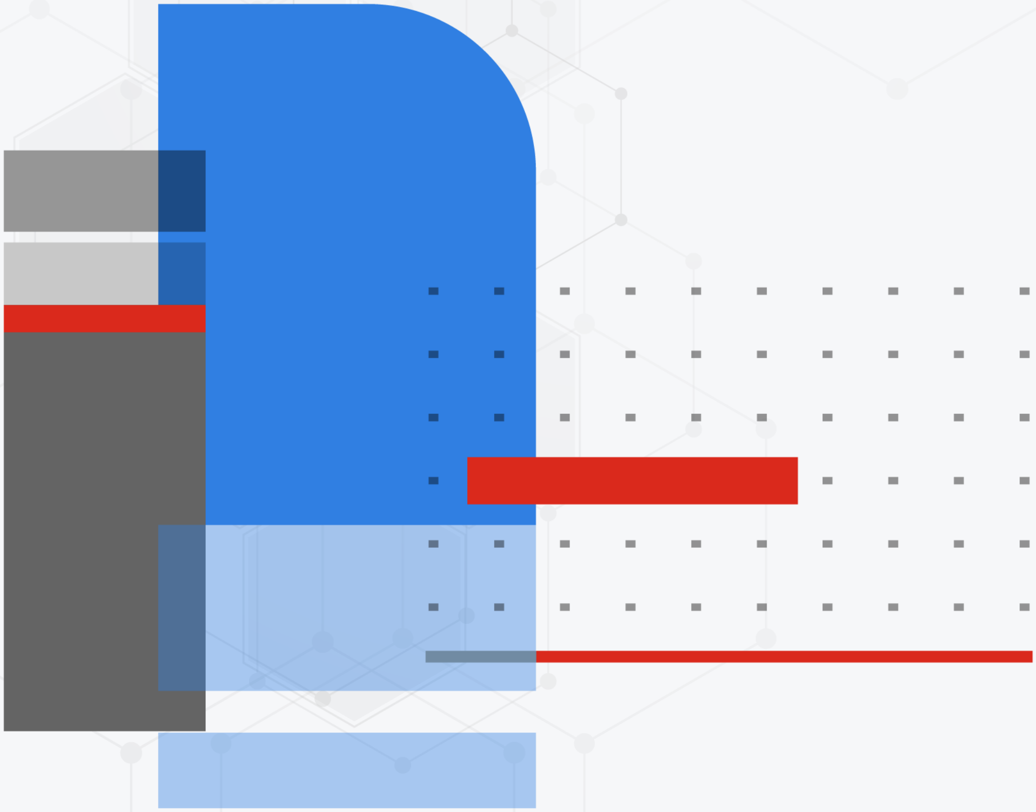
Release Notes

FortiAnalyzer Cloud 7.4.7



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

November 4, 2025
FortiAnalyzer Cloud 7.4.7 Release Notes
05-747-1166412-20251104

TABLE OF CONTENTS

Change log 5
FortiAnalyzer Cloud 7.4.7 release 6
Special notices 7
OT Security Service support 7
Attack Surface Rating and Compliance support 7
FortiClient logging 7
Upgrade information 8
FortiAnalyzer Cloud upgrade path 9
Mandatory upgrades 9
Downgrading to previous versions 10
Product integration and support 11
Software support 11
Web browser support 11
FortiOS support 11
FortiClient support 12
FortiMail support 12
FortiWeb support 12
Feature support 12
Language support 13
Model support 14
Resolved issues 15
Device Manager 15
Fabric View 15
FortiSOC 15
FortiView 16
Log View 16
Others 16
Reports 17
System Settings 17
Common Vulnerabilities and Exposures 18
Known issues 19
New known issues 19
Device Manager 19
Fabric View 19
Existing known issues 19
Device Manager 20
Fabric View 20
Log View 20
Others 20
Reports 20

Limitations of FortiAnalyzer Cloud 21
Logging support and daily log limits 23
FortiGate devices 23
Additional Storage licenses 24
Daily log limits for non-FortiGate devices 24
Storage add-on licenses 24
Viewing storage quota and disk usage in the Service Information widget 25

Change log

Date	Change Description
2025-06-16	Initial release of FortiAnalyzer Cloud 7.4.7.
2025-07-08	Updated Resolved issues on page 15.
2025-11-04	Updated Resolved issues on page 15.

