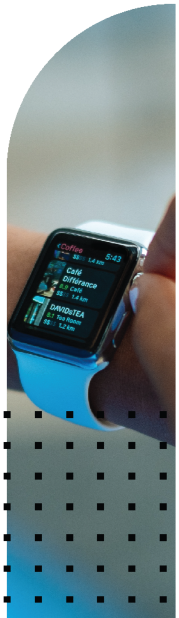
Cloud Deployment Guide

FortiAnalyzer 7.4.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 30, 2024
FortiAnalyzer 7.4.x Cloud Deployment Guide
05-74-843405-20240130

TABLE OF CONTENTS

Change Log 4
Introduction 5
Requirements 5
Licensing 6
Deploying FortiAnalyzer Cloud 7
Checking requirements and licenses 7
Deploying a FortiAnalyzer Cloud instance 8
Configuring FortiOS 10
Configuring FortiClient EMS 11
Configuring FortiMail 13
Using the FortiAnalyzer Cloud & Service portal 14
Accessing the portal and instances 14
Viewing information about instances 16
Upgrading firmware from the portal 17
Providing feedback 18
Using FortiAnalyzer Cloud 19
Upgrading firmware from the instance 19
Identifying the public IP address 19
Using the FortiAnalyzer Cloud toolbar 20
Service 20
Support 21
Notifications 21
Account 21
Enabling managed SOC service 22
Using account services 24
Adding a secondary account 24
Modifying a secondary account 26
Supporting IAM users and IAM API users 26
Adding IAM users 26
Adding API users 28
Supporting external IdP users 28

Change Log

Date	Change Description
2023-09-19	Initial release.
2023-01-30	Initial release of FortiAnalyzer Cloud 7.4.2.

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, is supported with a storage add-on license.

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.

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 24.

  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	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 to FortiGate 600	1GB/Day
2 RU and above or FGT-VM models with 8 CPU and above	FortiGate 800 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.

FortiAnalyzer Cloud requires one of the following licenses:

- **FortiAnalyzer Cloud subscription with SOCaaS:**

FortiGate hardware	FC-10-[FortiGate Model Code]-464-02-DD
FortiGate-VM	FC-10-[FortiGate VM Model Code]-464-02-DD

- **FortiAnalyzer Cloud subscription:**

FortiGate hardware	FC-10-[FortiGate Model Code]-585-02-DD
FortiGate-VM	FC-10-[FortiGate VM Model Code]-585-02-DD

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

- **Additional storage:**

+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

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.

Deploying FortiAnalyzer Cloud

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

1. Check requirements and licenses on FortiCloud. See Checking requirements and licenses on page 7.
2. On FortiCloud, deploy a FortiAnalyzer Cloud instance. See Deploying a FortiAnalyzer Cloud instance on page 8.
3. (Optional) Upgrade FortiAnalyzer Cloud to the latest available cloud version. See Upgrading firmware from the portal on page 17.
4. On FortiOS or FortiMail, enable logging to FortiAnalyzer Cloud:
   - For FortiOS, see Configuring FortiOS on page 10.
   - For FortiClient EMS, see Configuring FortiClient EMS on page 11.
   - For FortiMail, see Configuring FortiMail on page 13.

At the time of the 7.4 release, FortiAnalyzer Cloud supports new deployments in version 7.2 and upgrades to version 7.4.

Check the latest FortiAnalyzer Cloud Deployment Guide to see the current FortiAnalyzer Cloud versions available for deployment.

FortiAnalyzer Cloud 7.0.3 or later is required to support logging from non-FortiGate devices.

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:
   1. Go to *Products* > *Product List*.
   2. In the *View Options menu*, select *Group by Category*, and click *Apply*.

      The *Product List* is displayed by categories, such as *FortiGate*.
   3. 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 8.

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 24.

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.

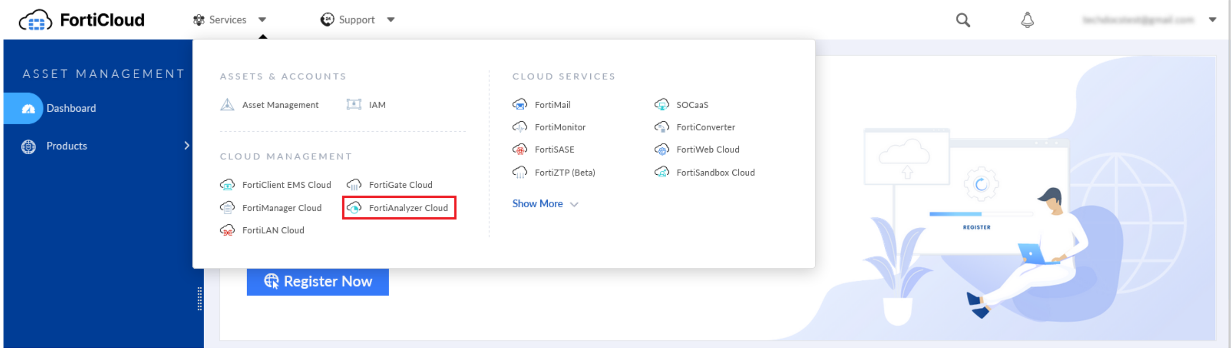
At the time of the 7.4 release, FortiAnalyzer Cloud supports new deployments in version 7.2 and upgrades to version 7.4.

Check the latest FortiAnalyzer Cloud Deployment Guide to see the current FortiAnalyzer Cloud versions available for deployment.

