



Release Notes  
Revision G

# McAfee Data Loss Prevention 11.0.0

For use with McAfee ePolicy Orchestrator

## Contents

- ▶ *About this release*
- ▶ *New features*
- ▶ *Enhancements*
- ▶ *Resolved issues*
- ▶ *Installation information*
- ▶ *Known issues*
- ▶ *Getting product information by email*
- ▶ *Find product documentation*

---

## About this release

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

**Release build** — McAfee® Data Loss Prevention (McAfee DLP) extension for McAfee® ePolicy Orchestrator® (McAfee® ePO™) build 11.0.0.20. The installation package includes:

- McAfee® Data Loss Prevention Discover (McAfee DLP Discover) server package for McAfee ePO build 11.0.0.103
- McAfee® Help Desk build 2.0.0.130

Also included in this release:

- McAfee DLP Prevent and McAfee DLP Monitor build 3419.102.

McAfee DLP Prevent and McAfee DLP Monitor require these McAfee ePO extensions:

- McAfee DLP Appliance Management 11.0.0.135 and later
- McAfee® Common UI build 1.3.0.258 and later
- McAfee® Appliance Management build 1.0.0.448 and later



McAfee DLP Prevent and McAfee DLP Monitor do not support the upgrade of a pre-release software version. To upgrade to a production release of the software, you must perform a new installation with the production version.

- McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) client for Microsoft Windows 11.0.0.1162
- McAfee® Data Loss Prevention Endpoint for Mac (McAfee DLP Endpoint for Mac) 11.0.0.85
- McAfee DLP diagnostic tool build 11.0.0.44

## McAfee DLP requirements

**Table 1-1 Hardware requirements**

Hardware type	Specifications
Servers	<b>McAfee DLP extension in McAfee ePO</b> <ul style="list-style-type: none"> <li>• RAM — 1 GB minimum (2 GB recommended)</li> <li>• Hard disk — 80 GB minimum</li> </ul>
McAfee DLP Prevent and McAfee DLP Monitor	Hardware appliance: <ul style="list-style-type: none"> <li>• Model 4400</li> <li>• Model 5500</li> <li>• Model 6600</li> </ul>
Endpoint computers	<ul style="list-style-type: none"> <li>• RAM — 1 GB minimum (2 GB recommended)</li> <li>• Hard disk — 300 MB minimum free disk space (500 MB recommended)</li> </ul>
Network	Minimum 100 megabit LAN serving all workstations and the McAfee ePO server

**Table 1-2 Virtual operating systems supported**

System type	Tested Versions
VDI systems	<b>McAfee DLP extension in McAfee ePO</b> <ul style="list-style-type: none"> <li>• Citrix XenDesktop 7.0 and 7.9</li> <li>• VMware View 5.3, 6.0, and 6.2</li> </ul>
Hypervisor	<b>McAfee DLP Prevent and McAfee DLP Monitor</b> <ul style="list-style-type: none"> <li>• VMware vSphere 5.5 or 6.0</li> <li>• VMware Server 5.5 or 6.0</li> </ul>
Remote desktops	<ul style="list-style-type: none"> <li>• Citrix XenApp 6.5 Feature Pack 2, 7.0, and 7.9</li> <li>• Microsoft Remote Desktop</li> </ul>


## Supported platforms, environments, and operating systems

After the initial release of the product, you can get the latest information about supported platforms, environments, and operating systems from the McAfee knowledgebase.

See [KB68147](#) for information about McAfee DLP Endpoint.

For McAfee Network DLP, McAfee DLP Prevent, and McAfee DLP Monitor, see [KB87112](#).

### Supported McAfee ePO and McAfee® Agent versions

Software	Tested Version
McAfee ePO	<ul style="list-style-type: none"> <li>• 5.1.3 or later</li> <li>• 5.3.1, 5.3.2 Hotfix 1144868</li> <li>• 5.9.0</li> </ul> <p>When running McAfee ePO in Microsoft Internet Explorer, use version 10.0 or later.</p>
McAfee Agent for Windows	<ul style="list-style-type: none"> <li>• 4.8.3</li> <li>• 5.0.3</li> <li>• 5.0.4</li> <li>• 5.0.5</li> </ul>
McAfee Agent for Mac	<ul style="list-style-type: none"> <li>• 5.0.2.185 or later (for OS X)</li> <li>• 5.0.4 or later (for macOS Sierra)</li> <li>• 5.0.5</li> <li>• 5.0.6</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">  You must install McAfee Agent 5.0.6.347.1 if you require support for MacOS 10.13 High Sierra.         </div>

The McAfee DLP appliances contain a version of the McAfee Agent which cannot be updated using McAfee ePO. Updates to the McAfee Agent for McAfee DLP appliances are delivered through patch updates.

