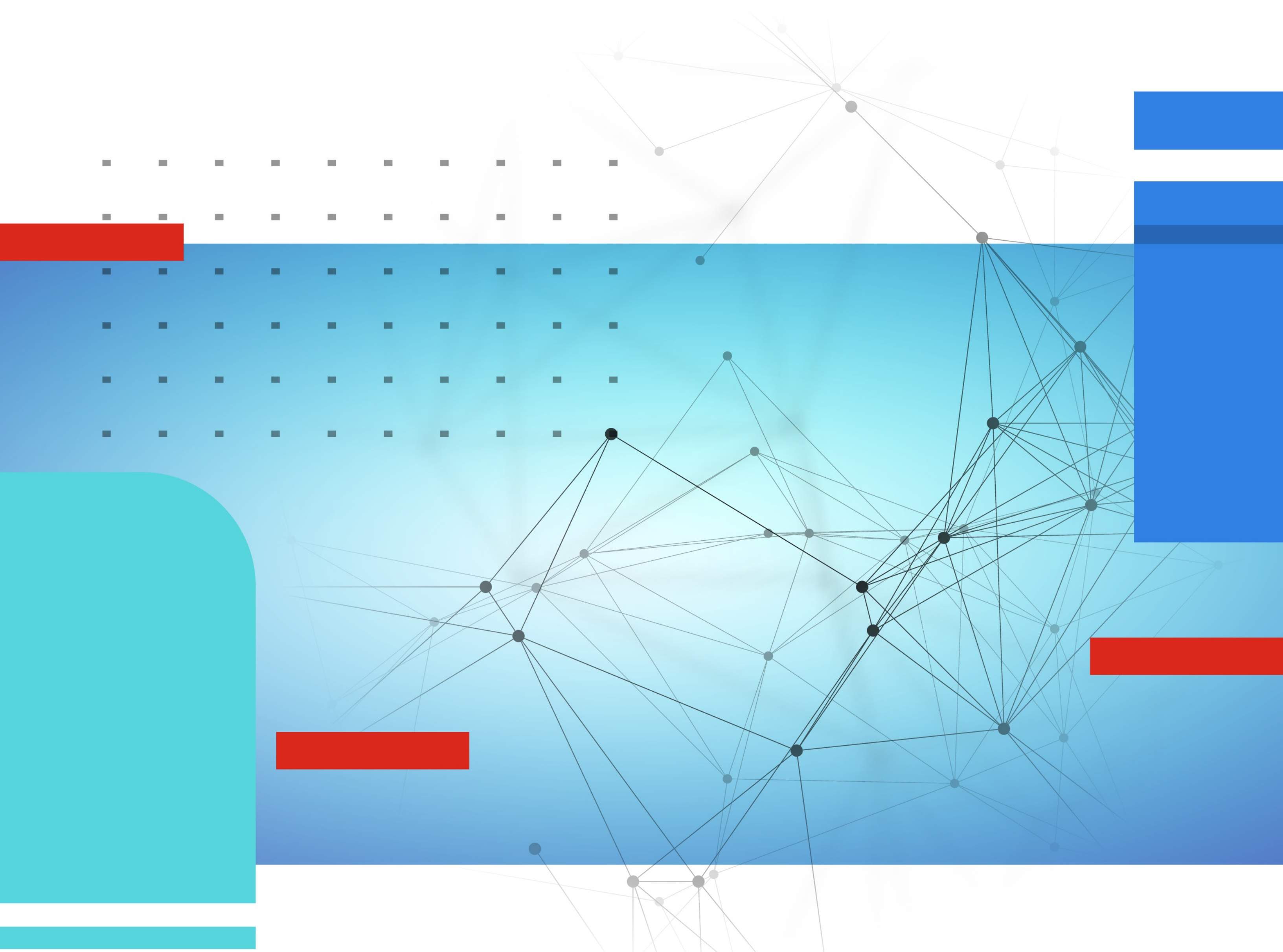
Release Notes

FortiDLP Agent 12.2.2



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

August 06, 2025
FortiDLP Agent 12.2.2 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 12.2.2.

