Release Notes

McAfee Endpoint Security 10.7.0

February 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.

What's new in the February 10.7.0 release

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

New platform support

The release includes a full installer package and can be used to install McAfee® Endpoint Security 10.7.0 for the first time or to upgrade from any previous Endpoint Security version.

This release is a candidate for same-day support for the upcoming Microsoft 20H1 Updates (Build 19025) for workstations and servers.

Additional Information

Note: If Endpoint Security 10.7 February 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 February Update's ability to successfully install.

The pop-up will not be experienced on Windows 7 SP1or 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	10.7.0.1481
Endpoint Security Platform extension	10.7.0.491
Endpoint Security Threat Prevention	10.7.0.1564
Endpoint Security Threat Prevention extension	10.7.0.506
Endpoint Security Firewall	10.7.0.1105
Endpoint Security Firewall extension	10.7.0.459
Endpoint Security Web Control	10.7.0.1306
Endpoint Security Web Control extension	10.7.0.463
Endpoint Security Adaptive Threat Protection	10.7.0.1740
Endpoint Security Adaptive Threat Protection extension	10.7.0.473
Threat Detection Reporting	1.0.0.294

Endpoint Security Migration Extension	10.7.0.275

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

Resolved issues in the February 10.7.0 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).

Platform

Component	Reference	Resolution
Interoperability	ENSW-25645	The CDI application now functions properly after the Endpoint Security upgrade.
Feature Fix	ENSW-29256	Access is no more granted for the execution of ESConfigTool for remote location.
Feature Fix	ENSW-26828	Event logs are now getting generated at the correct logging time on the client system.
Interoperability	ENSW-29181	Cisco AnyConnect Secure Mobility Client now connects successfully with any McAfee® Global Threat Intelligence™ network reputation setting.
Interoperability	ENSW-28917	Windows Defender status now correctly shows disabled when Endpoint Security is installed on the system.
Installation	ENSW-29332 / ENSW-96074	Systems now boot successfully after an Endpoint Security product upgrade.
Feature Fix	ENSW-29473	The Legacy McAfee self-protection by-pass mechanism no longer works post McAfee Endpoint Security installation.
Feature Fix	ENSW-26210	Using McAfee Endpoint Security client settings, user is now restricted to create file/folder at the location where they do not have edit permissions.
Feature Fix	ENSW-29269	Symbolic links are no longer allowed to be created in Endpoint Security folder.

Threat Prevention

Component	Reference	Resolution
Feature Fix	ENSW-25307	On Access Scan policy functions successfully when multiple policies are accessed at the same time.
Feature Fix	ENSW-25557	Endpoint Security Exploit Prevention custom rule now correctly reports TargetUserName.
Feature Fix	ENSW-25599	McAfee® Endpoint Security Threat Prevention Network (IPS) exclusions are now working properly without violations.
Feature Fix	ENSW-25666	Systems no more go into a hung state or display a blank screen when a threat is detected.

Feature Fix	ENSW-25722 / ENSW-25644	On-Demand scan now runs successfully at the scheduled time, after upgrading Endpoint Security 10.6.0.
User Interface	ENSW-26712	Endpoint Security threat event details now reports correct action status.
Feature Fix	ENSW-26881	User-defined application rule with multiple executables as exclusions or inclusions now functions properly.
Feature Fix	ENSW-27073	On-Demand scan now detects threats with the folder name containing dots '...'
Performance	ENSW-27311	After applying custom Low/High risk processes performance is no longer impacted.
Feature Fix	ENSW-28214	On scheduling scan policy using **Scan while idle** option, Endpoint Security logging shows **Not idle.** This issue is now fixed.
Performance	ENSW-28267	The CPU usage due to McShield.exe is now reduced on the IIS cluster servers.
Feature Fix	ENSW-28439	On-Demand scan console on client repeatedly resets elapsed time during scans.
Feature Fix	ENSW-28351	On-Access Scan ScriptScan URL exclusions now works consistently.
Feature Fix	ENSW-28779 / ENSW-29141	Endpoint Security events are now parsing to the database successfully.
Feature Fix	ENSW-28941	On-Demand Scan with or without **Use scan cache** (Windows Only) option now displays the correct scan results.
User Interface	ENSW-28998	Correct Access Protection rule name now displays in event logs and McAfee® ePolicy Orchestrator® threat events.
Feature Fix	ENSW-29254	On Demand Scan task successfully working with Scan on Idle state.
Feature Fix	ENSW-96184	Access protection rule **Browsers booting files from the Downloaded Program Files folder** now blocks the execution for Microsoft™ Edge and Internet Explorer.
User Interface	ENSW-96204	Display manage custom tasks are now retained on the client after McAfee Endpoint Security upgrade.
Feature Fix	ENSW-96252	Exploit Prevention S3 Signatures will no more be modified in McAfee Default Policy on Content Update.
Feature Fix	ENSW-28870	AMSI buffer overwrite will no longer be allowed to bypass AMSI protection.
Feature Fix	ENSW-27849	Endpoint Security now prevents any change of Windows Defender Application Control policy.

Firewall

Component	Reference	Resolution
Feature Fix	ENSW-25783	McAfee® Endpoint Security Firewall adaptive rule aggregator now retrieves valid results.
Installation	ENSW-26662	Endpoint Security modules are now successfully installed post removal of Endpoint Security Firewall.
Feature Fix	ENSW-28828	The network origin (catalog) is now getting displayed correctly, on importing and saving it from the catalog into a rule policy.
Feature Fix	ENSW-29113	The affected objects now display the propagation of the groups that contain the rule, while the rule is being modified.
Feature Fix	ENSW-29209	Wildcard '*' is now allowed on Endpoint Security client if used instead of drive

		letter in Endpoint Security Firewall rule policy.
Feature Fix	ENSW-29246	Signer field in Endpoint Security now accepts the special characters '+' and '@'.
User Interface	ENSW-29558	Endpoint Security Firewall defined network list is now getting saved properly.
Feature Fix	ENSW-95914	Firewall Policies are now visible in McAfee ePO on setting IPv6 as a subnet address in **Defined network** option of Firewall policy.
Feature Fix	ENSW-95857	System network traffic is now properly processed against "Firewall Rules" policy rule rather than Core Networking "Allow McAfee signed applications" rule.

Adaptive Threat Protection

Component	Reference	Resolution
Feature Fix	ENSW-26398	McAfee® Endpoint Security Adaptive Threat Protection (ATP) events for rule 239 are now successfully generated in observe mode.
Feature Fix	ENSW-26814	You can now disable Endpoint Security Adaptive Threat Protection using the McTray icon.
User Interface	ENSW-27465	The correct rule ID is now displayed in Adaptive Threat Protection logs and McAfee ePO.
Feature Fix	ENSW-96246	Real Protect static test file now gets detected by Real Protect.
Feature Fix	ENSW-96948	Enables FIPS mode for Real Protect when McAfee ePO is configured in FIPS mode.

Migration Assistant Extension

Component	Reference	Resolution
Feature Fix	ENSW-26170	Migration of **Trusted for IPS** to Endpoint Security Access Protection during Auto Migration is now successful.
Feature Fix	ENSW-28894	User-defined included and excluded processes now migrate successfully in Endpoint Migration Assistant.