### Compatible McAfee products

The McAfee DLP Endpoint client for Windows in this release has been tested for compatibility with the following McAfee managed product versions.

McAfee managed product	Tested versions
McAfee® Application Control	7.0.1 and 8.0.0.651
McAfee® Client Proxy	2.3.1
McAfee® Data Exchange Layer (DXL)	3.0.1 and 3.1.0
McAfee® Threat Intelligence Exchange (TIE) for Endpoint Security	1.3 and 10.2.2
McAfee® Drive Encryption	7.1.3 and 7.2.1
McAfee® Endpoint Security	10.2.1 and 10.5.1
McAfee® File and Removable Media Protection (FRP)	4.3.1.Hotfix 2, 5.0.2, and 5.0.3 McAfee File and Removable Media Protection 6.0 is supported to synchronize policy with the cloud.
McAfee® Host Intrusion Prevention System	8.0 patch 8 and patch 9
McAfee® Management of Native Encryption (MNE)	4.1.1
McAfee® Policy Auditor	6.2.2
McAfee® Risk Advisor	2.7.2
McAfee® Rogue System Detection (RSD)	5.0.4 and 5.0.5

McAfee managed product	Tested versions
McAfee® SiteAdvisor® Enterprise	3.5.5
McAfee® Virtual Technician	8.1.0
McAfee® VirusScan® Enterprise	8.8 patch 8 and patch 9

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

The McAfee DLP appliances have been tested for compatibility with the following McAfee managed product versions:

McAfee® Logon Collector 3.0.2.

### Supported software

McAfee DLP Endpoint 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	4.0.78
	Dropbox	25.4.28
	Google Drive	2.34
	iCloud	6.2.1
	Microsoft OneDrive	17.0.2015 – 17.3.6816.0313
	Syncplicity	4.5.3.920
Security and encryption applications	Microsoft Active Directory Rights Management Service (AD RMS)	2008 and 2012
	MobileIron	8.5.0
	MobileIron AdminPortal	8.5.0
	MobileIron Sentry	7.6.0
	Seclore FileSecure Policy Server	2.78.0.0
	Seclore Desktop Client	2.43.0.0
	Stormshield Data Security	9.1.20688
	Titus Classification Suite	4.6 HF 3
	Titus SDK	3.1.9.9
	TrueCrypt	7.0.1
Office and productivity applications	Adobe Acrobat Pro	X and XI
	Adobe Reader	11 and DC
	Google Chrome, 32-bit	37.0.2062.103 – 58.0.3029.96 (not including 54.x)
	Google Chrome, 64-bit	37.0.2062.103 – 58.0.3029.96 (not including 54.x)
	Lotus Notes client software	8.5.3 and 9.0.1
	Microsoft Edge	Microsoft Edge 40.15063.0.0 for RS2 is not supported. See <a href="#">KB89089</a> .
	Internet Explorer	11
	Microsoft Office, 32-bit and 64-bit	2010, 2013 SP1, and 2016

Application Type	Software	Tested Versions
	Microsoft Outlook, 32-bit and 64-bit	2010, 2013 SP1, and 2016
	Microsoft SharePoint	2010 and 2013
	Mozilla Firefox, 32-bit and 64-bit	48-53

## New features

The current release of the product includes these new features.

### McAfee DLP

**Incident Analytics** — A new tab on the **DLP Incident Manager** displays six charts that summarize the incident list. Each chart has a filter to adjust the display.

**Stakeholders** — McAfee DLP defines stakeholders as anyone with an interest in a particular incident, event, or case. It sends automatic emails to the stakeholders' list when an incident, event, or case is created or changed. Stakeholders can be added to the list automatically or manually to specific incidents, events, or cases.

### McAfee DLP Endpoint

**Web application control rules** — Application control rules monitor or block websites by URL, blocking all GET requests and preventing all access to the specified URL. Web application control rules are supported on McAfee DLP Endpoint for Windows.