Intended audience

These release notes are intended for anyone interested in learning about the FortiDLP Agent 12.2.2 release.

Related documentation

- *FortiDLP Agent Deployment Guide*

Current release

This section describes the FortiDLP Agent 12.2.2 release.

12.2.2

Released August 6th, 2025

New features and enhancements in 12.2.2

This release delivers the following new features and enhancements.

Windows Agent configuration default setting updates

To prevent interference with trusted security tools and tampering with the Agent out-of-the-box, the following Windows Agent configuration group options are now enabled by default:

- *Anti-malware process name exclusion*
- *Agent anti-tampering*.

If you do not require tamper protection, you should explicitly set the *Agent anti-tampering* option to *Off*.

For more information, see Agent configuration groups in the *FortiDLP Administration Guide*.

Resolved issues in 12.2.2

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(s)	Description
M1184270 M1184291	Windows	Previously, the Agent rejected the connection from the FortiDLP Email Plugin (Legacy) because it did not recognize Microsoft's recently updated code-signing certificate. This caused classic Outlook email events to go unreported.

Bug ID	Affected OS(s)	Description
		The Agent now accepts the new code-signing certificate, allowing monitoring for classic Outlook via the FortiDLP Email Plugin (Legacy) with FortiDLP Agent 12.2.2+. Email monitoring of classic Outlook for earlier Agent versions remains unsupported.
M1179134	Windows	In some cases, the content inspection process stopped unexpectedly and failed to restart.
G18424	Windows	If an error occurred that prevented the *Private browsing* Agent configuration group option from being set, the failure was not logged.
M1146970	Windows	The *Block print job* action was sometimes unreliable for the *Sensitive document printed using physical printer* policy template.
G16815	macOS	The Agent process sometimes stopped unexpectedly when certain system information was unavailable.
M1175190	macOS	When very long arguments were passed to a process, the Agent consumed an unexpected amount of disk space. Additionally, if muted processes ran and exited frequently, the Agent used larger than expected amounts of disk space.
G18430	Linux	Under certain circumstances, file rename tracking was unreliable.

Resolved issues for the FortiDLP Browser Extension

Bug ID	Affected OS(s)	Description
M1180166	All	Previously, the FortiDLP Browser Extension content script logs were recorded at the default level of the browser console. This information is now provided at the debug log level of the browser console for diagnostic purposes.
M1182584	macOS	The `uninstall` script provided in the macOS accessory bundle was sometimes unreliable.

Known limitations in 12.2.2

This release has the following known limitations.

Known limitations

Bug ID	Affected OS(s)	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	Data lineage information is not reported for file deletion operations.

Bug ID	Affected OS(s)	Description
	macOS	
G18057	macOS	Secure Data Flow (origin and lineage) copy tracking is supported on macOS 13.4+.
G17690	All	Content inspection can only be performed on the first 16 KiB of the raw web request body.
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. This limitation pertains to all FortiDLP Agent versions.
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. For FortiDLP Policies 8.3.2+, if the *SaaS apps* parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the *Unknown User account types* checkbox. For detailed information, 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 require the following modifier keys: • Control • Alt/Option • Alt Graph • Function/Secondary Function • Windows • Command.
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.

Bug ID	Affected OS(s)	Description
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 12.2.2.

12.2.1

Released July 28th, 2025

New features and enhancements in 12.2.1

This release delivers the following new features and enhancements.

Clipboard evidence capturing

You can now configure policies to capture clipboard text in an action.

Our evidence capturing capabilities have been expanded to include sensitive text copied and pasted to applications. For example, you can use this to address data exposure risks posed by the use of generative AI tools. The evidence is encrypted and sent to your managed external storage location, and it can then be decrypted using the FortiDLP Decryption Tool.

The new *Capture clipboard evidence* action requires FortiDLP Policies 8.4.0+ and FortiDLP Decryption Tool 1.1.0+.

For more information, see Capture clipboard evidence.

External storage of screenshot evidence

You now have the option of storing screenshot evidence in your managed external storage location instead of the FortiDLP Infrastructure, giving you more control over your data. When this is configured, the evidence is encrypted and sent to your storage location, and it can then be decrypted using the FortiDLP Decryption Tool.

