Release Notes

FortiDLP Agent 12.5.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 23, 2026
FortiDLP Agent 12.5.0 Release Notes
92-100-000000-20250116

TABLE OF CONTENTS

Introduction

These release notes describe the new features and enhancements, resolved issues, known limitations, and updates related to FortiDLP Agent version 12.5.0.

Intended audience

These release notes are intended for anyone interested in learning about the FortiDLP Agent 12.5.0 release.

Related documentation

- *FortiDLP Agent Deployment Guide*

Current release

This section describes the FortiDLP Agent 12.5.0 release.

12.5.0

Released April 14th, 2026

New features and enhancements in 12.5.0

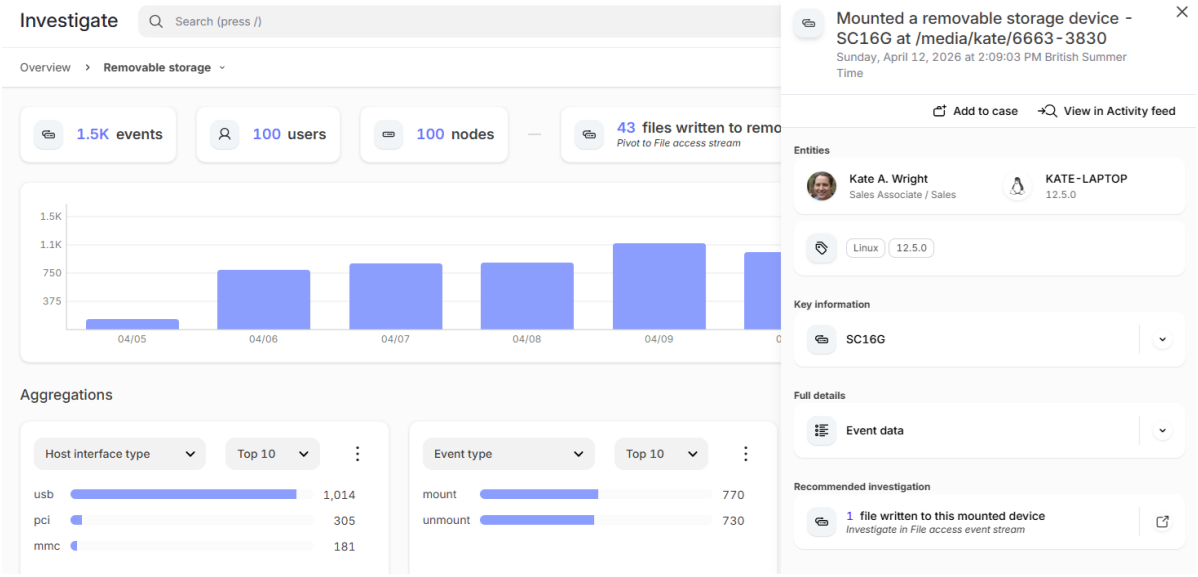
This release delivers the following new features and enhancements.

Enhanced removable storage visibility and device controls

Gain total insight into removable storage use and stop unauthorized devices from mounting.

The FortiDLP Agent now tracks mount activity for all removable storage media and blocks the mounting of unapproved volumes. This feature extends data loss prevention beyond traditional USB storage—for example, to integrated SD card readers—removing blind spots and allowing safe removable storage usage.

You can view storage mount and unmount events in the new *Removable storage* event stream, which provides detailed device and volume information. From there, you can also easily pivot to events for files written to removable storage. And to reduce the risk of data exfiltration and compliance violations, you can use the *Block removable storage volume mount* action.



This feature is supported on all OSes with FortiDLP Policies 8.6.0+.

For more information, see:

- Event streams and Block removable storage volume mount in the *FortiDLP Console User Guide*, and
- the Unauthorized removable storage volume mounted template in the *FortiDLP Policies Reference Guide*.