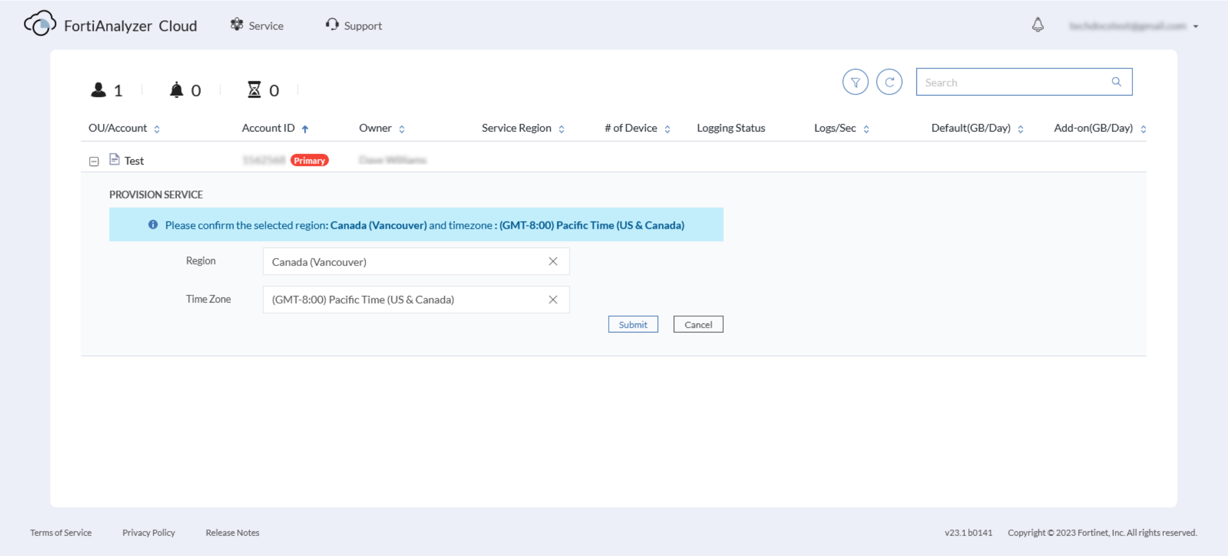
To deploy a FortiAnalyzer Cloud instance:

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:
   1. Select a *Region* for the FortiAnalyzer Cloud instance. In this example, the region is *Canada (Vancouver).*
   2. Select a *Time Zone* for the FortiAnalyzer Cloud instance.
4. Click *Submit*.



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

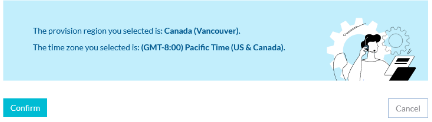
PROVISION SERVICE

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

Region: Canada (Vancouver)

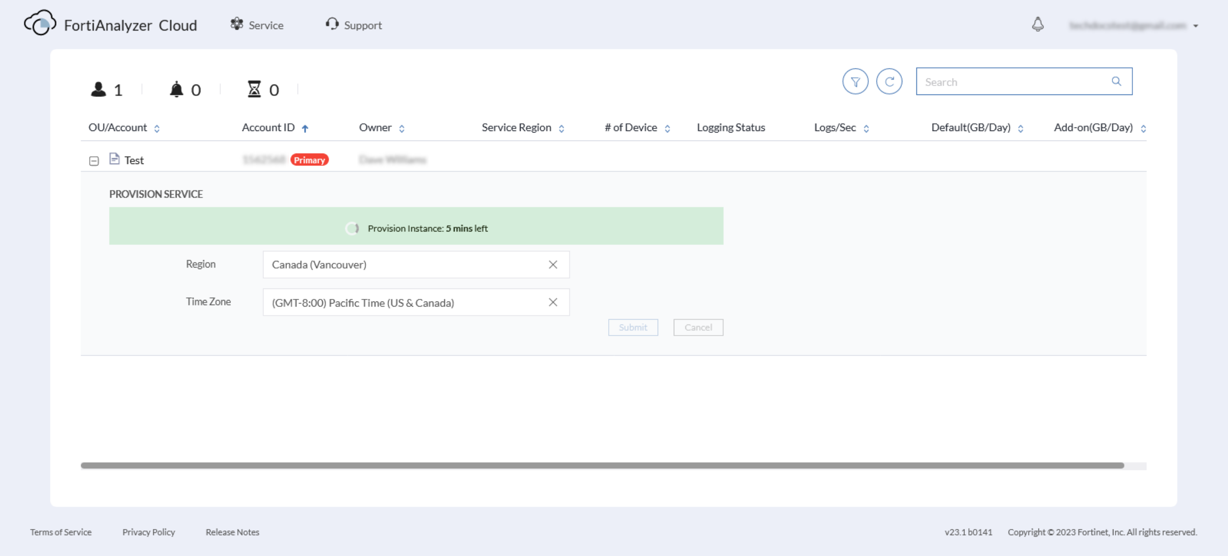
Time Zone: (GMT-8:00) Pacific Time (US & Canada)

5. A message asking you to confirm your selected region and time zone is displayed.
   a. Click *Confirm* to provision in the FortiAnalyzer Cloud instance.
   b. Click *Cancel* to stop provisioning the instance, and change the region.