This functionality requires FortiDLP Decryption Tool 1.1.0+.

Note: The *Take screenshot* and *Make shadow copy* actions have been renamed to *Capture screenshot evidence* and *Capture file evidence* respectively, reflecting unified evidence capturing processes.

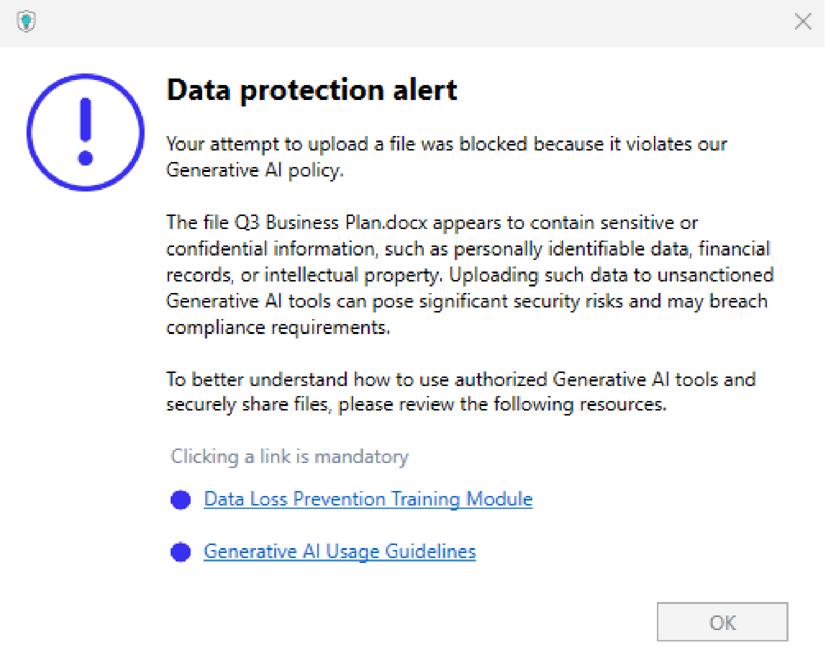
For more information, see:

- Capture screenshot evidence
- Evidence capturing

User coaching messages with multiple URLs

You can now configure the *Display message* action to include up to five user coaching URLs.

By presenting messages with multiple URLs, users can access more training resources at the time of a policy violation to increase their understanding of your organization's data protection practices.



Data protection alert

Your attempt to upload a file was blocked because it violates our Generative AI policy.

The file Q3 Business Plan.docx appears to contain sensitive or confidential information, such as personally identifiable data, financial records, or intellectual property. Uploading such data to unsanctioned Generative AI tools can pose significant security risks and may breach compliance requirements.

To better understand how to use authorized Generative AI tools and securely share files, please review the following resources.

Clicking a link is mandatory

● Data Loss Prevention Training Module

● Generative AI Usage Guidelines

This feature is provided for Windows and macOS.

For more information, see Configuring policy templates in the *FortiDLP Administration Guide*.

Resolved issues in 12.2.1

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(s)	Description
G14825	All	Previously, the insertion of a USB-based SD card reader into a node triggered a USB device event and/or a detection and action(s) (if the *Unauthorized USB storage device used* policy template was enabled) instead of the insertion of the SD card into the card reader. Also, if blocking was enabled, the entire card reader was blocked. Now, in this scenario, the insertion of the SD card into the card reader will trigger a detection and action(s). Further, blocking will only be applied to the SD card instead of the card reader. (USB device events will continue to be generated upon the insertion of the SD card reader.)

