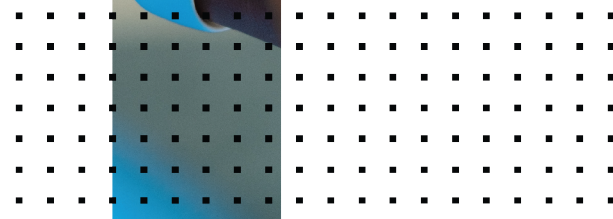
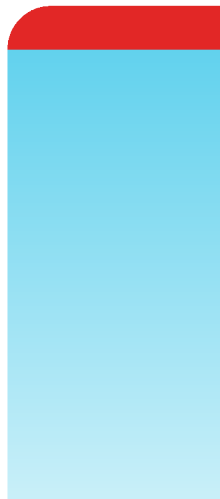


Cloud Deployment Guide

FortiAnalyzer 7.6.x



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



January 2nd, 2026

FortiAnalyzer 7.6.x Cloud Deployment Guide

05-76-1108639-20260102

TABLE OF CONTENTS

Change Log	4
Introduction	5
Requirements	5
Licensing	6
Deploying FortiAnalyzer Cloud	9
Checking requirements and licenses	9
Deploying a FortiAnalyzer Cloud instance	10
Configuring FortiOS	12
Configuring FortiClient EMS	13
Configuring FortiMail	15
Configuring FortiWeb	16
Configuring FortiNDR	20
Configuring third-party log forwarding from an on-premise FortiAnalyzer	21
Managing access tokens	22
Using FortiAnalyzer Cloud	24
Accessing your FortiAnalyzer Cloud instance	24
Access FortiAnalyzer Cloud through FortiCloud	24
Upgrading firmware from the instance	25
Identifying the public IP address	25
Using the FortiAnalyzer Cloud toolbar	26
Service	26
Support	27
Notifications	27
Account	27
Privacy and notification preferences	28
Access Settings	29
Email Notifications	29
Enabling managed SOC service from FortiAnalyzer Cloud	31
Configure log buffer cache size	33
Using FortiAI on FortiAnalyzer Cloud	34
Configuration and log backups	35
Using the FortiAnalyzer Cloud & Service portal	36
Viewing the FortiAnalyzer Cloud portal	36
Providing feedback	38
Using account services	40
Adding a secondary account	40
Modifying a secondary account	42
Supporting IAM users and IAM API users	42
Adding IAM users	42
Adding API users	45
Supporting external IdP users	46
Using multiple roles with external IdP users	46

Change Log

Date	Change Description
2025-12-15	Initial release of FortiAnalyzer Cloud 7.6.5.
2026-01-02	Updated Adding API users on page 45 .

Introduction

FortiAnalyzer Cloud is a cloud-based logging platform based on FortiAnalyzer.

FortiAnalyzer Cloud is designed for system health monitoring and alerting using Event Logs, Security Logs, and IOC scans. FortiAnalyzer Cloud can receive Traffic, UTM, and other logs from FortiGate devices.

Logging from non-FortiGate devices, such as FortiClient EMS, is supported with additional licensing.

Once the FortiGate device or non-FortiGate device has acquired the required license, FortiCloud can be used to create a FortiAnalyzer instance under the user account. You can launch the portal for the cloud-based FortiAnalyzer from FortiCloud, and its URL starts with the User ID.



SSL inspection for *.forticloud.com must be disabled on any upstream FortiGates in order to reach FortiAnalyzer Cloud.

This section includes the following topics:

- [Requirements on page 5](#)
- [Licensing on page 6](#)

Requirements

The following items are required before you can initialize FortiAnalyzer Cloud:

- Internet access
- Browser
- FortiCare/FortiCloud account with Fortinet Technical Support (<https://support.fortinet.com/>)
Create a FortiCloud account if you do not have one.

A primary FortiCloud account is required to deploy FortiAnalyzer Cloud. A primary FortiCloud account can invite other users to launch FortiAnalyzer Cloud as sub users. See [Adding a secondary account on page 40](#).



Only one FortiAnalyzer Cloud instance can be created per FortiCloud account.

- FortiAnalyzer Cloud SOCaaS subscription (optional)

See [Licensing on page 6](#) for further license details.

This entitles you to a fixed daily rate of logging dependent on the FortiGate model:

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 to FortiGate 90	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



- Logs from non-FortiGate devices, such as FortiClient and FortiMail require additional licensing. See [Licensing on page 6](#) for more information.
- See the FortiAnalyzer Cloud [release notes](#) for more information on supported software versions.

Licensing

License requirements are enforced when you log in to the FortiAnalyzer Cloud & Service portal.

For more information on license SKUs, see the [FortiCloud SaaS Management & Analytics Ordering Guide](#).

Logging from FortiGate

You can add one of the following FortiAnalyzer Cloud subscriptions to enable cloud-based central logging from a FortiGate hardware or VM device:

License Type	License SKU
FortiAnalyzer Cloud: Cloud based central logging and analytics	FC-10-[FortiGate Model/VM Model Code]-585-02-DD
FortiAnalyzer Cloud with SOCaaS	FC-10-[FortiGate Model/VM model Code]-464-02-DD

Logging from FortiEndpoint

The following FortiEndpoint licenses include cloud-based central logging with FortiAnalyzer Cloud:

DIY Solution	ZERO TRUST CONNECT	PREVENT	XDR	XDR + SOC	Entitled Log Rate
25-49	FC1-10-EMS05-	FC1-10-EMS05-	FC1-10-EMS05-	FC1-10-EMS05-	50 MB/day

DIY Solution	ZERO TRUST CONNECT	PREVENT	XDR	XDR + SOC	Entitled Log Rate
	1045-02-DD	1046-02-DD	1041-02-DD	1042-02-DD	
50-499	FC2-10-EMS05-1045-02-DD	FC2-10-EMS05-1046-02-DD	FC2-10-EMS05-1041-02-DD	FC2-10-EMS05-1042-02-DD	100 MB/day
500-1999	FC3-10-EMS05-1045-02-DD	FC3-10-EMS05-1046-02-DD	FC3-10-EMS05-1041-02-DD	FC3-10-EMS05-1042-02-DD	1 GB/day
2000-9999	FC4-10-EMS05-1045-02-DD	FC4-10-EMS05-1046-02-DD	FC4-10-EMS05-1041-02-DD	FC4-10-EMS05-1042-02-DD	4 GB/day
10000+	FC5-10-EMS05-1045-02-DD	FC5-10-EMS05-1046-02-DD	FC5-10-EMS05-1041-02-DD	FC5-10-EMS05-1042-02-DD	20 GB/day

For more information on the licenses available for FortiEndpoint, see the [FortiEndpoint Ordering Guide](#).

Logging from FortiWeb

License Type	License SKU
Support for logging from FortiWeb	FC-10-[FortiWeb Model/VM Model Code]-585-02-DD
Support for logging from FortiWeb with SOCaaS	FC-10-[FortiWeb Model/VM Model Code]-464-02-DD

Additional storage licenses, and logging from FortiClient, FortiMail and FortiNDR

Additional storage may also be added as required for FortiGate and FortiEndpoint logging. Multiple of the same SKU may be combined.

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

Additional storage	License 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

Add-on services

FortiAnalyzer Cloud supports licensed features, including :

- FortiAI
- Security Rating Update
- Industrial Security Service

For more information on supported add-on services for FortiAnalyzer Cloud, see the [FortiCloud SaaS Management & Analytics Ordering Guide](#).

Deploying FortiAnalyzer Cloud

The section describes how to deploy FortiAnalyzer Cloud. Following is an overview of the process.

To deploy FortiAnalyzer Cloud:

1. Check requirements and licenses on FortiCloud. See [Checking requirements and licenses on page 9](#).
2. On FortiCloud, deploy a FortiAnalyzer Cloud instance. See [Deploying a FortiAnalyzer Cloud instance on page 10](#).
3. (Optional) Upgrade FortiAnalyzer Cloud to the latest available cloud version. See [Upgrading firmware from the instance on page 25](#).
4. Enable logging to FortiAnalyzer Cloud:
 - For FortiOS, see [Configuring FortiOS on page 12](#).
 - For FortiClient EMS, see [Configuring FortiClient EMS on page 13](#).
 - For FortiMail, see [Configuring FortiMail on page 15](#).
 - For FortiWeb, see [Configuring FortiWeb on page 16](#).
 - For FortiNDR, see [Configuring FortiNDR on page 20](#).
 - For third-party logs, see [Configuring third-party log forwarding from an on-premise FortiAnalyzer on page 21](#).

Checking requirements and licenses

This section explains how to check whether you have the requirements and licenses needed for FortiAnalyzer Cloud.

To check for requirements and license for FortiAnalyzer Cloud:

1. Go to FortiCloud (<https://support.fortinet.com/>), and use your FortiCloud account credentials to log in. The FortiCloud portal is displayed.
2. Ensure that the license for the registered FortiGate units or non-FortiGate units include a FortiAnalyzer Cloud entitlement:
 - a. Go to *Products > Product List*.
 - b. In the *View Options menu*, select *Group by Category*, and click *Apply*.
The *Product List* is displayed by categories, such as *FortiGate*.
 - c. Expand the *FortiGate* category and click on a device to view its details, and confirm that the device *Entitlement* includes FortiAnalyzer Cloud.
3. Deploy the FortiAnalyzer Cloud instance. See [Deploying a FortiAnalyzer Cloud instance on page 10](#).

Deploying a FortiAnalyzer Cloud instance

This section explains how to deploy FortiAnalyzer Cloud. You can select a region, and then deploy the instance of FortiAnalyzer Cloud to the region.

A primary FortiCloud account is required to deploy FortiAnalyzer Cloud. A primary FortiCloud account can invite other users to launch FortiAnalyzer Cloud as sub users. See [Adding a secondary account on page 40](#).

When deploying FortiAnalyzer Cloud to receive logs from non-FortiGate devices, such as FortiClient, a storage add-on license is also required.

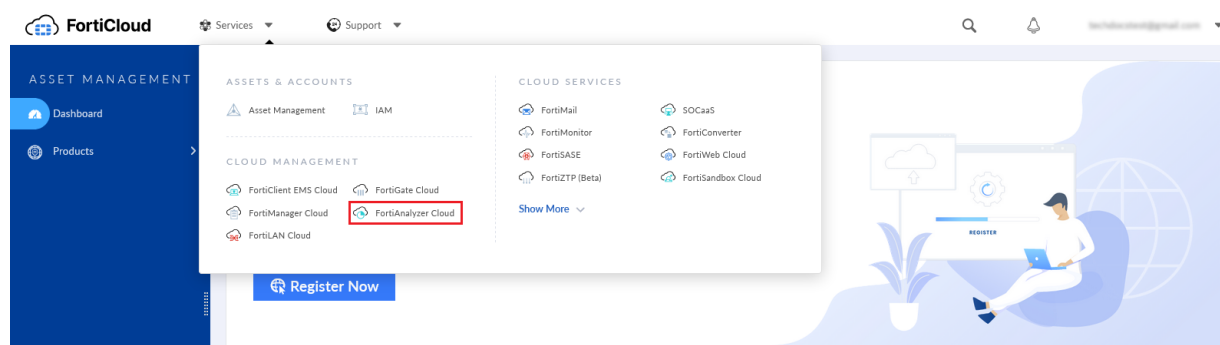
Only one FortiAnalyzer Cloud instance can be created per FortiCloud account.

To deploy a FortiAnalyzer Cloud instance:

1. If not done already, go to FortiCloud (<https://support.fortinet.com/>), and use your FortiCloud account credentials to log in.

The FortiCloud portal is displayed.

2. From the Services menu, select *FortiAnalyzer Cloud*.



The *FortiAnalyzer Cloud & Service* portal is displayed.

3. On the *FortiAnalyzer Cloud & Service* portal:
 - a. Select a *Region* for the FortiAnalyzer Cloud instance. In this example, the region is *Canada (Vancouver)*.
 - b. Select a *Time Zone* for the FortiAnalyzer Cloud instance.
4. Click *Submit*.

FortiAnalyzer Cloud

Service Support

1 0 0

Search

OU/Account Account ID Owner Service Region # of Device Logging Status Logs/Sec Default(GB/Day Add-on(GB/Day)

Test

PROVISION SERVICE

Please confirm the selected region: Canada (Vancouver) and timezone : (GMT-8:00) Pacific Time (US & Canada)

Region Canada (Vancouver)

Time Zone (GMT-8:00) Pacific Time (US & Canada)

Submit Cancel

Terms of Service Privacy Policy Release Notes

v23.1 b0141 Copyright © 2023 Fortinet, Inc. All rights reserved.

5. Confirm your selected region and time zone.

The provision region you selected is: Canada (Vancouver).
The time zone you selected is: (GMT-8:00) Pacific Time (US & Canada).

Confirm Cancel

6. Click *Submit*.
7. Review and accept the *Terms of Service* and *Privacy Policy*. Privacy settings can be configured in the instance. See [Privacy and notification preferences on page 28](#).
8. FortiAnalyzer Cloud instance is provisioned in a few minutes.

FortiAnalyzer Cloud

Service Support

1 0 0

Search

OU/Account Account ID Owner Service Region # of Device Logging Status Logs/Sec Default(GB/Day Add-on(GB/Day)

Test

PROVISION SERVICE

Provision Instance: 5 mins left

Region Canada (Vancouver)

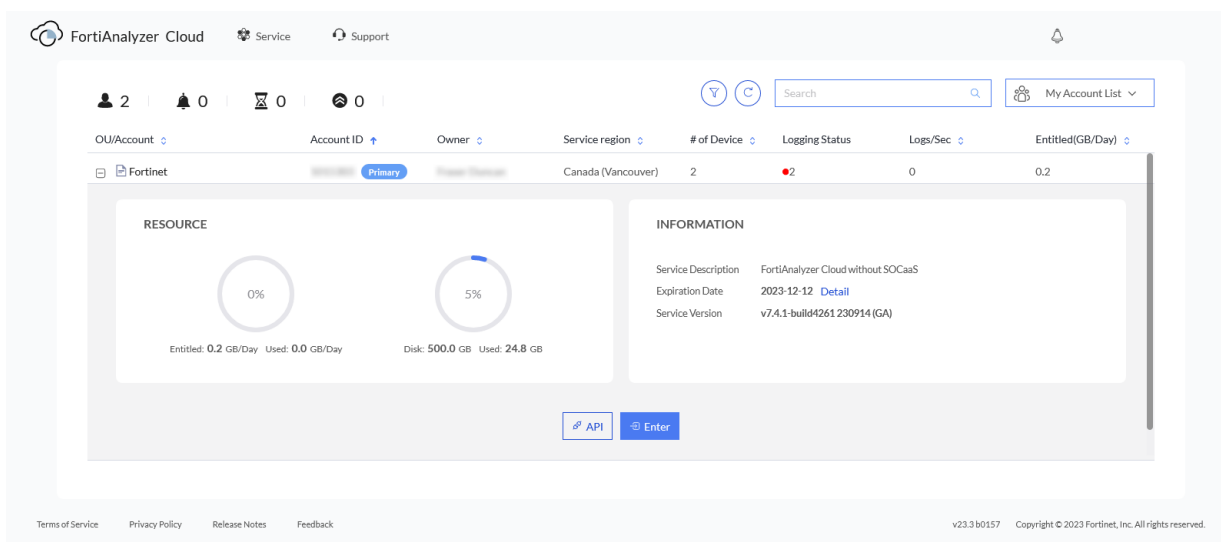
Time Zone (GMT-8:00) Pacific Time (US & Canada)

Submit Cancel

Terms of Service Privacy Policy Release Notes

v23.1 b0141 Copyright © 2023 Fortinet, Inc. All rights reserved.