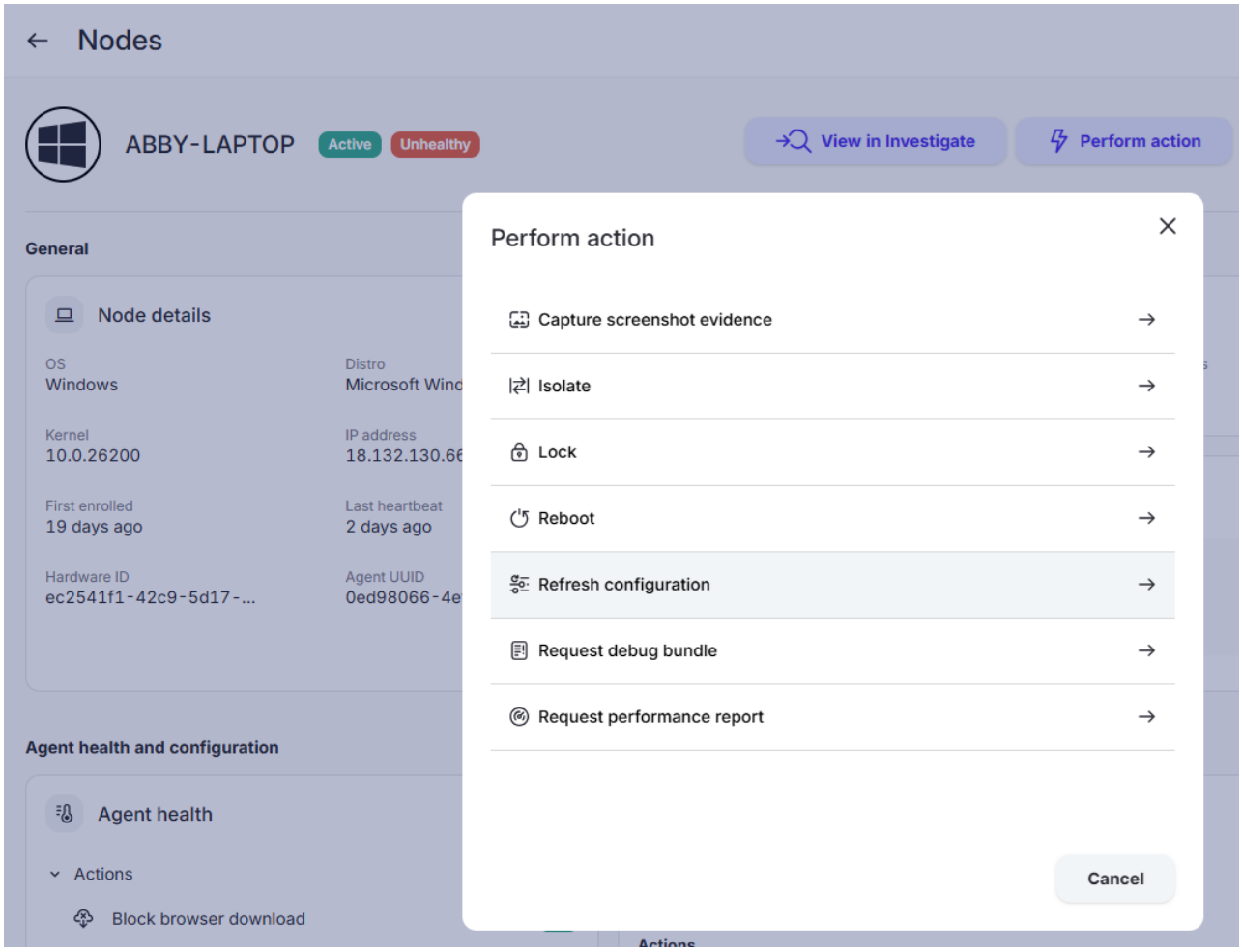
The *USB device* event stream will remain supported, capturing attach events for USB storage and composite devices.

Review related policies if you customized the detection description for the *Unauthorized USB storage device inserted* template (now renamed to *Unauthorized removable storage volume mounted*) to ensure the upgrade completed successfully.

'Refresh configuration' action

You can now apply configuration updates to nodes on demand.

