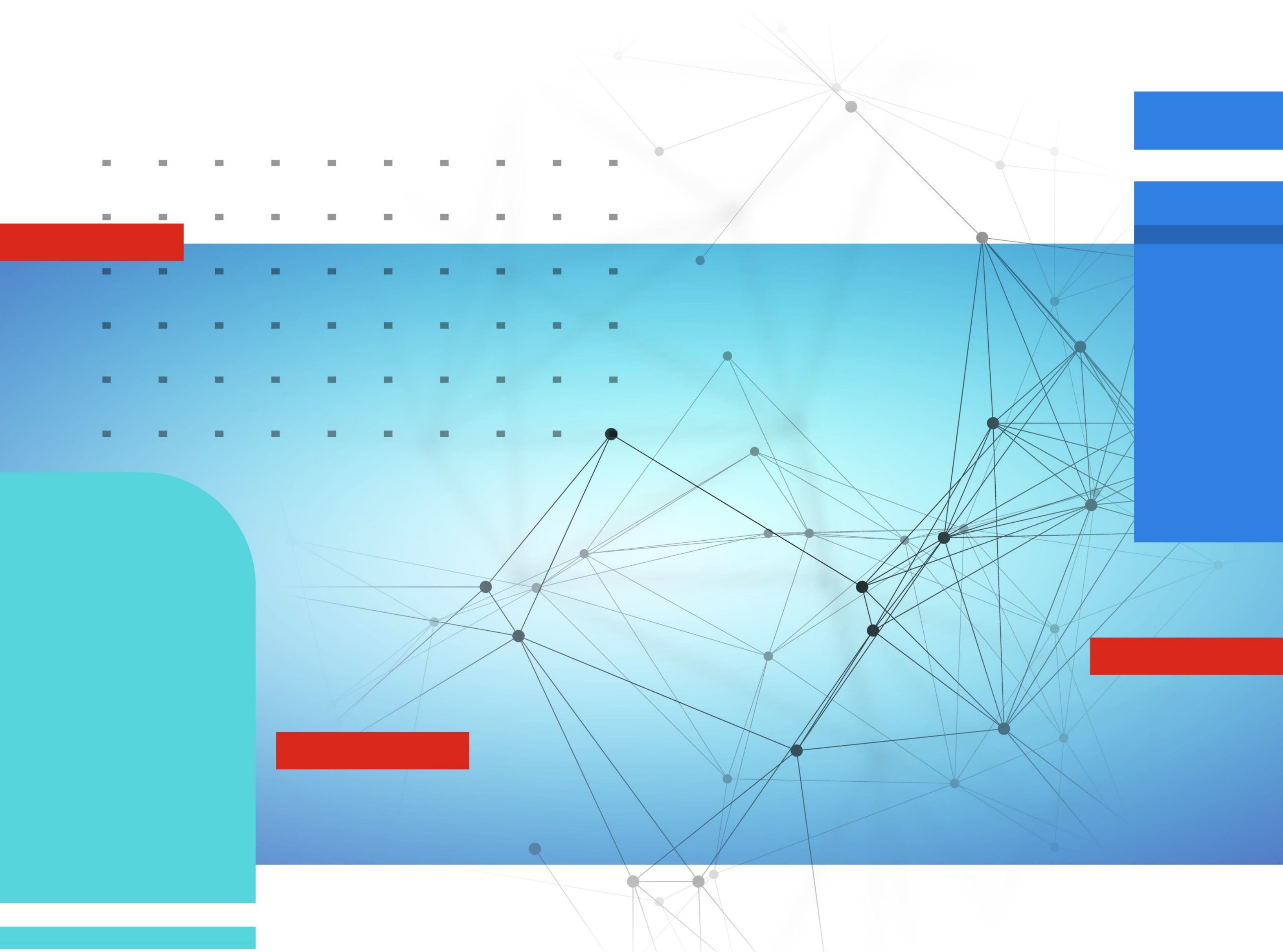
Release Notes

FortiDLP Agent 12.1.3



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

July 01, 2025
FortiDLP Agent 12.1.3 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 12.1.3.

Intended audience

These release notes are intended for anyone interested in learning about the FortiDLP Agent 12.1.3 release.