9. Once provisioned, expand the account, and click *Enter* to access the FortiAnalyzer Cloud instance.



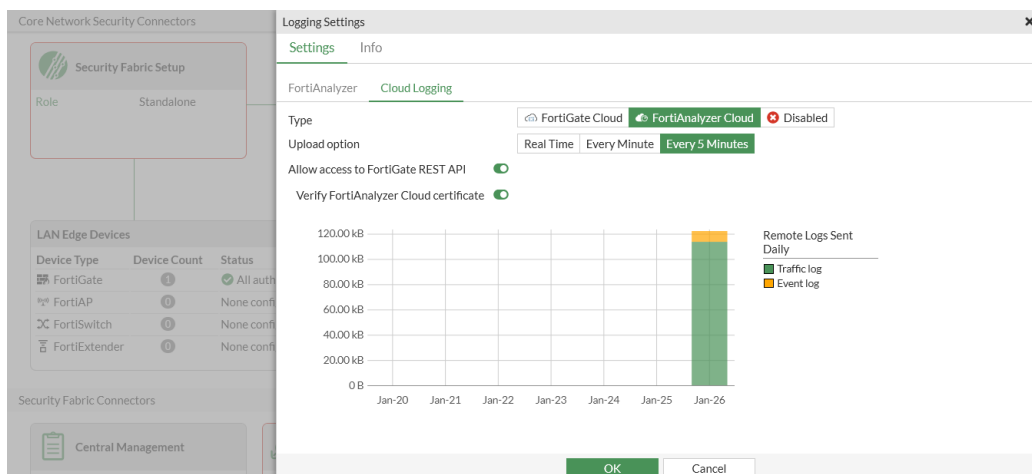
10. (Optional) Upgrade FortiAnalyzer Cloud to 7.6.x. See [Upgrading firmware from the instance on page 25](#).
11. Configure FortiOS to work with FortiAnalyzer Cloud. See [Configuring FortiOS on page 12](#).

Configuring FortiOS

This section explains how to enable FortiOS to send logs to FortiAnalyzer Cloud.

To configure FortiOS:

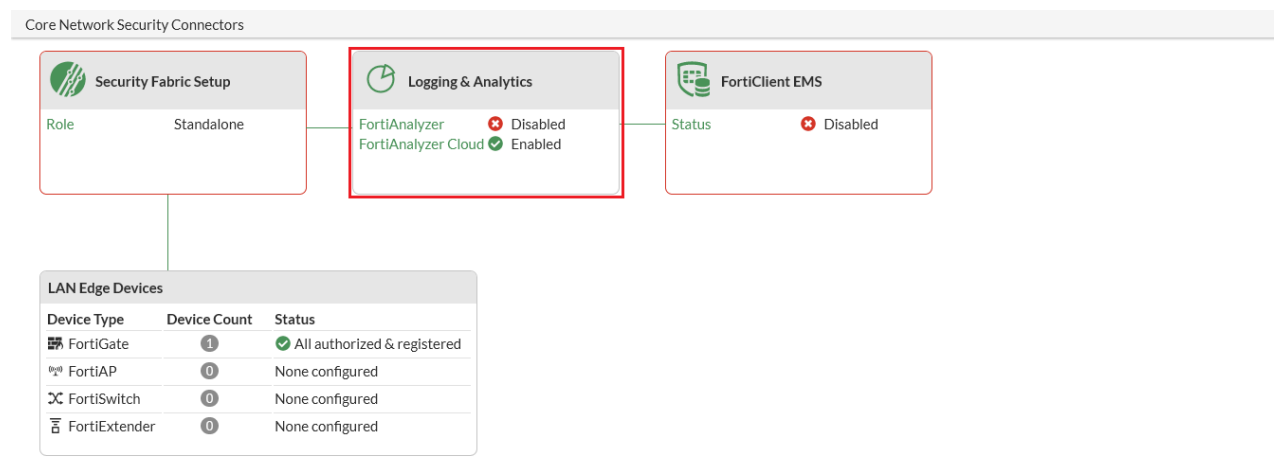
1. In FortiOS, enable FortiAnalyzer Cloud.
 - a. Go to *Security Fabric > Fabric Connectors*, and edit the *Logging and Analytics* card.
 - b. Select the *Cloud Logging* tab, and set the *Type* to FortiAnalyzerCloud.
 - c. Configure the remaining settings to your preference, and click *OK*.



2. In the FortiAnalyzer Cloud instance, go to *Device Manager* and authorize the FortiGate. In some cases, FortiAnalyzer automatically authorizes the FortiGate, and you can skip this step. For

example, FortiAnalyzer can automatically authorize a FortiGate when both devices are part of the same FortiCloud account, and the FortiAnalyzer API can verify the serial number and entitlement for the FortiGate with FortiCare. FortiAnalyzer cannot automatically authorize a FortiGate in an HA cluster or in a Security Fabric.

When successfully authorized, the cloud logging status displays as *Enabled*.



Configuring FortiClient EMS

This section explains how to enable FortiClient EMS 7.0.3 and later to send FortiClient logs to FortiAnalyzer Cloud.

To configure FortiClient EMS:

1. In FortiClient EMS, enable logging to FortiAnalyzer Cloud.
 - a. Go to *Endpoint Profiles > System Settings*.
 - b. Edit the desired profile.
 - c. Under *Log*, enable *Upload Logs to FortiAnalyzer/FortiManager*, and select the types of logs you'd like to send to FortiAnalyzer Cloud.
 - d. In the *IP Address/Hostname* option, enter the fully qualified domain name for the FortiAnalyzer Cloud instance.

Upload UTM Logs	☒
Upload System Event	☒
Upload Security Event	☒
Upload Vulnerability Logs	☐
Upload Event Logs	☐
Send Software Inventory	☐
Send OS Events	☒
Event telemetry interval	60 seconds
IP Address/Hostname	728060.ca-west-3.faz.test.forticloud.
SSL Enabled	☒
Upload Schedule	2 minutes
Log Generation Timeout	90 seconds
Log Retention	60 days

- e. Configure other fields as desired, and save the profile.
2. In the FortiAnalyzer Cloud instance, go to *Device Manager*, and authorize FortiClient EMS. Once FortiClient EMS can reach FortiAnalyzer Cloud, it uploads logs to FortiAnalyzer Cloud as defined by the upload schedule.
3. In FortiAnalyzer Cloud, go to *Log View* to see the log details.

All FortiClient Last 1 Hour 09:21:45 To 10:21:44							logDetails	
#	Date/Time	User	Host Name	Registered to Device	Source IP	Destination IP	Remote Name	
1	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	16	www.espn.com	Date/Time 10:09:01
2	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	16	www.espn.com	Destination End User ID 3
3	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	16	www.espn.com	Destination Endpoint ID 101
4	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	16	www.espn.com	Destination IP 47873
5	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	16	www.espn.com	Destination Port 47873
6	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	16	www.espn.com	Device ID FCTEMS8821006498
7	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	Device IP 192.168.1.6
8	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	Device MAC 00-15-5d-51-6a-44
9	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	Device Name EMSCloud
10	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	Device Time 2022-11-17 10:09:01
11	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	Direction outbound
12	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	Event Type traffic
13	10:07:33	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	79.136	www.goal.com	FortiClient SN FCT8001811593155

FortiClient Version 7.0.7.0345	FortiClientEMS Serial FCTEMS8821006498
FortiGate Serial N/A	Host Name DESKTOP-3SH9CE6
Level info	Log ID 96900
Message Traffic log	OS Microsoft Windows 10 Enterprise
PC Domain N/A	Policy Name Default
Protocol 6	Received
Registered to Device EMSCloud	Remote Name www.espn.com
Security Action blocked	Security Event webfilter
Sent	Service https
Session ID 1575651575	Site default
Source IP 192.168.1.6	Source Name msedge.exe
Source Port 7136	Source Product Microsoft Edge
Sub Type system	Threat General Interest - PersonalSpor
Time Stamp 2022-11-17 10:09:01	Type traffic
UEBA Endpoint ID 1025	UEBA User ID 1025
URL https://www.espn.com/	User Douglas Kephart
User Initiated 0	

Configuring FortiMail

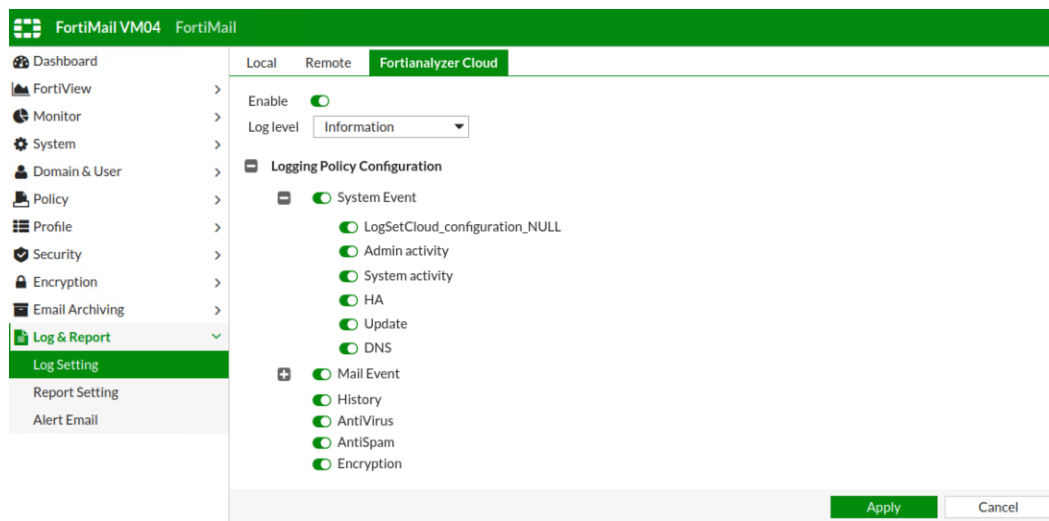
This section explains how to enable FortiMail 7.2.0 and later to send logs to FortiAnalyzer Cloud.

To configure FortiMail:

1. In FortiMail, enable logging to FortiAnalyzer Cloud.

- a. Go to *Log & Report > Log Setting*.
- b. On the *FortiAnalyzer Cloud* tab, toggle on the *Enable* option, and click *Apply*.

As long as FortiMail has the correct license registered with FortiCare, a connection is established with FortiAnalyzer Cloud.

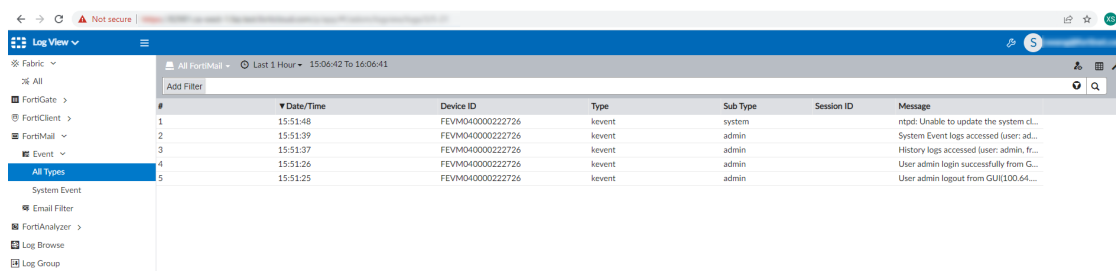


2. In the FortiAnalyzer Cloud instance, go to *Device Manager*, and authorize FortiMail.



After FortiMail is authorized, FortiAnalyzer Cloud can start receiving logs.

3. In FortiAnalyzer Cloud, go to *Log View* to see the logs.



Configuring FortiWeb

FortiWeb supports FortiAnalyzer Cloud, enabling users to store and analyze FortiWeb logs in the cloud.

A valid FortiAnalyzer Cloud (FAZ Cloud) license entitlement and a FortiAnalyzer Cloud storage license are required for log transmission. Upon license expiration, FortiWeb ceases log forwarding, and FortiAnalyzer Cloud rejects incoming logs.

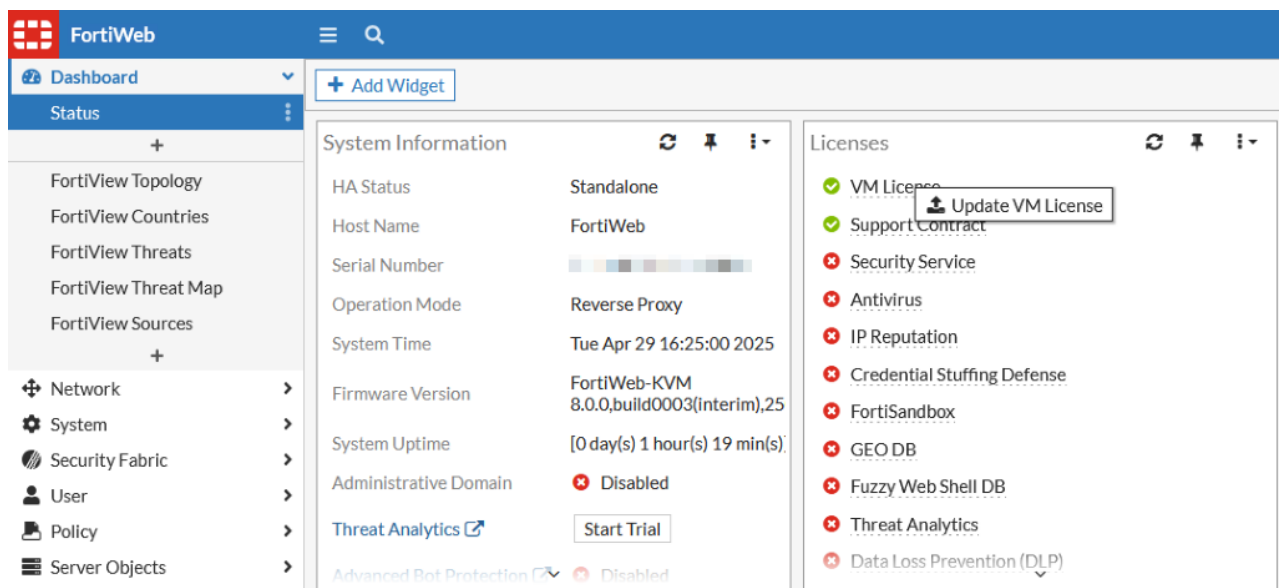
Before configuring FortiAnalyzer Cloud on FortiWeb, verify that the FortiAnalyzer Cloud license is active to ensure proper connectivity and log forwarding. You can check the license status directly from the FortiWeb Dashboard to confirm whether the service is enabled and valid.

FortiWeb must be registered to the same FortiCloud account as FortiAnalyzer Cloud.