### McAfee DLP Endpoint for Mac

#### Support for manual classifications

Mac users can now manually apply content fingerprints or content classifications to their files.

#### Cloud protection rules

McAfee DLP Endpoint for Mac can now manage files uploaded to cloud applications.

### McAfee DLP Discover

**Support for database scans** — McAfee DLP Discover can now scan the following databases:

Database Vendor	Version	Tested build number
Microsoft SQL	SQL Server 2008 R2	10.50.6000
	SQL Server 2012	11.0.5085
	SQL Server 2016	13.0.1601
MySQL, commercial editions only	5.7	5.7.17e
Oracle	Oracle Database 11g Release 2	11.2.04
	Oracle Database 12c Release 1	12.1.0.2



DB2 database scanning will be made available after the McAfee DLP 11.0 release as a patch update.

**Registered document support** — A new scan type, **Document Registration**, scans CIFS, SharePoint, or Box repositories and extracts fingerprint signatures. The signatures are stored in a master database and distributed to slave databases throughout the network. Databases can be distributed across LANs or LAN/WAN networks.

---

## Enhancements

The current release of the product includes these enhancements.

### McAfee DLP

The McAfee DLP console in McAfee ePO has the following enhancements:

- **Out-of-the-box classifications** — The **Classification** console contains many predefined classifications and definitions that can be used as-is or duplicated and changed. Source code classification is now included, and the classifications have been improved to reduce false positives.
- **Incident access by type** — The Permission Sets setting for **Incident Manager** includes an **Incident Access by Type** setting. Specified reviewers can view any combination of data protection, device control, endpoint discovery, or network discovery incidents.
- **Custom resolution and status** — Settings in the **DLP Settings** console allow you to create custom resolution and status definitions for DLP Incident Manager, DLP Operations, and Case Management.
- **Dictionary definitions** — Dictionary definitions are now in a single table, with a **Quick find** option to speed up editing.
- **Email incidents** — Email addresses and display names are now listed on the incident detail page.
- **Event Parser enhancements** — The Event Parser has improved performance.
- **DLP Appliance Management extension** — The McAfee DLP Prevent extension for McAfee ePO is now the **DLP Appliance Management** extension and includes settings for McAfee DLP Monitor.

### McAfee DLP Endpoint for Windows

- **DLP Chrome extension** — When **Supported Chrome versions** is not updated in the client policy, the DLP Chrome extension blocks file uploads and monitors text uploads.
- **User Notification** — User notifications can display Rich Text by inserting HTML code in the definition.
- **End-User groups** — Added support for domain\name format (MSDS principal name).
- **Improved Classification of Compound Files** — The McAfee DLP classification engine now analyzes embedded files separately. For example, when classifying a ZIP or Microsoft Office file, it applies the classification to each embedded file.
- **Removable storage protection rules** — Removable storage protection rules have enhanced performance. McAfee DLP Endpoint now allows the operating system to copy all analyzed files that do not contain sensitive information when a folder is copied to removable storage.  
Removable storage protection rules can now block incoming and outgoing files. The rule can now protect files copied from the removable storage to the local hard drive.
- **Endpoint Discovery Rule** — Messages quarantined by a McAfee DLP email scan now have a McAfee shield icon next to them in a user's inbox or .PST folder in Microsoft Outlook.

### McAfee DLP Endpoint for Mac

- This version of McAfee DLP Endpoint for Mac supports MacOS 10.13 (High Sierra).



You must install McAfee Agent 5.0.6.347.1 if you require support for MacOS 10.13 High Sierra.

- Incidents now report the short match string, which contains up to three hit highlights as a single string.
- Incidents and operational events now report the user principal name (UPN).

- Removable storage protection rule incidents in the DLP Incident Manager now report all device properties.
- Removable storage device rules and plug-and-play device rules now support serial number and user exceptions.

### McAfee DLP Monitor

McAfee DLP 11.0 includes McAfee DLP Monitor with the following enhancements:

- **Unified policy management** — McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) and McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor) share a common classification engine and policies.
- **Unified incident and case management** — View McAfee DLP Monitor incidents and cases in the standard McAfee® ePolicy Orchestrator® (McAfee® ePO™) dashboard. McAfee ePO can manage up to 50 million incidents.
- **Common text extraction engine** — The common text extraction engine provides consistency between McAfee DLP Endpoint and McAfee DLP Monitor for the types of files where text can be extracted and analyzed.