FortiAnalyzer Cloud 7.4.7 release

This document provides information about FortiAnalyzer Cloud version 7.4.7 build 6767.

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 7.4.7.

OT Security Service support

FortiAnalyzer Cloud 7.4.7 supports the *OT Security Service* with the following SKUs:

- `FC1-10-AZCLD-159-DD`
- `FC2-10-AZCLD-159-DD`
- `FC3-10-AZCLD-159-DD`

Attack Surface Rating and Compliance support

FortiAnalyzer Cloud 7.4.7 supports *Attack Surface Rating and Compliance* with the following SKUs:

- `FC1-10-AZCLD-175-DD`
- `FC2-10-AZCLD-175-DD`
- `FC3-10-AZCLD-175-DD`

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.

In FortiAnalyzer Cloud 7.4.3 and later, administrators must perform firmware upgrades from within the FortiAnalyzer Cloud Dashboard or firmware upgrade notification drawer.

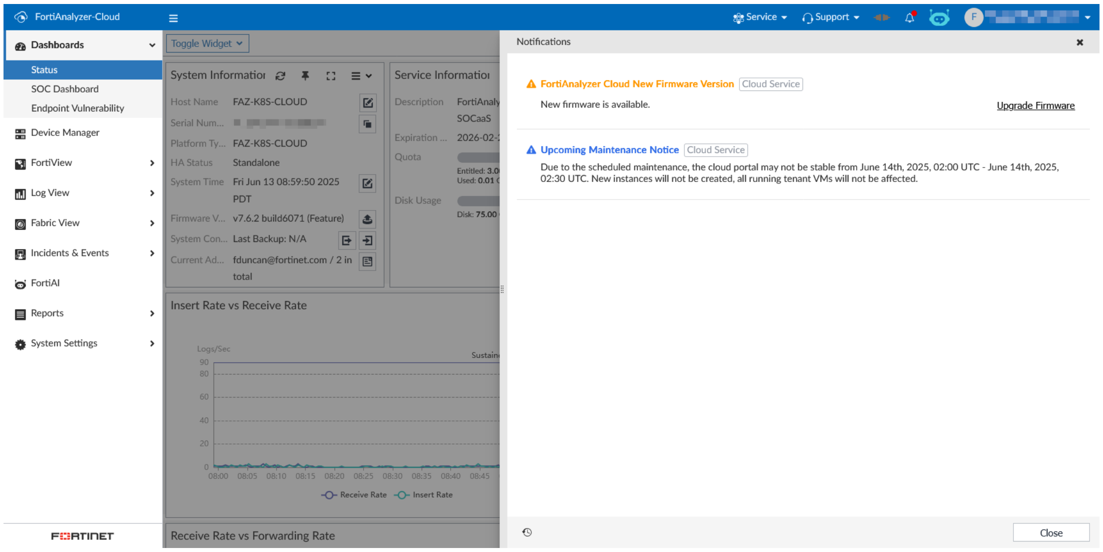
An administrator with *Super_User* permissions is required to perform the upgrade.

To keep FortiAnalyzer Cloud secure and up to date, it is recommended that you upgrade your 7.4 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. See Mandatory upgrades on page 9.

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.



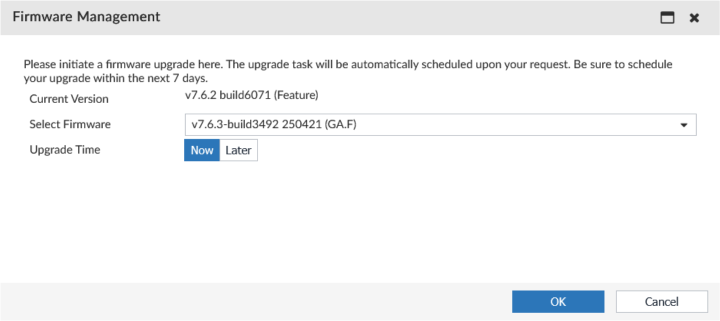
Host Name FAZ-K8S-CLOUD
Serial Num... [redacted]
Platform Ty... FAZ-K8S-CLOUD
HA Status Standalone
System Time Fri Jun 13 08:59:50 2025 PDT
Firmware V... v7.6.2 build6071 (Feature)
System Con... Last Backup: N/A
Current Ad... fduncan@fortinet.com / 2 in total

