Revision A

McAfee Data Loss Prevention Endpoint for Windows 11.0.400 Release Notes

(McAfee ePolicy Orchestrator)

Contents

About this release

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

Release build — 11.0.400

- McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) client 11.0.400.152 for Microsoft Windows
- McAfee® Data Loss Prevention (McAfee DLP) extension 11.0.400.8 for McAfee® ePolicy Orchestrator® (McAfee® ePO™)

This release was developed for use with:

Software	Tested version
McAfee ePO	• 5.3.3 HF1230649 • 5.9.1
McAfee® Agent for Windows	• 5.0.6 • 5.5.0

For information on all supported platforms, environments, and operating systems see KB68147

Purpose This release resolves the master bypass vulnerability issue and includes enhancements and fixes problems that were reported in the previous version.

Rating — Mandatory

Mandatory	Critical	High Priority	Recommended

- Required for all environments.
- Failure to apply Mandatory updates might result in a security breach.
- Mandatory patches and hotfixes resolve vulnerabilities that might affect product functionality and compromise security.
- You must apply these updates to maintain a viable and supported product.

For more information, see KB51560.

Compatibility with other McAfee Products

The following McAfee products and versions have been tested for compatibility with this release.

McAfee product	Tested version
McAfee® Application Control	7.0.1, 8.0 HF5, and 8.1
McAfee® Client Proxy	2.3.3 and 2.3.4
McAfee® Data Exchange Layer (DXL)	3.1, 4.0, and 4.1
McAfee® Threat Intelligence Exchange (TIE) for Endpoint Security	10.2.3
McAfee® Drive Encryption	7.1.3, 7.2.4, and 7.2.5
McAfee® Endpoint Security	10.2.2, 10.5.3, and 10.5.4
McAfee® File and Removable Media Protection (FRP)	4.3.1.Hotfix 2, 5.0.5, and 5.0.6
McAfee® Host Intrusion Prevention	8.0 Patches 8, 9, 10, and 11
McAfee® Management of Native Encryption (MNE)	3.0.1 and 4.1.3
McAfee® Policy Auditor	6.2
McAfee® Risk Advisor	2.7.2
McAfee® Rogue System Detection (RSD)	5.0.5
McAfee® SiteAdvisor® Enterprise	3.5 Patch 5
McAfee® Virtual Technician	8.1.0
McAfee® VirusScan® Enterprise	8.8 Patches 8, 9, 10, and 11

McAfee DLP Endpoint is also compatible with the latest release of the WebMER tool.

Tested software

McAfee DLP supports the following third-party software products. These versions have been tested for compatibility with this release.

Application type	Software	Tested Versions
Cloud applications	Box	4.0.7906.0
	Dropbox	48.4.58
	Backup and Sync from Google (Google Drive)	3.41.9267.0638

Application type	Software	Tested Versions
	iCloud	7.2.0.67
	Microsoft OneDrive	18.065.0329.0002
	Syncplicity	5.4.0.15260
Security and encryption applications	Boldon James Email and Office Classifier	3.11
	Boldon James File Classifier	3.10.1
	Microsoft Rights Management Service (RMS) client	1.0.2004.0, 1.0.3274.818
	Seclore FileSecure Policy Server	2.78.0.0
	Seclore Desktop Client	3.6.2
	Stormshield Data Security	9.1.20688
	Titus Classification Suite	4.7 HF 3
	Titus SDK	3.1.13.4
	TrueCrypt	7.0.1
Office and productivity applications	Adobe Acrobat Pro	X and XI
	Adobe Reader	11.0.10 and DC 2018.009.20044
	Google Chrome, 32-bit and 64-bit	55.0.2883.75-66.0.3359.117
	Lotus Notes client software	8.5.3 and 9.0.1
	Microsoft Edge	Microsoft Edge 38-41.
	Internet Explorer	11
	Microsoft Office, 32-bit and 64-bit	2010, 2013 SP1, and 2016
	Microsoft Outlook, 32-bit and 64-bit	2010, 2013 SP1, and 2016
	Microsoft SharePoint	2010, and 2013
	Mozilla Firefox, 32-bit and 64-bit	48–59
Virtual operating systems	Citrix XenApp	6.5 FP2
	Citrix XenDesktop	7.6 Patch 3 (PVS), 7.11, and 7.15 LTSR Cumulative Update 1 (CU1)
	VMware Horizon	7.4

What's new

The current release of the product includes these enhancements and changes.