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

6. FortiAnalyzer Cloud instance is provisioned in a few minutes.



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

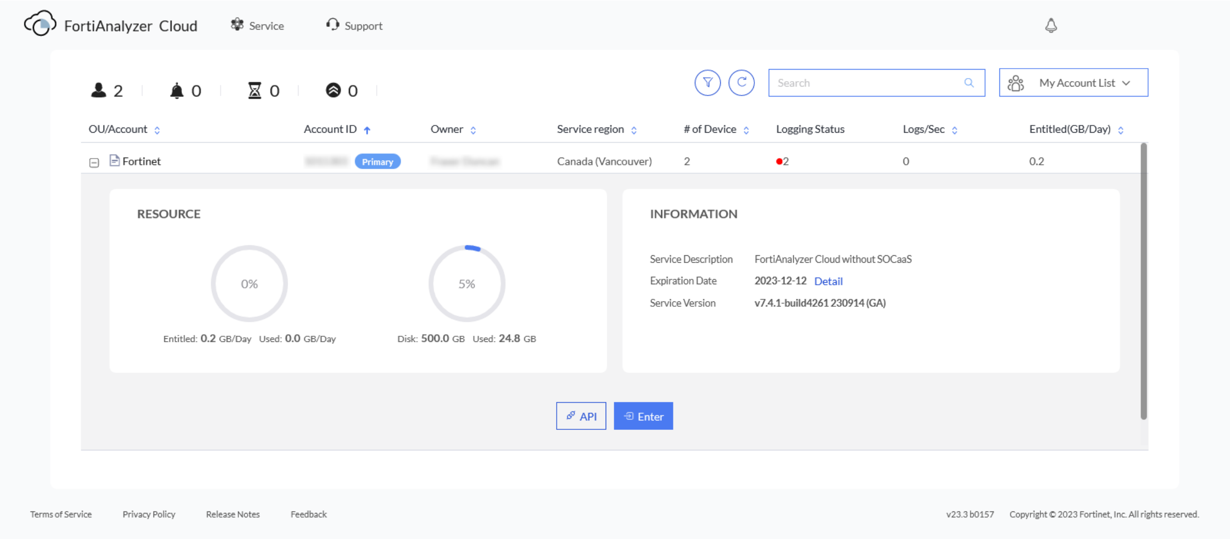
PROVISION SERVICE

Provision Instance: **5 mins left**

Region: Canada (Vancouver)

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

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



OU/Account	Account ID	Owner	Service region	# of Device	Logging Status	Logs/Sec	Entitled(GB/Day)
Fortinet	[redacted] Primary	[redacted]	Canada (Vancouver)	2	●2	0	0.2

RESOURCE

0% — Entitled: 0.2 GB/Day Used: 0.0 GB/Day

5% — Disk: 500.0 GB Used: 24.8 GB

INFORMATION

Service Description: FortiAnalyzer Cloud without SOCaaS

Expiration Date: 2023-12-12 Detail

Service Version: v7.4.1-build4261 230914 (GA)

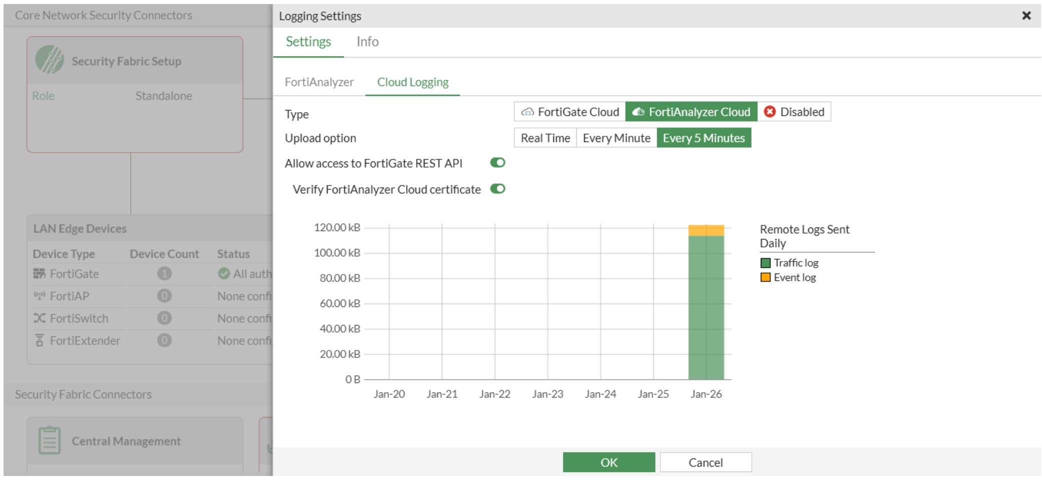
8. (Optional) Upgrade FortiAnalyzer Cloud to 7.4.x. See Upgrading firmware from the portal on page 17.
9. Configure FortiOS to work with FortiAnalyzer Cloud. See Configuring FortiOS on page 10.

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*.



Type: FortiGate Cloud [✓ FortiAnalyzer Cloud] Disabled

Upload option: Real Time Every Minute [✓ Every 5 Minutes]

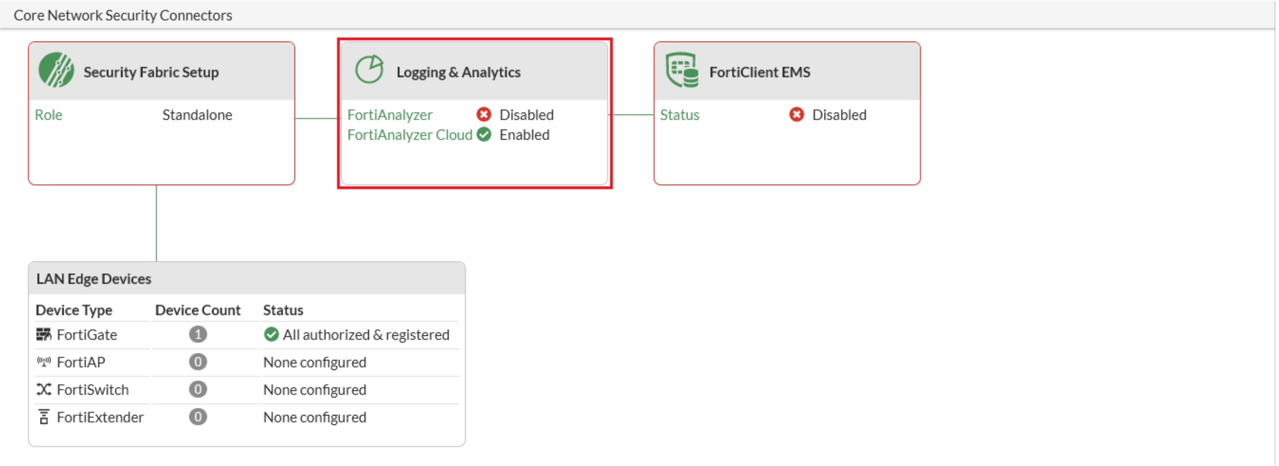
Allow access to FortiGate REST API: ●

Verify FortiAnalyzer Cloud certificate: ●

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* .



