Release Notes

McAfee Drive Encryption 7.2.2

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

We do not support the automatic upgrade of a pre-release software version (POC or test builds). To upgrade to a production release of the software, uninstall the existing version first.

Release build - 7.2.2.14

This release was developed for use with:

McAfee® ePolicy Orchestrator® (McAfee® ePO®) 5.1.0, 5.1.1, 5.1.2, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.9.0.

McAfee® ePolicy Orchestrator® (McAfee® ePO®) Deep Command 2.2.0, 2.3.0, 2.4.0.

Purpose

This McAfee® Drive Encryption 7.2 Patch 2 (DE 7.2.2) release adds enhancements and fixes problems that were reported in previous versions.
Rating

• **High Priority** – McAfee rates this release as a high priority for all environments to avoid a potential business impact. Apply this update as soon as possible.

For more information about patch ratings, see [KB51560](#).

New features

This release of the product includes these new features.

**Support for Windows 10 Fall Creators Update (also known as Windows 10 RS3)**

Drive Encryption 7.2.2 provides support for deployments on Windows 10 Fall Creators Update (also referred to as Windows 10 RS3, version 1709).

For further information about upgrading from Windows 10 Anniversary Update (RS1) to Windows 10 Creators Update (RS2), or Windows 10 Fall Creators Update (RS3), see [KB89000](#).

**Updates to default theme**

The default theme for preboot is updated with a modern flattened appearance and color scheme. On screen keyboards are updated to have the same flattened appearance and color scheme, but are not part of the theme.

Custom themes must be recreated if the modern look is required.

See [KB89841](#) for more information.

Enhancements

**Change to the way FIPS mode is indicated**

When McAfee Drive Encryption is installed in FIPS mode, a **FIPS** entry appears in the Modules window. Previously, this was displayed in the title bar in preboot.

**Support for Device Guard in FIPS mode**

Drive Encryption 7.2.2 is the first release to support Drive Encryption running in FIPS mode on a Windows 10 system, with Device Guard enabled. For further information about support for Windows 10 Device Guard with McAfee Drive Encryption, see [KB86009](#).

**Additional smart card support**

Support for the following smart cards is included in this release:

• ATOS (previously Siemens) CardOS 5.3 token

• Oberthur AuthentIC PKI Smart Card - support added for V8 Cosmo card

**Incompatible Product Detection**

Incompatible Product Detection is updated in McAfee Drive Encryption for the following:
Resolved issues

The following issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the release notes for the specific release.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Issue description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1187815</td>
<td>Fixed: DETech Standalone does not detect a USB Floppy Drive even though USB support is enabled.</td>
</tr>
<tr>
<td>1189124</td>
<td>Fixed: Autoboot fails if the TPM If Available policy is enabled in Drive Encryption 7.2.x.</td>
</tr>
<tr>
<td>1195815</td>
<td>Fixed: Microsoft firmware updates fail on Surface Pro 4 when Drive Encryption 7.1.x is upgraded to Drive Encryption 7.2.x.</td>
</tr>
<tr>
<td>1183032</td>
<td>Fixed: SSO no longer functions for new smart card users in Drive Encryption 7.2.x if the policy Must Match Username is enabled.</td>
</tr>
<tr>
<td>1152041</td>
<td>Fixed: Characters appear in the Username and Password fields by moving the mouse in preboot.</td>
</tr>
<tr>
<td>1204410</td>
<td>Fixed: A version mismatch is detected between DE TECH/WinTec and the installed version of McAfee Drive Encryption.</td>
</tr>
<tr>
<td>1204769</td>
<td>Fixed: Upgrading a system that runs Opal encryption from Drive Encryption 7.1.3.590 to Drive Encryption 7.2.x fails.</td>
</tr>
<tr>
<td>1212685</td>
<td>Fixed: HP 640/650G2 and 820/840/850G3 computers stop responding if the policy is set to turn off when at preboot for a specified period of time.</td>
</tr>
<tr>
<td>1207340</td>
<td>Fixed: RT - Error 1406. Could not write value dwIsFullScreen to key: \Software\McAfee \Endpoint\Common\BusinessObjectRegistry\SYSTEMINFO occurs when you upgrade from McAfee Endpoint Security 10.2 to McAfee Endpoint Security 10.2.1 with Drive Encryption 7.2.x installed.</td>
</tr>
<tr>
<td>1214124</td>
<td>Fixed: Upgrade from Windows 10 version 1511 to Windows 10 version 1703 fails when McAfee Drive Encryption is in FIPS mode.</td>
</tr>
</tbody>
</table>

Additional information

Migration from McAfee Endpoint Encryption for PC (EEPC) 5.x.x to McAfee Drive Encryption

Support for migration from McAfee Endpoint Encryption for PC (EEPC) 5.x.x to McAfee Drive Encryption is no longer provided, because EEPC 5.x is End of Life (EOL). For further information, see KB89717.

Hardware compatibility

Version 69 of the XML Hardware Compatibility file is included with the release. For further information, see KB81900.

Known issues

For a list of known issues in this product release, see KB84502.
Privacy notice

The Data Protection Self-Service Portal (DPSSP) collects users' login names, system names, IP addresses, and audit data. Access to this information is available in DPSSP reports within McAfee ePO. Make sure that access to these reports is authorized and appropriately managed.

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.