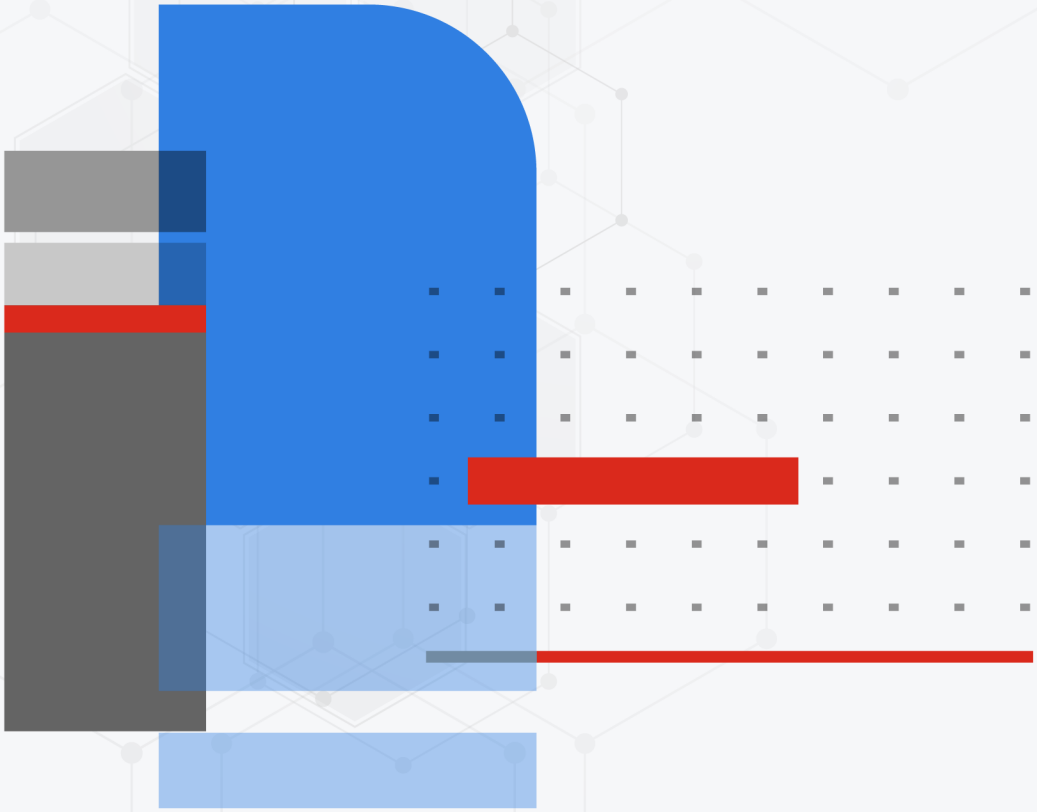
Release Notes

FortiAnalyzer Cloud 7.2.10



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 14, 2025
FortiAnalyzer Cloud 7.2.10 Release Notes
05-7210-1129463-20251014

TABLE OF CONTENTS

Change log **4**
FortiAnalyzer Cloud 7.2.10 release **5**
Special notices **6**
Shell access has been suspended 6
FortiClient logging 6
Upgrade information **7**
Downgrading to previous versions 8
Product integration and support **9**
Software support 9
Web browser support 9
FortiOS support 9
FortiClient support 10
FortiMail support 10
Feature support 10
Language support 11
Model support 11
Resolved Issues **12**
FortiView 12
Log View 12
Others 12
Reports 13
Common Vulnerabilities and Exposures 13
Known Issues **14**
New known issues 14
Existing known issues 14
Fabric View 14
FortiSOC 14
FortiView 15
Log View 15
Others 15
Reports 15
System Settings 16
Limitations of FortiAnalyzer Cloud **17**
Logging support and daily log limits **18**
FortiGate devices 18
Additional Storage licenses 19
Daily log limits for non-FortiGate devices 19
Storage add-on licenses 19
Viewing device and storage quota usage in the license information widget 19

Change log

Date	Change Description
2025-03-06	Initial release.
2025-10-14	Updated Resolved Issues on page 12

FortiAnalyzer Cloud 7.2.10 release

This document provides information about FortiAnalyzer Cloud version 7.2.10 build 6359.

The recommended minimum screen resolution for the FortiAnalyzer Cloud GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Special notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer Cloud version 7.2.10.

Shell access has been suspended

Shell access has been suspended in FortiAnalyzer Cloud 7.2.7.

