Release Notes

McAfee Endpoint Security 10.5.3

Contents

- *About this release*
- *What's new*
- *Resolved issues*
- *Installation information*
- *Known issues*
- *Getting product information by email*
- *Where to find product documentation*

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 existing version.

Release date

November 13, 2017

Release build

Endpoint Security 10.5.3.3152.7

Endpoint Security Common 10.5.3.3178.1 — extension 10.5.3.3063.1

Endpoint Security Threat Prevention 10.5.3.3264.1 — extension 10.5.3.3098.1

Endpoint Security Firewall 10.5.3.3108.1 — extension 10.5.3.3045.1

Endpoint Security Web Control 10.5.3.3087.4 — extension 10.5.3.3044.1

Endpoint Security Adaptive Threat Protection 10.5.3.3113.4 — extension 10.5.3.3044.1

Endpoint Security Migration Assistant — extension 10.5.3.3040

Endpoint Security Package Designer 10.5.3.3023.1

This release was developed for use with:

- McAfee® Endpoint Security 10.5.x
- McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.1.1 and later
- McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud)

Important notes about this release

Endpoint Security 10.5.3 lists these products and versions in the **Master Repository** on the McAfee ePO server.

Product	Version	Minor version
Endpoint Security Common Patch	10.5.0	3
Endpoint Security Common	10.5.0	3178.1
Endpoint Security Threat Prevention Patch	10.5.0	3
Endpoint Security Threat Prevention	10.5.0	3264.1
Endpoint Security Firewall Patch	10.5.0	3
Endpoint Security Firewall	10.5.0	3108.1
Endpoint Security Web Control Patch	10.5.0	3
Endpoint Security Web Control	10.5.0	3087.4
Endpoint Security Adaptive Threat Protection	10.5.0	3113.4

Endpoint Security 10.5.3 lists these products and versions in the **About** dialog box of McAfee Agent and Endpoint Security, and McAfee ePO product properties.

Product	Version
Endpoint Security Common	10.5.3.3178.1
Endpoint Security Threat Prevention	10.5.3.3264.1
Endpoint Security Firewall	10.5.3.3108.1
Endpoint Security Web Control	10.5.3.3087.4
Endpoint Security Adaptive Threat Protection	10.5.3.3113.4

Purpose

This release of McAfee Endpoint Security contains improvements and fixes, including:

- Microsoft Windows 10 Fall Creators Update support
- Installation improvements
- Increased stability
- Network Intrusion Prevention (Network IPS) technology and Exploit Prevention Expert Rules, which expand intrusion prevention functionality

We recommend that you verify this update in test and pilot groups before mass deployment.

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.

New Microsoft product support

- Microsoft Windows 10 Fall Creators Update
- Microsoft Windows Server 2016 RS3

Installation, upgrade, and migration enhancements

VSCore 15.7 with InstallAll — Deploys all kernel-level drivers required to provide security services, for example, regulating access to registries, processes, and memory, to the products that use VSCore. This prevents incompatibilities between older and newer versions of drivers.

Endpoint Security Package Designer update — Adds the ability to select executable files to include in custom deployment packages. (McAfee ePO on-premise only)

Migration Assistant update — Adds the ability to migrate the Network IPS configuration in McAfee Host IPS, whether it's enabled, and how long to retain blocked hosts. (McAfee ePO on-premise only)

Support for Endpoint Upgrade Assistant 1.5 — McAfee® Endpoint Upgrade Assistant is a McAfee ePO extension that simplifies and automates the tasks required to upgrade. It analyzes the endpoints in a McAfee ePO environment, detects the supported McAfee products that are installed, and determines the minimum requirements for upgrading to current versions of the products. (McAfee ePO on-premise only)

Use the Endpoint Upgrade Assistant to simplify the upgrade planning and preparation time, reduce required reboots and uninstall failures, and create and track the status of deployment tasks. Use the Upgrade Automation feature to upgrade all supported McAfee products with a single deployment task.

For customers who do not use McAfee ePO for deployments, the new release adds the ability to upgrade using the Endpoint Upgrade Assistant. The new Package Creator tool creates product installers for deployment with third-party tools. For help using the Endpoint Upgrade Assistant and Package Creator, see PD27281.

Common enhancements

- Adds the option to select a language for activity logging.
- Adds the ability to set the size of an event database from 50–999 MB. The default is 50 MB.
- Adds the ability to include the certificate of a third-party application as a trusted process through McAfee ePO.

