves an issue where McAfee® Endpoint Security Firewall blocks legitimate

	ENSW-96720	incoming traffic.
User Interface	ENSW-101862	Resolves an issue in the "`Endpoint Security Firewall=> Rules Policy =>Add Rule UI`" where Macintosh was not listed under the '`Applications`' section when the Macintosh extension was installed.

Web Control

Component	Reference	Resolution
Feature Fix	ENSW-99827	Resolves an issue where search annotations were not displaying for "yahoo.co.jp" search results.
Feature Fix	ENSW-99682	Resolves an issue where Endpoint Security Web Control blocks downloaded files from internal sites even when the IP subnet range is excluded.

claimed as the property of others.