FortiClient logging

When configuring logging from FortiClient to FortiAnalyzer Cloud, you must manually enter the fully qualified domain name (FQDN) of the FortiAnalyzer Cloud instance in the *IP Address/Hostname* field. It is important that this information is entered accurately to ensure your data is sent to the correct FortiAnalyzer Cloud instance.

For more information on configuring FortiClient logging to FortiAnalyzer Cloud, see the FortiClient documentation on the Fortinet Docs Library.

Upgrade information

A notification is displayed in the FortiAnalyzer Cloud notification drawer when a new version of the firmware is available. You can chose to upgrade immediately or schedule the upgrade for a later date.

Administrators must perform firmware upgrades from within the FortiAnalyzer Cloud *Dashboard* or firmware upgrade notification drawer.

An administrator with *Super_User* permissions is required to perform the upgrade.

To keep FortiAnalyzer Cloud secure and up to date, it is recommended that you upgrade your 7.2 release to the latest release build.

An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade.

To upgrade firmware from the notification drawer:

1. Go to FortiAnalyzer Cloud (https://fortianalyzer.forticloud.com/), and use your FortiCloud account credentials to log in. An administrator with Super_User permissions is required to perform the upgrade.
2. Expand the notification drawer to view information about available firmware upgrades.
3. Click *Upgrade Firmware* to update the firmware immediately or to schedule upgrade of the firmware for a later date.
   Alternatively, you can access firmware upgrade options from the FortiAnalyzer Cloud Dashboard.

   The *Later* option for *Upgrade Time* is only available for one week after the firmware is released.
4. Click *OK* to perform or schedule the upgrade.

To upgrade firmware from the Dashboard:

1. Log in to your FortiAnalyzer Cloud instance.
2. Go to *Dashboard* in the tree menu.
3. In the *System Information* widget, select the upgrade icon next to the firmware version.
   The *Firmware Management* dialog appears. The current firmware version is displayed along with upgrade options.
4. In the *Select Firmware* field, choose an available firmware version.
5. In the *Upgrade Time* choose *Now* or *Later*.
   - *Now*: Begin the upgrade immediately.
   - *Later*: Schedule the upgrade for a later time.
6. Click *OK*. The upgrade will be completed based on the selected options.

Downgrading to previous versions

Downgrade to previous versions of FortiAnalyzer Cloud firmware is not supported.

Product integration and support

This section lists FortiAnalyzer Cloud 7.2.10 support of other Fortinet products. It also identifies what FortiAnalyzer Cloud features are supported for log devices and what languages FortiAnalyzer Cloud GUI and reports support.

The section contains the following topics:

- Software support on page 9
- Feature support on page 10
- Language support on page 11
- Model support on page 11

Software support

FortiAnalyzer Cloud 7.2.10 supports the following software:

- Web browser support on page 9
- FortiOS support on page 9
- FortiClient support on page 10
- FortiMail support on page 10

Web browser support

FortiAnalyzer Cloud version 7.2.10 supports the following web browsers:

- Microsoft Edge version 114
- Mozilla Firefox version 96
- Google Chrome version 114

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAnalyzer Cloud version 7.2.10 supports the following FortiOS versions:

See the FortiAnalyzer 7.2.10 Release Notes for the latest supported FortiOS versions.

- 7.2.0 and later.
- 7.0.0 and later.
- 6.4.4 and later because of license requirements.

FortiClient support

FortiAnalyzer Cloud version 7.2.10 supports the following FortiClient versions:

See the FortiAnalyzer7.2.10 Release Notes for the latest supported FortiClient versions.

- 7.2.0 and later
- 7.0.3 and later

FortiMail support

FortiAnalyzer Cloud version 7.2.10 supports the following FortiMail versions:

See the FortiAnalyzer 7.2.10 Release Notes for the latest supported FortiMail versions.

- 7.2.0 and later

Feature support

FortiAnalyzer Cloud version 7.2.10 provides the following feature support:

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiClient	✓	✓	✓	✓
FortiMail	✓	✓	✓	✓

Language support

The following table lists FortiAnalyzer Cloud language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French	✓	✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Russian		✓
Spanish	✓	✓

To change the FortiAnalyzer Cloud language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiAnalyzer Cloud, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiAnalyzer Cloud. For more information, see the *FortiAnalyzer Administration Guide*.

Model support

FortiAnalyzer Cloud supports the same FortiGate and FortiMail models as FortiAnalyzer 7.2.10. For a list of supported models, see the *FortiAnalyzer 7.2.10 Release Notes* on the Document Library.

Resolved Issues

The following issues have been fixed in FortiAnalyzer Cloud version 7.2.10.

To inquire about a particular bug, please contact Customer Service & Support.

FortiView

Bug ID	Description
1046491	FortiView SD-WAN view does not display the proper info for any range higher than "1 last hour".

