Release Notes

McAfee Endpoint Security 10.7.0

November 2020 Update

For use with ePolicy Orchestrator

Contents

Rating

The rating defines the urgency for installing this update.

Rating – Mandatory

Mandatory	Critical	High Priority	Recommended

Mandatory

- Required for all environments.
- Failure to apply Mandatory updates might result in a security breach.
- Mandatory updates 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 10.7.0 November Update release

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

Application Support

The following applications are now supported for use with McAfee® Endpoint Security:

Microsoft Chromium Edge browser via McAfee® Endpoint Security Web Control

Windows servers and desktops hosting a container can now install Endpoint Security for host protection

Installation and use of Endpoint Security on the host of a container (e.g. Docker) has been validated with Windows Server 2016 1607 and Windows 10 1809 platforms, due to version prevalence. Support validation for containers on further OS platforms will be provided via a future product release. If you are using containers, then it is highly recommended to reboot after Endpoint Security has been upgraded to 10.7.0 November Update. Installation of Endpoint Security inside of a container is not supported.

Feature Enhancements

Now available:

New syntax enables Expert Rules to trigger an On-demand Scan of a target process

Requires two arguments; both the process to be scanned (ACTOR_PROCESS and/or TARGET_PROCESS) and the ScanAction. For more information and examples of use of these arguments, see the Endpoint Security 10.7 Product Guide.

Additional Information

Note: If Endpoint Security 10.7.0 November 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 November 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	10.7.0.2174
Endpoint Security Platform extension	10.7.0.760
Endpoint Security Threat Prevention	10.7.0.2298
Endpoint Security Threat Prevention extension	10.7.0.840
Endpoint Security Firewall	10.7.0.1540

Endpoint Security Firewall extension	10.7.0.751
Endpoint Security Web Control	10.7.0.1891
Endpoint Security Web Control extension	10.7.0.808
Endpoint Security Adaptive Threat Protection	10.7.0.2481
Endpoint Security Adaptive Threat Protection extension	10.7.0.769
Endpoint Security Migration extension	10.7.0.355
Endpoint Security Threat Detection Reporting extension	1.0.0.522

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

For information regarding the latest Security Bulletin updates, please see Security Bulletin.

Resolved issues in the 10.7.0 November Update release

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

Platform

Component	Reference	Resolution
User Interface	ENSW-106441	Resolves an issue where the events that are generated in Endpoint Security console are in OS language instead of the language selected for "Client Interface Language".
Installation	ENSW-97547	Resolves an issue where the virtual machines freeze when Endpoint Security is installed on a Hyper-V host.
Feature Fix	ENSW-28019	Resolves an issue where Endpoint Security installation failure on an incompatible version of Windows 10 OS when installed via McAfee® ePolicy Orchestrator® (McAfee® ePO™), is not reported properly.

Threat Prevention

Component	Reference	Resolution
Feature Fix	ENSW-106839	Resolves an issue where applications that require VBScript fails to load and Windows script host errors are reported after uninstallation of McAfee® VirusScan® Enterprise or migration to Endpoint Security.
Feature Fix	ENSW-106575	Resolves an issue where On-Access scan policy is not getting enforced on the client when the number of exclusions is very high.
Feature Fix	ENSW-106172	Resolves an issue where Access Protection exclusions do not accept valid digital signature due to 'å' letter and throw "Invalid signer" error if applied through the Endpoint Security console.
Feature Fix	ENSW-105903/ ENSW-104122	Resolves an issue where On-Access scan is scanning Windows updates even when the "`Scan trusted installers`" option is disabled in policy.
Feature Fix	ENSW-105787/ ENSW-102773	Resolves an issue where when On-Access scan is enabled, applications executed from mapped network drive gives a delayed response.
Interoperability	ENSW-104617	Resolves an issue where On-Access scan causes delay in opening of Microsoft office applications.
Feature Fix	ENSW-104401	Resolves an issue where Windows defender displays incorrect operating system version while installation of Endpoint Security.
User Interface	ENSW-103217	Resolves an issue where when policy migration from McAfee VirusScan Enterprise 8.8 to Endpoint Security in McAfee ePO 5.10 is performed, specific user-defined Access Protection rules in Japanese appears garbled.
Feature Fix	ENSW-103069	Resolves an issue where a McAfee driver causes virtual NIC to stop sending and receiving data.
User Interface	ENSW-103018	Resolves an issue where build numbers for all McAfee Endpoint Security modules are not getting displayed in threat events.
Installation	ENSW-102731	Resolves an issue where McAfee Endpoint Security installation fails because of leftover VSCore registry entries and files/folders of a previously installed version.
Feature Fix	ENSW-102483	Resolves an issue where event 1202 is not getting generated. When "`User can defer scans`" option is enabled, On-Demand scan schedule task when triggered through McAfee ePO displays status as "Scan resumed" instead of "Scan started".

Feature Fix	ENSW-101816	Resolves an issue where Exploit Prevention intermittently delays RDP connection with the server.
Feature Fix	ENSW-99137	Resolves an issue where McAfee ePO is unable to parse events due to database restriction of 512 characters. New limit is set to 1024 and strings exceeding this limit are truncated.

Adaptive Threat Protection

Component	Reference	Resolution
Feature Fix	ENSW-104134	Resolves an issue where some McAfee® Endpoint Security Adaptive Threat Protection (ATP) events are not getting parsed in McAfee ePO due to column size restriction of FileCompany.
Feature Fix	ENSW-102730	Resolves an issue where MfeDeepRem folder continues to expand in size on external drives thus limiting its functionality.
Performance	ENSW-102217	Resolves an issue where Adaptive Threat Protection consumes more memory with McAfee® Active Response (MAR) installed on the system.
Feature Fix	ENSW-100499	Resolves an issue where third party .Net applications crash when Endpoint Security Adaptive Threat Protection 10.7 is installed on the system.
Feature Fix	ENSW-25007	Resolves an issue where some trusted applications are set to 'unknown'.

Firewall

Component	Reference	Resolution
Feature Fix	ENSW-105717	Resolves an issue where IPv6 address formats are not being handled properly which leads to allowed traffic being blocked.
Feature Fix	ENSW-103609	Resolves an issue where FirewallEventMonitor.log does not report time correctly (AM/PM). Logs are now generalized to 24 HR format.
Feature Fix	ENSW-100490	Resolves an issue where event 35010 (Firewall timed groups are enabled from McTray) is not getting generated.

Web Control

Component	Reference	Resolution
Feature Fix	ENSW-106171	Resolves an issue where clicking on "`Search`" > "`Test Pattern`" in Endpoint Security Web Control "`View Effective Policy`" from the system tree throws an unknown error.
Feature Fix	ENSW-104374/ ENSW-103034/ ENSW-101874	Resolves an issue where Web Control blocks functioning of third-party applications when "`enable annotations in non browser based email`" is selected in policy.
Feature Fix	ENSW-102625	Resolves an issue where some Web control events are not getting parsed in McAfee ePO due to column size restriction of DomainName.

Copyright © 2020 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.