Related documentation

- *FortiDLP Agent Deployment Guide*

Current release

This section describes the FortiDLP Agent 12.1.3 release.

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

Fortinet identifier	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.

Fortinet identifier	Affected OS(s)	Description
G18116	All	It was possible for the Agent's process to stop unexpectedly when processing file access events.
G17834	Windows and 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 and 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 and 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

Fortinet identifier	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

Fortinet identifier	Affected OS(s)	Description
G17561	Windows and 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. 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 *UnknownUser 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

Fortinet identifier	Affected OS(s)	Description
		• 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*.

Previous releases

This section describes the recent releases previous to FortiDLP Agent 12.1.3.

12.1.0

Released April 28th, 2025 | Updated June 10th, 2025

New features and enhancements in 12.1.0

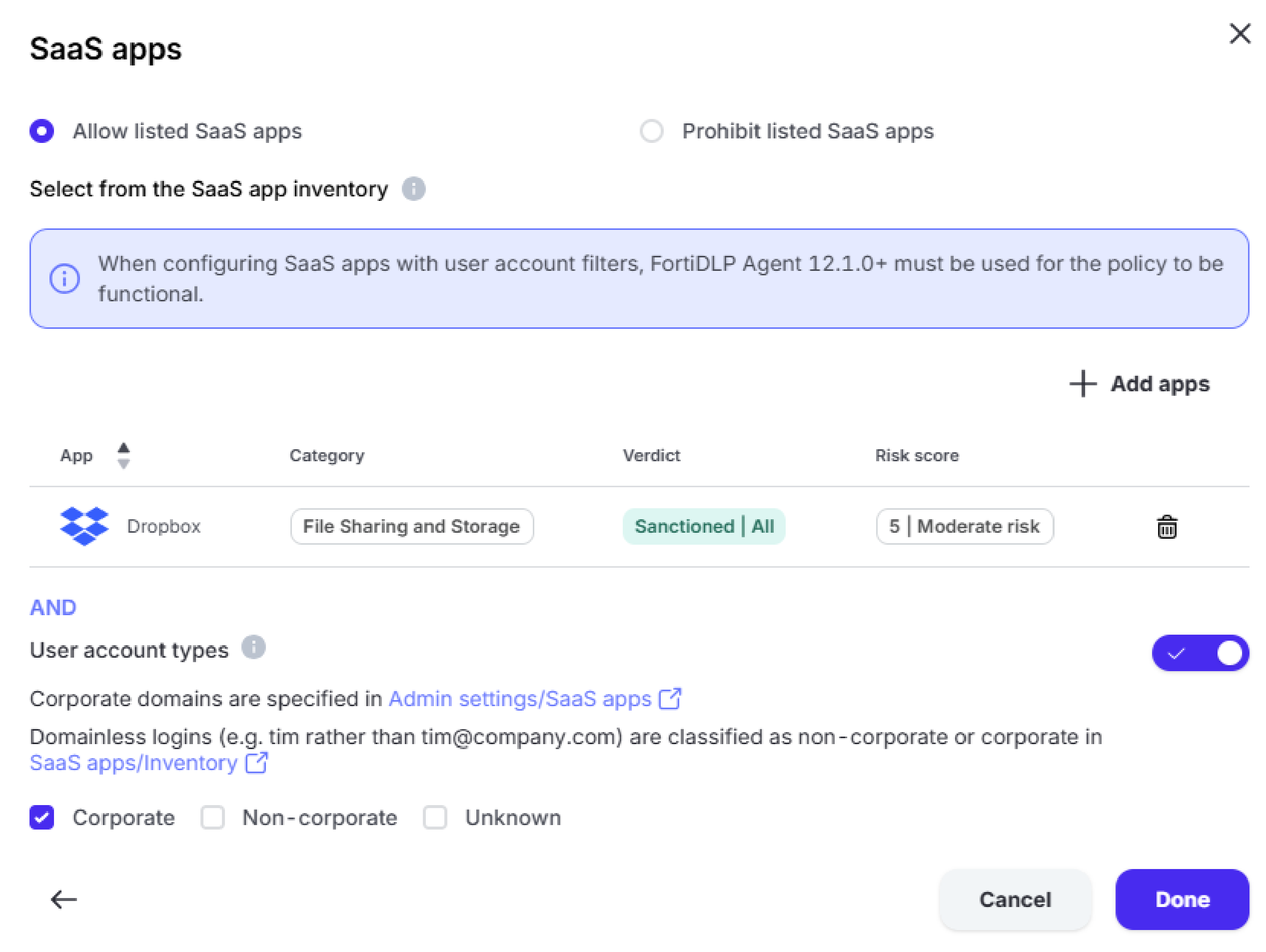
This release delivers the following new features and enhancements.