Instead of waiting for new settings to propagate (which happens every five minutes by default), you can use the *Refresh configuration* action to immediately retrieve policy and Agent configuration updates and put them into effect on a node.



This action is supported on all OSes and can be executed manually via the *Nodes* module.

For more information, see Refresh configuration in the *FortiDLP Console User Guide*.

German Personally Identifiable Information (PII) policy assets

New policy assets are available to detect unauthorized activities involving German PII.

These content inspection pattern assets are provided with FortiDLP Policy Templates 8.6.0 and are supported on all OSes.

For more information, see Out-of-box assets in the *FortiDLP Policy Assets Reference Guide*.

Deployment considerations in 12.5.0

We have moved the Windows Agent's content inspection process binary to a new directory to optimize upgrades.

To ensure interoperability, update your antivirus scanning exclusions to replace the previous process path with the new one.

- Old path: `C:\Program Files\Jazz Networks\Agent\contentng\contentng.exe`
- New path: `C:\Program Files\Jazz Networks\Agent\content-inspector\contentng.exe`

For more information, see Excluding FortiDLP Agent processes, directories, and files from antivirus scanning in the *FortiDLP Agent Deployment Guide*.

Resolved issues in 12.5.0

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(es)	Description
G19788	All	During keyword matching, the content inspection process did not release memory as expected, which could lead to increased memory usage over time.
G19159	All	Detection of OpenSSL-encrypted files was unreliable.
• M1167824 • G18544	All	Detection of large, encrypted DOC and XLS files was unreliable.
• M1168259 • G19779	All	Detection of RAR files was only supported if the file names of the contained files were encrypted.
G19778	• Windows • macOS	The Agent process stopped unexpectedly when certain printing policies were triggered.

Bug ID	Affected OS(es)	Description
G19639	• Windows • macOS	Misconfigured Agent HTTP proxy server settings caused the Agent to stop unexpectedly.
G19643	• Windows • macOS	Basic authentication credentials used for Agent proxy server authentication were recorded in the Agent log.
M1171535	Windows	Previously, if Google Drive for Desktop was in a non-English language, the Agent could not generate policy detections for activity on this app.
G19550	Windows	In rare cases, following an upgrade, the Agent stopped unexpectedly when initializing Microsoft sensitivity label inspection.
G19377	Windows	Occasionally, the Agent did not report *File access* events.
G19436	Windows	When Agent tamper protection was enabled, the MSI installer's repair function could not be used.
G19635	Windows	When the MSI installer's repair function was used, drivers were not reinstalled. This prevented the repair and required the Agent to either be upgraded or uninstalled.
M1271380	Windows	Under certain circumstances, the Agent removed externally-managed browser registry key configurations.
• G19242 • M1236819 • M1238253	macOS	Certain *USB device* event information was inconsistent with Windows and Linux.
M1225437	macOS	Performance improvements have been made to the Endpoint Security System Extension.
G19547	macOS	Agent performance reports did not include graphical CPU and memory information for the Agent process.
G19355	Linux	A failed login could result in the Agent using excessive CPU, causing performance issues until the node restarted.
M1233360	Linux	The Agent could not be installed on Red Hat Enterprise Linux 9.6 due to a kernel version numbering update.
G12592	Linux	The Agent's content inspection process has been sandboxed for increased security.
G19787	Linux	A communication failure between the Agent process and the content inspection process caused the content inspection process to stop unexpectedly.

Resolved issues for the FortiDLP Browser Extension

Bug ID	Affected OS(es)	Description
M1237311	All	In rare cases, compatibility issues with certain websites caused unexpected behavior.

Bug ID	Affected OS(es)	Description
		 This fix requires a future FortiDLP Policies release, following FortiDLP Policies 8.6.0.
G19676	All	Improvements have been made to Agent health reporting.