Core Network Security Connectors

Security Fabric Setup
Role Standalone

Logging & Analytics
FortiAnalyzer ✗ Disabled
FortiAnalyzer Cloud ✓ Enabled

FortiClient EMS
Status ✗ Disabled

LAN Edge Devices

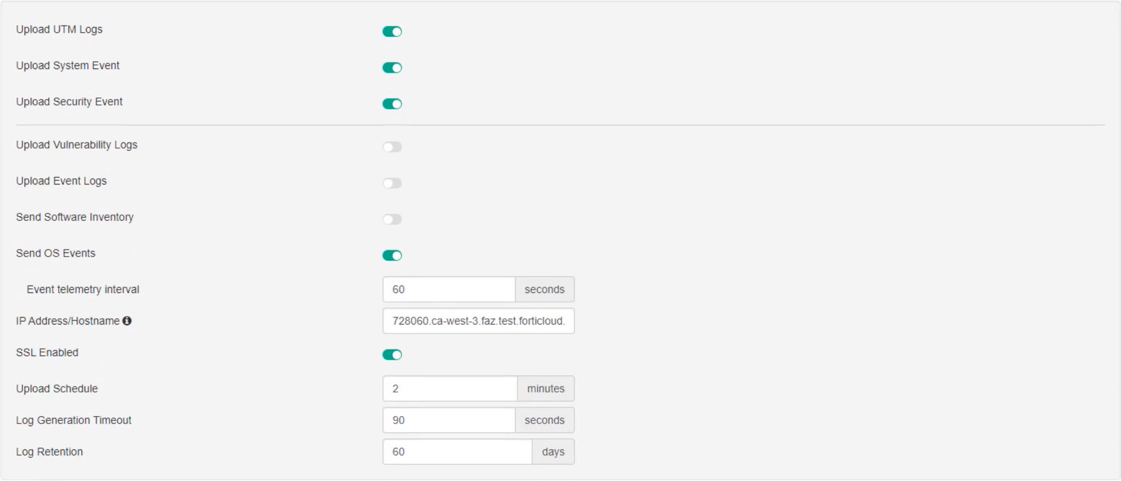
Device Type	Device Count	Status
FortiGate	1	✓ All authorized & registered
FortiAP	0	None configured
FortiSwitch	0	None configured
FortiExtender	0	None configured

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.



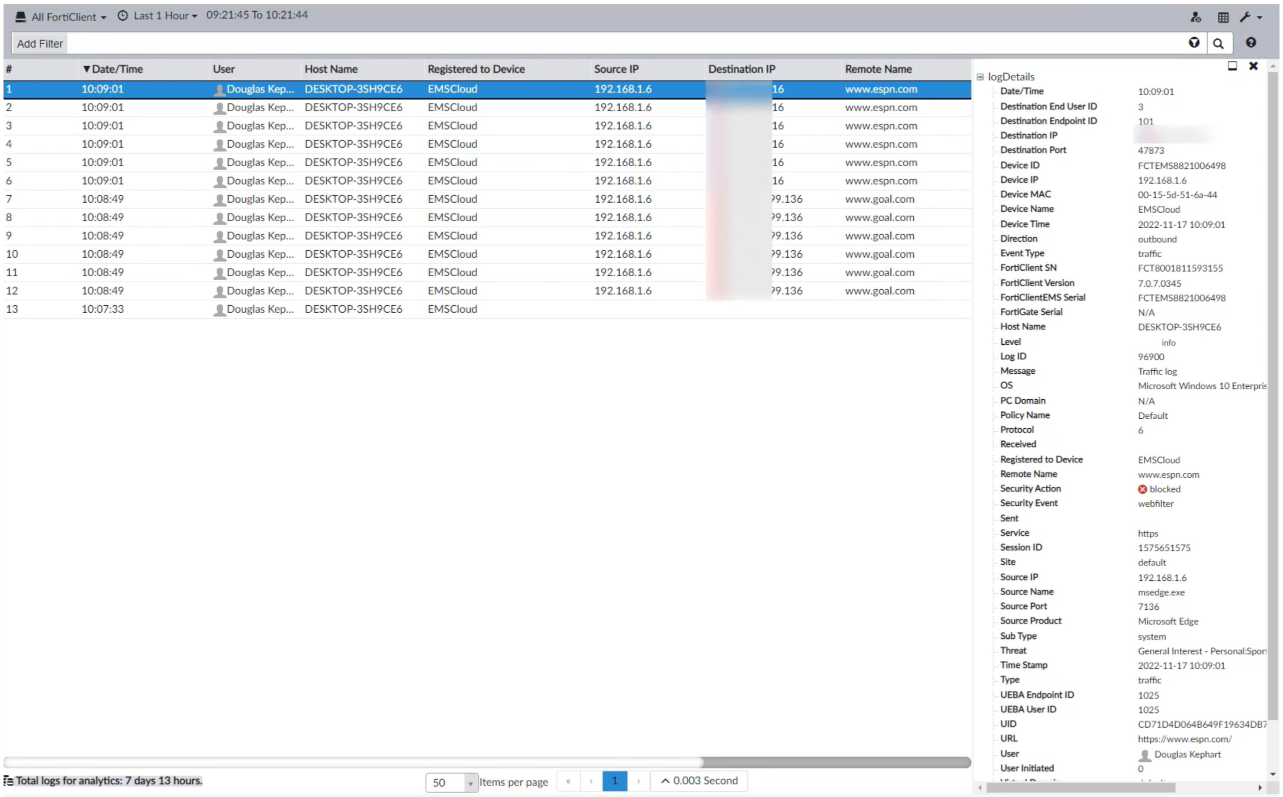
Upload UTM Logs	●
Upload System Event	●
Upload Security Event	●
Upload Vulnerability Logs	○
Upload Event Logs	○
Send Software Inventory	○
Send OS Events	●
Event telemetry interval	60 seconds
IP Address/Hostname	728060.ca-west-3.faz.test.forticloud.
SSL Enabled	●
Upload Schedule	2 minutes
Log Generation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



#	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	[redacted]	www.espn.com
2	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.espn.com
3	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.espn.com
4	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.espn.com
5	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.espn.com
6	10:09:01	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.espn.com
7	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.goal.com
8	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.goal.com
9	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.goal.com
10	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.goal.com
11	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.goal.com
12	10:08:49	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud	192.168.1.6	[redacted]	www.goal.com
13	10:07:33	Douglas Kep...	DESKTOP-3SH9CE6	EMSCloud			

