



Release Notes

FortiDLP Agent 12.2.1



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 12.2.1 Release Notes

92-100-000000-20250116

TABLE OF CONTENTS

Introduction	4
Intended audience	4
Related documentation	4
Current release	5
12.2.1	5
New features and enhancements in 12.2.1	5
Resolved issues in 12.2.1	6
Known limitations in 12.2.1	8
Upcoming domain changes	11
Previous releases	12
12.1.3	12
New features and enhancements in 12.1.3	12
Resolved issues in 12.1.3	12
Known limitations in 12.1.3	14
Operating system support updates in 12.1.3	15
12.1.0	15
New features and enhancements in 12.1.0	16
Resolved issues in 12.1.0	19
Known limitations in 12.1.0	21
Operating system support updates in 12.1.0	23
Deploying and maintaining the FortiDLP Agent	24

Introduction

These release notes describe the new features and enhancements, resolved issues, known limitations, and updates related to FortiDLP Agent version 12.2.1.

Intended audience

These release notes are intended for anyone interested in learning about the FortiDLP Agent 12.2.1 release.

Related documentation

- [*FortiDLP Agent Deployment Guide*](#)

Current release

This section describes the FortiDLP Agent 12.2.1 release.

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.

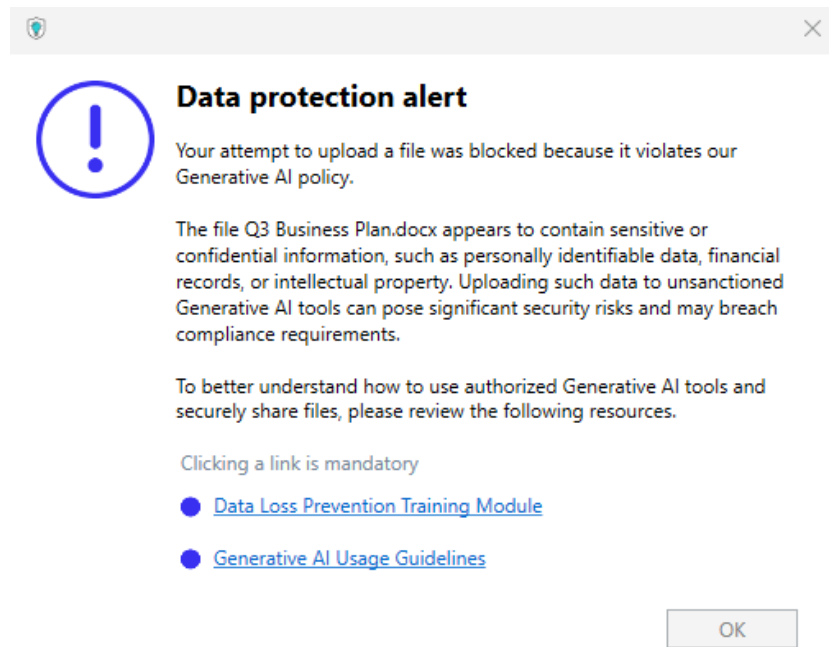
For more information, see:

- [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.



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

Fortinet identifier	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 <i>Unauthorized USB storage device used</i> 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.

Fortinet identifier	Affected OS(s)	Description
		<p>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.)</p> <p>Additionally, updating or disabling the <i>Unauthorized USB storage device used</i> 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.</p> <hr/> <div>  <p>FortiDLP Policies 8.4.0+ is required.</p> </div> <hr/>
M1146665	All	When the <i>Sensitive file upload</i> policy template was enabled with <i>File origin parameters</i> defined, the Agent sometimes failed to capture the origin of downloaded files.
G16065	Windows and 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 and 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	<p>The sandboxing applied to the file content inspection process contentng.exe could, under certain conditions, prevent other desired processes from running.</p> <p>The sandboxing on the process contentng.exe has now been disabled until a full fix can be applied.</p>
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	<p>Previously, the Agent did not report the full life cycle of <i>Display message</i> actions in the <i>Action log</i>.</p> <p>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.</p>

Fortinet identifier	Affected OS(s)	Description
G18474	macOS	At times, the Agent stopped unexpectedly when blocking a USB file transfer.
G18380	Linux	When the <i>Unauthorized USB storage device inserted</i> policy template was enabled without enabling the <i>Block USB storage device</i> action, the Agent did not raise a detection when an unauthorized USB storage device was inserted.

Resolved issues for the FortiDLP Browser Extension

Fortinet identifier	Affected OS(s)	Description
M1169437	macOS	The FortiDLP Browser Extension for Safari's installation status was misreported as "Install incomplete" in the <i>Nodes</i> module when the installation succeeded.

Resolved issues for the FortiDLP Email Plugin (Legacy)

Fortinet identifier	Affected OS(s)	Description
M1166814	Windows	The FortiDLP Email Plugin (Legacy) was misreported as "Install failed" in the <i>Nodes</i> module when the <i>Agent-initiated legacy email plugin installation</i> 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

Fortinet identifier	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 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.

Fortinet identifier	Affected OS(s)	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	<p>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.</p> <p>For FortiDLP Policies 8.3.2+, if the <i>SaaS apps</i> parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the <i>UnknownUser account types</i> checkbox.</p> <p>For detailed information, see the FortiDLP Policies Reference Guide.</p>
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	<p>The <i>Unauthorized text typed</i> and <i>Unauthorized text typed into website</i> policy templates cannot detect keywords that require the following modifier keys:</p> <ul style="list-style-type: none"> • Control • Alt/Option • Alt Graph • Function/Secondary Function • Windows • Command.
G13836	Windows macOS	<p>Regex pattern matches cannot be detected by the <i>Unauthorized email sent or received</i> policy template when content that is separated by line breaks is pasted into the email body of New Outlook.</p> <p>This limitation does not apply to Classic Outlook.</p>
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.