Log View

Bug ID	Description
617397	Admin user with admin profile with datamask enabled can't download log. Download is missing in "Tools" menu.

Others

Bug ID	Description
965803	Due to some Redis-related issues, the "`diagnose log device`" command displays 'Information Not Available' for all ADOMs, and newly generated reports are not visible on the GUI.
1068015	The sqlplugind process may fail to start, repeatedly crash, and result in a segmentation fault after the upgrade. This issue has been observed only when the core dump for sqlplugind was enabled prior to the upgrade using the following command: diagnose debug coredump enable sqlplugind.
1068211	GUI stops working and displays incorrect/partial data and keeps restarting httpd daemon.

Reports

Bug ID	Description
1064871	Report generation takes hours or gets stuck at some percentage due to the "ERROR: trailing junk after numeric literal at or near...".

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
1103781	FortiAnalyzer Cloud 7.2.10 is no longer vulnerable to the following CVE Reference: • CVE-2024-50571

Known Issues

Known issues are organized into the following categories:

- New known issues on page 14
- Existing known issues on page 14

To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

New known issues

There are no new issues identified in 7.2.10.

Existing known issues

The following issues have been identified in a previous version of FortiAnalyzer Cloud and remain in FortiAnalyzer Cloud 7.2.10.

Fabric View

Bug ID	Description
918006	An issue with the EMS Asset Inventory has been identified. When running the playbook, no assets or inventory are displayed on FortiAnalyzer Cloud, and the *Fabric View* lists remain empty.

FortiSOC

Bug ID	Description
872637	The status of FortiGate Connectors under *FortiSOC* is intermittently down.

FortiView

Bug ID	Description
875592	Admins with read/write access might keep/set filters for different Administrators (with read/write access).
954542	When the time range is extensive, FortiAnalyzer Cloud may experience limitations in handling data points, resulting in potential omissions of data entries in the final results for *FortiView* SD-WAN Monitors widgets.
989446	*FortiView* SD-WAN Bandwidth Overview displays no data.
1029156	Filter setting is getting shared automatically for users belonging to same LDAP group.

Log View

Bug ID	Description
1020783	Log View may occasionally display "No record found" instead of logs, especially when users attempt to navigate to additional pages.
1075987	The log is incorrectly displayed as "SSH count" on the log details page of *Log View*.

Others

Bug ID	Description
925250	The sqlreportd process may consume excessive resources on the FortiAnalyzer Cloud when retrieving logs from multiple FortiGates ("more than 100 FortiGates") at the same time. Consequently, users may experience some performance slowdowns.

Reports

Bug ID	Description
895106	Top destination by bandwidth dataset does not exclude long-live session.
937700	Source IP on the Report is shown as the Victim in the default Security Analysis report.
1013026	Network Interface Utilization Charts are blank in *Reports*.

System Settings

Bug ID	Description
766197	An admin user limited to a device group can view all device's log.

Limitations of FortiAnalyzer Cloud

All FortiAnalyzer modules are supported in FortiAnalyzer Cloud; however, the following features are not supported or are not relevant to the FortiAnalyzer Cloud deployment at this time:

- Logging Topology
- ADOMs
- Advanced ADOM mode
- High-Availability Mode
- Log Forwarding: Except when combined with FortiCare Elite Service or SOCaaS.
- Fetcher Management
- Remote Certificates
- The License Information widget includes differences from on-premises FortiAnalyzer. For more information, see Viewing device and storage quota usage in the license information widget on page 19.
- Remote Authentication Server
- SAML SSO
- SNMP monitoring tool
- FortiAnalyzer Cloud cannot be used as a managed device on FortiManager.
- Trusted Hosts
- Upload logs to cloud storage
- Security Rating Compliance Reports
- Logging from FortiClient EMS for Chromebook

FortiAnalyzer Cloud supports logs from FortiGate devices and non-FortiGate devices, such as FortiClient.

FortiAnalyzer Cloud can be integrated into the Cloud Security Fabric when the root FortiGate is running firmware version 6.4.4 or later.

The FortiAnalyzer Cloud portal does not support IAM user groups.

Logging support and daily log limits

The daily log limits available for FortiGate devices depend on the FortiGate platform. These daily log limits can be expanded with an additional storage license. Adding additional storage licenses also enables FortiAnalyzer Cloud to receive logs from other supported devices like FortiMail.

- FortiGate devices on page 18
- Additional Storage licenses on page 19
- Daily log limits for non-FortiGate devices on page 19

For more information on licensing and SKUs, see the FortiAnalyzer Cloud Deployment Guide and FortiAnalyzer Cloud Datasheet.

