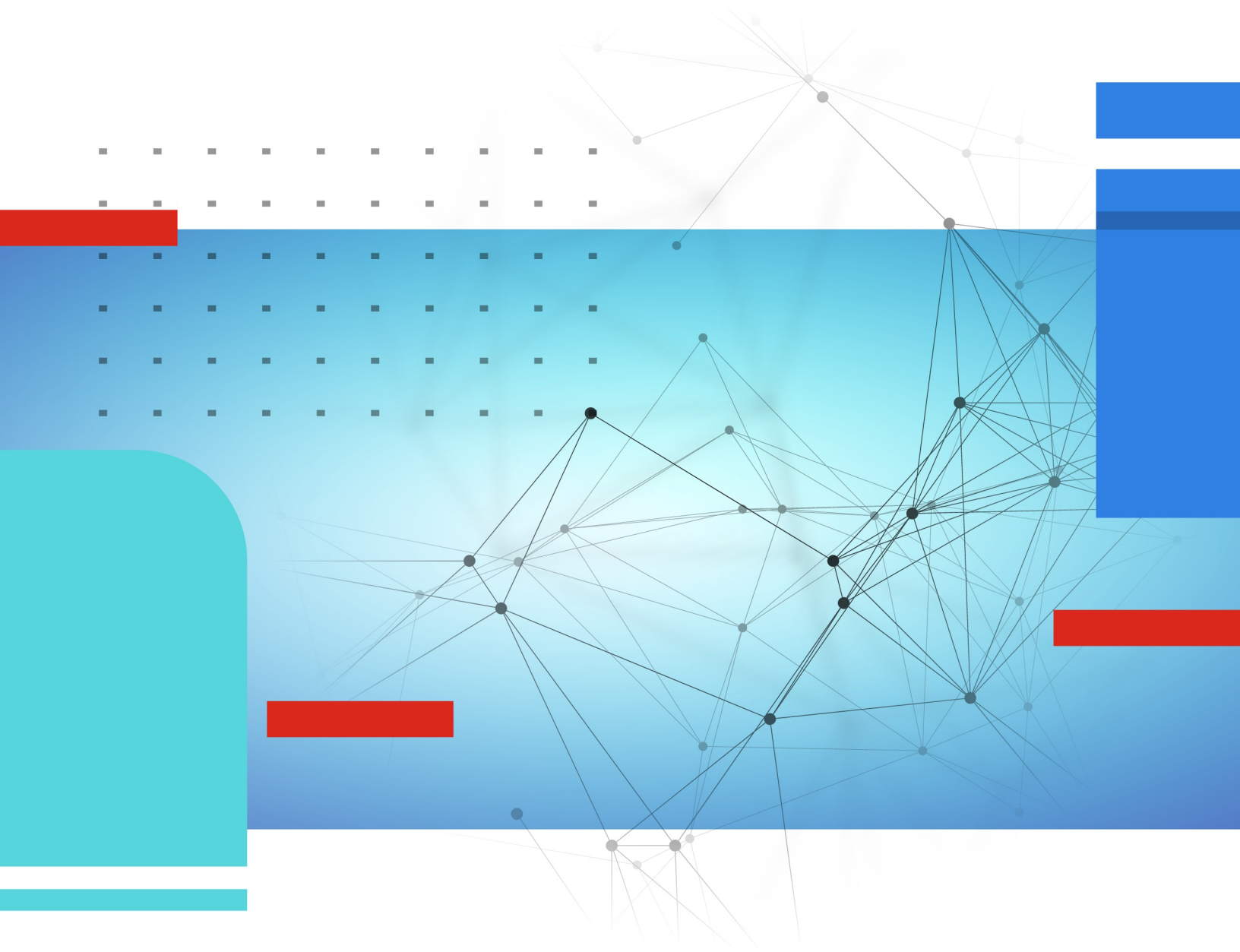
Release Notes

FortiDLP Agent 12.3.2



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

October 28, 2025
FortiDLP Agent 12.3.2 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 12.3.2.

Intended audience

These release notes are intended for anyone interested in learning about the FortiDLP Agent 12.3.2 release.

Related documentation

- *FortiDLP Agent Deployment Guide*

Current release

This section describes the FortiDLP Agent 12.3.2 release.

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
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+.
G17690	All	Content inspection can only be performed on the first 16 KiB of the raw web request body.

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. 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.
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 12.3.2

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.

Previous releases

This section describes the recent releases previous to FortiDLP Agent 12.3.2.