Bug ID	Affected OS(s)	Description
		Additionally, updating or disabling the *Unauthorized USB storage device used* policy to allow use of a previously blocked mass storage device no longer requires the system to be rebooted or the storage device to be re-inserted. FortiDLP Policies 8.4.0+ is required.
M1146665	All	When the *Sensitive file upload* policy template was enabled with *File origin parameters* defined, the Agent sometimes failed to capture the origin of downloaded files.
G16065	Windows macOS	The Agent sometimes attempted to close a file it had already closed when uploading screenshot or file evidence. This did not prevent the upload, but the Agent logged the file close attempt as an error.
G18326	Windows macOS	If the Agent started running before fleet management tools had set the enrollment token, the Agent could not find the token to enroll itself.
M1163252	Windows	The sandboxing applied to the file content inspection process `contentng.exe` could, under certain conditions, prevent other desired processes from running. The sandboxing on the process `contentng.exe` has now been disabled until a full fix can be applied.
G18350	Windows	When syncing users from an Entra ID directory, the Agent did not associate users with their nodes if their `username` differed from their `nickname`.
G18205	macOS	On Monterey 12, when USB file transfer blocking was enabled and a USB storage device was inserted, the Removable Storage app sometimes closed unexpectedly.
G18029	macOS	Previously, the Agent did not report the full life cycle of *Display message* actions in the *Action log*. The Agent now provides granular logging, detailing when users view messages, interact with messages (for example, by clicking a mandatory link), and close or attempt to close message dialogs without completing required steps.
G18474	macOS	At times, the Agent stopped unexpectedly when blocking a USB file transfer.
G18380	Linux	When the *Unauthorized USB storage device inserted* policy template was enabled without enabling the *Block USB storage device* action, the Agent did not raise a detection when an unauthorized USB storage device was inserted.

Resolved issues for the FortiDLP Browser Extension

Bug ID	Affected OS(s)	Description
M1169437	macOS	The FortiDLP Browser Extension for Safari's installation status was misreported as "Install incomplete" in the *Nodes* module when the installation succeeded.

Resolved issues for the FortiDLP Email Plugin (Legacy)

Bug ID	Affected OS(s)	Description
M1166814	Windows	The FortiDLP Email Plugin (Legacy) was misreported as "Install failed" in the *Nodes* module when the *Agent-initiated legacy email plugin installation* configuration option was enabled and a fleet management tool was used to set the registry keys, even when the installation succeeded.

Known limitations in 12.2.1

This release has the following known limitations.

Known limitations

Bug ID	Affected OS(s)	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+.
G17690	All	Content inspection can only be performed on the first 16 KiB of the raw web request body.
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. This limitation pertains to all FortiDLP Agent versions.
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.

Bug ID	Affected OS(s)	Description
		For FortiDLP Policies 8.3.2+, if the *SaaS apps* parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the *Unknown User account types* checkbox. For detailed information, 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 require the following modifier keys: • Control • Alt/Option • Alt Graph • Function/Secondary Function • Windows • Command.
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.

12.1.3

Released June 17th, 2025

New features and enhancements in 12.1.3

This release delivers the following new features and enhancements.

Enrollment diagnostics command

We've made it easier to debug enrollment issues.

By running `agent show comms` in a command-line interface, you can now view the status of network communication between the FortiDLP Agent and the FortiDLP Cloud, including the enrollment status.

The command helps diagnose common connectivity issues, such as failure to connect to the network or resolve a server name. It is especially useful for identifying man-in-the-middle (MITM) proxy issues, where a firewall or proxy transparently replaces certificates with its own, preventing the Agent from enrolling.

For more information, see Resolving FortiDLP Agent connectivity issues in the *FortiDLP Agent Deployment Guide*.

Resolved issues in 12.1.3

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(s)	Description
G17956	All	A disk storage initialization error prevented the Agent from starting.
G18300	All	Where an Agent's enrollment data became corrupt, this resulted in a restart loop. In this scenario, the Agent will now enter an unenrolled state and await re-enrollment.
G18116	All	It was possible for the Agent's process to stop unexpectedly when processing file access events.
G17834	Windows macOS	The Agent unnecessarily retrieved lineage information when performing file origin filtering in policies. The Agent now only retrieves lineage information when raising a detection.
M1156885	Windows macOS	Previously, when the *USB file transfer blocking action* Agent configuration option was set to *On*, health reporting did not indicate that a reboot was needed to enable the feature. The *Block file transfer to USB storage device* health component will now report a *Restart needed* state in this scenario.
G17522	macOS Linux	Process binary names were occasionally misreported.
G17939	Windows	The `jazzdesktop` process terminated when it was launched in an unsupported way.
M1163252	Windows	A content inspection permission error sometimes prevented `C:\` drive folder access or prevented the content inspection process from starting.
G18299	Linux	*Login* events were either reported nonsequentially or not reported at all.