Description FortiAnaly SOCaaS
Expiration ... 2026-02-
Quota Entitled: 3.0 Used: 0.01
Disk Usage Disk: 75.00

FortiAnalyzer Cloud New Firmware Version Cloud Service
New firmware is available. Upgrade Firmware

Upcoming Maintenance Notice Cloud Service
Due to the scheduled maintenance, the cloud portal may not be stable from June 14th, 2025, 02:00 UTC - June 14th, 2025, 02:30 UTC. New instances will not be created, all running tenant VMs will not be affected.

3. Click *Upgrade Firmware* to update the firmware immediately or to schedule upgrade of the firmware for a later date.



Firmware Management

Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request. Be sure to schedule your upgrade within the next 7 days.

Current Version v7.6.2 build6071 (Feature)

Select Firmware v7.6.3-build3492 250421 (GA.F)

Upgrade Time [✓ Now] Later

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.

FortiAnalyzer Cloud upgrade path

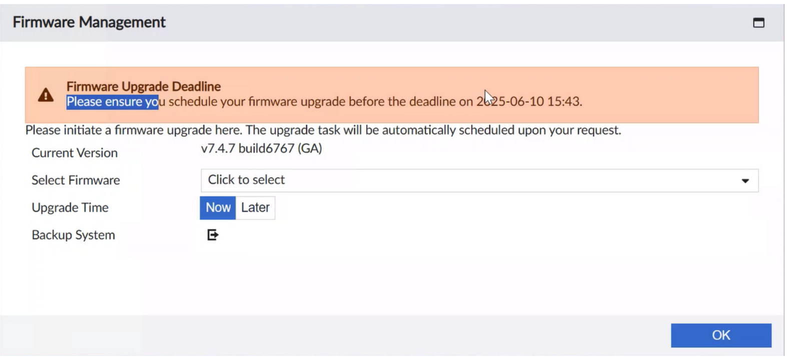
When upgrading FortiAnalyzer Cloud between major/minor versions, you must first upgrade to the latest patch release for the current version and any intermediate versions.

For example, in order to upgrade FortiAnalyzer Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

The FortiAnalyzer Cloud firmware version selection menu only displays the next eligible version that your instance can be upgraded to in the path. In the example above, the 7.4 firmware would not be displayed as an option until you have updated to the latest available 7.2 patch version.

Mandatory upgrades

When a firmware upgrade is mandatory, a *Firmware Management* dialog window will appear when you access your instance. This dialog provides details about the upgrade deadline and options for upgrading your firmware version. You can choose to upgrade immediately or schedule the upgrade for a later time. This dialog cannot by bypassed.



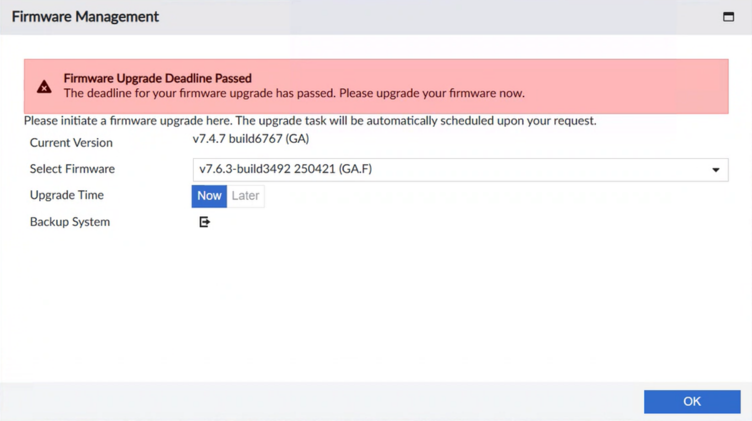
Firmware Management

Firmware Upgrade Deadline
Please ensure you schedule your firmware upgrade before the deadline on 2025-06-10 15:43.

Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.

Current Version	v7.4.7 build6767 (GA)
Select Firmware	Click to select
Upgrade Time	Now Later
Backup System	

After the deadline has passed, you can still connect to your instance's GUI to see the *Firmware Management* dialog window, however, you will only have the option to upgrade immediately. This dialog cannot by bypassed and you will not be able to access your instance until the upgrade is completed.



Firmware Management

Firmware Upgrade Deadline Passed
The deadline for your firmware upgrade has passed. Please upgrade your firmware now.

Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.

Current Version	v7.4.7 build6767 (GA)
Select Firmware	v7.6.3-build3492 250421 (GA.F)
Upgrade Time	Now Later
Backup System	

Downgrading to previous versions

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

Product integration and support

This section lists FortiAnalyzer Cloud 7.4.7 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 11
- Feature support on page 12
- Language support on page 13
- Model support on page 14

Software support

FortiAnalyzer Cloud 7.4.7 supports the following software:

- Web browser support on page 11
- FortiOS support on page 11
- FortiClient support on page 12
- FortiMail support on page 12
- FortiWeb support on page 12

Web browser support

FortiAnalyzer Cloud version 7.4.7 supports the following web browsers:

- Google Chrome version 135
- Microsoft Edge version 135
- Mozilla Firefox 138

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

FortiOS support

FortiAnalyzer Cloud version 7.4.7 supports the following FortiOS versions:

See the FortiAnalyzer 7.4.7 Release Notes for the latest supported FortiOS versions.

- 7.4.0 and later.
- 7.2.0 and later.
- 7.0.0 and later.

FortiClient support

FortiAnalyzer Cloud version 7.4.7 supports the following FortiClient versions:

See the FortiAnalyzer 7.4.7 Release Notes for the latest supported FortiClient 7.0 versions.

- 7.4.0 and later
- 7.2.0 and later
- 7.0.3 and later

FortiMail support

FortiAnalyzer Cloud version 7.4.7 supports the following FortiMail versions:

See the FortiAnalyzer 7.4.7 Release Notes for the latest supported FortiMail versions.

- 7.4.0 and later
- 7.2.0 and later

FortiWeb support

FortiAnalyzer Cloud version 7.4.7 supports the following FortiWeb versions:

- 7.6.3 and later

Feature support

FortiAnalyzer Cloud version 7.4.7 provides the following feature support:

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiClient EMS/FortiEndpoint	✓	✓	✓	✓
FortiMail	✓	✓	✓	✓
FortiWeb	✓	✓	✓	✓

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 7.4.7. For a list of supported models, see the *FortiAnalyzer 7.4.7 Release Notes* on the Document Library.

Resolved issues

The following issues have been fixed in FortiAnalyzer Cloud version 7.4.7. To inquire about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
927113	FortiAnalyzer Cloud displays incorrect EMS server version, IP address, and connectivity status.
1058791	Some devices not being authorized, but showing up under "authorized device list".

Fabric View

Bug ID	Description
1078817	The FortiClient EMS Cloud Fabric Connector (existing/newly added) may not function properly, causing FortiAnalyzer Cloud to potentially fail in establishing a successful connection with the FortiClient EMS Cloud due to this issue.

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).
922053	Mismatched Username Detected for the Same IP Address in IOC Compromised Hosts.
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.
1046491	*FortiView* SD-WAN view does not display the proper info for any range higher than "1 last hour".
1050052	In some cases, the compromised host entry may display different FSSO users and source IPs than the actual users and source IPs on the drill-down page.
1114751	The widget "Top SD-WAN SLA Issues" appears empty when a specific interface and "All devices" are selected. This issue may occur if there are at least 10 devices with empty values for latency, jitter, or packet loss.

Log View

Bug ID	Description
1075987	The log is incorrectly displayed as "SSH count" on the log details page of *Log View*.
1093743	Log filter doesn't search more than one IP address for one field.
1114303	Privacy masking does not work properly.