SaaS App Security | User account context in policies

SaaS app user account context is now Generally Available with FortiDLP Policies 8.3.2+.

To make it easier to implement web app security controls, the *SaaS apps* template parameter has been integrated with the corporate domain list defined in *Admin settings > SaaS apps*. This allows you to select account type filters when building policies, such as *Corporate* or *Non-corporate*, instead of specifying account domains (see image on next page). Account type filtering of destination SaaS apps is provided for all OSs, and account type filtering of origin SaaS apps is provided for Windows and macOS.

Further enhancements have been made to align the *Policies* and *SaaS apps* modules and to streamline configuration of SaaS app custom values and assets.



SaaS apps

● Allow listed SaaS apps ○ Prohibit listed SaaS apps

Select from the SaaS app inventory

When configuring SaaS apps with user account filters, FortiDLP Agent 12.1.0+ must be used for the policy to be functional.

App	Category	Verdict	Risk score
Dropbox	File Sharing and Storage	Sanctioned | All	5 | Moderate risk

AND

User account types

Corporate domains are specified in Admin settings/SaaS apps

Domainless logins (e.g. tim rather than tim@company.com) are classified as non-corporate or corporate in SaaS apps/Inventory

☑ Corporate □ Non-corporate □ Unknown

The former *User account domains* and *Monitor unknown user accounts* (Preview) template parameters are now Legacy, as this functionality has been built into the *SaaS apps* parameter. We advise customers who have participated in the Preview phase of this feature to upgrade to FortiDLP Agent 12.1.0+ then migrate to the enhanced feature.

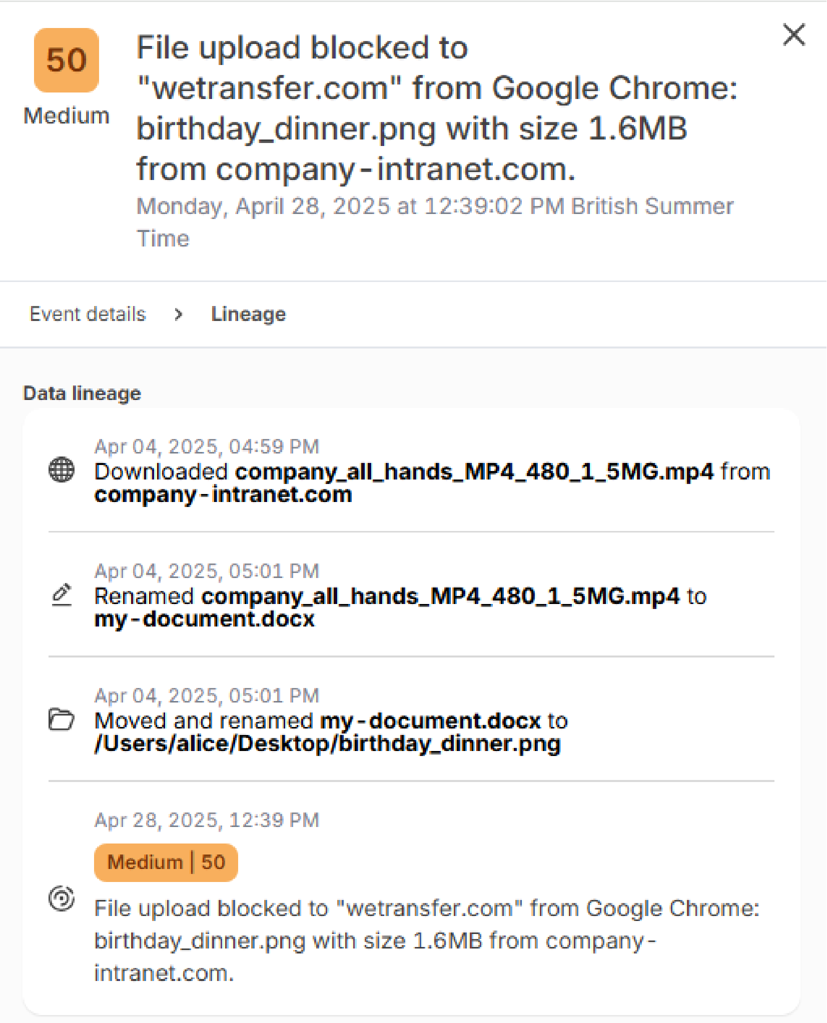
For more information, see SaaS apps and SaaS apps origin.

