McAfee Drive Encryption 7.2.9 Release Notes

Contents

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.

For the latest information about supported platforms, environments, and operating systems, see KB79422.

Release build - McAfee Drive Encryption 7.2.9.5

This release was developed for use with:

- McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.9.0, 5.9.1, and 5.10.0

Purpose

The McAfee Drive Encryption 7.2.9 release provides fixes for problems that were reported in previous versions.

Rating — Recommended

Mandatory	Critical	High Priority	**Recommended**

- Required for all environments.
- Apply this update at the earliest convenience.
- A patch that resolves non-severe issues or improves product quality is considered Recommended.
- Not applicable to hotfixes, because hotfixes are only created in response to a business-impacting issue.

For more information, see KB51560.

Important changes introduced in recent updates

The following enhancements and changes have been made since the last major product release.

Standardization of password recovery phonetics

The phonetics used for the recovery component has been standardized across the McAfee encryption products (McAfee Drive Encryption, McAfee® File and Removable Media Protection (FRP), and McAfee® Management of Native Encryption (MNE). These products have adopted a set based on the NATO phonetic alphabet, with all content in English-only (en-us) irrespective of the client system locale.

User-based policy default password

From McAfee Drive Encryption 7.2.5, the default password has changed to 1234567 for new installations or when duplicating the McAfee Default product policy. The minimum default password is enforced when you change your password. A minimum password length of seven characters is now required.

See KB90465 for more information.

Automatic Decryption of BitLocker Encrypted system

When recent versions of Microsoft Windows are installed, the hard drive might automatically be encrypted by BitLocker before any credentials or other protectors are supplied to it. For the exact conditions under which this situation can arise, see the Microsoft BitLocker documentation.

From Drive Encryption 7.2.6 HF1247725, when the Drive Encryption client software is installed, it detects if the system is already encrypted by BitLocker (and does not have any protection). The automatic decryption of BitLocker is then triggered. After BitLocker finishes decrypting the hard drive, the system is ready for Drive Encryption activation.

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.

Reference	Issue description
1268921	The keyboard language on a Lenovo P52 is now changed correctly when selecting a language other than English-US.
1269831	User certificates are now found with ATOS (Siemens) CardOS 5.3 on UEFI systems.
1264395	User certificates are now found with ATOS (Siemens) CardOS 5.3 on Legacy systems.

Reference	Issue description
1268379	This release ensures SafeNet Java 72k is detected on Pre-Boot with HP EliteBook X360 1030 G3.
1265394	This release fixes CCID Protocol error on PBA with ID-One PIV cards after upgrading Drive Encryption from 7.2.6 to 7.2.8.
1250486	This release enables the importing of user certificates from the 'usercert' Active Directory attribute.
1250930	Keyboard and mouse now work correctly when connected to Lenovo USB-C dock on Drive Encryption activated systems.
1268517	This release hardens the recovery key export mechanism to eradicate recovery issues in Drive Encryption activated systems.
1266253, 1263433	Internal keyboard now works correctly on Pre-Boot on Fujitsu Celsius H780 laptop (UEFI mode).
1267074, 1268295	This release fixes a rare blue screen "Driver Power State Failure" on shutdown of Drive Encryption installed system when USB drives are inserted.
1253129	External mouse and touchpad now work on PBA on ASUS P2540UB in EFI mode.
1256659	This release fixes a Microsoft Windows update error caused by an empty SetupConfig.ini file.
1224553	This release provides a workaround for smart card readers that do not perform automatic protocol negotiations and would otherwise reject the communication parameters specified by the smart card ATR (Answer to Reset) settings.

Additional information

Reported UEFI version

The versions reported within the Modules dialog of McAfee Drive Encryption UEFI preboot shows as 7.2.9.4.

Hardware compatibility file

This release package incorporates version 91 of the Hardware Compatibility XML file. See KB81900 for further information and the latest version of the file, which is attached to the article.

Opal compatibility

See KB81136 for the latest information about self-encrypting drives that support the Opal standard and that are compatible with McAfee Drive Encryption. The article lists supported SATA and NVMe Opal drives.

DETech standalone floppy disk support

The option to install DETech on a standalone floppy disk is not supported in DE 7.2.5 and later, because DETech does not fit on a single disk or disk image. Use a USB drive instead.

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, 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.