Threat Prevention — Exploit Prevention enhancements

Expert Rules — Provides additional parameters and allows much more flexibility than the custom rules you create in the Access Protection policy. Expert Rules are text-based custom rules that you create in the Exploit Prevention policy in Threat Prevention. Threat Prevention enforces Expert Rules on the client system the same as any other rule.

Exploit Prevention includes two types of Expert Rules:

- AAC-based rules — Protects files, processes, and registry items.
- McAfee Host IPS-based rules — Prevents buffer overflow and illegal API use, and protects Windows Services.

Best practice: Before writing Expert Rules, familiarize yourself with the Tcl programming language and understand the McAfee proprietary syntax when using Expert Rules.

For more information about Expert Rules, including syntax structures and examples, see PD27227.

For videos about how to use Expert Rules, see KB89677.

Network IPS — Monitors network activity to protect client systems from threats. The Network IPS protection filter driver inspects all data that flows between the client system and the network and takes specified actions on known attacks.

Network IPS also enables you to automatically block network intruder hosts for a specified period, even if the action for the Network IPS signature isn't set to Block. You can see the list of blocked hosts in the Endpoint Security Client in the Exploit Prevention category under Threat Prevention settings.

New protection signatures — The Exploit Prevention content includes the following new signatures, which you can manage in the **Signatures** section of the Exploit Prevention policy:

Signature ID	Description	Type
1157	USB Storage Device Inserted	Registry
6088	Microsoft Office DLL planting vulnerability	File
6089	Microsoft Office DLL side load vulnerability	File
6093	Microsoft Office OneNote DLL side load vulnerability	File
6094	Adobe Acrobat Reader DLL side load vulnerability	File

Threat Prevention — On-Access Scan enhancements

On-access scan update — Adds the option to disable read/write scanning of Shadow Copy volumes for system users. By default, this option is not selected.

Scan email attachments update — The **Scan email attachments** option is now called **Detect suspicious email attachments**.

Adaptive Threat Protection enhancements

Real Protect sensitivity — Adds the ability to configure the sensitivity level to use with client-based scanning when determining whether a file matches known malware.

Updated components

- VSCore 15.7.0.601.12
- SysCore 15.7.0.662

- AMCore 1.5.0.4060.3

  AMCore Content 3125 or greater is required.
- McAfee Agent 5.0.6
- McAfee Anti-Malware Engine 5900

Resolved issues

The current release of the product resolves these issues. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

The resolved issues cover all management platforms.

Migration

Reference	Resolution
1192753	Groups with duplicate rules in the **Host IPS Catalog** now successfully migrate to the **Firewall Catalog**.
1196358	McAfee Host IPS Trusted Network policies that contain Internet Protocol version 6 subnets now correctly migrate to the Endpoint Security policy.

Common

Reference	Resolution
1191919	You can now configure the event database size from 50–999 MB.
1195840	Self Protection events now report the correct product version to McAfee ePO by correctly storing and retrieving information from the registry.
1198960	An Endpoint Security installation no longer fails in the presence of McAfee Drive Encryption due to an inability to write to HKEY_CURRENT_USER\Software\McAfee\Endpoint\Common \BusinessoBjectRegistry\SystemInfo\.
1199374	A Windows system restore no longer fails on systems where Endpoint Security is installed.
1201609	TIC log no longer stops when Adaptive Threat Protection debug logging is enabled. LoggerBL.xml is updated in the installer and always overwrites the file on the system. This means that logger settings are replaced by defaults until policy enforcement returns the configured settings.
1210456	Endpoint Security now successfully deploys installation, patch, and hotfix packages when they are in the same McAfee ePO repository.

Threat Prevention

Reference	Resolution
1181771	Windows systems no longer periodically show the Windows Action Center prompt to enable McAfee security software.
1182718	On-demand scans now successfully work with exclusions for potentially unwanted program.
1191580	dllhost.exe no longer crashes after deploying a Sysprep image or performing a Cortana search on a Windows 10 Creators Update system when Exploit Prevention is enabled.
1191719	An update to network file caching now prevents a printing delay.
1193467	McShield.exe no longer consumes high CPU.
1193756	

Reference	Resolution
1194014	McShield.exe no longer experiences high CPU when opening applications.
1197122	The Threat Prevention installer no longer removes IBM Lotus Notes version 9 when upgrading to Endpoint Security.
1198993	Quarantine items with invalid time values no longer cause Threat Prevention to crash, and Threat Prevention now appears in the Endpoint Security Client **About** window.
1204316	The correct AMCore content version now appears in the Endpoint Security Client and McAfee ePO after an update.
1204416	McShield.exe no longer consumes high CPU when saving policies.
1205489	Installation of Endpoint Security 10.5.1 Hotfix 2 from the command line no longer fails on the first attempt.
1209107	The Event Manager now deletes corrupted event database files and replaces them with new event database files.
1211550	Exploit Prevention Content updates no longer overwrite customized rules in the Application Protection Rules policy.
1215606	Websense services now successfully start after a system restart with Endpoint Security installed.