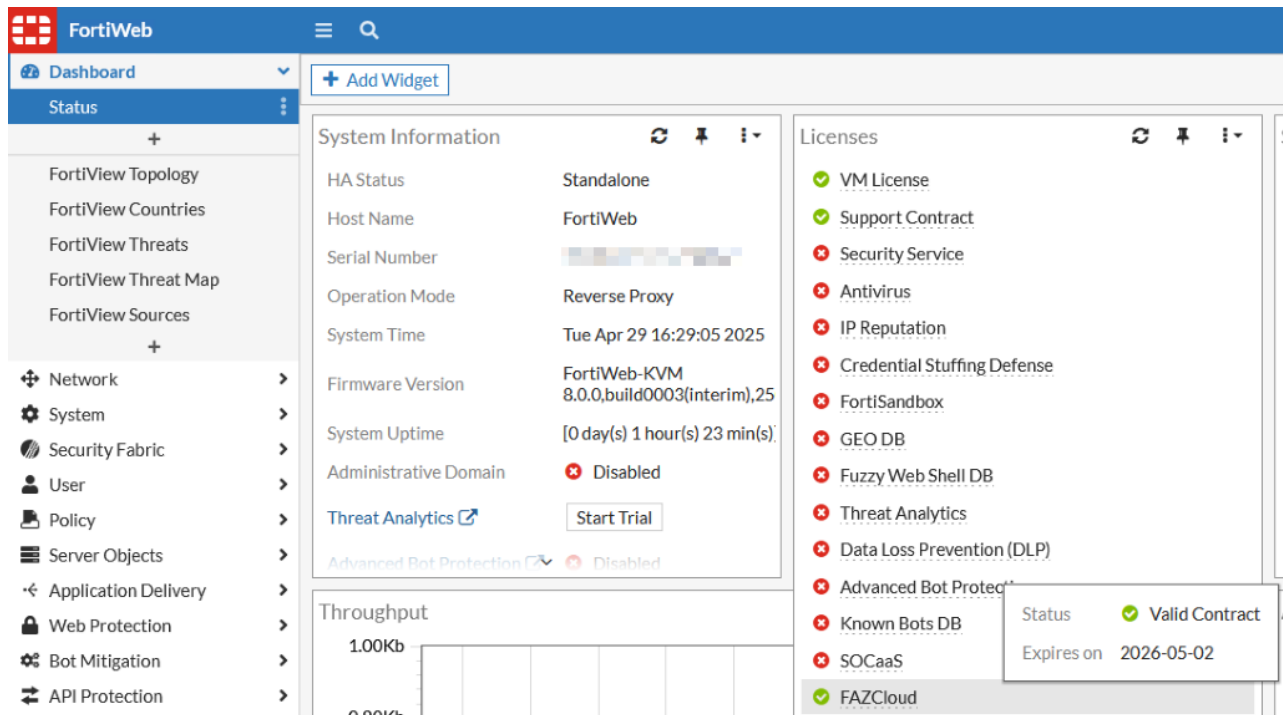
For more information on enabling logging from FortiWeb, see the [FortiWeb Administration Guide](#).

To configure FortiWeb logging to FortiAnalyzer Cloud:

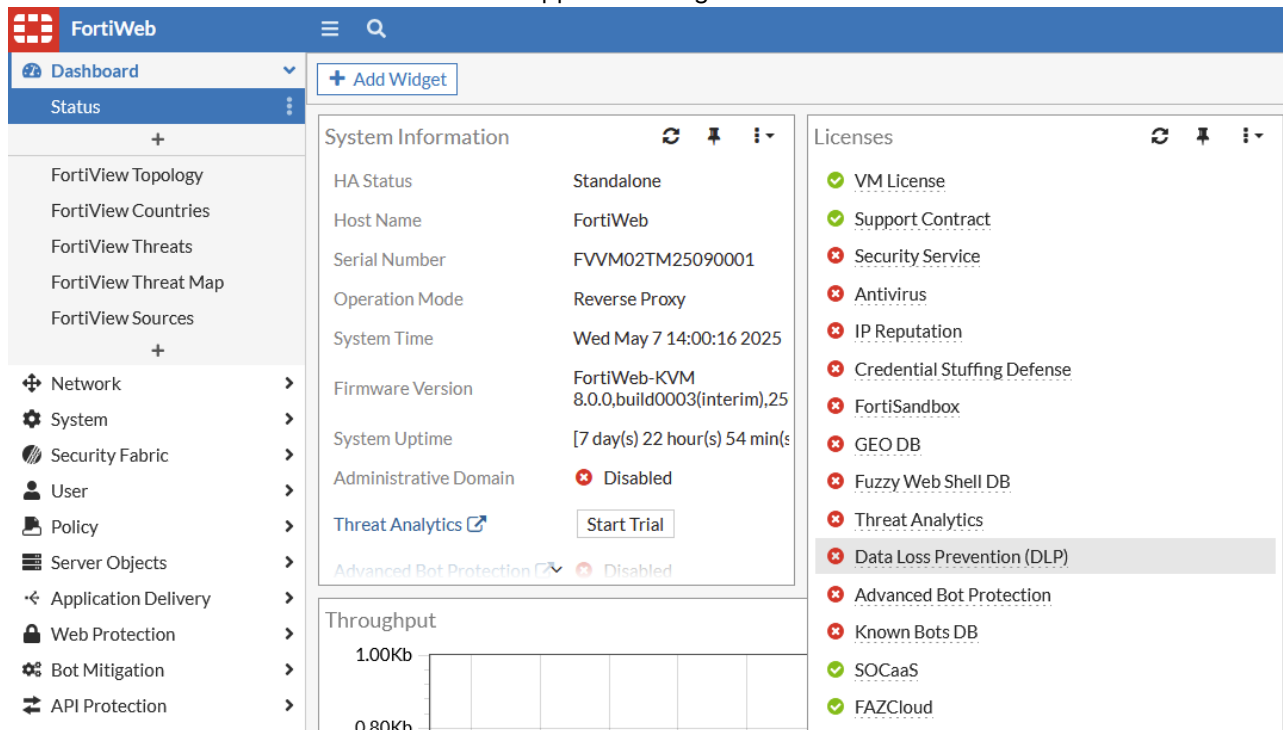
1. On the FortiWeb *Dashboard* > *Status* page, upload the license file which includes the FortiAnalyzer Cloud entitlement.
Once the license file is uploaded, FortiWeb will reboot.



2. From the FortiWeb *Dashboard* > *Status* page, you can view the FortiAnalyzer Cloud (FAZCloud) license status in the Licenses widget.



If a SOCaaS license is also added it will also appear with a green checkmark in the licenses lists.

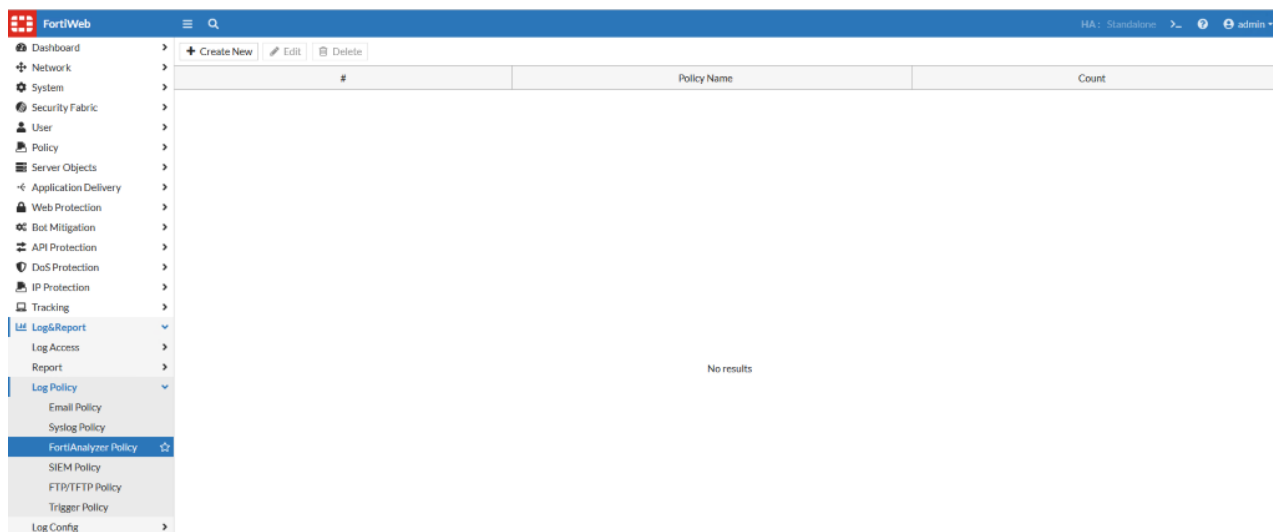


3. On FortiAnalyzer Cloud, go to Device Manager.

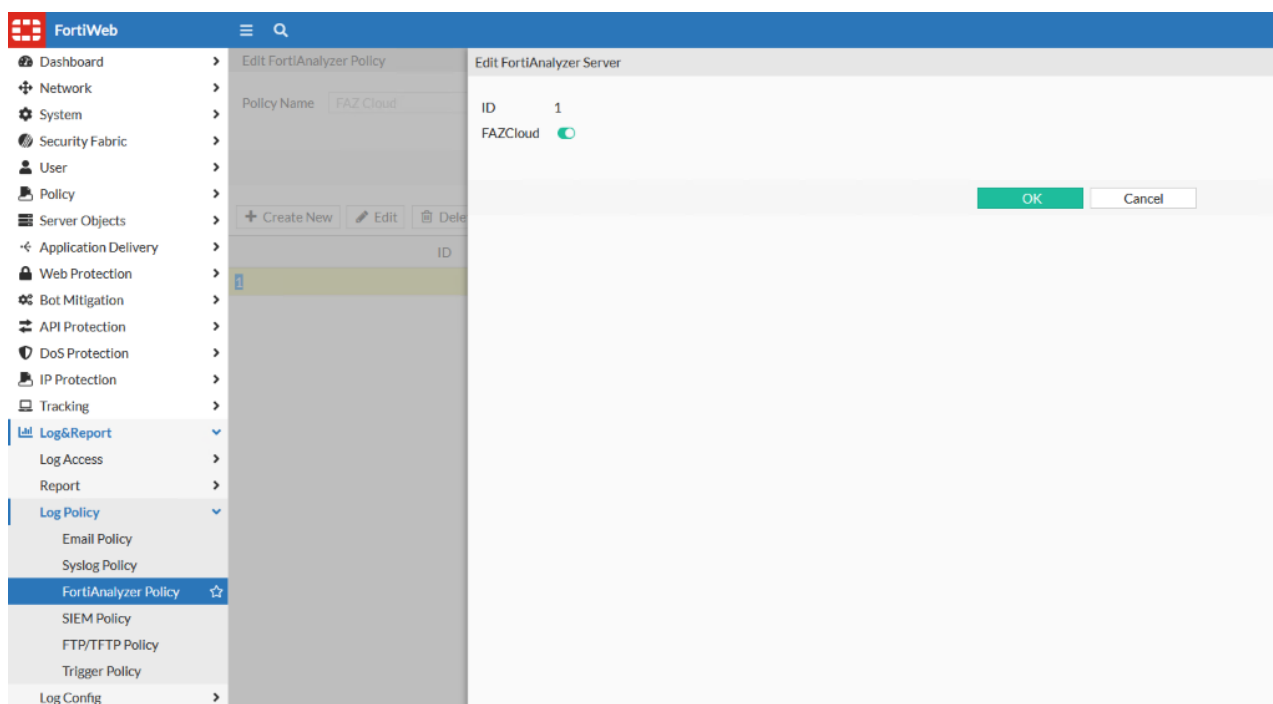
FortiWeb will be automatically added and authenticated to FortiAnalyzer Cloud. You can alternatively manually add the FortiWeb device by entering its serial number in the *Add Device* wizard.

To configure a log policy on FortiWeb:

1. On FortiWeb, go to *Log&Report > Log Policy > FortiAnalyzer Policy*. Click *Create New*.



2. Enter a name for the policy and click *OK*.
3. Click *Create New* to open a slide window. Enable *FAZCloud*, and click *OK*.



4. In *Log&Report > Log Config > Global Log Settings*, enable *FortiAnalyzer* and select the *Log Level*, *FortiAnalyzer Policy*, and *Log Type*.

The screenshot shows the FortiWeb configuration interface. The left sidebar contains a menu with options: Dashboard, Network, System, Security Fabric, User, Policy, Server Objects, Application Delivery, Web Protection, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Log&Report, Log Access, Report, Log Policy, Log Config, Global Log Settings (selected), Other Log Settings, and Sensitive Data Logging.

The main configuration area is titled "Global Log Settings" and includes the following sections:

- Disk:** Log Level (Information), When log disk is full (Overwrite oldest logs), Log Type (Event Log, Attack Log, Traffic Log).
- Syslog:** Syslog Policy (empty), Log Level (Information), Facility (reserved for local use 7), Log Type (Event Log, Attack Log, Traffic Log).
- Custom Fields:** A table with columns "Name" and "Value", and an "Add" button.
- Alert Mail:** Email Policy (empty), Log Type (Event Log, Attack Log).
- FortiAnalyzer:** Log Level (Debug), FortiAnalyzer Policy (FAZ Cloud), Log Type (Event Log, Attack Log, Traffic Log).
- SIEM:** Log Level (Information), SIEM Policy (empty), Log Type (Event Log, Attack Log, Traffic Log).

An "Apply" button is located at the bottom right of the configuration area.

5. Click *Apply*.
6. On FortiAnalyzer Cloud, view FortiWeb logs under *Log View > Logs*.

The screenshot shows the FortiAnalyzer Cloud Log View interface. The left sidebar contains a menu with options: Dashboards, Device Manager, FortiView, Log View (selected), Log Settings, Fabric View, Incidents & Events, FortiAI, Reports, and System Settings.

The main area displays a table of logs with the following columns: #, Date/Time, Device ID, Level, User Interf..., Action, and Message.

#	Date/Time	Device ID	Level	User Interf...	Action	Message
1	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 5, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0
2	2025-04-29 1		information	GUI	login	User admin logged in successfully from GUI->HTTPS(10.254.18.124)
3	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 6, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0
4	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 6, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0
5	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 5, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0
6	2025-04-29 1		information	GUI	logout	User admin timed out on GUI->HTTPS(10.254.18.124)
7	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 5, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0
8	2025-04-29 1		information	GUI	edit	Change configuration attribute fortianalyzer-policy(->FAZ Cloud) for 'log forti-analyzer'
9	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 49, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0
10	2025-04-29 1		information	GUI	delete	Delete configuration for 'log fortianalyzer-policy' 'FAZ on-prem VM'
11	2025-04-29 1		information	GUI	delete	User admin deleted fortianalyzer-policy FAZ on-prem VM from GUI(10.254.18.124)
12	2025-04-29 1		information	GUI	add	Add configuration attribute is-fazcloud(default)->enable for 'log fortianalyzer-policy -> fortianalyzer-server-list' 'FAZ Cloud -> 1'
13	2025-04-29 1		information	GUI	add	Add configuration for 'log fortianalyzer-policy -> fortianalyzer-server-list' 'FAZ Cloud -> 1'
14	2025-04-29 1		information	GUI	add	User admin added fortianalyzer-policy FAZ Cloud member 1 from GUI(10.254.18.124)
15	2025-04-29 1		information	system	monitor	Performance statistics: Average CPU: 5, Memory: 23, Total Connections: 0, Total Connections / Second: 0, Total Http Throughput: 0

Configuring FortiNDR

This section explains how to send FortiNDR logs to FortiAnalyzer Cloud.

Sending logs from FortiNDR to FortiAnalyzer Cloud has following prerequisites:

- FortiAnalyzer Cloud must include a storage add-on license. See [Licensing on page 6](#).
- Both products must be registered to the same FortiCloud account.
- You must use a supported FortiNDR firmware version and model. See the [FortiAnalyzer Cloud Release Notes](#).

To configure FortiNDR to send logs to FortiAnalyzer Cloud:

1. In FortiNDR, go to *Log & Report > Log Settings*.
2. Select *Enable* for *Send logs to FortiAnalyzer Cloud* under *FortiAnalyzer Cloud settings*, and click *Apply*.