Others

Bug ID	Description
1001388	FortiAnalyzer Cloud in Collector Mode does not forward logs for all FortiGates to the FortiAnalyzer Cloud working in Analyzer Mode.
1068211	GUI stops working and displays incorrect/partial data and keeps restarting httpd

Bug ID	Description
	daemon.
1069672	On the FortiGate, the log test CLI command shows that logs are queued and the test buttons in the GUI often fail. The issue occurs intermittently.
1081045	Some intermittent GUI issues have been observed due to a crash in the 'fazsvcd' daemon.
1089725	Progressively slower GUI performance caused by increasing memory usage of the "init" daemon.
1098690	After an upgrade, users (prior to the upgrade) who were created and assigned to a custom admin profile (with the super_user_profile enabled) may encounter a GUI issue. Upon successful login, the login prompt disappears, but only the background color remains visible with no additional GUI elements loaded.

Reports

Bug ID	Description
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*.
1123597	When the report or chart filter is set to "All Devices", the chart displays data as expected. However, when the report or chart is filtered to a specific device, the message "No matching log data for this report" appears in the chart.

System Settings

Bug ID	Description
766197	An admin user limited to a device group can view all device's log.
985489	When disabling the automatic adjustment for daylight saving time, the date and time on the dashboard update accordingly. However, the date and time of logs received by the FortiAnalyzer Cloud in *Log View* do not appear to update.
1050063	FortiAnalyzer Cloud experiences issues when log forwarding is configured (Log forward filter).
1058282	Remote administrators may be unable to review the Event Logs, as the GUI might display the following message: "Web Server Error 500."

Bug ID	Description
1080217	Occasionally, when the FortiAnalyzer Cloud is rebooted (for maintenance or upgrade), the FortiGate may lose the FortiAnalyzer Cloud's serial number from the `config log fortianalyzer settings`. This can result in the following error message being displayed on the FortiGate: 'FortiAnalyzer certificate is not verified.'

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1125741	FortiAnalyzer Cloud 7.4.7 is no longer vulnerable to the following CVE Reference: • CVE-2025-24474
1157806	FortiAnalyzer Cloud 7.4.7 is no longer vulnerable to the following CVE Reference: • CVE-2025-53845

Known issues

Known issues are organized into the following categories:

- New known issues
- Existing known issues

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

New known issues

The following issues have been identified in version 7.4.7.

Device Manager

Bug ID	Description
1156269	In *Device Manager*, when switching to *Map View* mode, the page does not load properly. This issue has been observed primarily in Chrome.

Fabric View

Bug ID	Description
1164209	Using ITSM Connectors may cause the connection status of previously configured connectors to disappear from the Playbook. **Workaround:** Recreate EMS/CASB connector for new default playbooks or resave the connector password and then manually create a playbook to execute EMS/CASB connector actions.

Existing known issues

The following issues have been identified in a previous version of FortiAnalyzer Cloud and remain in FortiAnalyzer Cloud 7.4.7.

Device Manager

Bug ID	Description
1140464	In FortiAnalyzer Cloud, the *Device Manager* displays "(Beta 0)" for the FortiGate versions. This has been observed when FortiAnalyzer Cloud is receiving forwarded logs from another FortiAnalyzer Cloud operating in Collector mode.

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.

Log View

Bug ID	Description
989022	FortiAnalyzer Cloud doesn't display FortiClient analytics and raw logs in *Log View* when EMS FortiFlex license is being used.

Others

Bug ID	Description
1111426	Swap usage exceeding 2 GB significantly degrades system performance.

Reports

Bug ID	Description
895106	Top destination by bandwidth dataset does not exclude long-live session.
1069669	The filter feature for 'subnet' in *Reports* does not work accurately.