Secure Data Flow | Data lineage

The FortiDLP Agent now tracks the history of files downloaded from the web—from origin to final destination.

Data lineage increases visibility of important resources by capturing the operations performed on files before exfiltration, such as renames, copies, and moves. With this added context, analysts can more easily establish user intent and protect data from theft and misuse.

Lineage is shown for detections as an extension of file origin information as well as in the *Incidents* and *Cases* modules. High-level lineage details can also be included in detections sent to third-party systems via webhooks and to SIEM tools.



File upload blocked to "wetransfer.com" from Google Chrome: birthday_dinner.png with size 1.6MB from company-intranet.com.

Monday, April 28, 2025 at 12:39:02 PM British Summer Time

Apr 04, 2025, 04:59 PM
Downloaded **company_all_hands_MP4_480_1_5MG.mp4** from **company-intranet.com**

Apr 04, 2025, 05:01 PM
Renamed **company_all_hands_MP4_480_1_5MG.mp4** to **my-document.docx**

Apr 04, 2025, 05:01 PM
Moved and renamed **my-document.docx** to **/Users/alice/Desktop/birthday_dinner.png**

Apr 28, 2025, 12:39 PM
Medium | 50
File upload blocked to "wetransfer.com" from Google Chrome: birthday_dinner.png with size 1.6MB from company-intranet.com.

This feature is available for Windows and macOS with FortiDLP Policies 8.3.0+.

For more information, see:

- Detection details panel
- Webhook payload fields
- SIEM event message fields.

Secure Data Flow | Web origin-aware detections

The FortiDLP Agent's capability to track files downloaded from the web—across file moves, renames, and copies—is now Generally Available.

Through origin-based data protection, the Agent monitors browser-downloaded files as they travel through endpoints and optionally uses their origin as a detection trigger.

This feature is provided for Windows and macOS. Origin tracking is automatically enabled, and origin-aware detections can be configured with FortiDLP Policies 8.3.0+.

For more information, see File and attachment origin parameters in the *FortiDLP Policies Reference Guide*.

Safari browser monitoring

Broaden your visibility into web activity and sensitive data movement by monitoring Safari, a major browser for macOS endpoints.

This new capability is available with FortiDLP Agent 12.1.0+, FortiDLP Policies 8.3.0+, and the new FortiDLP Browser Extension for Safari.

The extension can be deployed in bulk via MDM providers that support configuration of Safari extensions (via Declarative Device Management).

If your MDM solution does not cover the above support, the extension can alternatively be enabled by end users on their devices, complying with Apple's security and privacy policies.

For details, see Bulk deploying the FortiDLP Browser Extension for Safari to macOS and Installing the FortiDLP Browser Extension for Safari on macOS in the *FortiDLP Agent Deployment Guide*.

Linux data identification support

The FortiDLP Agent now provides keyword/key phrase and regex file content inspection and web clipboard content inspection for all supported Linux distributions. Additionally, it offers Microsoft sensitivity label inspection.

This powerful functionality, which is Generally Available with FortiDLP Policy Templates 8.3.0+, strengthens data loss prevention for supported channels, such as web and print.

For details about content inspection, see Content inspection parameters in the *FortiDLP Policies Reference Guide*.

For sensitivity label setup information, see Enabling Microsoft sensitivity label detection on Linux in the *FortiDLP Agent Deployment Guide* and Microsoft sensitivity labels in the *FortiDLP Administration Guide*.