## 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.

**Table 4-1 McAfee DLP issues**

Reference	Issue description
CVE-2017-3948	The cross site scripting (XSS) vulnerability in IMG tags has been fixed.
1176005	McAfee DLP Discover server package can now be installed locally. All components now install and initialize properly when the installation is run as an administrator.
1194751	The issue with Microsoft Internet Explorer has been resolved. Internet Explorer no longer hangs when McAfee DLP Endpoint client is installed.
	Issues with Google Chrome 58.0.3029.81 have been resolved. Chrome no longer hangs when McAfee DLP Endpoint client is installed.
1160509	Console no longer slows down when running McAfee DLP queries.
1178131	McAfee DLP queries do not cause high CPU usage in the SQL server.
1178714	Total content size column displays correctly in reports and in the DLP Incident Manager.
1180655	DLP Incident Manager correctly displays multiple incidents across multiple pages. The display no longer locks on a single page.
1181605	Filtered incidents are displayed correctly. All options, including next page, are displayed correctly.
1182201	Nvarchar values no longer overflow integer columns.
118329	Nvarchar data types convert correctly to datetime data types in German.
1186011	McAfee DLP queries consistently return results. The issue of McAfee ePO timing out is resolved.
1186545	When classification name is used in filters, all incidents are displayed. The issue of missing incidents is resolved.
1159682	You can now use the comparison <b>Contains</b> when defining a USB device serial number in a device definition.
1158617	The McAfee DLP UI for protection rule exclusions no longer lock up when the McAfee ePO language is set to German.

**Table 4-1 McAfee DLP issues (continued)**

Reference	Issue description
1156561	Drilling down into an incident in McAfee ePO <b>Queries and Reports</b> displays the same properties that are displayed in the incident in the DLP Incident Manager.
1156646	Threat events log and Incident List events now match.

**Table 4-2 McAfee DLP Endpoint issues**

Reference	Issue description
1173261	The <b>Modified</b> time stamp is now reported correctly when copying a file with 0 KB to a network share. The problem was caused by McAfee DLP Endpoint clearing tags, which changes the modified time. The time is now saved and restored after the file is copied.
1163596	Email protection rules to block external emails no longer block mail to internal distribution lists.
1146792	McAfee DLP Endpoint now works with the UniAccess application, and does not prevent Microsoft Word, Internet Explorer, or Google Chrome from launching.
1167816	Microsoft Outlook no longer crashes when sending a reply or accessing a calendar. The issue was resolved by adding checks for NULL for a list of properties.
1168337	Application file access protection rules now work correctly with QQ instant messaging. The issue was caused by QQ using LoadLibrary API. McAfee DLP Endpoint now checks that the file is opened as a data file in LoadLibrary.
1177547	Application file access protection rules now work correctly with wandoujia.exe mobile phone data transfer.
1174397	Shutting down a VDI client running on XenDesktop 7.8 does not cause a blue screen. The issue was resolved by changing the order in which McAfee DLP checks problem codes to see if it is disabling devices.
1129866	Microsoft Office OpenXML files are now blocked correctly when uploaded using the Google Chrome browser. The issue was caused by Chrome opening other files with the same headers. The McAfee DLP Endpoint client now has a mechanism to create unique headers in Chrome.

### McAfee DLP Prevent resolved issues

McAfee DLP Prevent includes Network Time Protocol (NTP) version 4.2.8 patch 10 to address the CVE-2016-9042 vulnerability in the ntpd server.

McAfee DLP 11.0 contains all McAfee DLP Prevent fixes up to version 10.0.203.

---

## Installation information

For information about installing or upgrading McAfee DLP software, see *McAfee Data Loss Prevention Product Guide*.

---

## Known issues

For a list of known issues in this product release, see the McAfee KnowledgeBase 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](https://sns.secure.mcafee.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.

### Product documentation

Every McAfee product has a comprehensive set of documentation.

*McAfee Data Loss Prevention Product Guide*

*McAfee Data Loss Prevention Release Notes*

*McAfee Data Loss Prevention Hardware Guide*

*McAfee Data Loss Prevention Appliances Quick Start*

*McAfee Data Loss Prevention Migration Guide*

For corrections related to the McAfee Data Loss Prevention 11.x product documentation, see [KB89326](#).