Resolved issues for the FortiDLP Email Add-in and FortiDLP Email Plugin (Legacy)

Bug ID	Affected OS(es)	Description
G19676	• Windows • macOS	Improvements have been made to Agent health reporting for the FortiDLP Email Add-in.
M1224963	Windows	Where the FortiDLP Email Plugin (Legacy) was enabled, the *Send* button in classic Outlook was sometimes unresponsive during email replies.
M1233378	Windows	Where the FortiDLP Email Plugin (Legacy) was enabled, an unexpected DAT file was sometimes attached to emails sent from a classic Outlook mailbox that was not hosted by Exchange.

Known limitations in 12.5.0

This release has the following known limitations.

Existing known limitations

The following limitations have been identified in a previous FortiDLP Agent version and remain in FortiDLP Agent 12.5.0.

Existing known limitations

Bug ID	Affected OS(es)	Description
G19100	Windows	Origin tracking cannot be performed on files that are dragged and dropped to classic Outlook.
G17162	• Windows • macOS	A known issue with Outlook's add-in service may interfere with the FortiDLP Email Add-in, which can cause a dialog box to be displayed when a user sends an email.
M1173708	All	When Microsoft Edge is used, file uploads to Microsoft Copilot cannot be detected. On Windows, the Copilot sidebar can be disabled by setting the `HKLM/SOFTWARE/Policies/Microsoft/Edge/HubsSidebarEnabled` registry key to `0`.
G17561	• Windows	Data lineage information is not reported for file deletion operations.

Bug ID	Affected OS(es)	Description
	• macOS	
G18057	macOS	Secure Data Flow (origin and lineage) copy tracking is supported on macOS 13.4+.
G17690	All	For browser-based web request policies—for example, those involving form submissions—content inspection is limited to the first 16 KiB of the raw web request body to maintain browser stability. This limitation does not affect file uploads, clipboard operations, or other file-based content inspection channels.
G17058	All	Microsoft sensitivity label inspection is not supported for encrypted files.
• G17543 • G14710	• Windows • macOS	Wi-Fi connection events are not supported for Windows 11 24H2, Windows 11 24H2 (LTS), or macOS 14.5 or later.
• G14247 • G15123 • G15017	All	Web login user account context is not recognized for password-free logins, where a one-time code, face, fingerprint, pin, or security key is used for authentication. Such logins will be reported as unknown logins. Further, two-factor authentication (2FA) logins may generate detections regardless of users successfully authenticating using this method.  If the *SaaS apps* policy template parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the *Unknown User account types* checkbox. For details, see the *FortiDLP Policies Reference Guide*.
G15467	Windows	Content inspection cannot be performed on any part of a file that has been converted into image format. This applies to most print jobs sent from a browser, as the entire print job is often an image file, and sometimes applies to PDFs that are created via the print to/save to PDF operations from a source file having specifically formatted word boundaries.
G12150	• Windows • macOS	The *Unauthorized text typed* and *Unauthorized text typed into website* policy templates cannot detect keywords that use the following keys: • Windows: `Ctrl`, `Alt`, `AltGr`, `Win`, `Fn`. • macOS: `Control`, `Option`, `Command`, `Fn`.
G13836	• Windows • macOS	Regex pattern matches cannot be detected by the *Unauthorized email sent or received* policy template when content that is separated by line breaks is pasted into the email body of new Outlook. This limitation does not apply to classic Outlook.

Bug ID	Affected OS(es)	Description
G12880	All	Content inspection cannot be performed on files that are not saved locally and are dragged and dropped to browsers or are copied and pasted to browsers.
G8267	All	Due to a limitation present in Chromium-based browsers, when upload blocking policies are enabled, file directories cannot be uploaded using drag and drop. In this situation, a banner will display to instruct the user to use the file selector instead.

Previous releases

This section describes the recent releases previous to FortiDLP Agent 12.5.0.

12.4.2

Released January 13th, 2026 | Updated March 12th, 2026

New features and enhancements in 12.4.2

This release delivers the following new features and enhancements.

Direct enrollment via Microsoft GPO

It's now simpler to deploy the FortiDLP Agent using Microsoft GPO.

By configuring a GPO registry item with an enrollment code, you can seamlessly install and enroll the Agent on targeted devices.

For more information, see Bulk deploying the FortiDLP Agent to Windows in the *FortiDLP Agent Deployment Guide*.