12.2.3

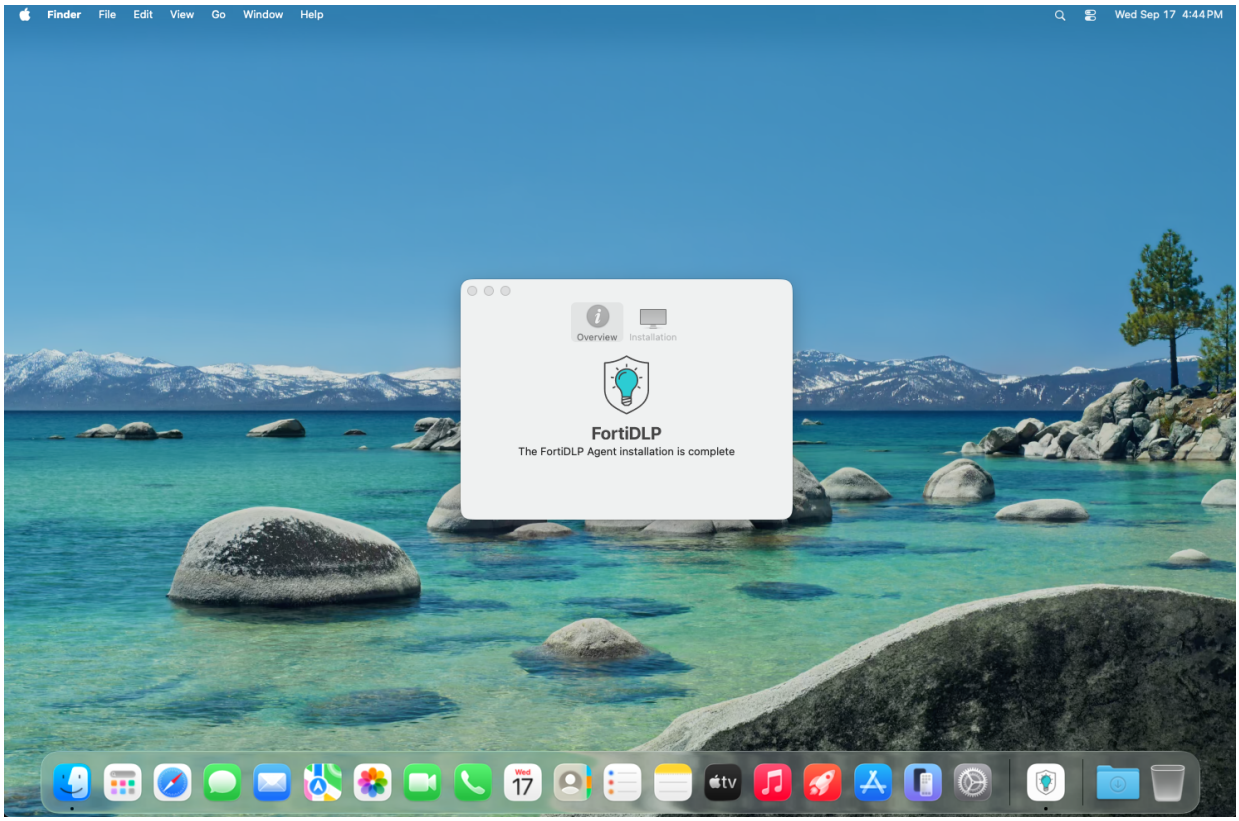
Released August 26th, 2025 | Updated September 23rd, 2025

New features and enhancements in 12.2.3

This release delivers the following new features and enhancements.

macOS Tahoe 26 support

We're excited to offer General Availability (GA) support for macOS 26 with FortiDLP Agent 12.2.3.



For instructions on deploying the Agent to this new macOS version, see the following sections in the *FortiDLP Agent Deployment Guide*:

- Manually deploying the FortiDLP Agent to macOS
- Bulk deploying FortiDLP Agent components to macOS.

Resolved issues in 12.2.3

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Bug ID	Affected OS(es)	Description
M1195039	All	In some cases, the content inspection process stopped unexpectedly.

Known limitations in 12.2.3

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 12.2.3.

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+.
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.

Bug ID	Affected OS(es)	Description
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.
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.

12.2.2

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(es)	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. 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.

Bug ID	Affected OS(es)	Description
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(es)	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(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+.
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.

Bug ID	Affected OS(es)	Description
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.
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.

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*.

www.fortinet.com