Total logs for analytics: 7 days 13 hours.

logDetails

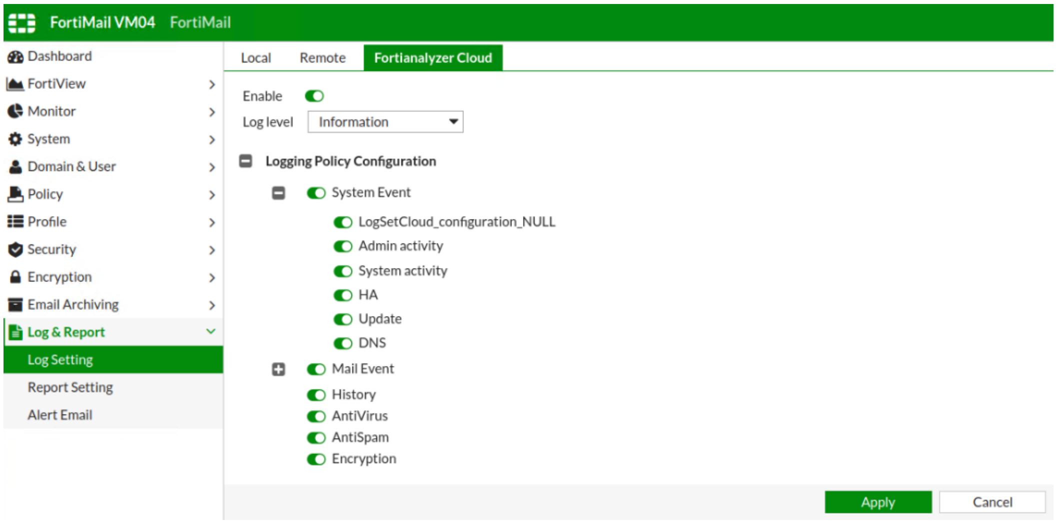
Date/Time	10:09:01
Destination End User ID	3
Destination Endpoint ID	101
Destination IP	[redacted]
Destination Port	47873
Device ID	FCTEMS8821006498
Device IP	192.168.1.6
Device MAC	00-15-5d-51-6a-44
Device Name	EMSCloud
Device Time	2022-11-17 10:09:01
Direction	outbound
Event Type	traffic
FortiClient 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 Enterpris
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 - Personal:Sport
Time Stamp	2022-11-17 10:09:01
Type	traffic
UEBA Endpoint ID	1025
UEBA User ID	1025
UID	CD71D4D064B649F19634DB7
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:

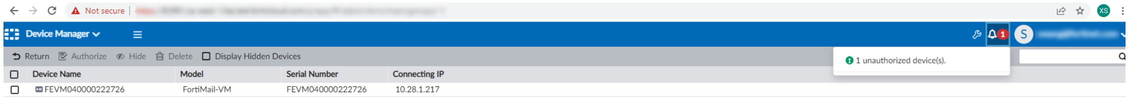
1. In FortiMail, enable logging to FortiAnalyzer Cloud.
   a. Go to *Log & Report > Log Setting*.
   b. On the *FortiAnalyzer Cloud* tab, toggle on the *Enable* option, and click *Apply*.
   As long as FortiMail has the correct license registered with FortiCare, a connection is established with FortiAnalyzer Cloud.



Enable ●
Log level: Information

Logging Policy Configuration
- System Event
  - LogSetCloud_configuration_NULL
  - Admin activity
  - System activity
  - HA
  - Update
  - DNS
- Mail Event
- History
- AntiVirus
- AntiSpam
- Encryption

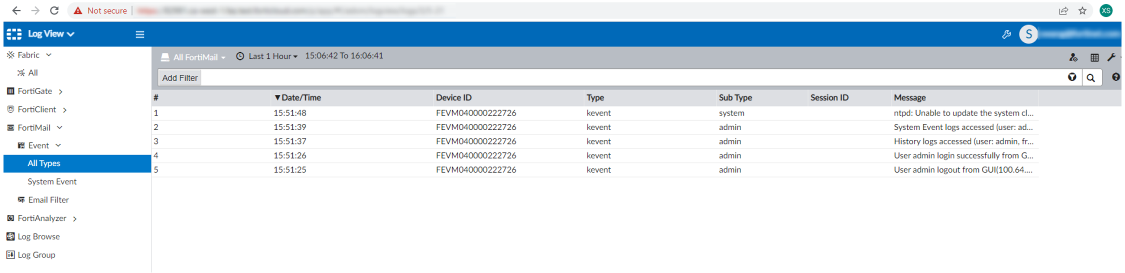
2. In the FortiAnalyzer Cloud instance, go to *Device Manager*, and authorize FortiMail.



Device Name	Model	Serial Number	Connecting IP
FEVM040000222726	FortiMail-VM	FEVM040000222726	10.28.1.217

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

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



15:06:42 To 16:06:41

#	▼Date/Time	Device ID	Type	Sub Type	Session ID	Message
1	15:51:48	FEVM040000222726	kevent	system		ntpd: Unable to update the system cl...
2	15:51:39	FEVM040000222726	kevent	admin		System Event logs accessed (user: ad...
3	15:51:37	FEVM040000222726	kevent	admin		History logs accessed (user: admin, fr...
4	15:51:26	FEVM040000222726	kevent	admin		User admin login successfully from G...
5	15:51:25	FEVM040000222726	kevent	admin		User admin logout from GUI(100.64....

Using the FortiAnalyzer Cloud & Service portal

After deploying a FortiAnalyzer Cloud instance, you can use the FortiAnalyzer Cloud & Service portal to access deployed instances.