Deployment considerations in 12.4.2

This release introduces the following new process and files for print monitoring on Windows devices. Exclude them from your antivirus scanning to ensure interoperability.

- `C:\Program Files\Jazz Networks\Agent\arm64\withdll.exe`
- `C:\Program Files\Jazz Networks\Agent\spool_shim.dll`
- `C:\Program Files\Jazz Networks\Agent\arm64\spool_shim.dll`

For more information, see Excluding FortiDLP Agent processes, directories, and files from antivirus scanning in the *FortiDLP Agent Deployment Guide*.

Resolved issues in 12.4.2

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(es)	Description
G19208	All	The Agent could stop unexpectedly during keyword content inspection.
G19040	All	The Agent could use excessive CPU when identifying applications. Improvements have been made to reduce this.
• M1203747 • G19383	All	Content inspection was not supported for Roshal ARchive (RAR) files.
G19282	All	Occasionally, if an error occurred during content inspection, the file could not be modified or deleted until the Agent restarted.
M1230539	• Windows • macOS	For Agent Proxy Support, if the `proxy_pac_file_url` key was used, and the script file was returned with a compressed encoding by the HTTP server, the file would be rejected.
G19378	Windows	The Agent could stop unexpectedly during device shutdown.
G18845	Windows	Some FortiEDR processes were not part of out-of-box process exclusion.
G19379	Windows	Improvements have been made to reduce interference with user applications on which content inspection is running.
G19380	Windows	Improvements have been made to the reliability of the Agent kernel module installation.
G19020	macOS	Sometimes, non-Latin characters were incorrectly rendered in the *Display message* dialog box.
G18938	macOS	Improvements have been made to the synchronization of keyword matching during content inspection.
M1219567	Linux	The Firefox Agent health component could fail to identify when Firefox was running, resulting in an incorrect state of `unused`.
G19381	Linux	Improvements have been made to the reliability of user session tracking.
G19382	Linux	Improvements have been made to the reliability of device identification.
G18820	Linux	Improvements have been made to the reliability of Agent installation.
G19003	Linux	The Agent kernel module had a compatibility issue with Linux 6.18.0.

Known limitations in 12.4.2

This release has the following known limitations.

New known limitations

The following limitations have been identified in FortiDLP Agent version 12.4.2.

New known limitations

Bug ID	Affected OS(es)	Description
M1171535	Windows	If Google Drive for Desktop is in a non-English language, the Agent cannot generate policy detections for activity on this app.

Existing known limitations

The following limitations have been identified in a previous FortiDLP Agent version and remain in FortiDLP Agent 12.4.2.

Existing known limitations

Bug ID	Affected OS(es)	Description
G19100	Windows	Origin tracking cannot be performed on files that are dragged and dropped to classic Outlook.
G17162	• Windows • macOS	A known issue with Outlook's add-in service may interfere with the FortiDLP Email Add-in, which can cause a dialog box to be displayed when a user sends an email.
M1173708	All	When Microsoft Edge is used, file uploads to Microsoft Copilot cannot be detected. On Windows, the Copilot sidebar can be disabled by setting the `HKLM/SOFTWARE/Policies/Microsoft/Edge/HubsSidebarEnabled` registry key to `0`.
G17561	• Windows • macOS	Data lineage information is not reported for file deletion operations.
G18057	macOS	Secure Data Flow (origin and lineage) copy tracking is supported on macOS 13.4+.
G17690	All	For browser-based web request policies—for example, those involving form submissions—content inspection is limited to the first 16 KiB of the raw web request body to maintain browser stability. This limitation does not affect file uploads, clipboard operations, or other file-based content inspection channels.