Firewall

Reference	Resolution
1184449	Endpoint Security Firewall now correctly starts after a system restart with a correct state and no longer blocks packets when the Firewall was disabled from the context menu before restarting.
1188069	Only one instance of a location now appears in the **Firewall Catalog**, regardless of how many groups contain the location.
1190907	Location Aware Groups now successfully work with Big IP VPN tunnels.
1193034	Firewall rules from the **Policy Catalog** now correctly function when added to subsequent groups in a Firewall policy.
1194924	Endpoint Security Firewall no longer blocks the process when process IDs are not returned from Firecore and successfully continues to the next rule.
1195190	A thread no longer hangs in Endpoint Security Firewall, which prevented it from applying policies.
1198251	Location Aware Groups now correctly function on systems with two Ethernet adapters.
1198530	Location Aware Groups function with IP addresses that are defined in the registry and no longer cause mfefw.exe to consume high CPU. The number of matching locations no longer increases with every policy enforcement. To reduce the number of locations, disable the **Retain existing user-added rules and Adaptive mode rules when this policy is enforced** setting in the **Firewall Options** policy.
1200295	Domain reachability now successfully connects with the alias domain in configurations where the server couldn't download certificates from the Endpoint Security Client.
1204936	Mfefw.exe no longer experiences sustained high CPU.
1210815	

Adaptive Threat Protection

Reference	Resolution
1199556	Files marked as Known Trusted by Enterprise Reputation are no longer processed by Dynamic Application Containment (DAC) rules.
1199945	Adaptive Threat Protection no longer submits erroneous application and DLL telemetry to the Threat Intelligence Exchange (TIE) server when that telemetry was already sent.

Reference	Resolution
1201425	DAC no longer blocks trusted files when the files are opened from a UNC path.
1205806	Adaptive Threat Protection no longer blocks files marked as Known Trusted by Enterprise Reputation.

Web Control

Reference	Resolution
1181847	Web Control no longer enforces empty user-based policies for domain users when no Policy Assignment Rules are configured in McAfee ePO.
1186850	The mfeavfk driver is now in a correct state after installing Endpoint Security, and installed components now correctly appear in McAfee ePO reports.

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.

You must check in the Endpoint Security Common patch package to the **Master Repository** on the McAfee ePO server before you can check in any other Endpoint Security module patch package.

Upgrade support

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

Important information about Exploit Prevention

The Endpoint Security 10.5.3 installation package includes the McAfee Exploit Prevention Content 10.5.0.7850. This content version adds support for the new digital signatures used by Endpoint Security 10.5.3. The installation updates the content on systems running Endpoint Security with previous versions of the content.

Management software

- McAfee ePO 5.1.1
- McAfee ePO 5.3.1
- McAfee ePO 5.9.0
- McAfee ePO Cloud

  For the latest Endpoint Security management entitlement and license information, see KB87057.
- McAfee Agent 5.0 Patch 2 (5.0.2.333) (minimum)

  McAfee Agent 5.0.5 or later (recommended)

For systems running an earlier version of McAfee Agent:

- On systems managed by McAfee ePO, upgrade the 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 self-managed systems, no action is required to upgrade version 4.0 and later. For earlier versions, upgrade McAfee Agent manually.

Supported legacy products (required for migration only)

Migration supports all patch levels for these legacy products.

- McAfee® VirusScan® Enterprise 8.8
- McAfee® VirusScan® Enterprise for Linux 2.0.2
- McAfee® Host Intrusion Prevention 8.0
- McAfee® SiteAdvisor® Enterprise 3.5
- McAfee® Endpoint Protection for Mac 2.3 or McAfee® VirusScan for Mac 9.8

Products and platforms no longer supported

- McAfee Agent 5.0.2.132
- McAfee Agent 5.0.1
- McAfee Agent 5.0.0
- Windows Server 2008
- Windows Vista Service Pack 2 (SP2)

Known issues

For a list of known issues in this product release, see KB82450.