This section includes the following procedures about using the portal:

- Accessing the portal and instances on page 14
- Viewing information about instances on page 16
- Upgrading firmware from the portal on page 17
- Providing feedback on page 18

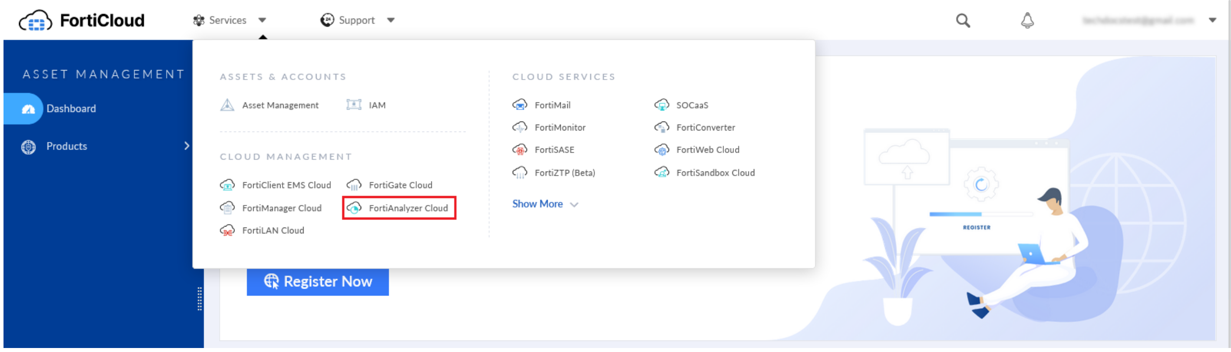
Accessing the portal and instances

After deploying one or more FortiAnalyzer Cloud instances, you can access the instances from the FortiAnalyzer Cloud & Service portal.

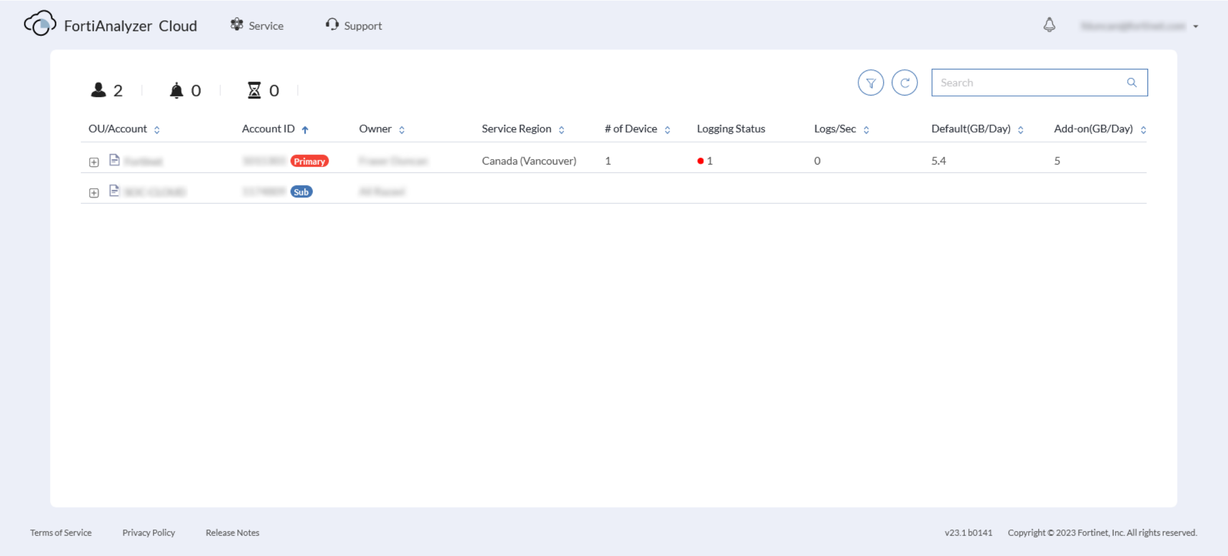
When you access the FortiAnalyzer Cloud & Service portal, an automatic instance login process begins.

To access the portal and instances:

1. 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* under *Cloud Management*.



   You are automatically logged in to your FortiAnalyzer instance.
3. If you have access to multiple instances and are logged in to the FortiAnalyzer instance, you can return to the portal by clicking your name in the top-right corner and selecting *FortiAnalyzer Cloud*. The *FortiAnalyzer* Cloud & Service portal is displayed.



👤 2 🔔 0 ⌛ 0

OU/Account	Account ID	Owner	Service Region	# of Device	Logging Status	Logs/Sec	Default(GB/Day)	Add-on(GB/Day)
[redacted]	[redacted] Primary	[redacted]	Canada (Vancouver)	1	● 1	0	5.4	5
[redacted]	[redacted] Sub	[redacted]						

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

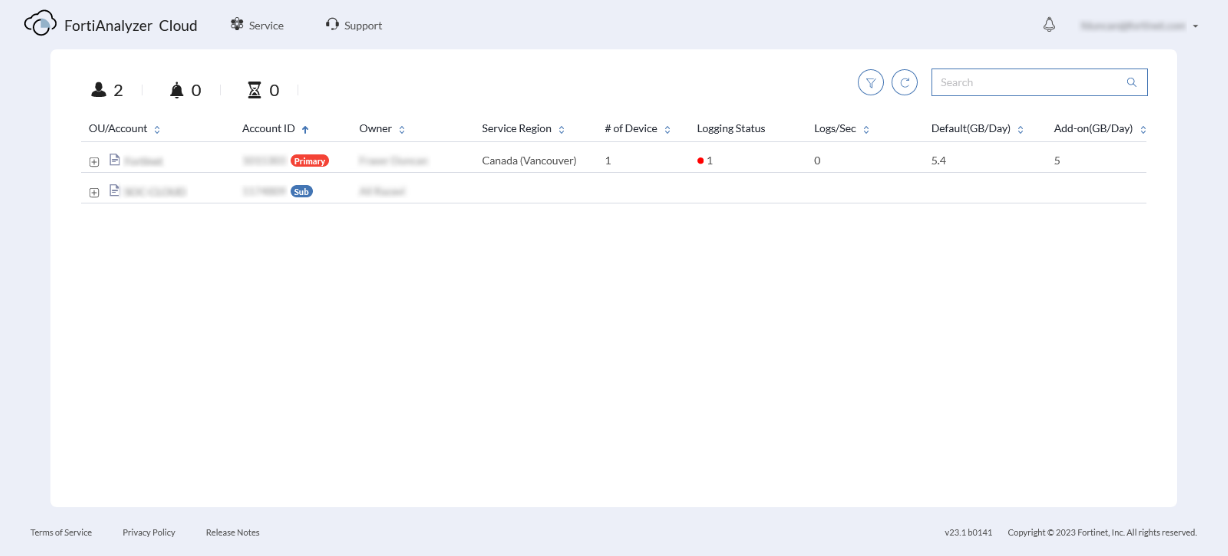
	FortiAnalyzer Cloud. See also Viewing information about instances on page 16 and Upgrading firmware from the portal on page 17.