Bug ID	Affected OS(es)	Description
G17058	All	Microsoft sensitivity label inspection is not supported for encrypted files.
• G17543 • G14710	• Windows • macOS	Wi-Fi connection events are not supported for Windows 11 24H2, Windows 11 24H2 (LTS), or macOS 14.5 or later.
• G14247 • G15123 • G15017	All	Web login user account context is not recognized for password-free logins, where a one-time code, face, fingerprint, pin, or security key is used for authentication. Such logins will be reported as unknown logins. Further, two-factor authentication (2FA) logins may generate detections regardless of users successfully authenticating using this method.  If the *SaaS apps* policy template parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the *Unknown User account types* checkbox. For details, see the *FortiDLP Policies Reference Guide*.
G15467	Windows	Content inspection cannot be performed on any part of a file that has been converted into image format. This applies to most print jobs sent from a browser, as the entire print job is often an image file, and sometimes applies to PDFs that are created via the print to/save to PDF operations from a source file having specifically formatted word boundaries.
G12150	• Windows • macOS	The *Unauthorized text typed* and *Unauthorized text typed into website* policy templates cannot detect keywords that use the following keys: • Windows: `Ctrl`, `Alt`, `AltGr`, `Win`, `Fn`. • macOS: `Control`, `Option`, `Command`, `Fn`.
G13836	• Windows • macOS	Regex pattern matches cannot be detected by the *Unauthorized email sent or received* policy template when content that is separated by line breaks is pasted into the email body of new Outlook. This limitation does not apply to classic Outlook.
G12880	All	Content inspection cannot be performed on files that are not saved locally and are dragged and dropped to browsers or are copied and pasted to browsers.
G8267	All	Due to a limitation present in Chromium-based browsers, when upload blocking policies are enabled, file directories cannot be uploaded using drag and drop. In this situation, a banner will display to instruct the user to use the file selector instead.

Operating system support updates in 12.4.2

This release contains the following OS support updates.

New support

This Agent version is the first to support Windows ARM64 processors (requires Windows 11).

Ending support

This Agent version is the last to support macOS Ventura 13.

12.3.2

Released October 28th, 2025

New features and enhancements in 12.3.2

This release delivers the following new features and enhancements.

Out-of-box process exclusion

The FortiDLP Agent now automatically excludes process binaries for common security and IT tools.

To avoid interference with trusted endpoint tools and optimize performance, the Agent provides process exclusion by default for all OSes.

The new out-of-box process exclusion list will be combined with administrator-configured process exclusion lists to disable monitoring of approved software.

For more information, see Out-of-box process exclusion.

Dynamic browser and email app identification

The FortiDLP Agent now dynamically retrieves the latest identification information, for example, code-signing certificates, of browser and email apps that it needs to communicate with, so an Agent upgrade is no longer required to accommodate this.

Resolved issues in 12.3.2

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(es)	Description
G18689	All	In performance reports, process event counts could be inaccurate for processes that did not run for the whole sample window.
M1166974	All	Improvements have been made to the reliability of content inspection for form data on websites.
G18700	All	Improvements have been made to the reliability of content inspection for source code.
G19083	All	Improvements have been made to the reliability of Agent communications.
G19084	All	Improvements have been made to content inspection memory consumption.
G18051	All	The *Content Inspection* Agent health component did not have a description.
M1195483	Windows	If there was a syntax error in a content inspection pattern for clipboard or email policies, the contents of the email or clipboard was reported in the error log.
G19018	Windows	For Agent Proxy Support (Preview), if the `proxy_pac_file_ url` GPO registry key was updated, this would only be applied to the PAC script after 24 hours. The script is now refreshed immediately after the update.
M1193321	Windows	The Agent previously did not detect optical USB drives, such as DVD players.
G19085	Windows	If certain logs were not created, the Agent could stop unexpectedly.
G19086	Windows	Rarely, USB blocking could cause the Agent to stop unexpectedly.
G18579	macOS	More files than expected were tracked for origin-based tracking, resulting in higher system resource usage than necessary.
G19087	macOS	The Agent could stop unexpectedly if the operating system could not provide internal storage information.
M1201768	Linux	Improvements have been made to reduce excessive log messages.
G19088	Linux	Improvements have been made to prevent the Agent kernel module from being removed from the running kernel.
G19089	Linux	Improvements have been made to the robustness of the Agent module kernel loader.