Resolved issues in 12.1.0

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Fortinet identifier	Affected OS(s)	Description
G17476	macOS	The macOS accessory bundle was previously available for download from the Next DLP Support Portal. The bundle is now accessible from the FortiDLP Console, within the installer *Artifacts* menu at *Admin settings > Agent deployment*. It is also available on the file system post Agent installation at `/Library/Application Support/Ava/Reveal/`.

Fortinet identifier	Affected OS(s)	Description
G17825 M1112333	All	Agent installers previously included the legacy Next DLP Product License Agreement / EULA and Warranty Terms. Agent installers now provide Fortinet's Product License Agreement / EULA and Warranty Terms, which are saved to the file system during installation.
G17907	All	Previously, the `agent config refresh` command exited before the configuration refresh completed, without reporting errors.
G17906	All	When a file shadowing storage vendor configuration was invalid, the Agent would continuously attempt to upload shadow copies to the storage bucket but not succeed. The Agent now reports this as a failed action.
G17897	All	Spurious errors were recorded in the Agent logs for actions due to a license validation issue.
M1138827	All	The Agent emitted unnecessary log message failures when polling for an enrollment code after enrollment completed.
G17798	All	The Agent sometimes stopped unexpectedly when accessing the process cache during high load.
G17800	All	The Agent occasionally stopped unexpectedly during content inspection.
M1130952	Windows and macOS	False error messages relating to web origin-aware detections were recorded in the Agent logs.
G16532	Windows and macOS	Previously, process path exclusion configurations could only be matched to the full path of a binary file. Path arguments can now be used on all OSs to provide more fine-grained process exclusion controls. For details, see Creating Agent configuration groups in the *FortiDLP Administration Guide*.
G17003	Windows	Previously, it was possible for the Agent to access an XLSX file at the same time as Excel, causing a corrupted version of the file to be saved.
G12592	Windows	The Agent's content inspection system has been sandboxed for improved security.
G17617	Windows	The Agent shutdown service was occasionally unreliable.
G17799	Windows	When print monitoring was enabled, the Agent could stop unexpectedly when processing print requests for a printer that is no longer available.
G17015	macOS	Login/logout events were sometimes not reported when a user locked/unlocked their device.

Fortinet identifier	Affected OS(s)	Description
G17610	Linux	The Agent sometimes stopped unexpectedly after a user logged in to their device.
G17554	Linux	A synchronization issue sometimes caused the Agent userland process to stop unexpectedly.
G17908	Linux	Kernel module code is now licensed as GNU General Public License version 2 only (GPLv2).
G17909	Linux	Memory usage has been optimized for the kernel module.
M1144463	Linux	Devices running certain kernel versions, such as 6.8.0 on Ubuntu 22.04 LTS, encountered system startup issues.

Resolved issues for the FortiDLP Browser Extension

Fortinet identifier	Affected OS(s)	Description
G16183	All	Firefox browser event exports occasionally failed when initiated from the FortiDLP Console's *Activity feed*.
M1131543	All	The FortiDLP Browser Extension for Firefox caused the browser to consume excessive memory when debugging tools were used.
M1121652	All	Browser login account context information was not reported for Google. This has been resolved in v3.4.9 of the FortiDLP Browser Extension.
G17098	All	It was possible for an internal communications failure to occur within the FortiDLP Browser Extension, preventing reporting of browser upload events. A new advanced Agent configuration setting has been added to control the FortiDLP Browser Extension's script injection behavior after an update, which is supported with the upcoming extension version, 3.5.1. For details, see Advanced Agent configuration settings in the *FortiDLP Administration Guide*.
M1130908 G17898	All	The FortiDLP Browser Extension blocked browser file access for certain websites and extensions due to unnecessary patching. New advanced Agent configuration settings have been added to control the FortiDLP Browser Extension's script injection behavior, which are supported with the upcoming extension version, 3.5.1. For details, see Advanced Agent configuration settings in the *FortiDLP Administration Guide*.
G17664	All	Browser components were reported as healthy when browser events were not being delivered to the Agent.
G17762	macOS	In certain circumstances, the FortiDLP Browser Extension for Safari (Preview) caused the Agent to stop unexpectedly.

Resolved issues for the FortiDLP Email Add-in

Fortinet identifier	Affected OS(s)	Description
G17563	Windows and macOS	A FortiDLP Email Add-in certificate error sometimes caused the Agent to stop unexpectedly.