Viewing information about instances

After accessing the FortiAnalyzer Cloud & Service portal, you can expand each account and view information about the account and any deployed instances.

To view information about instances:

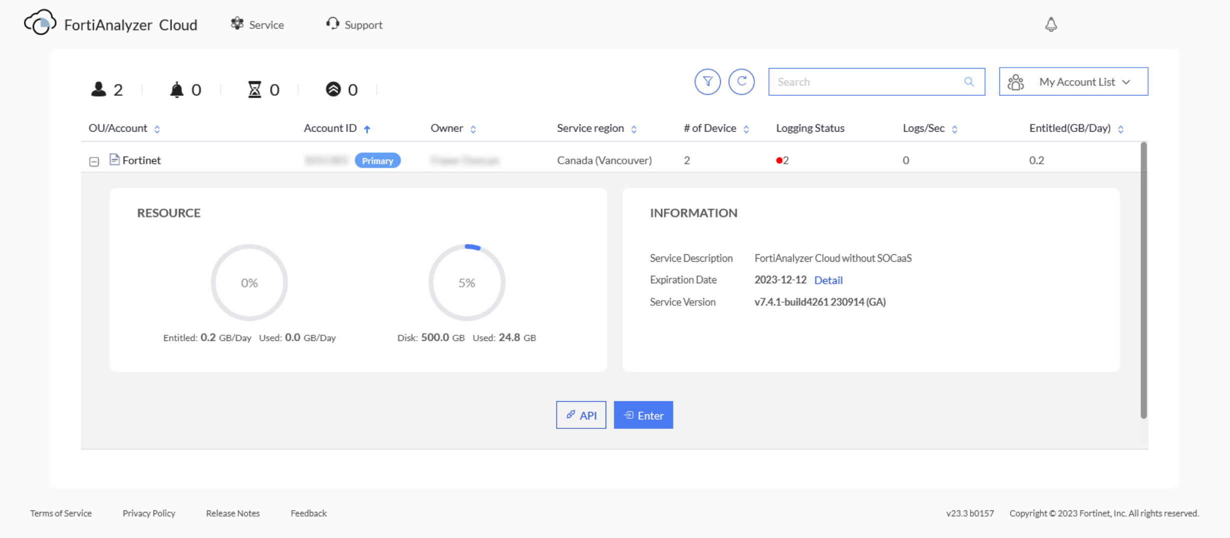
1. Access the portal. See Accessing the portal and instances on page 14.
   The FortiAnalyzer Cloud & Service portal is displayed.



OU/Account	Account ID	Owner	Service Region	# of Device	Logging Status	Logs/Sec	Default(GB/Day)	Add-on(GB/Day)
[redacted]	[redacted] Primary	[redacted]	Canada (Vancouver)	1	● 1	0	5.4	5
[redacted]	[redacted] Sub	[redacted]						

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 8.
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.



OU/Account	Account ID	Owner	Service region	# of Device	Logging Status	Logs/Sec	Entitled(GB/Day)
Fortinet	[redacted] Primary	[redacted]	Canada (Vancouver)	2	●2	0	0.2

RESOURCE

0% — Entitled: 0.2 GB/Day Used: 0.0 GB/Day

5% — Disk: 500.0 GB Used: 24.8 GB

INFORMATION

Service Description FortiAnalyzer Cloud without SOCaaS
Expiration Date 2023-12-12 Detail
Service Version v7.4.1-build4261 230914 (GA)

Upgrading firmware from the portal

FortiAnalyzer Cloud firmware can be upgraded. The FortiAnalyzer Cloud & Service portal displays a message when a new version of firmware is available.

The following types of upgrade are available:

- Required

  For required firmware upgrades, you have a limited amount of time (such as two weeks) to upgrade the firmware after it is released. If you take no action after the grace period ends, you can no longer access the instance until you upgrade to the required firmware.
- Optional

  For optional firmware upgrades, you can choose whether to upgrade to the latest firmware.

The primary account holder can upgrade firmware from the FortiAnalyzer Cloud & Service portal.

See also Upgrading firmware from the instance on page 19.

To upgrade firmware from the portal:

1. Access the portal. See Accessing the portal and instances on page 14.

   The FortiAnalyzer Cloud & Service portal is displayed.
2. Expand your account.
3. Click the upgrade icon ⇪ to view information about available upgrades.

   The *Service Version Upgrade* window opens.
   a. Click *Upgrade Now* to update the firmware immediately.
   b. Click *Upgrade Later* to schedule upgrade of the firmware for a later date.
4. Close the *Service Version Upgrade* window, and click *Enter* to open FortiAnalyzer Cloud.

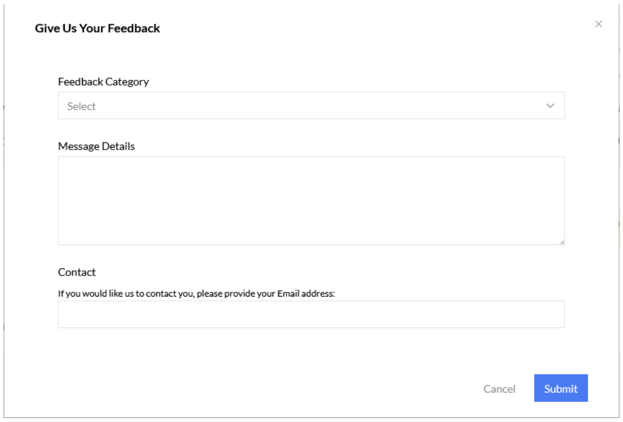
Providing feedback

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 20.