Security vulnerability resolved

The security vulnerability that bypassed the master release code challenge/response mechanism has been resolved. See SB10233 for information on the vulnerability and remediation.

Limitation: The secured master release code is only supported by specific versions of other McAfee DLP products. It must not be used with unsupported products. See KB90417 for information on supported versions.

Attach evidence in email notification task

Attaching evidence to an email notification task or incident details/incident list dialog to send email has been enhanced. The setting now allows three options in addition to attaching a CSV file with evidence list information.

- Attach incident details page
- Attach decrypted evidence files
- Attach decrypted match-string HTML files

The more granular setting gives the administrator the option of attaching only the evidence files without letting the user know which incident details or match strings triggered the incident.

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.

Table 3-1 Master bypass vulnerability issue

Reference	Issue description
CSE-VDR 2017-37450560, SBC-2017-3954SBC-2017-3954	The security vulnerability that bypassed the master release code challenge/response mechanism has been resolved. See SB10233 for information on the vulnerability and remediation. **Limitation:** The secured master release code is only supported by specific versions of other McAfee DLP products. It must not be used with unsupported products. See KB90417 for information on supported versions.

Table 3-2 Other issues

Reference	
1220799	Rollup tasks no longer use excessive CPU resources and complete in a reasonable time.
1236776	Rollup tasks are no longer reset when McAfee DLP extension is installed in McAfee ePO.
1228027	Content fingerprinting of saved email drafts is detected by McAfee DLP Endpoint upon logoff or reboot.
1228047	Queries no longer take excessive CPU resources. The root cause of the issue was running SQL queries without limiting the size of the result. Now query retrieval is limited to 50 rows by default.
1230025	Sensitive content in PDF can now be classified based on custom properties.
1233610, 1235198	Saving the client configuration after upgrading from McAfee DLP 10.0.300 to 11.x no longer causes an error in some Microsoft SQL server configurations.
1234003	Screen capture rules now capture evidence from all monitors, not just the primary monitor.
1234247	A **DLP: data in-use/in-motion** query with display as Boolean Pie Chart no longer displays an error message.
1234640	When two email accounts are managed from the same Outlook application and the **Send immediately when connected** configuration is disabled in Outlook, emails sent by the non-default account are now sent. They are no longer kept in the Outbox folder.
1235133	Printing a PDF from a web page proceeds normally. McAfee DLP Endpoint doesn't disable Adobe protected mode in the printer hook.
1236556	The section on the **DLP Settings** | **General** page that sets policy validation has been enhanced with a **No Policy Validation** option. This option speeds up applying a policy by ignoring validation.

Table 3-2 Other issues *(continued)*

Reference	
1237293	The Luhn10 = 5 validator was renamed.
1238150	McAfee DLP Endpoint no longer intermittently blocks Google Chrome from launching.
1238569	Policy conversion from a version 9.3.x policy completes without error, even when an advanced pattern in 9.3 does not have a valid GUID. Policy conversion failure was only observed in version 11.0.300.
1238719	Opening Google Chrome with multiple tabs no longer causes high CPU consumption of McAfee DLP Endpoint process fcnm.exe when Chrome is running.

Installation information

For information about installing or upgrading McAfee DLP 11.0.400 (11.0 Update 4) software, see the McAfee Data Loss Prevention 11.0 Installation Guide.

The recommended installation of the client software uses the McAfee ePO infrastructure for deployment to the endpoints.

You can also deploy McAfee DLP Endpoint client software to your network using third-party enterprise software deployment tools.

Known issues

For a list of known issues in this product release, see this McAfee Knowledge Base article: KB89301.

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.