Resolved issues for the FortiDLP Browser Extension

Bug ID	Affected OS(s)	Description
M1161867	All	Previously, the *Browser DNS over HTTPS (DoH)* and *Private browsing* Agent configuration options were applied even when the *Browser extension installation (Agent v11.1.1 or later)* option was set to *Managed with external tool*. These options are now only applied if the the *Browser extension installation (Agent v11.1.1 or later)* option is set to *Agent-managed installation/uninstallation*.
G18298	All	The `repair_broken_content_script_comms` advanced Agent configuration key, which repairs FortiDLP Browser Extension communications for Google Chrome, was unreliable.
M1152270	All	The FortiDLP Browser Extension prevented drag-and-drop file uploads on certain websites.
G18075	All	File upload visibility could be lost following a FortiDLP Browser Extension update.
M1147167	Windows	When Windows Startup Boost was enabled, inaccurate health data could be reported for the FortiDLP Browser Extension.

Known limitations in 12.1.3

This release has the following known limitations.

Known limitations

Bug ID	Affected OS(s)	Description
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	Content inspection can only be performed on the first 16 KiB of the raw web request body.
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. This limitation pertains to all FortiDLP Agent versions.
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.

Bug ID	Affected OS(s)	Description
		For FortiDLP Policies 8.3.2+, if the *SaaS apps* parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the *Unknown User account types* checkbox. For detailed information, 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 require the following modifier keys: • Control • Alt/Option • Alt Graph • Function/Secondary Function • Windows • Command.
G14825	All	The insertion of a USB-based SD card device reader into a node will trigger a USB devices event and/or a detection and action(s) (if the *Unauthorized USB storage device used* policy template is enabled) instead of the insertion of the SD card into the device reader. On Windows, a configuration option is available to alter this behavior, identifying the SD card's insertion into the device reader as the trigger for events, detections, and/or actions. For details, contact Fortinet Support.
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 12.1.3

This release contains the following OS support updates.

New support

- This Agent provides support for Linux kernel version 6.15.0 and Red Hat Enterprise Linux kernel version 5.14.0-575.el9.

Upcoming domain changes

As part of our product rebrand, we will soon be moving to the `fortidlp.forticloud.com` domain.

On August 1, 2025, the legacy `nextdlp.com` domain will be deprecated. Please ensure you update your firewall rules ahead of this date to allow FortiDLP Agents to communicate with the FortiDLP Cloud using the new domain.

The following table outlines the new entries you should add to your allowlist.

Allowlist entry	New domain
Edge node	• US (Iowa): `edge.us-0.fortidlp.forticloud.com` • US (Virginia): `edge.us-1.fortidlp.forticloud.com` • EU: `edge.eu-0.fortidlp.forticloud.com` • Qatar: `edge.me-0.fortidlp.forticloud.com` • Saudi Arabia: `edge.me-1.fortidlp.forticloud.com`
Action artifact uploads (screenshots, debug bundles, and performance reports)	• US (Iowa): `uploads.us-0.fortidlp.forticloud.com` • US (Virginia): `uploads.us-1.fortidlp.forticloud.com` • EU: `uploads.eu-0.fortidlp.forticloud.com` • Qatar: `uploads.me-0.fortidlp.forticloud.com` • Saudi Arabia: `uploads.me-1.fortidlp.forticloud.com`
Automatic upgrades	`updates.fortidlp.forticloud.com`
FortiDLP Email Add-in for New Outlook	`outlook-addin.fortidlp.forticloud.com`
FortiDLP Browser Extension for Firefox	`firefox-extension.fortidlp.forticloud.com`

Additionally, we recommend adding `no-reply@fortidlp.forticloud.com` to your email safe senders list.

For more information on firewall rule configuration, see Allowing communication between the FortiDLP Agent and FortiDLP Cloud in the *FortiDLP Agent Deployment Guide*.

Deploying and maintaining the FortiDLP Agent

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

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.