Updates to documentation

Some updates to Endpoint Security 10.5.3 are not reflected in the product guide or Help.

Documentation	Incorrect information	Updated information
McAfee Endpoint Security 10.5.0 Product Guide and Common Help	Missing information — **Event Logging** section, **Limit the size (MB) of event DB** option	Limits the size of event databases to the specified maximum size (between 50 MB and 999 MB). The default is 50 MB. This text will be included in the next version of the documentation.
McAfee Endpoint Security 10.5.0 Product Guide and Threat Prevention Help, *Exploit Prevention* topic	Missing information — **Network Intrusion Prevention** section, **Enable Network Intrusion Prevention** option and **Automatically block network intruders** option	**Enable Network Intrusion Prevention** option — Enables Network Intrusion Prevention (NIPS) and enforces network IPS signatures. Selecting this option exposes Network IPS signatures in the Signatures list. **Automatically block network intruders** option — Blocks intruder hosts for a specified number of seconds. Select this option to block all attempted actions from intruder hosts, even if the action for the Network IPS signature isn't set to **Block**. • **Number of seconds (1-9999) to block** — Specifies the number of seconds to automatically block intruders. **Automatically block network intruders** This text will be included in the next version of the documentation.
McAfee Endpoint Security 10.5.0 Product Guide and Threat Prevention Help, *On-Access Scan* topic	Missing information — **Disable read/write scan of Shadow Copy volumes for SYSTEM process** option	Disables read/write scans of Volume Shadow Copy (VSC) volumes by SYSTEM process (PID 4) only. Threat Prevention continues to scan all other access to VSC volumes by all other processes (other than SYSTEM), based on **On-Access Scan** settings. This option provides improved performance. (Disabled by default) This text will be included in the next version of the documentation.

Documentation	Incorrect information	Updated information
McAfee Endpoint Security 10.5.0 Product Guide and Threat Prevention Help, *On-Access Scan* topic	Missing information — **Detect suspicious email attachments** (Previously called **Scan email attachments**.) (Windows only)	Scans and detects suspicious files saved to disk by email client applications, such as Outlook or Windows Mail. This option enables aggressive email-attachment detection using heuristic signatures, which detect most executables, scripts, and .jar files by policy, rather than looking for malware. Select this option to scan all downloads, including archives and their contents, and MIME-encoded files. Archives are scanned 2 levels deep. This option also prevents executables and scripts downloaded by email clients from running. If an email client update downloads an executable, the update might not work. Although this option doesn't affect attachments downloaded from browser-based email, on-access scan examines those downloads. Disabling this option doesn't prevent the on-access scanner from scanning email attachments — it just disables the additional heuristic signatures. (Disabled by default) This text will be included in the next version of the documentation.
McAfee Endpoint Security 10.5.0 Product Guide and Threat Prevention Help, *On-Demand Scan* topic and *Custom On-Demand Scan client task* topic	Missing information — **Files that have been migrated to storage** option	This option doesn't apply to files stored in Microsoft OneDrive. The on-demand scanner doesn't download OneDrive files or scan files that haven't been downloaded. This text will be included in the next version of the documentation.
McAfee Endpoint Security 10.5.0 Product Guide and Adaptive Threat Protection Help, *Options* topic	Missing information — **Real Protect Scanning** section, **Sensitivity level** option	Configures the sensitivity level to use with client-based scanning when determining whether the file matches known malware. • **Low** • **Medium** (Default) • **High** The higher the sensitivity level, the higher the number of malware matches. But, allowing more detections might result in more false positive results. This text will be included in the next version of the documentation.
McAfee Endpoint Security 10.5.0 Installation Guide	Appendix A **Adaptive Threat Protection installation** (unmanaged only)	Removed. Information about system requirements and product configuration will be integrated into other topics in the next version of the documentation.
McAfee Endpoint Security 10.5.0 Migration Guide	Missing information — **Migration notes for IPS Rules settings** topic (McAfee ePO on-prem only)	Added a section about Network IPS configuration settings that migrate.

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 McAfee Endpoint Security Expert Center at https://community.mcafee.com/community/business/expertcenter/products/ens.

To view frequently asked questions about Endpoint Security, including installation information, configuration best practices, troubleshooting tips, and more, see KB86704.

0-00

McAfee
Together is power.