The screenshot shows the FortiNDR-VM-KVM interface with the 'Log Settings' page open. The left sidebar lists various system components, with 'Log & Report' expanded and 'Log Settings' selected. The main content area is divided into three sections:

- FortiAnalyzer/FortiSIEM settings:** Includes a toggle for 'Send logs to FortiAnalyzer/FortiSIEM' (set to 'Enable'), a dropdown for 'Type' (set to 'OFTPS (FortiAnalyzer only)'), and input fields for 'Log Server Address' (0.0.0.0) and 'Port' (514).
- Syslog Server settings:** Includes a toggle for 'Send logs to Syslog Server 1' (set to 'Enable'), a dropdown for 'Type' (set to 'Syslog Protocol'), and input fields for 'Log Server Address' (0.0.0.0) and 'Port' (514).
- FortiAnalyzer Cloud settings:** Includes a toggle for 'Send logs to FortiAnalyzer Cloud' (set to 'Enable') and a 'Test connection' button.

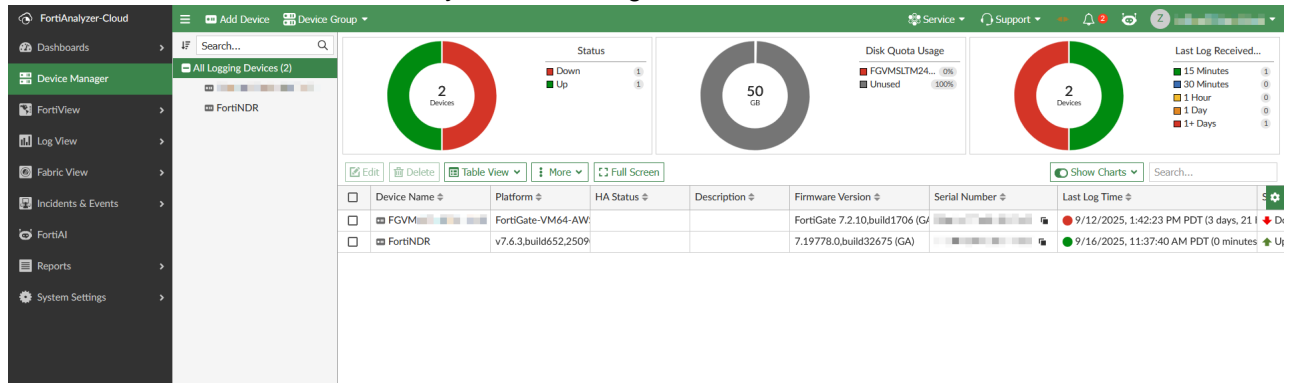
At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons. The 'Apply' button is highlighted in red.



If a valid FortiAnalyzer Cloud storage add-on license is not registered in FortiCloud, attempting to enable the *Send logs to FortiAnalyzer Cloud* setting will fail.

3. In FortiAnalyzer Cloud, go to the *Device Manager* and click *Add Device*.

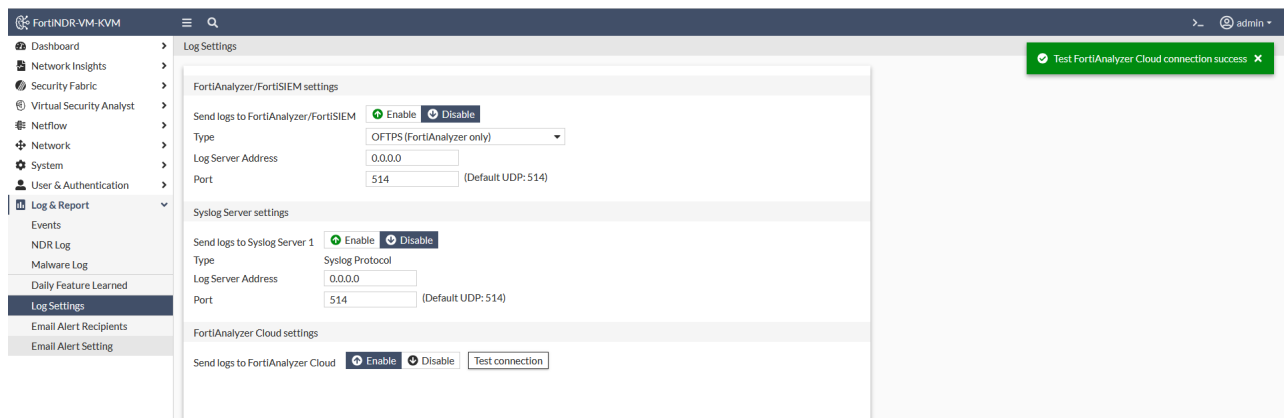
4. Add the FortiNDR device to FortiAnalyzer Cloud using its serial number.



5. On FortiNDR, use the *Test connection* button to test and troubleshoot network connections. When FortiNDR has the correct license registered with FortiCare, the connection will be established with FortiAnalyzer Cloud, and a *Test FortiAnalyzer Cloud connection success* message is displayed.

In the event that *Test connection* fails, check the following:

- Verify that the correct license registered in FortiCloud.
- Ensure that the FortiNDR model is supported by your FortiAnalyzer Cloud. See the [FortiAnalyzer Cloud Release Notes](#).
- Ensure that the FortiNDR device information (serial number and model) is added manually to the device list in your FortiAnalyzer Cloud instance.



6. Once FortiNDR is configured to send logs to FortiAnalyzer Cloud, you can configure log categories and severity level on FortiNDR using the CLI config system syslog cloud settings. See the [FortiNDR CLI Reference Guide](#) for more information.

Configuring third-party log forwarding from an on-premise FortiAnalyzer

FortiAnalyzer Cloud cannot directly accept third-party application logs. Instead, an on-premise FortiAnalyzer can be configured to securely forward logs to FortiAnalyzer Cloud using a FortiAnalyzer Cloud connector. In this way, FortiAnalyzer Cloud can be used for centralized logging for third-party applications.

The FortiAnalyzer Cloud connector requires an access token from FortiAnalyzer Cloud to establish a secure connection with FortiAnalyzer Cloud.

Access tokens can be created, renewed, edited, and deleted from the FortiAnalyzer Cloud GUI.

Once a token has been created, you can configure a FortiAnalyzer Cloud connector on the on-premise FortiAnalyzer to enable it to forward logs to FortiAnalyzer Cloud.

See the [FortiAnalyzer Administration Guide](#) for details.

To configure logging from third-party devices:

1. On your on-premise FortiAnalyzer, configure third-party application logging. See [Adding devices](#).
2. On FortiAnalyzer Cloud, create an access token for the *FortiAnalyzer Cloud connector*. [Managing access tokens on page 22](#).
3. On your on-premise FortiAnalyzer, create the *FortiAnalyzer Cloud connector* using your access token. See [Active connectors](#).

Once the connector has been enabled, the on-premises FortiAnalyzer will forward logs to FortiAnalyzer Cloud.

The *FortiAnalyzer Cloud connector* can query FortiAnalyzer Cloud with the token. FortiAnalyzer will suspend forwarding logs to FortiAnalyzer Cloud when the token is expired or invalid.



On the FortiAnalyzer Cloud account, a valid add on storage license (for example FC1-10-AZCLD-463-01-24) is necessary. Without the license, creating or renewing of the token will fail.

Managing access tokens

To create a FortiAnalyzer Cloud access token:

1. In the FortiAnalyzer Cloud GUI, open the portal toolbar menu on the username.
2. Click *Access Token Settings*.
3. Click *Create New*.
4. Enter the following information to configure the token:

Token Name	Enter a name for the token.
Comment	Optionally, provide a comment.

5. Click *OK* to show the token.
An option is available to copy the token text. Please keep the token safe and secure. The token won't show again in the webpage and can only be downloaded.

To edit or delete a FortiAnalyzer Cloud access token:

1. In the FortiAnalyzer Cloud GUI, open the portal toolbar menu on the username.
2. Click *Access Token Settings*
The *Access Token* menu is displayed with a list of configured access tokens.
3. Select an access token from the list and click *Edit* or *Delete*.

To renew a FortiAnalyzer Cloud access token:

1. In the FortiAnalyzer Cloud GUI, open the portal toolbar menu on the username.
2. Click *Access Token Settings*.
The *Access Token* menu is displayed with a list of configured access tokens.
3. Select an access token from the list and click *Renew*. Click *OK* to confirm the renewal.
A new token that is valid for 90 days will replace the selected token.

To download a FortiAnalyzer Cloud access token:

1. In the FortiAnalyzer Cloud GUI, open the portal toolbar menu on the username.
2. Click *Access Token Settings*.
The *Access Token* menu is displayed with a list of configured access tokens.
3. Select an access token from the list and click *Download*.
4. Enter an *Encrypt Password* for the token, and click *OK*. Download of a zipped file including the token will start.
5. To unzip the downloaded file, you will need to enter the *Encrypt Password* configured in the previous step. After the *Encrypt Password* is entered, the token in the file will be available to be used in the FortiAnalyzer Cloud connector.

Using FortiAnalyzer Cloud

After you have deployed FortiAnalyzer Cloud and configured FortiOS, you are ready to use the instance. Using FortiAnalyzer Cloud is similar to using FortiAnalyzer.

For information about using FortiAnalyzer and FortiAnalyzer Cloud, see the [FortiAnalyzer 7.2.1 Administration Guide](#).

This section includes the following topics that are specific to using FortiAnalyzer Cloud:

- [Accessing your FortiAnalyzer Cloud instance on page 24](#)
- [Upgrading firmware from the instance on page 25](#)
- [Using the FortiAnalyzer Cloud toolbar on page 26](#)
- [Enabling managed SOC service from FortiAnalyzer Cloud on page 31](#)
- [Using FortiAI on FortiAnalyzer Cloud on page 34](#)

Accessing your FortiAnalyzer Cloud instance

After deploying one or more FortiAnalyzer Cloud instances, you can access the instances through one of the methods below:

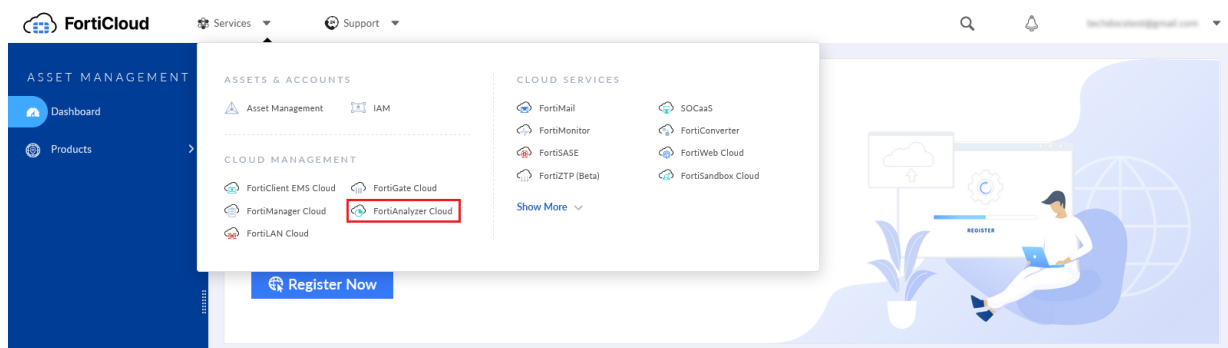
1. Go to <https://fortianalyzer.forticloud.com>. After authentication, you are redirected to your own FortiAnalyzer Cloud instance.
2. Go directly to your instance using the specific URL for your instance (e.g. `https://{account_id}.{region}.fortianalyzer.forticloud.com`). You can obtain your instance's URL from your browser's address bar once you have accessed FortiAnalyzer Cloud through one of the previous methods.
3. Access FortiAnalyzer Cloud through FortiCloud. See [Access FortiAnalyzer Cloud through FortiCloud on page 24](#).

Access FortiAnalyzer Cloud through FortiCloud

To access FortiAnalyzer Cloud through FortiCloud:

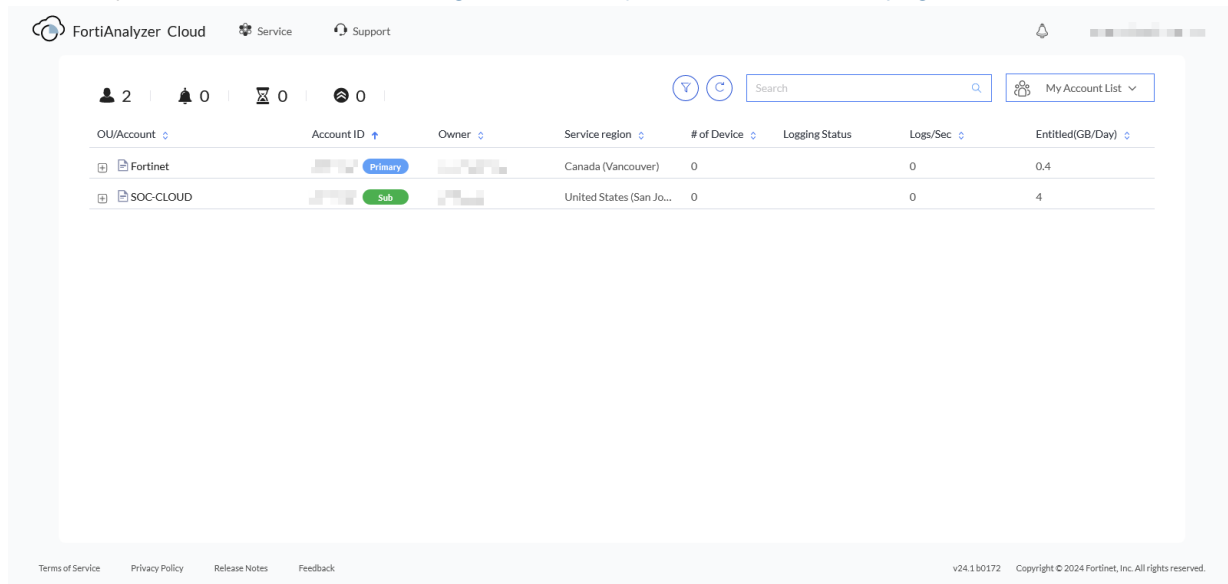
1. Go to FortiCloud (<https://support.fortinet.com/>), and use your FortiCloud account credentials to log in. The FortiCloud portal is displayed.

- From the **Services** menu, select *FortiAnalyzer Cloud* under *Cloud Management*.



You are automatically logged in to your FortiAnalyzer instance.

- You can navigate between accounts or return to the FortiAnalyzer Cloud portal using the options in the FortiAnalyzer Cloud toolbar. See [Using the FortiAnalyzer Cloud toolbar on page 26](#).



Upgrading firmware from the instance

For information about upgrading firmware, see the [FortiAnalyzer Cloud Release Notes](#).

Identifying the public IP address

You can use the FortiAnalyzer Cloud CLI to determine the public IP address for FortiAnalyzer Cloud.

To determine the public IP address:

1. Access the instance. See [Accessing your FortiAnalyzer Cloud instance on page 24](#).
2. Open the CLI console by clicking the CLI option from the FortiAnalyzer Cloud toolbar. See [Using the FortiAnalyzer Cloud toolbar on page 26](#).
3. In the CLI console, run the following commands:


```
diagnose debug enable
diagnose test application vmd 20
173.243.137.11
```

In this example, the public IP address for FortiAnalyzer Cloud is 173.243.137.11. You can use the public IP address to set up connections with third-party services, such as LDAP or AWS Management Portal for vCenter.