Fortinet identifier	Affected OS(s)	Description
G8267	All	<p>Due to a limitation present in Chromium-based browsers, when upload blocking policies are enabled, file directories cannot be uploaded using drag and drop.</p> <p>In this situation, a banner will display to instruct the user to use the file selector instead.</p>

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 `nextd1p.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	<ul style="list-style-type: none"> US (Iowa): <code>edge.us-0.fortidlp.forticloud.com</code> US (Virginia): <code>edge.us-1.fortidlp.forticloud.com</code> EU: <code>edge.eu-0.fortidlp.forticloud.com</code> Qatar: <code>edge.me-0.fortidlp.forticloud.com</code> Saudi Arabia: <code>edge.me-1.fortidlp.forticloud.com</code>
Action artifact uploads (screenshots, debug bundles, and performance reports)	<ul style="list-style-type: none"> US (Iowa): <code>uploads.us-0.fortidlp.forticloud.com</code> US (Virginia): <code>uploads.us-1.fortidlp.forticloud.com</code> EU: <code>uploads.eu-0.fortidlp.forticloud.com</code> Qatar: <code>uploads.me-0.fortidlp.forticloud.com</code> Saudi Arabia: <code>uploads.me-1.fortidlp.forticloud.com</code>
Automatic upgrades	<code>updates.fortidlp.forticloud.com</code>
FortiDLP Email Add-in for New Outlook	<code>outlook-addin.fortidlp.forticloud.com</code>
FortiDLP Browser Extension for Firefox	<code>firefox-extension.fortidlp.forticloud.com</code>

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 12.2.1.

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 <i>USB file transfer blocking action</i> Agent configuration option was set to <i>On</i> , health reporting did not indicate that a reboot was needed to enable the feature. The <i>Block file transfer to USB storage device</i> health component will now report a <i>Restart needed</i> 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	<i>Login</i> 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 <i>Browser DNS over HTTPS (DoH)</i> and <i>Private browsing</i> Agent configuration options were applied even when the <i>Browser extension installation (Agent v11.1.1 or later)</i> option was set to <i>Managed with external tool</i> . These options are now only applied if the <i>Browser extension installation (Agent v11.1.1 or later)</i> option is set to <i>Agent-managed installation/uninstallation</i> .
G18298	All	The <i>repair_broken_content_script_comms</i> 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	<p>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.</p> <p>For FortiDLP Policies 8.3.2+, if the <i>SaaS apps</i> parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the <i>UnknownUser account types</i> checkbox.</p> <p>For detailed information, see the FortiDLP Policies Reference Guide.</p>
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	<p>The <i>Unauthorized text typed</i> and <i>Unauthorized text typed into website</i> policy templates cannot detect keywords that require the following modifier keys:</p> <ul style="list-style-type: none"> • Control • Alt/Option • Alt Graph • Function/Secondary Function

Fortinet identifier	Affected OS(s)	Description
		<ul style="list-style-type: none">• Windows• Command.
G14825	All	<p>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 <i>Unauthorized USB storage device used</i> policy template is enabled) instead of the insertion of the SD card into the device reader.</p> <p>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.</p>
G13836	Windows macOS	<p>Regex pattern matches cannot be detected by the <i>Unauthorized email sent or received</i> policy template when content that is separated by line breaks is pasted into the email body of New Outlook.</p> <p>This limitation does not apply to Classic Outlook.</p>
G12880	All	<p>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.</p>
G8267	All	<p>Due to a limitation present in Chromium-based browsers, when upload blocking policies are enabled, file directories cannot be uploaded using drag and drop.</p> <p>In this situation, a banner will display to instruct the user to use the file selector instead.</p>

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.

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.

Add apps

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



Cancel

Done



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.

50

Medium

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

×

Event details > Lineage

Data lineage

- 🌐

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 <i>Artifacts</i> menu at <i>Admin settings > Agent deployment</i> . It is also available on the file system post Agent installation at <code>/Library/Application Support/Ava/Reveal/</code> .
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 <code>config refresh</code> 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.

Fortinet identifier	Affected OS(s)	Description
		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 <i>FortiDLP Administration Guide</i> .
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.
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 <i>Activity feed</i> .
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.

Fortinet identifier	Affected OS(s)	Description
		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 <i>FortiDLP Administration Guide</i> .
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 <i>FortiDLP Administration Guide</i> .
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.

Fortinet identifier	Affected OS(s)	Description
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	<p>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.</p> <p>For FortiDLP Policies 8.3.2+, if the <i>SaaS apps</i> parameter is set, you can generate detections when activities associated with unknown logins occur by selecting the <i>Unknown User account types</i> checkbox.</p> <p>For detailed information, see the FortiDLP Policies Reference Guide.</p>
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	<p>The <i>Unauthorized text typed</i> and <i>Unauthorized text typed into website</i> policy templates cannot detect keywords that require the following modifier keys:</p> <ul style="list-style-type: none"> • Control • Alt/Option • Alt Graph • Function/Secondary Function • Windows • Command.
G14825	All	<p>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 <i>Unauthorized USB storage device used</i> policy template is enabled) instead of the insertion of the SD card into the device reader.</p> <p>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.</p>
G13836	Windows macOS	Regex pattern matches cannot be detected by the <i>Unauthorized email sent or received</i> policy template when content that is separated by line breaks is pasted into the email body of New Outlook.

Fortinet identifier	Affected OS(s)	Description
		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.

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

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.