FortiGate devices

FortiAnalyzer Cloud supports logs from FortiGates. Each FortiGate with an entitlement is allowed a fixed daily rate of logging.

When determining the daily log limit for FortiAnalyzer Cloud, the form factor of the FortiGate model determines the log limits. The chart below identifies some FortiGate models for each form factor as an example.

The following rates are based on the FortiAnalyzer Cloud a la carte subscription:

Form Factor	Example FortiGate Model	Total daily log limit for FortiAnalyzer-VM v6.4 and later
Desktop or FGT-VM models with 2 CPU	FortiGate 30 series, FortiGate 90 series	200MB/Day
1RU or FGT-VM models with 4 CPU	FortiGate 100 series, FortiGate 600 series, FortiGate 800 series, FortiGate 900 series	1GB/Day
2 RU and above or FGT-VM models with 8 CPU and above	FortiGate 1000 series and higher	5GB/Day

Once the limit has been reached, users must purchase additional storage in order for FortiAnalyzer Cloud to maintain logs for 12 months. You can purchase additional storage licenses to expand the daily logging limits for your FortiGate devices. For more information about daily log limits included with additional storage licenses, see Additional Storage licenses on page 19.

Additional Storage licenses

Additional storage licenses are available to expand the base daily logging limits. Multiple of the same SKU may be combined.

Added daily log limit	SKU
+5 GB/day	FC1-10-AZCLD-463-01-DD
+50 GB/day	FC2-10-AZCLD-463-01-DD
+500 GB/day	FC3-10-AZCLD-463-01-DD

Daily log limits for non-FortiGate devices

Purchasing any of the additional storage licenses above (for example, FC1-10-AZCLD-463-01-DD) also enables FortiAnalyzer Cloud to receive logs from FortiClient and FortiMail in addition to expanding the amount of logs it may store from FortiGates.

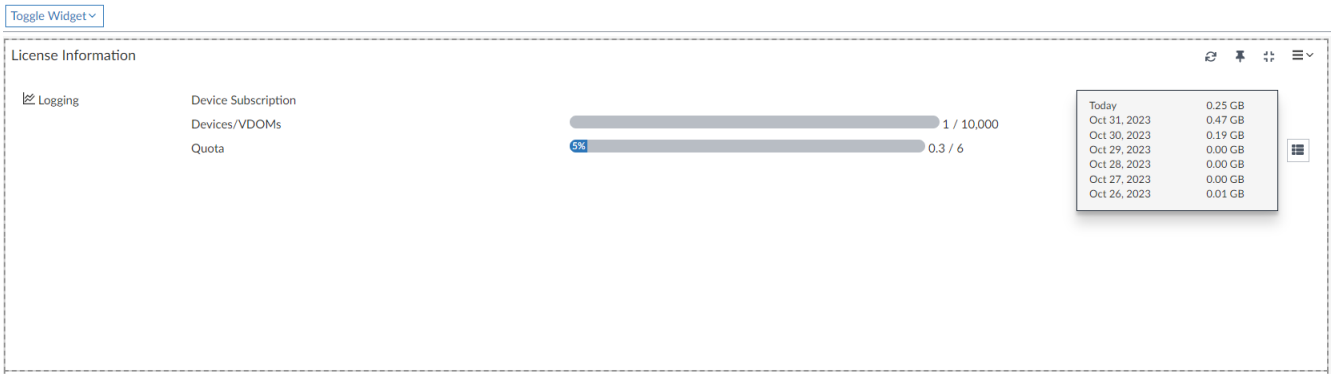
Storage add-on licenses

The impact of storage add-on licenses depends on whether FortiAnalyzer Cloud is receiving logs from FortiGate devices.

To see information about FortiAnalyzer Cloud licensing, see the FortiAnalyzer Cloud Deployment guide.

Viewing device and storage quota usage in the license information widget

The license information widget on the FortiAnalyzer Cloud Dashboard displays the following information:



Device/VDOMs	The total number of devices and VDOMs connected to FortiAnalyzer Cloud, and the total number of device and VDOM licenses.
Quota	Quota displays the current day's storage quota usage. This includes storage space used by both raw logs and database logs. You can click the list icon to see a breakdown of quota usage over the past 7 days. The *Quota* field differs from the *GB/Day* field and `diagnose fortilogd logvol-adom all` command in on-premise FortiAnalyzers which only shows the *raw log volume* for the last 7 days.

Information about other Dashboard widgets shared between on-premises FortiAnalyzer and FortiAnalyzer Cloud can be found in the FortiAnalyzer Administration 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.