Using the FortiAnalyzer Cloud toolbar

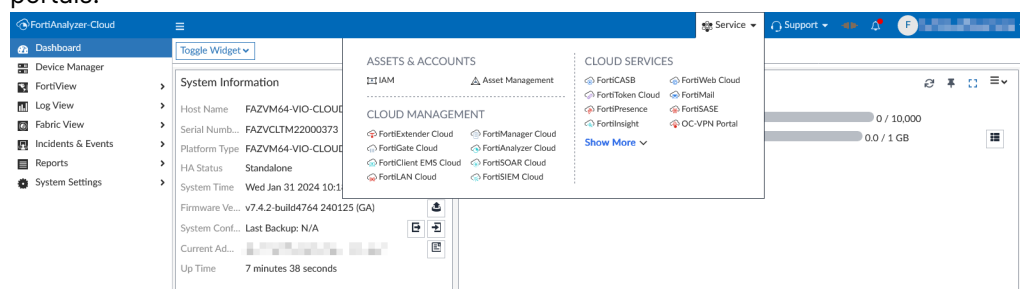
You can access FortiCloud services and support links from the FortiAnalyzer Cloud toolbar.

The FortiAnalyzer toolbar includes the following dropdown menus:

- [Service on page 26](#)
- [Support on page 27](#)
- [Notifications on page 27](#)
- [Account on page 27](#)

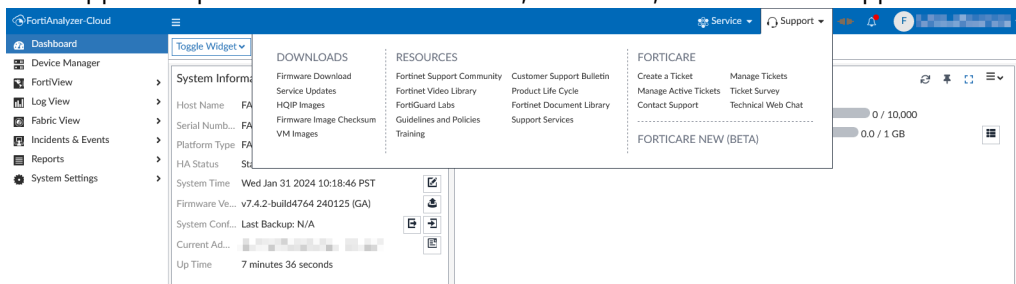
Service

The Service dropdown includes FortiCloud services (for example, IAM and Asset Management) and other cloud portals.



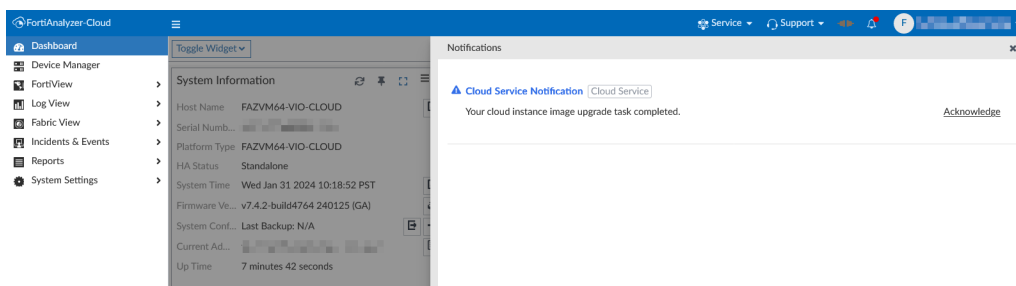
Support

The support dropdown includes downloads, resources, and FortiCare support links.



Notifications

Click the notification icon  to open the notification drawer and view and interact with notifications for FortiAnalyzer Cloud.

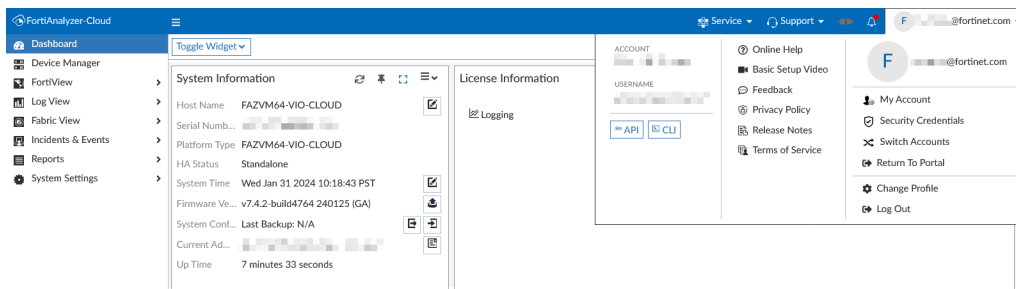


Account

The account dropdown includes links and services related to your FortiCloud account and the FortiAnalyzer instance. Available options include the following:

Account	Your account ID.
Username	Your current username.
API and CLI	Open the API User or CLI pane.
Help Content	Links for Online Help, Basic Setup Videos, Feedback, Privacy Policy, Release Notes, and Terms of Service.
FortiCloud Account Links	FortiCloud account links including My Account, Security Credentials, Subscriptions, Return to Portal, ChangeProfile, and Log Out.
My Account	Go to the FortiCloud Account Profile page.

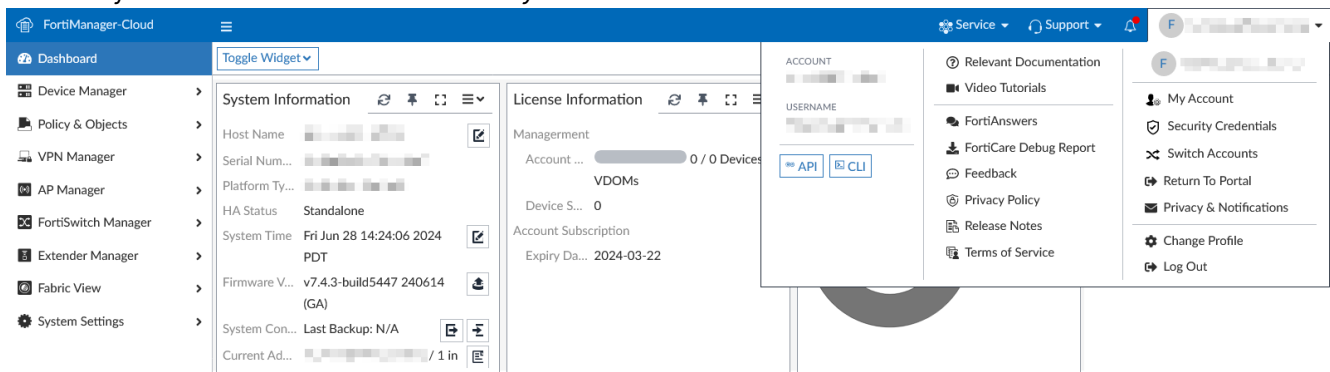
Security Credentials	Go to the FortiCloud Security Credentials page.
Switch Accounts	Switch between available accounts.
Return to Portal	Return to the FortiAnalyzer Cloud portal.
Change Profile	Change FortiAnalyzer Cloud profile options including avatar and theme.
Privacy & Notifications	Click to access the <i>Privacy & Notification</i> menu where you can configure access settings for the FortiCloud team as well as email notification preferences. See Privacy and notification preferences on page 28 .
Log Out	Log out of FortiAnalyzer Cloud.



Privacy and notification preferences

You can configure privacy and notification preferences from within the FortiAnalyzer Cloud instance.

To access your privacy and notification preferences, click your user account dropdown from the FortiAnalyzer Cloud toolbar and click *Privacy & Notification*.



In *Privacy & Notifications*, you can configure the following:

- [Access Settings on page 29](#)
- [Email Notifications on page 29](#)

Access Settings

Access settings determine what level of access Fortinet's cloud operation team has in order to diagnose and perform maintenance on your cloud instance. The following access levels are available:

Privacy & Notifications ✕

Access Settings

☒ **Service Maintenance (Recommended)**

Fortinet's cloud operation team can access diagnostic data and perform maintenance operations on your cloud instance. However, they only have access to system-level data and do not access personal data like logs, reports, or device configurations. This level ensures the smooth operation of services.

☐ **Full Access**

Fortinet personnel can access your account with full privileges for support services, including personal data such as logs, reports, and device configurations for troubleshooting.

☐ **No Access**

The most restrictive control, where Fortinet personnel has no access to your cloud instance. With no access, the cloud operation team cannot access diagnostic data or perform maintenance tasks, and the smooth operation of the service cannot be guaranteed when this level is selected.

Service Maintenance (Recommended)

Fortinet's cloud operation team can access diagnostic data and perform maintenance operations on your cloud instance. However, they only have access to system-level data and do not access personal data like logs, reports, or device configurations. This level ensures the smooth operation of services.

This is the default level of access.

Full Access

Fortinet personnel can access your account with full privileges for support services, including personal data such as logs, reports, and device configurations for troubleshooting.

No Access

The most restrictive control, where Fortinet personnel has no access to your cloud instance. With no access, the cloud operation team cannot access diagnostic data or perform maintenance tasks, and the smooth operation of the service cannot be guaranteed when this level is selected.

Select your preferred access level and click *OK*.

FortiAnalyzer Cloud records changes to access settings in the *Event Log*.

Email Notifications

Email notification preferences can be configured through your FortiAnalyzer instance.

To configure email notification preference:

1. Select your account dropdown from the FortiAnalyzer Cloud toolbar.
2. Select *Privacy & Notifications*.
3. Enable the *Receive Email Notifications* toggle to enable email notifications for the account owner or disable it to stop email notifications.

4. Optionally, you can enable the *Other Recipients* toggle to configure email notifications for other users:

Email Notification

☒ **Receive Email Notifications**
Enable or disable email alerts sent to the account owner. Disabling emails does not stop notifications in the notification bell.

☒ **Other Recipients**
Add other users to receive email alerts in addition to the account owner.

Status	Name	Trigger	Email Recipients	Description	Action
☒	New Email	New Release Notifica...	 x +		x +

Status	Toggle the notification preference on or off. Notifications are only sent when the status of the notification preference is enabled.
Name	Enter a name for the notification preference.
Trigger	Select a trigger condition from the dropdown menu from one of the following: • New Release Notification • Storage Over Usage • Service Renewal Notification
Email Recipients	Click to add at least one email recipient. You can select IAM/Sub users from the populated list or click the <i>Email Address</i> tab to add additional emails. You can also click the x icon next to each email recipient to remove them from the email notification.
Description	Add an optional description.
Action	You can use the action field to delete an email notification preference or create additional notifications preferences.

5. Click *OK*. FortiAnalyzer Cloud records changes to email notification preferences in the *Event Log*.

Unsubscribing from email notifications

An unsubscribe link is included in notification emails. Clicking the unsubscribe option will unsubscribe the account owner from all cloud email notifications. If you are not logged in when you click the unsubscribe option you will be prompted to log in before the action is completed.

When the account is unsubscribed using this link, the *Receive Email Notifications* toggle under *Privacy & Notifications > Email Notification* settings will be set to disabled. Account owners can also disable the Receive Email Notifications toggle directly from *Privacy & Notifications*.

To unsubscribe non-account owner user from email notifications, you can remove their email account from the *Other Recipients* notification preference in *Privacy & Notifications*.

Enabling managed SOC service from FortiAnalyzer Cloud

FortiCloud SOCaaS provides scalable security operations services designed to help you maintain continuous Cyber Awareness and control of your Fortinet Security Fabric network. For more information, see SOCaaS in the [Fortinet Document Library](#).

With a valid license, you can enable the *Managed SOC Service* option in FortiAnalyzer Cloud. When enabling the service, you are redirected to the SOCaaS Portal where you can complete the onboarding process.



- The SOCaaS license includes a complimentary FortiAnalyzer Cloud instance.
- The daily log limit for FortiAnalyzer Cloud is based on the FortiGate model and can be increased by purchasing the FortiAnalyzer Cloud storage add-on licenses. See [Licensing on page 6](#)

To disable the service, submit a service request from the SOC portal.

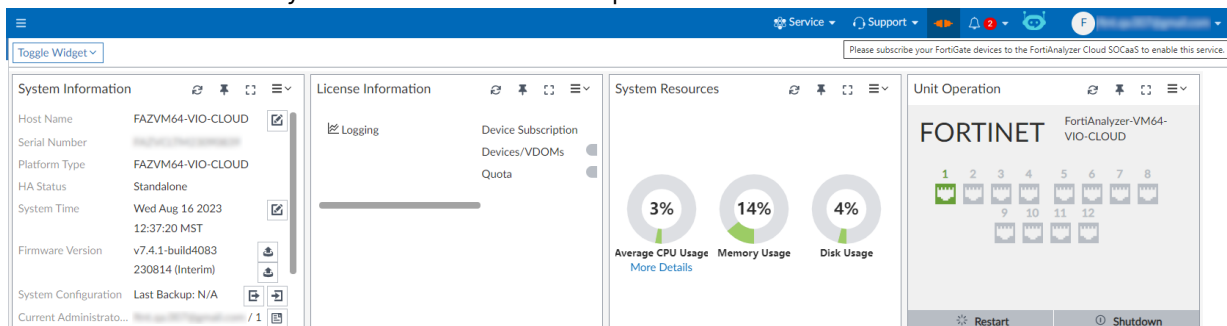
Prerequisites

Before you configure FortiAnalyzer Cloud to send logs to SOCaaS, ensure the following:

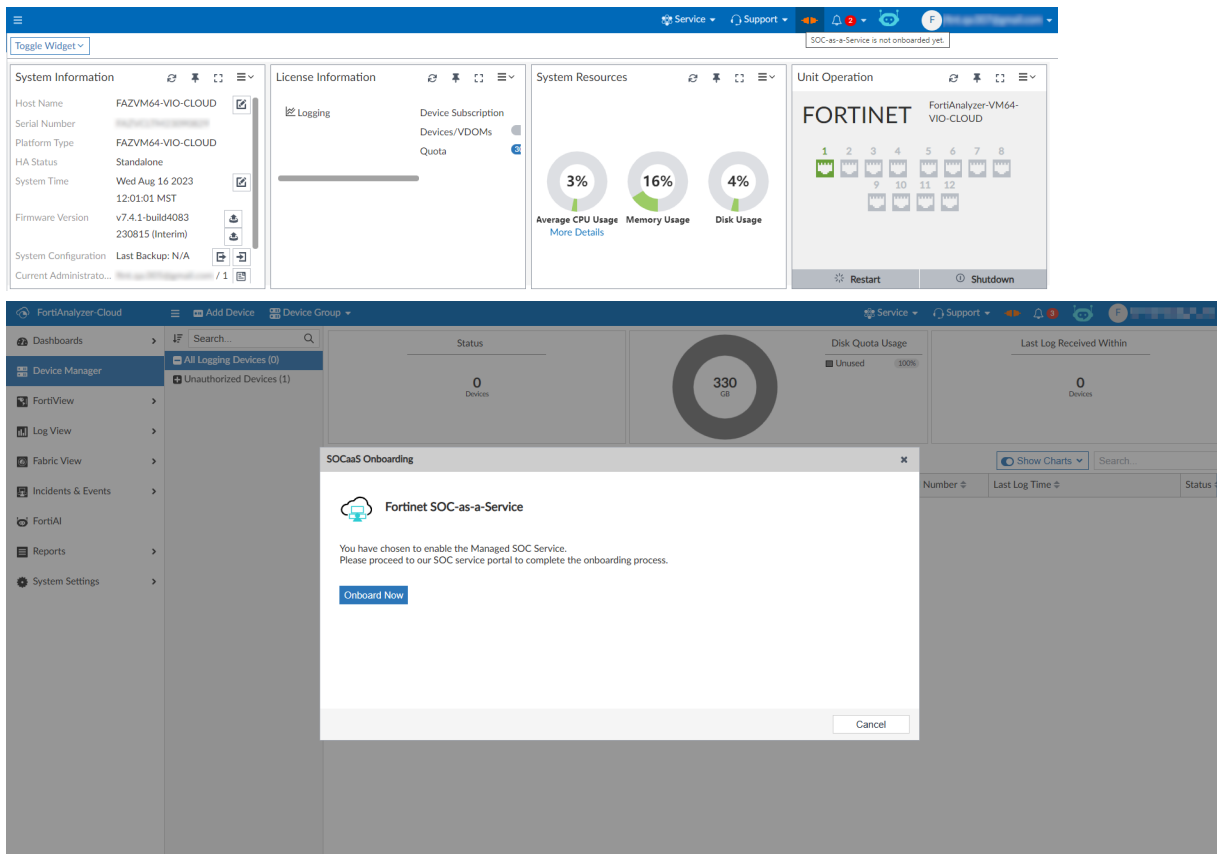
1. You have provisioned the FortiAnalyzer Cloud instance on the region of your choice. See [Deploying a FortiAnalyzer Cloud instance on page 10](#).
2. You have configured the FortiGate to send the entitled device logs to the SOCaaS collection point (FortiAnalyzer Cloud) that will forward the logs. See [Configuring FortiOS on page 12](#).