Resolved issues for the FortiDLP Browser Extension

Bug ID	Affected OS(es)	Description
M1187383	All	For a file download that is encoded in the browser, the tab name is now attributed to the browser event instead of the data URL.
G19090	All	Version 3.5.5 of the FortiDLP Browser Extension for Firefox is now bundled with the Agent for backward compatibility.

Known limitations in 12.3.2

This release has the following known limitations.

New known limitations

The following limitations have been identified in FortiDLP Agent version 12.3.2.

New known limitations

Bug ID	Affected OS(es)	Description
G19100	Windows	Origin tracking cannot be performed on files that are dragged and dropped to classic Outlook.
G17162	• Windows • macOS	A known issue with Outlook's add-in service may interfere with the FortiDLP Email Add-in, which can cause a dialog box to be displayed when a user sends an email.

Existing known limitations

The following limitations have been identified in a previous FortiDLP Agent version and remain in FortiDLP Agent 12.3.2.

Existing known limitations

Bug ID	Affected OS(es)	Description
M1173708	All	When Microsoft Edge is used, file uploads to Microsoft Copilot cannot be detected. On Windows, the Copilot sidebar can be disabled by setting the `HKLM/SOFTWARE/Policies/Microsoft/Edge/HubsSidebarEnabled` registry key to `0`.
G17561	• Windows • macOS	Data lineage information is not reported for file deletion operations.
G18057	macOS	Secure Data Flow (origin and lineage) copy tracking is supported on macOS 13.4+.

Bug ID	Affected OS(es)	Description
G17690	All	For browser-based web request policies—for example, those involving form submissions—content inspection is limited to the first 16 KiB of the raw web request body to maintain browser stability. This limitation does not affect file uploads, clipboard operations, or other file-based content inspection channels.
G17058	All	Microsoft sensitivity label inspection is not supported for encrypted files.
• G17543 • G14710	• Windows • macOS	Wi-Fi connection events are not supported for Windows 11 24H2, Windows 11 24H2 (LTS), or macOS 14.5 or later.
• G14247 • G15123 • G15017	All	Web login user account context is not recognized for password-free logins, where a one-time code, face, fingerprint, pin, or security key is used for authentication. Such logins will be reported as unknown logins. Further, two-factor authentication (2FA) logins may generate detections regardless of users successfully authenticating using this method.  If the *SaaS apps* policy template parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the *Unknown User account types* checkbox. For details, see the *FortiDLP Policies Reference Guide*.
G15467	Windows	Content inspection cannot be performed on any part of a file that has been converted into image format. This applies to most print jobs sent from a browser, as the entire print job is often an image file, and sometimes applies to PDFs that are created via the print to/save to PDF operations from a source file having specifically formatted word boundaries.
G12150	• Windows • macOS	The *Unauthorized text typed* and *Unauthorized text typed into website* policy templates cannot detect keywords that use the following keys: • Windows: `Ctrl`, `Alt`, `AltGr`, `Win`, `Fn`. • macOS: `Control`, `Option`, `Command`, `Fn`.
G13836	• Windows • macOS	Regex pattern matches cannot be detected by the *Unauthorized email sent or received* policy template when content that is separated by line breaks is pasted into the email body of new Outlook. This limitation does not apply to classic Outlook.
G12880	All	Content inspection cannot be performed on files that are not saved locally and are dragged and dropped to browsers or are copied and pasted to browsers.
G8267	All	Due to a limitation present in Chromium-based browsers, when upload blocking policies are enabled, file directories cannot be uploaded using drag and drop.

Bug ID	Affected OS(es)	Description
		In this situation, a banner will display to instruct the user to use the file selector instead.

Operating system support updates in 12.3.2

This release contains the following OS support updates.

New support

This Agent version provides support for Windows 11 25H2.

Ending support

This Agent is the last to support Windows 10 22H2 and Windows 11 22H2.

Deploying and maintaining the FortiDLP Agent

For detailed information regarding deploying, upgrading, and downgrading the FortiDLP Agent, see the *FortiDLP Agent Deployment Guide*.

www.fortinet.com