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
- DLP/IPS archives
- High-Availability Mode
- Log Forwarding: FortiAnalyzer Cloud does not support log forwarding, except when integrated with *FortiCare Elite Services* or *SOCaaS*—logs can then be forwarded only to the respective service portals.
- Fetcher Management
- Remote Certificates
- The FortiAnalyzer Cloud Dashboard widget availability differs from on-premises FortiAnalyzer:
  - The License Information widget is replaced with the Service Information widget which includes differences from on-premises FortiAnalyzer. For more information, see Viewing storage quota and disk usage in the Service Information widget on page 25.
  - FortiAnalyzer Cloud does not support the *System Resources*, *Unit Operation*, *Alert Message Console*, *Disk I/O*, and *Disk Quota Usage* widgets.
  - FortiAnalyzer Cloud includes *Historical Log Rate*, *Average Log Rate*, *Average Quota*, and *Historical Quota Usage* widgets that are not available in on-premises FortiAnalyzers.
- 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 can not be configured as Supervisor in a FortiAnalyzer Fabric.

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 23
- Additional Storage licenses on page 24
- Daily log limits for non-FortiGate devices on page 24

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 24.

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.

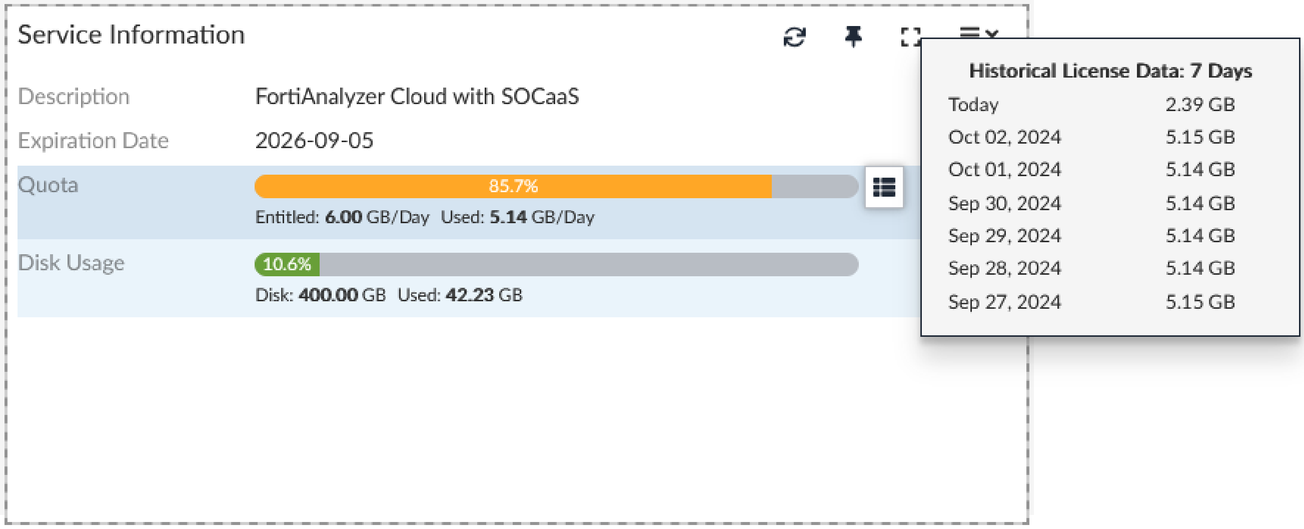
Storage add-on licenses

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 storage quota and disk usage in the Service Information widget

The Service Information widget on the FortiAnalyzer Cloud Dashboard displays the following information:



Service Information

Description	FortiAnalyzer Cloud with SOCaaS
Expiration Date	2026-09-05
Quota	85.7% Entitled: 6.00 GB/Day Used: 5.14 GB/Day
Disk Usage	10.6% Disk: 400.00 GB Used: 42.23 GB

Historical License Data: 7 Days

Today	2.39 GB
Oct 02, 2024	5.15 GB
Oct 01, 2024	5.14 GB
Sep 30, 2024	5.14 GB
Sep 29, 2024	5.14 GB
Sep 28, 2024	5.14 GB
Sep 27, 2024	5.15 GB

Description	The service description.
Expiration Date	The expiration date of the license.
Quota	Quota displays the current day's storage entitlement and usage. This includes storage space used by both raw logs and database logs. Click the list icon to see a breakdown of quota usage over the past 7 days. The *Quota* field on FortiAnalyzer Cloud 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.
Disk Usage	Displays the amount of disk currently being used as well as the total available disk size.

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

FORTINET®

www.fortinet.com

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