To configure FortiAnalyzer Cloud:

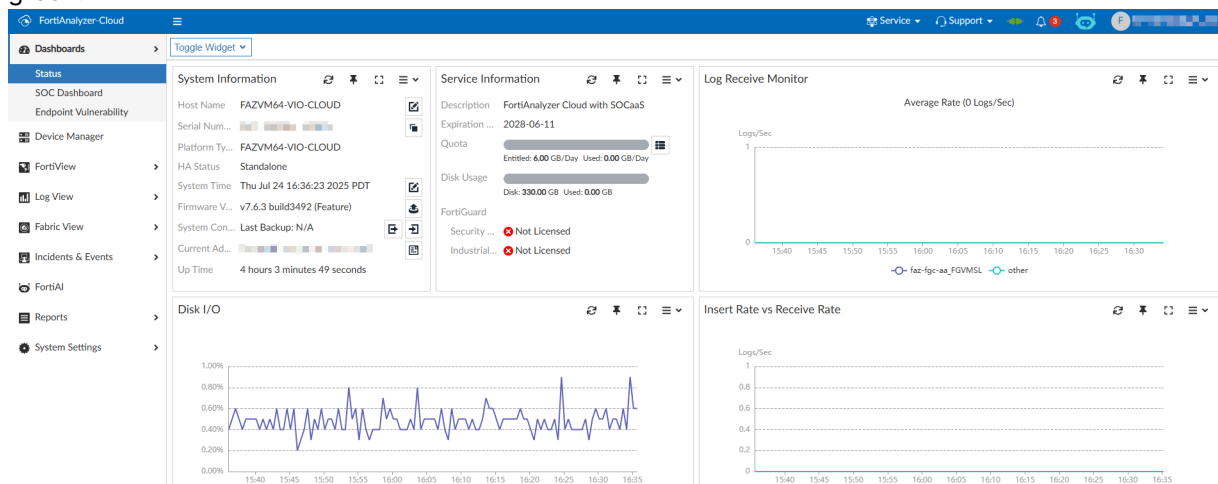
1. Log in to FortiAnalyzer Cloud.
2. Click on the *SOCaaS* connection icon at the top of the GUI. A SOCaaS entitlement is required to enable the service.
 - a. Without the correct entitlement, a message is displayed advising you to subscribe your FortiGate devices to the FortiAnalyzer Cloud SOCaaS subscription.



- b. With the correct entitlement, the SOCaaS Onboarding window opens. Click *Onboard Now* to be redirected to the SOCaaS portal where you can complete your onboarding. See the [SOCaaS User Guide](#).



- Once onboarded to SOCaaS, the FortiAnalyzer Cloud SOCaaS icon is no longer clickable and is displayed in green.



- Configure a log buffer cache size that accommodates 24 hours of logs in your FortiAnalyzer Cloud to avoid log dropping in case of abrupt disconnection between your FortiAnalyzer and SOCaaS. See [Configure log buffer cache size on page 33](#).

Configure log buffer cache size

In case of abrupt disconnection between FortiAnalyzer Cloud and SOCaaS, logs will only be cached for the amount of time allowed based on the cache size available. Logs exceeding the available cache storage time are dropped. To avoid log dropping in such cases, we recommended that you configure a log buffer cache size that accommodates 24 hours of logs in FortiAnalyzer Cloud using the following formula:

$$\text{Average Lograte} * 200 * \text{seconds in 1 day (86400)} * 1.2 = \text{Cache Size logfwd}$$

For more information on log forwarding buffers and how log forwarding space allocation works, see the [FortiAnalyzer Administration Guide](#).

Determining the average log rate

The average log rate is the average logs received on your FortiAnalyzer device for 24 hours.

To retrieve average log rate data for your FortiAnalyzer:

1. Go to *Dashboards > Status*.
2. Open the *Settings* for the *Insert Rate vs. Receive Rate* widget.
3. From the *Time Period* dropdown, select *Last 24 Hours*.
4. Click *OK*.
5. View the graph details, and use the peak log rate as the number for the average lograte count. Use this average log rate to calculate the buffer cache size.

The following table provides three example scenarios for calculating the log forwarding buffer cache size for a small, medium, and enterprise business:

Customer size	Average log rate	Calculation	Buffer cache size
Small	100 logs/sec	$100 * 200 * 86400 * 1.2$	2GB
Medium	1000 logs/sec	$1000 * 200 * 86400 * 1.2$	20GB
Enterprise	10000 logs/sec	$10000 * 200 * 86400 * 1.2$	200GB

For more information about sizing, see the [FortiAnalyzer Architecture Guide](#).

6. In the FortiAnalyzer CLI, set the log buffer cache size in GB using the following command

```
config system global
set log-forward-cache-size <integer>
```

7. When prompted, enter Y to confirm the change.

For more information about log forwarding buffers and how log forwarding space allocation works, see [Log forwarding buffer](#).

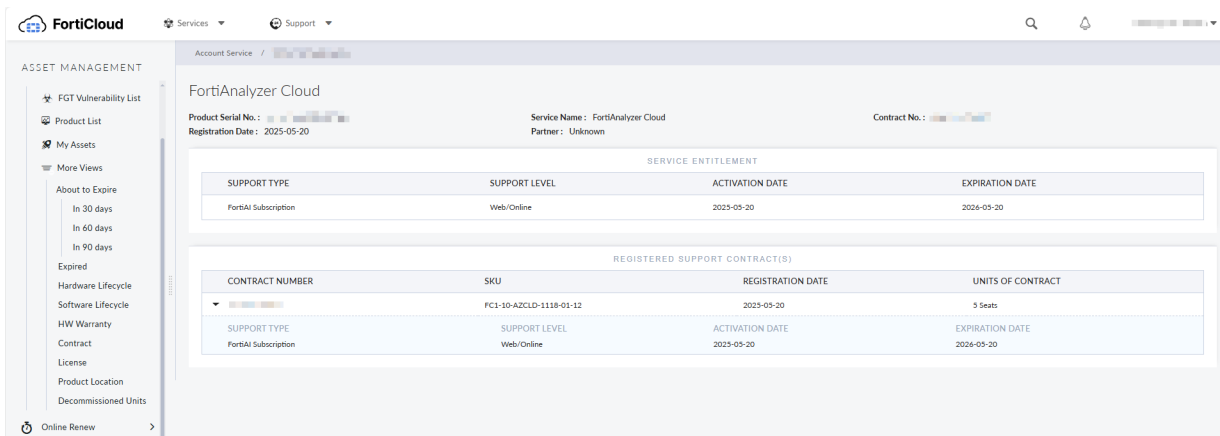
Using FortiAI on FortiAnalyzer Cloud

The FortiAI service can only be enabled on FortiAnalyzer Cloud when a valid license has been registered on FortiCloud. Without a valid license, you will see an option to instead *Purchase FortiAI License*.

To use FortiAnalyzer on FortiAnalyzer Cloud:

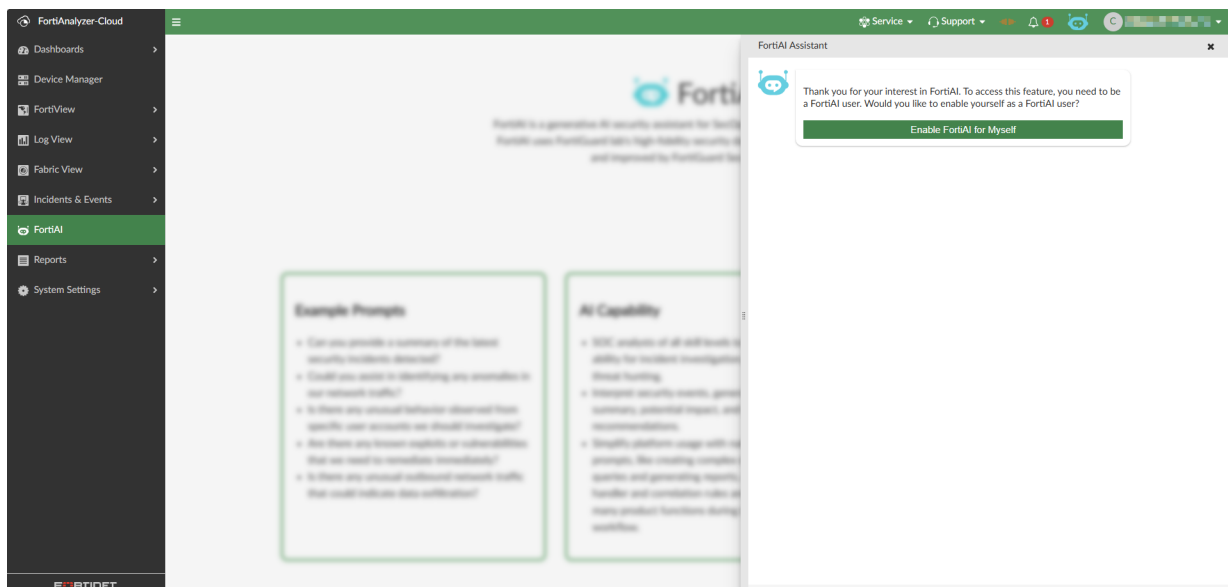
1. Register your FortiAI license on FortiCloud.

After registration is complete, the FortiAI subscription can be found as a registered support contract within the FortiAnalyzer Cloud asset in FortiCloud.

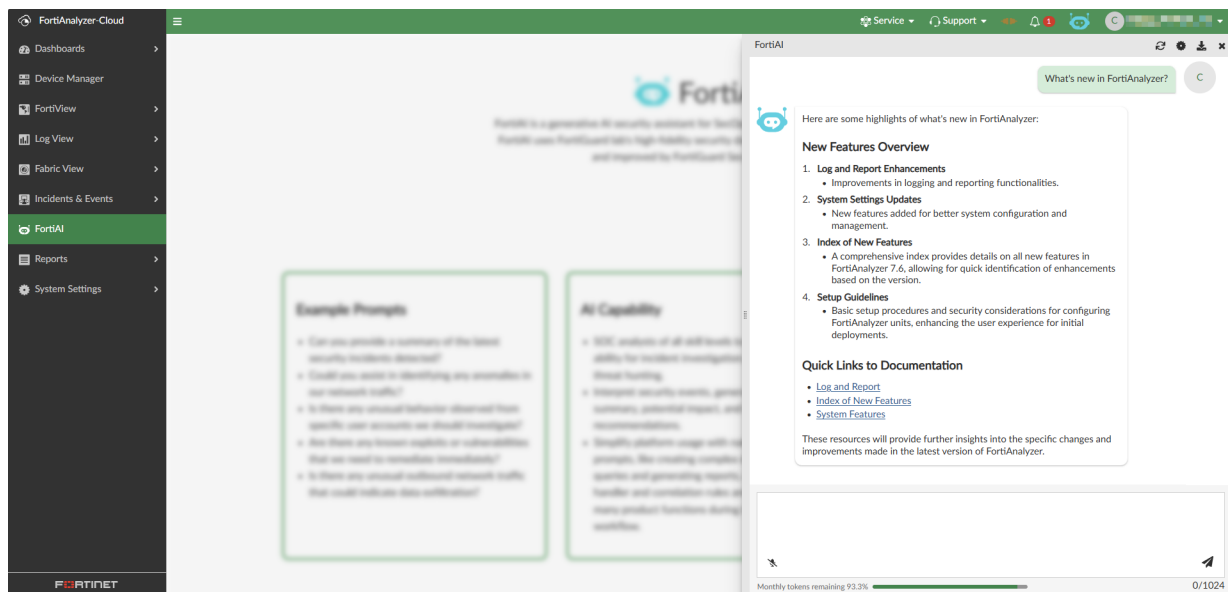


2. Go to FortiAnalyzer Cloud and enable the FortiAI service.

- Sign into FortiAnalyzer Cloud.
- Click on the FortiAI icon in the toolbar.
- Click *Enable FortiAI for Myself*.



3. Enter a query to begin using FortiAI.



Configuration and log backups

Customers are encouraged to create back ups of their FortiAnalyzer configuration and set a log backup strategy. Creation and maintenance of these backups are the customer's own responsibility.

For more information on how to back up your configuration and set a log backup strategy, see the following resources:

- [Backing up the system](#)
- [Set up a log backup strategy](#)

Using the FortiAnalyzer Cloud & Service portal

After deploying a FortiAnalyzer Cloud instance, you can use the FortiAnalyzer Cloud & Service portal to view and navigate between instances.

- [Viewing the FortiAnalyzer Cloud portal on page 36](#)
- [Providing feedback on page 38](#)

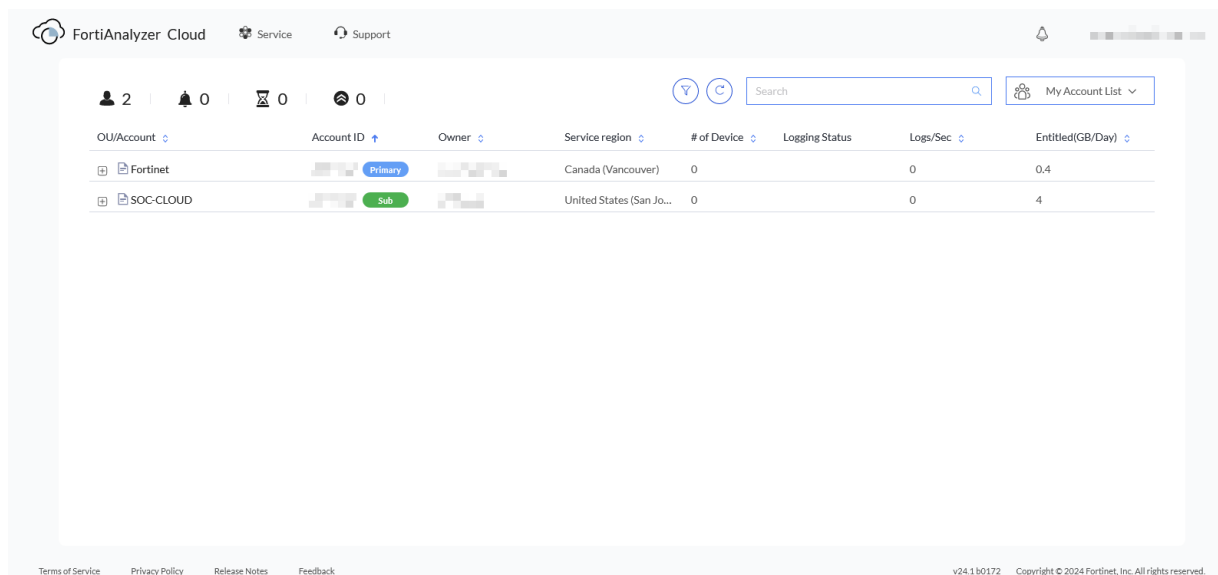
Viewing the FortiAnalyzer Cloud portal

After accessing your FortiAnalyzer Cloud instance, you can navigate to the FortiAnalyzer Cloud portal by opening the toolbar and choosing *Return to Portal*. See [Using the FortiAnalyzer Cloud toolbar on page 26](#).