Known limitations in 12.1.0

This release has the following known limitations.

Known limitations

Fortinet identifier	Affected OS(s)	Description
M1163252	Windows	A content inspection permission error may prevent `C:\` drive folder access or prevent the content inspection process from starting.
G17561	Windows and 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. 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*.

Fortinet identifier	Affected OS(s)	Description
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 12.1.0

This release contains the following OS support updates.

Ending support

- This Agent version will be the last to support Ubuntu 20.04 LTS.

12.0.5

Released March 4th, 2025 | Updated June 10th

FortiDLP Agent 12.0.5 is only available for Windows and macOS OSs.

If you use our automatic upgrade functionality, we recommend that you target FortiDLP Agent 12.1.0 for Linux using a separate Agent configuration group.

Resolved issues in 12.0.5

This release provides fixes for the following issues.

Resolved issues for the FortiDLP Agent

Fortinet identifier	Affected OS(s)	Description
17385	All	On startup, the Agent sometimes logged a false communications error.
17425	All	Where an external tool stopped communications between the Agent and the FortiDLP Browser Extension, the Agent could exceed expected CPU consumption when attempting to reconnect.
17455	Windows	Where a content inspection policy was configured with an invalid regular expression, this sometimes prevented the deletion of files from remote file shares.
15033	Windows	Previously, an excessive number of log messages were recorded when identifying processes for network connection events.
17592 17467	Windows	Startup logging has been improved for the Jazz Desktop process.
17593	Windows	Performance improvements have been made to optimize communication between the kernel module and userland service.
17238	macOS	A connection error caused the Network System Extension to stop unexpectedly.

Fortinet identifier	Affected OS(s)	Description
17363	macOS	The uninstallation script provided in the macOS accessory bundle contained an error that prevented the FortiDLP Agent app from being removed.
16322	macOS	When web origin-aware detections (Preview) were enabled along with file copy tracking, delays could occur when opening, closing, and copying files in certain Microsoft Office applications.
17594	macOS	The Network System Extension sometimes leaked mach ports when the Endpoint Security System Extension was not present.
17323	Linux	The Agent configuration group *Private browsing* setting was ineffective for Microsoft Edge.
17591	Linux	Reliability improvements have been made to login event reporting.

Resolved issues for the FortiDLP Browser Extension

Fortinet identifier	Affected OS(s)	Description
17353	All	Previously, the FortiDLP Browser Extension for Firefox did not update as expected: • For Agent-managed installations (via Agent configuration groups), the extension would update to a new version but then revert to v3.4.2 after Firefox was closed. • For manual or bulk installations using fleet management tools, where the `install_url` was not set to `https://firefox-extension.reveal.nextdlp.com/e528d90e863641e5afbd-firefox-latest.xpi`, the extension would update to a new version but then revert to the version provided in the Agent after Firefox was closed.
17400	macOS	Previously, the FortiDLP Browser Extension for Firefox could not be installed using the `browserInstallFirefox.mobileconfig` MDM profile provided in the macOS accessory bundle.

Known limitations in 12.0.5

This release has the following known limitations.

Known limitations

Fortinet identifier	Affected OS(s)	Description
17058	All	Microsoft sensitivity label inspection is not supported for encrypted files.

Fortinet identifier	Affected OS(s)	Description
17543 14710	Windows macOS	Wi-Fi connection events are not supported for Windows 11 24H2, Windows 11 24H2 (LTS), and macOS 14.5 or later. This limitation pertains to all FortiDLP Agent versions.
14247 15123 15017	All	Browser login account context (Preview), which is provided via the *User account domains* policy template parameter), 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 *User account domains* parameter is set, you can generate detections when activities associated with unknown logins occur by turning the *Monitor unknown user accounts* toggle on during template configuration. For details, refer to the *FortiDLP Policies Reference Guide*.
15467	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.
12150	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.
14825	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.

Fortinet identifier	Affected OS(s)	Description
13836	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.
12880	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.
8267	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.

Executable updates in 12.0.5

The following Dynamic Link Libraries (DLLs) have been removed from the Windows Agent executable's `C:\Program Files\Jazz Networks\Agent\` directory:

- `protobuf.dll`
- `protobuf-lite.dll`

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