Release Notes

McAfee Endpoint Security 10.5.0
For use with McAfee ePolicy Orchestrator

Contents
- About this release
- New features
- Resolved issues
- Installation instructions
- Known issues
- 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.

New features
The current release of the product includes these new features.
**Adaptive Threat Protection enhancements**

Threat Intelligence is now named Adaptive Threat Protection.

- Dynamic Application Containment — Adds the ability to contain a specific instance of an application.
- New McAfee-defined queries — Includes additional predefined queries for Real Protect.
- Real Protect scanner — Inspects suspicious files and activities on an endpoint to detect malicious patterns using machine-learning techniques. Using this information, the scanner can detect zero-day malware.

*Adaptive Threat Protection isn’t supported on systems managed by McAfee ePO Cloud.*

**Firewall enhancements**

Ability to determine if a domain is reachable using the HTTPS protocol.

**Threat Prevention enhancements**

- Ability to configure a Windows registry scan location for on-demand scans.
- Ability to create a custom Access Protection rule to protect Windows services.
- Management of Exploit Prevention signatures and Application Protection rules.
- Ability to display false-positive mitigation events using the Endpoint Security Threat Prevention: False Positive Mitigation Events query.

**Web Control enhancements**

- Support for 64-bit Firefox.

**Endpoint Migration Assistant enhancements**

- Automatic migration of settings for the entire System Tree or one group.
- Simultaneous migration of workstation and server settings in the Threat Prevention policies.
- Automatic migration of Firewall Trusted Applications to Access Protection.
- Migration of additional Firewall signatures to support all Exploit Prevention features.

**Resolved issues**

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

- McAfee Endpoint Security 10.2 Release Notes — PD26588
- McAfee Endpoint Security 10.1 Patch 2 Release Notes — PD26322
- McAfee Endpoint Security 10.1 Patch 1 Release Notes — PD26448
- McAfee Endpoint Security 10.1 Release Notes — PD26220
- McAfee Endpoint Security 10.0 Patch 1 Release Notes — PD26003
- McAfee Endpoint Security 10.0 Release Notes — PD25363
### Installation

<table>
<thead>
<tr>
<th>Reference</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1164762</td>
<td>VSCore now successfully installs during Endpoint Security installation.</td>
</tr>
<tr>
<td>1162713</td>
<td>The DAT version now correctly updates after installation.</td>
</tr>
<tr>
<td>1157462</td>
<td>Endpoint Security installation now automatically removes third-party software.</td>
</tr>
<tr>
<td>1140210</td>
<td>Windows Explorer no longer hangs on a client when accessing files on a server running Threat Prevention.</td>
</tr>
</tbody>
</table>

### Common

<table>
<thead>
<tr>
<th>Reference</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1156420</td>
<td>If the Custom On-Demand Scan client task setting Do not scan when the system is in presentation mode is selected, a scheduled scan now correctly runs when a system is locked.</td>
</tr>
<tr>
<td>1151408</td>
<td>Custom on-demand scans that are set to run weekly no longer run every day.</td>
</tr>
<tr>
<td>1149816</td>
<td>Performing a system restore no longer produces an access-denied error message.</td>
</tr>
</tbody>
</table>

### Threat Prevention

<table>
<thead>
<tr>
<th>Reference</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1158941</td>
<td>Queries using the Endpoint Security Platform custom properties now retrieve data as expected.</td>
</tr>
<tr>
<td>1158562</td>
<td>Enable On-Access Scan on system startup is no longer re-enabled after a system restarts.</td>
</tr>
<tr>
<td>1157626</td>
<td>Blue Screen (BugCheck 3b) no longer occurs on servers after Endpoint Security is installed.</td>
</tr>
<tr>
<td>1155418</td>
<td>Endpoint Security now correctly places these certificates in the Intermediate Certification Authorities store: • COMODO RSA Code Signing CA • Verisign Class 3 Code Signing 2010 CA</td>
</tr>
<tr>
<td>1154040</td>
<td>When sending an Automatic Response email notification, the Target File Name field now correctly displays the full path and file name.</td>
</tr>
<tr>
<td>1146894</td>
<td>Client systems no longer hang when running the StataSE application from a network share folder.</td>
</tr>
<tr>
<td>1146604</td>
<td>Query results now only contain results for the systems in the group that the user has permissions to view.</td>
</tr>
<tr>
<td>1144864</td>
<td>A blue screen no longer occurs when Sophos LAN Crypt and Threat Prevention are installed.</td>
</tr>
</tbody>
</table>

### Firewall

<table>
<thead>
<tr>
<th>Reference</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1156143</td>
<td>mfefw.exe no longer causes high CPU usage when a policy is enforced.</td>
</tr>
<tr>
<td>1153020</td>
<td>The Firewall Client Rules page now displays valid rules after running the Endpoint Security Firewall Property Translator server task.</td>
</tr>
<tr>
<td>1145366</td>
<td>Location Aware Groups (LAG) using connection-specific DNS suffixes now work properly.</td>
</tr>
</tbody>
</table>
## Web Control

<table>
<thead>
<tr>
<th>Reference</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1162914</td>
<td>The user-based policy for Block and Allow List is now enforced correctly on the client.</td>
</tr>
<tr>
<td>1156051</td>
<td>The Web Control add-on no longer causes a delay of more than .25 seconds when starting Internet Explorer 11.</td>
</tr>
</tbody>
</table>

## Installation instructions

Use this information while installing Endpoint Security.

For more information, see the *McAfee Endpoint Security Installation Guide*.

**Best practice:** Restart the client system after installing this release of the product.

## Requirements

This release supports deploying Endpoint Security to Windows operating systems — self-managed and from McAfee ePO or McAfee ePO Cloud.

For a complete list of current system requirements, see [KB82761](#).

### Important information about McAfee Host IPS

The Endpoint Security version 10.5 installation package includes McAfee Host Intrusion Prevention Content 8.0.0.7364. This content version is required by McAfee Host IPS and adds support for the new digital signatures used by Endpoint Security version 10.5. The installation updates the content on systems running McAfee Host IPS with previous versions of the content.

### Management software

- McAfee ePO 5.1.1 or later
  
  McAfee ePO 5.3.1 or later is recommended.

- 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) or later
  
  McAfee Agent 5.0.4 is recommended.

For systems running an earlier version of McAfee Agent:

- On McAfee ePO systems, you need to upgrade the McAfee Agent manually before deployment.

- On McAfee ePO Cloud systems, 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. You need to upgrade earlier versions of McAfee Agent manually.

For more information, see the *McAfee Endpoint Security Installation Guide*.
**Supported legacy products (required for migration only)**

Migration supports all patch levels for these legacy products.

- VirusScan Enterprise 8.8
- 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 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.

**Product documentation**

Every McAfee product has a comprehensive set of documentation.

McAfee Endpoint Security includes the following documentation:

- *McAfee Endpoint Security Release Notes* (this document)
- *McAfee Endpoint Security Installation Guide*
- *McAfee Endpoint Security Migration Guide*
- McAfee Endpoint Security Client Help
- Endpoint Security Common Help
- Endpoint Security Threat Prevention Help
- Endpoint Security Firewall Help
- Endpoint Security Web Control Help
- Endpoint Security Adaptive Threat Protection Help

**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.intelsecurity.com/signup_login to register and select your product information options.
Find product documentation
On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

Task
1  Go to the ServicePortal at https://support.mcafee.com and click the Knowledge Center tab.
2  In the Knowledge Base pane under Content Source, click Product Documentation.
3  Select a product and version, then click Search to display a list of documents.