In the FortiAnalyzer Cloud portal, you can expand each account and view information about the account and any deployed instances.

To view information about instances:

1. Access the portal. See [Accessing your FortiAnalyzer Cloud instance on page 24](#).
The FortiAnalyzer Cloud & Service portal is displayed.

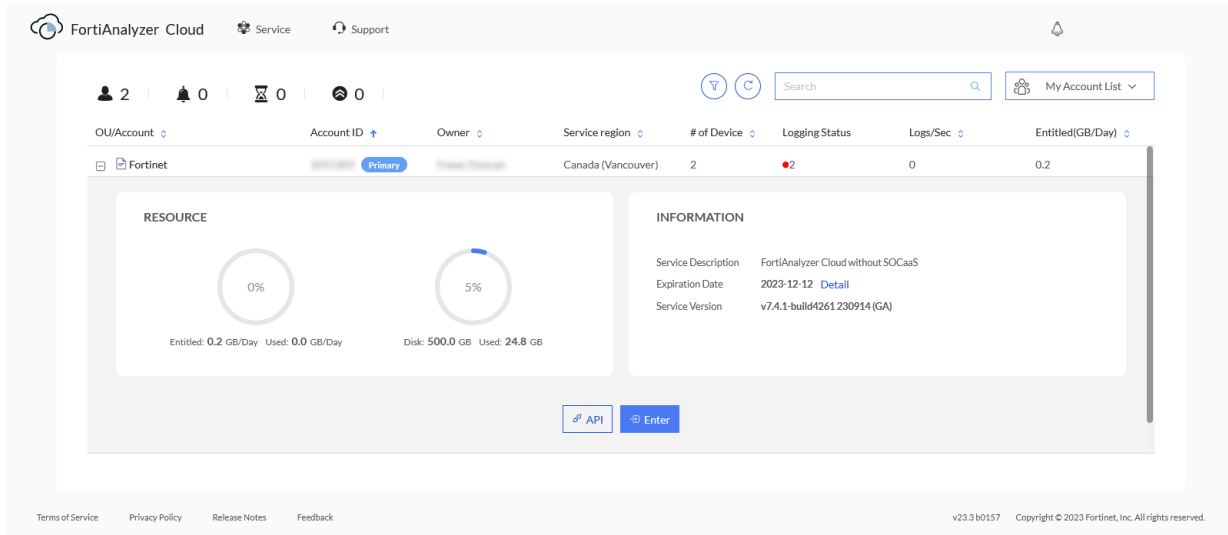


2. Expand an account with no instances deployed.
The account details are displayed. If it is a primary account, you can provision a new instance. See [Deploying a FortiAnalyzer Cloud instance on page 10](#).

3. Expand an account with deployed instances.

Information about the VM resources and the instance is displayed.

When a firmware upgrade is available, you can click the upgrade icon  to view additional information about the upgrade, choose upgrade immediately, or schedule an upgrade for later. You can also click *Enter* to access the instance.



The following options are displayed:

Dashboard

The top-left includes a dashboard summary of the accounts displayed on the pane:

- **Accounts:** Displays the number of accounts you can access.
- **Alarms:** Displays the number of notifications or alarms that need your attention. Notifications and alarms display in the banner. For alarms, you can also scroll down through the accounts to find an alarm icon on affected accounts.
- **Expiring:** Displays the number of licenses that will expire soon.

Filter

Click to view options to filter by license status and quota/storage alarm.

Refresh

Click to manually retrieve the latest license information from FortiCare and refresh the pane.

Information from FortiCare is also automatically retrieved on a regular interval.

Account Search

Use to search for accounts. In the *Search* box, type search criteria, and press *Enter*. Delete the search criteria, and press *Enter* to display all accounts again.

Accounts summary in table view

Each account displays as a row with the following columns:

- **OU/Account:** The OU/Account this instance is configured for.
- **Account ID:** The account ID.
- **Owner:** The name of the owner.
- **Service Region:** The region where the instance is deployed.
- **# of Device:** The number of devices connected to the instance.
- **Logging Status:** The logging status of connected devices.
- **Logs/Sec**
- **Entitled (GB/Day)**

Expand the pane to view additional information:

- *Service Description*: A short description of the FortiAnalyzer Cloud service.
- *Expiration Date*: The license expiration date.
- *Service Version*: The FortiAnalyzer Cloud version.
- *Enter*: Enter the FortiAnalyzer Cloud instance.
- *API*: Open the *User API Helper* pane with information about API usage for FortiAnalyzer Cloud.

See also [Viewing the FortiAnalyzer Cloud portal on page 36](#).

Providing feedback

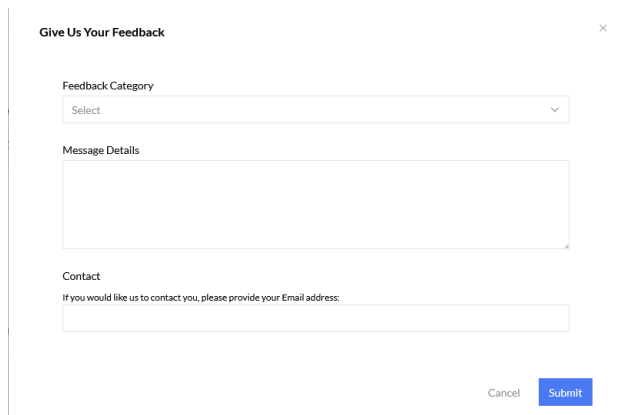
Feedback form

In FortiAnalyzer Cloud, you can submit feedback about your cloud experience to Fortinet.

The *Feedback* button is available in the following places:

- The footer on the *FortiAnalyzer Cloud & Service* portal.
- The FortiAnalyzer Cloud portal account dropdown inside the FortiAnalyzer Cloud instance. See [Using the FortiAnalyzer Cloud toolbar on page 26](#).

After clicking the feedback button, you will be presented with a feedback dialog where you can provide comments and suggestions.



FortiAnalyzer Cloud survey

Periodically, a FortiAnalyzer Cloud survey will be shared through the FortiAnalyzer notification menu inviting you to participate in a short survey about your experience with FortiAnalyzer Cloud. When available, you can access this survey through the notifications menu and click *Start Survey* to begin.

Notifications

Survey

Cloud Service

We'd love to hear from you! Our survey is ready, please click the link to share your thoughts

[Start Survey](#)

Cloud Service Notification

Cloud Service

Your cloud instance firmware has been upgraded from v7.4.6-build9266 250116 (GA.M) to v7.4.7-build6767 250606 (GA.M)

[Acknowledge](#)

Close

Using account services

The FortiCare/FortiCloud account offer several services. This section includes the following topics:

- [Adding a secondary account on page 40](#)
- [Modifying a secondary account on page 42](#)
- [Supporting IAM users and IAM API users on page 42](#)

For information about using FortiCloud portal, see the [FortiCloud Account Services](#) page on the [Fortinet Document Library](#).

Adding a secondary account

Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. By default, the secondary account holder is assigned the default administrator profile named *Restricted_User*. However, the primary account holder can modify the admin profile for the secondary user.

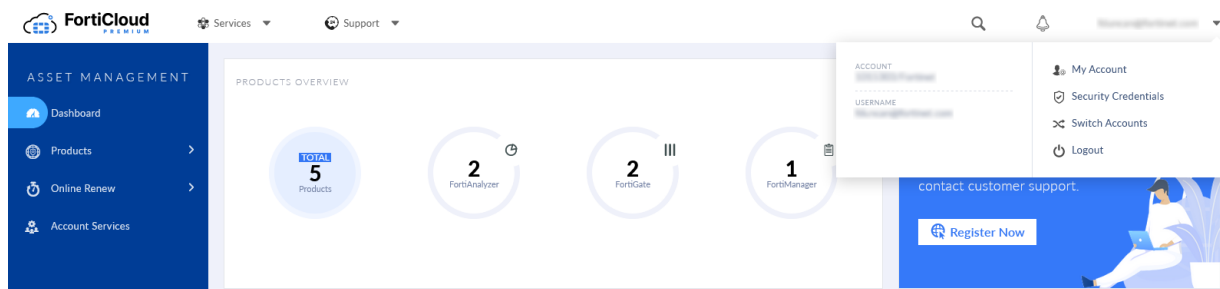
A secondary account allows the Fortinet support team to troubleshoot the FortiAnalyzer Cloud deployment.



With FortiAnalyzer Cloud 7.0.x and later, you can use the Identity and Access Management (IAM) portal, and you can migrate secondary accounts to the IAM portal. In IAM portal, secondary accounts are called sub users. For information about migrating sub users, see the [Identity & Access Management Guide](#).

To add a secondary account:

1. Go to FortiCloud (<https://support.fortinet.com/>), and use your FortiCloud account credentials to log in.
2. From the top-right corner, click your login name, and select *My Account*.



3. Click *Manage User*.
4. Click the new user icon to add a new user.

- When creating an account for the Fortinet support team, specify an email for the secondary account, and select *Full Access* or *Limit Access*.

A user with full access has the same access level as a primary account user. A user with limited access can only manage the assigned product serial number and will be unable to receive renewal notices or create additional secondary account users.

- Log in to the personal FortiCare portal. Under FortiAnalyzer Cloud section, you will see an account listed as a secondary member.
- Click the entry to expand the view.
- Ask the new user to log in to FortiAnalyzer Cloud.

After the new user logs in to FortiAnalyzer Cloud, the user is displayed on the *FortiAnalyzer Cloud* instance, and the administrator can modify the account. See [Modifying a secondary account on page 42](#).



A secondary account can access the portal thirty days after it expires.

Modifying a secondary account

The new user must log in to FortiAnalyzer Cloud for the account to be displayed in the FortiAnalyzer instance. When new users log in to the account, they are automatically assigned the default administrator profile named *Restricted_User*.

After the new user has logged in to the account, the primary user or a super user can modify the account.

For information about creating a secondary account, see [Adding a secondary account on page 40](#).

To modify a secondary account:

1. Log in to FortiAnalyzer Cloud.
2. Go to *System Settings > Administrators*.
3. Edit the administrator, and assign a different profile.

Supporting IAM users and IAM API users

FortiAnalyzer Cloud 7.0.x and later supports user credentials created in the Identity & Access Management (IAM) portal. On FortiCloud, you can create IAM users and IAM API users, and use them with FortiAnalyzer Cloud.

For more information about using the IAM portal, see the [Identity & Access Management Administration Guide](#).

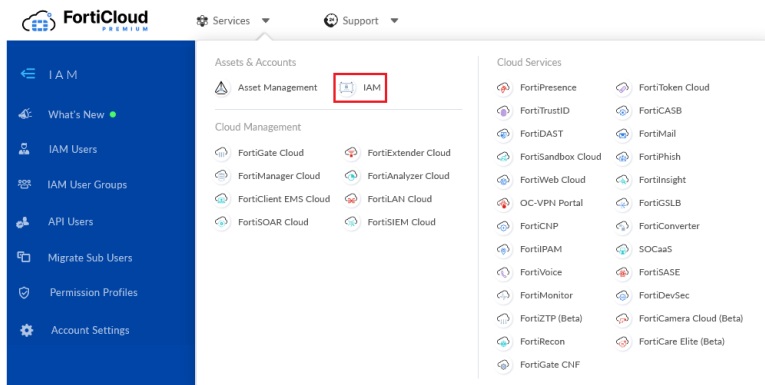
See also [Adding IAM users on page 42](#) and [Adding API users on page 45](#).

Adding IAM users

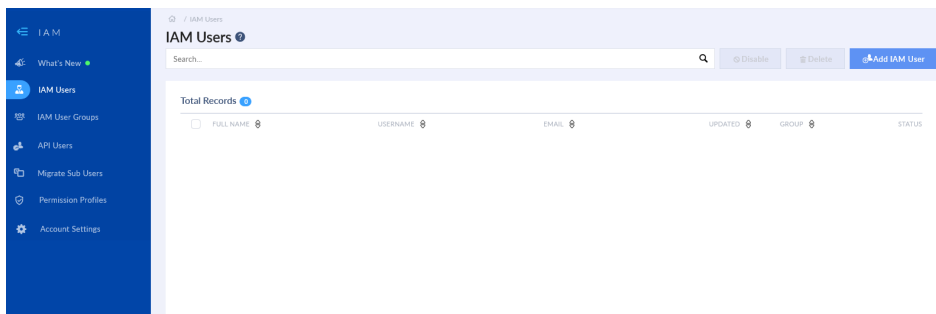
FortiAnalyzer Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiAnalyzer Cloud.

To add an IAM user:

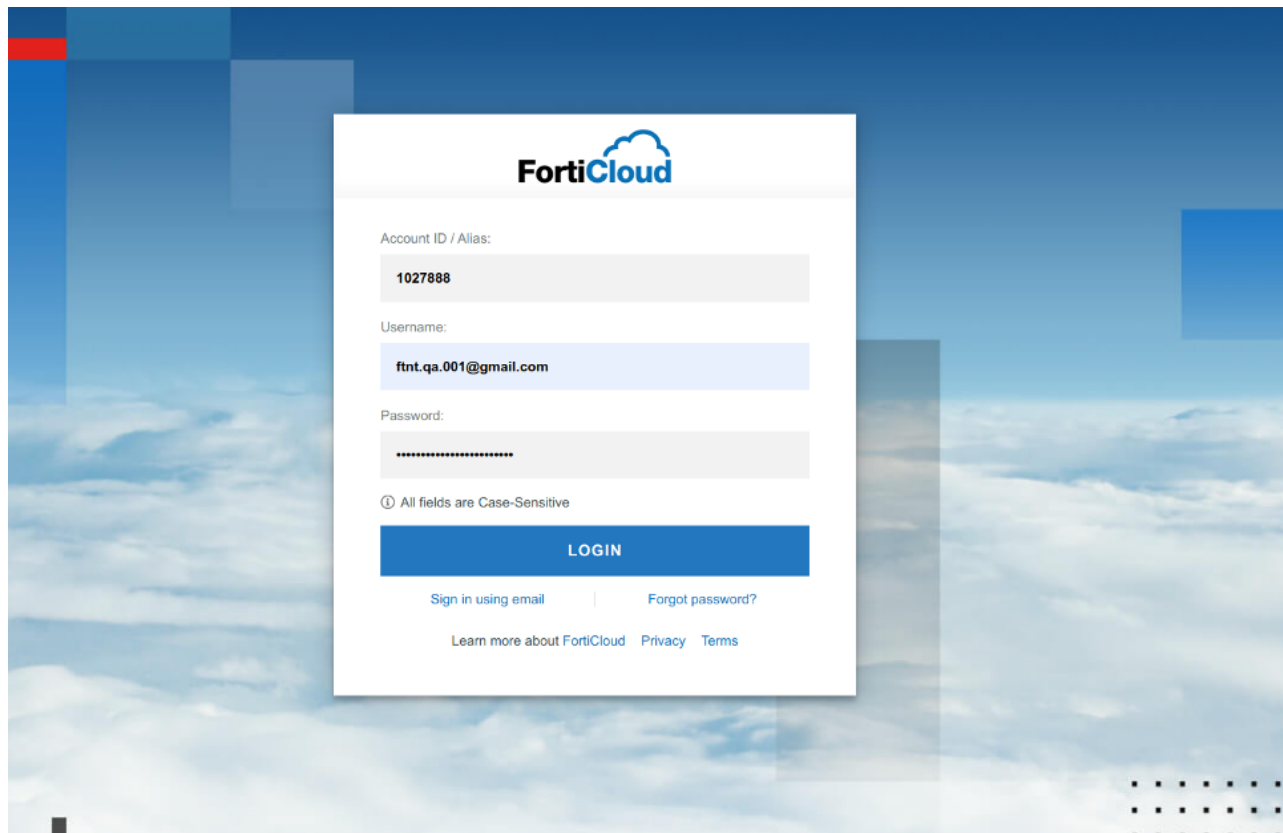
1. Go to FortiCloud (<https://support.fortinet.com/>), and log in.
2. From the *Services* menu, select *IAM*.



The IAM portal is displayed.



3. Create a new IAM user.
For more information, see [Adding IAM Users](#) in the *Identity & Access Management (IAM)* guide on the Fortinet Documents Library.
4. Add an IAM user group, and add the user to it.
For more information, see [Adding IAM User Groups](#) in the *Identity & Access Management (IAM)* guide on the Fortinet Documents Library.
5. Generate an IAM user login password.
For more information, see [Generating the password reset link](#) in the *Identity & Access Management (IAM)* guide on the Fortinet Documents Library.
6. The IAM user can use the credentials to log in to FortiCloud.



After logging in to FortiCloud, the IAM user has access to *FortiAnalyzer Cloud & Service* portal.

7. Enter the FortiAnalyzer Cloud instance, and go to *System Settings > Administrators* to view the IAM user.

FortiCloud IAM User Permissions

See the table below for an explanation of how each of the FortiCloud user permissions are associated with a FortiAnalyzer admin profile:

FortiCloud User Permission	Associated FortiManager Admin Profile
Admin	Assigned to the <i>Super_User</i> admin profile.
Read-Write	Assigned to the <i>Standard_User</i> admin profile.
Read-Only	Assigned to the <i>Restricted_User</i> admin profile.
Custom	<i>Custom</i> users are assigned to the <i>Restricted_User</i> admin profile the first time they log in. A <i>Super_User</i> administrator can assign a new or existing FortiManager admin profile to the user. The new admin profile will be applied to the user when they next log in to FortiAnalyzer Cloud.

You cannot change the FortiAnalyzer Cloud admin profiles assigned to users using the *Admin*, *Read-Write*, or *Read-Only* FortiCloud user permissions.

Adding API users

API users can access FortiCloud services, including FortiAnalyzer Cloud, through the API.

In order to send API requests to FortiAnalyzer Cloud, you must first obtain an access token from FortiCloud using OAuth 2.0. You can use the access token to generate a session ID which is required to send an JSON API request to FortiAnalyzer.

To use the FortiAnalyzer Cloud API:

1. Create an API user in FortiCloud and download your API credentials. See [Adding an API user](#) in the FortiCloud Account Services documentation for instructions on how to add API users.
2. Obtain an access token from FortiCloud using your credentials. See [Accessing FortiAPIs - Authentication and authorization](#) for information on authentication and authorization for FortiAPIs.
3. Use the access token to get a FortiAnalyzer Cloud API session ID using the `https://<FortiAnalyzer_cloud_url>/p/forticloud_jsonrpc_login/` endpoint.

HTTP Method	POST
Endpoint	<code>https://<FortiAnalyzer_cloud_url>/p/forticloud_jsonrpc_login/</code>
Request Body	<pre>{ "access_token": "<access token obtained in step 2>" }</pre>
Response example	<pre>{ "session": "ykF3W6G8CfZv+xecsZBC00n6P0TEbs0*****" }</pre>

4. Send API requests to the `https://<FortiAnalyzer_cloud_url>/jsonrpc` endpoint with the session included in the body.

For example:

HTTP Method	POST
Endpoint	<code>https://<FortiAnalyzer_cloud_url>/jsonrpc</code>
Request Body	<pre>{ "method": "get", "params": [{ "url": "/sys/status" }], "id": 1, "verbose": 1, "session": "ykF3W6G8CfZv+xecsZBC00n6P0TEbs0*****", }</pre>



The FortiAnalyzer Cloud API uses session-based authentication. The number of simultaneous API sessions allowed for an API user is controlled by the user's max login setting. By default, this setting is set to 20.

```
config system admin user
  edit <user>
    set login-max 20
```

Supporting external IdP users

External IdP user support enables users to log into FortiAnalyzer Cloud with their company-provided user credentials using a third-party SAML identity provider.

For more information on managing external IdP roles and users for cloud products, see the [FortiCloud Identity & Access Management \(IAM\)](#) user guide.

Using multiple roles with external IdP users

For more information on external IdP users for FortiCloud, see [External IdP roles](#).

Logging in as an external IdP user with multiple roles:

1. When logging in as an IdP user that has multiple roles, the account selection page is displayed allowing users to select which instance to access.

External IdP users can have multiple roles assigned to a single FortiAnalyzer Cloud instance.

The screenshot shows a user interface for logging into FortiAnalyzer Cloud. On the left, a 'Welcome Back!' message is displayed with the text 'FEDERATED LOGIN', 'fazcloud_fac', 'USERNAME', and 'idp-multi1'. Below this is a photo of a woman working on a laptop. On the right, a 'Select a Role to Proceed' dialog box is shown. It contains a search bar and a table with columns for 'ACCOUNT ID', 'COMPANY', and 'ROLE NAME'.

ACCOUNT ID	COMPANY	ROLE NAME
1691225	Faz	idp_admin
1691225	Faz	idp_custom
1691225	Faz	idp_readwrite
1691226	Faz	idp_admin
1691226	Faz	idp_custom
1691228	Faz	idp_admin
1691228	Faz	idp_readwrite

2. After selecting an instance and role, the portal will use the associated role for the login.

The screenshot shows the FortiAnalyzer Cloud interface. On the left is a sidebar with navigation options: Device Manager, FortiView, Log View, Fabric View, Incidents & Events, and Reports. The main area displays a 'Status' section with a green circle indicating '20 Devices' are 'Up'. To the right, a donut chart shows '400 GB' of storage. Below these are two circular progress indicators. The top right corner shows the user's profile: 'idp-multi1@fazcloud_fac'. The bottom right corner has a 'My Account' section with links for Switch Roles, Return To Portal, Privacy & Notifications, Change Profile, and Log Out. The central part of the dashboard features a table of logging devices.

Device Name	Platform	HA Status	Description	Firmware Version	Serial Number	Last Log Time	Status
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:50 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:51 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:50 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:50 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:50 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:51 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:50 PM PDT (0 minutes)	Up
FortiGate-VM64	FortiGate-VM64			FortiGate 5.0		6/25/2024, 12:12:50 PM PDT (0 minutes)	Up

3. Click *Switch Roles* or *Return To Portal* in the FortiAnalyzer Cloud toolbar to return to the FortiAnalyzer Cloud role selection page. On the role selection page, you can select another account and role.

The screenshot shows the 'Make a Selection to Proceed' page. On the left is a blue sidebar with a 'Welcome Back!' message and a 'ThirdParty' button. The main area has a search bar 'Search an Account' and a list of accounts under the heading 'Accounts'. The accounts are listed with their email addresses and roles.

Account	Role
1691225@faz01@faz.ca idp_admin	idp_admin
1691225@faz01@faz.ca idp_readwrite	idp_readwrite
1691225@faz01@faz.ca idp_custom	idp_custom
1691226@faz02@faz.ca idp_admin	idp_admin
1691226@faz02@faz.ca idp_custom	idp_custom
1691228@faz04@faz.ca idp_admin	idp_admin
1691228@faz04@faz.ca idp_readwrite	idp_readwrite

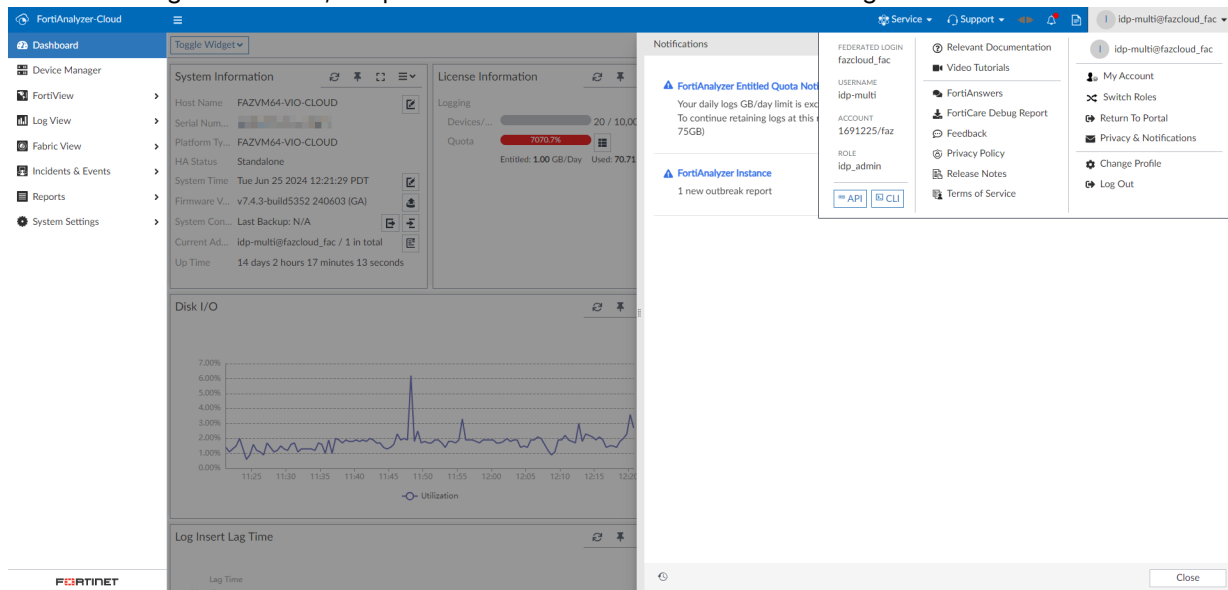
Logging in as an external IdP user with multiple roles in an Organizational Unit:

1. When logging in as an external IdP user with multiple roles in an Organizational Unit (OU), the account selection page is displayed allowing you to select an instance, role, and OU.

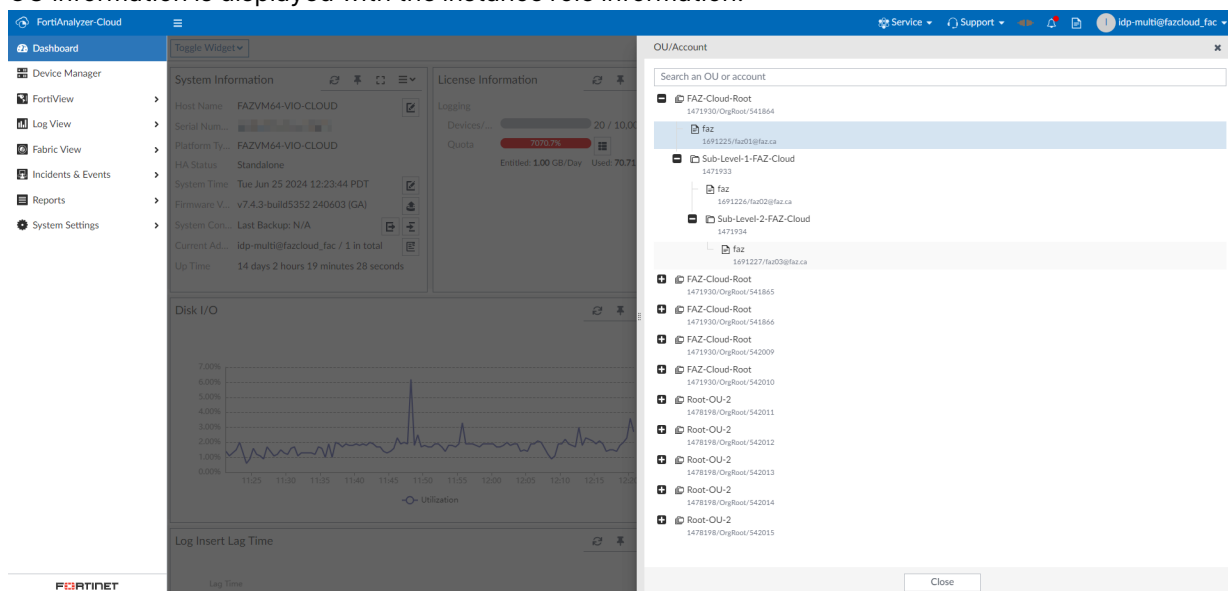
The screenshot shows the 'Select a Role to Proceed' page. On the left is a white sidebar with a 'Welcome Back!' message and a 'ThirdParty' button. The main area has a search bar 'Search an OU or account' and a table of roles. The roles are listed with their account IDs, company names, and role names.

Account ID	Company	Role Name
1691225	Faz	idp_admin
1691225	Faz	idp_admin_ou
1691225	Faz	idp_custom_match
1691225	Faz	idp_custom_match_ou
1691225	Faz	idp_custom_res_ou
1691225	Faz	idp_readonly
1691225	Faz	idp_readonly_ou
1691225	Faz	idp_readwrite_ou
1691226	Faz	DTCA_CFG_NetEng_FortiCloud_NE_Opera

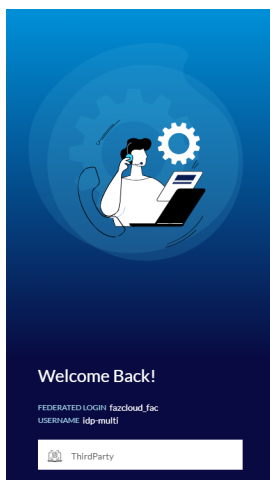
2. After selecting an instance, the portal will use the selected role for the login.



3. OU information is displayed with the instance role information.



4. Click *Switch Roles* or *Return To Portal* to return to the FortiAnalyzer Cloud role selection page. On the role selection page, you can select another role or OU to use for login.



Make a Selection to Proceed

Q	Search an Account
1691225 idp_admin_ou FAZ-Cloud-Root	1471930:OrgRoot/541864
faz	1691225/faz01@faz.ca idp_admin_ou
Sub-Level-1-FAZ-Cloud	1471933
faz	1691226/faz02@faz.ca idp_admin_ou
Sub-Level-2-FAZ-Cloud	1471934
1691225 idp_readwrite_ou FAZ-Cloud-Root	1471930:OrgRoot/541865
1691225 idp_readonly_ou FAZ-Cloud-Root	1471930:OrgRoot/541866
1691225 idp_custom_res_ou FAZ-Cloud-Root	1471930:OrgRoot/542009
1691225 idp_custom_match_ou FAZ-Cloud-Root	1471930:OrgRoot/542010
1691228 idp_admin_ou Root-OU-2	1478198:OrgRoot/542011
1691228 idp_readwrite_ou Root-OU-2	1478198:OrgRoot/542012



www.fortinet.com

Copyright© 2026 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.