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



Give Us Your Feedback

Feedback Category

Select

Message Details

Contact

If you would like us to contact you, please provide your Email address:

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:

- Upgrading firmware from the instance on page 19
- Identifying the public IP address on page 19
- Using the FortiAnalyzer Cloud toolbar on page 20
- Enabling managed SOC service on page 22

Upgrading firmware from the instance

The primary and secondary account holders can upgrade firmware from the *Dashboard* module in the FortiAnalyzer Cloud instance.

For information about upgrading firmware from the FortiAnalyzer & Service portal, see Upgrading firmware from the portal on page 17.

To upgrade firmware from the instance:

1. Access the instance. See Accessing the portal and instances on page 14.
2. In FortiAnalyzer Cloud, go to *Dashboard*.
3. In the *System Information* widget, click the *Upgrade Firmware* button beside *Firmware Version*.
   The *Firmware Management* dialog box is displayed.
4. From the *Select Firmware* list, select the firmware version, and click *OK*.

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 the portal and instances on page 14.
2. Open the CLI console by clicking the CLI option from the FortiAnalyzer Cloud toolbar. See Using the FortiAnalyzer Cloud toolbar on page 20.
3. In the CLI console, run the following commands:

```
FMG-VM64-VIO-CLOUD # config system admin setting
```

```
set shell-access enable
Enter new password: <password>
Confirm new password: <password>
End
FMG-VM64-VIO-CLOUD # execute shell
Enter password:
bash$
bash$ curl ifconfig.me
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

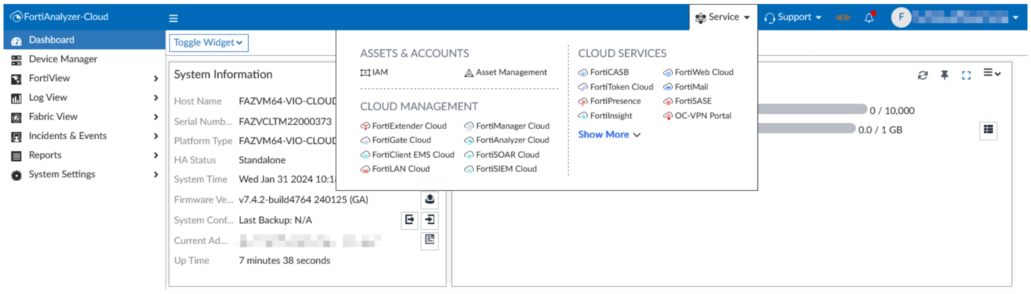
You can access FortiCloud services and support links from the FortiAnalyzer Cloud toolbar.

The FortiAnalyzer toolbar includes the following dropdown menus:

- Service on page 20
- Support on page 21
- Notifications on page 21
- Account on page 21

Service

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

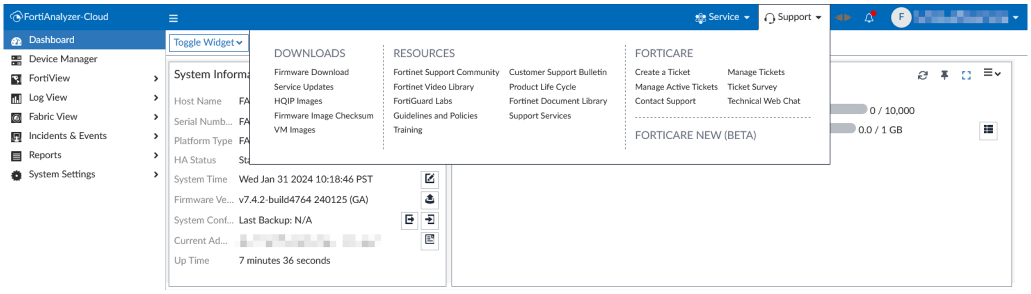


System Information

Host Name	FAZVM64-VIO-CLOUD
Serial Numb...	FAZVCLTM22000373
Platform Type	FAZVM64-VIO-CLOUD
HA Status	Standalone
System Time	Wed Jan 31 2024 10:1
Firmware Ve...	v7.4.2-build4764 240125 (GA)
System Conf...	Last Backup: N/A
Current Ad...	[redacted]
Up Time	7 minutes 38 seconds

Support

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

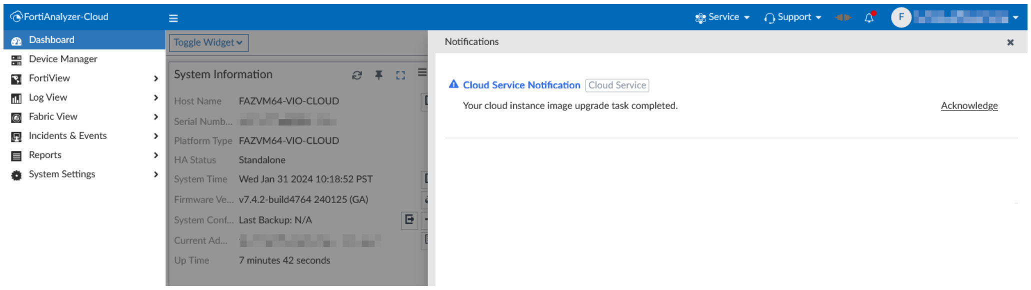


System Informa

Host Name FA
Serial Numb... FA
Platform Type FA
HA Status St
System Time Wed Jan 31 2024 10:18:46 PST
Firmware Ve... v7.4.2-build4764 240125 (GA)
System Conf... Last Backup: N/A
Current Ad... [redacted]
Up Time 7 minutes 36 seconds

Notifications

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



System Information

Host Name FAZVM64-VIO-CLOUD
Serial Numb... [redacted]
Platform Type FAZVM64-VIO-CLOUD
HA Status Standalone
System Time Wed Jan 31 2024 10:18:52 PST
Firmware Ve... v7.4.2-build4764 240125 (GA)
System Conf... Last Backup: N/A
Current Ad... [redacted]
Up Time 7 minutes 42 seconds

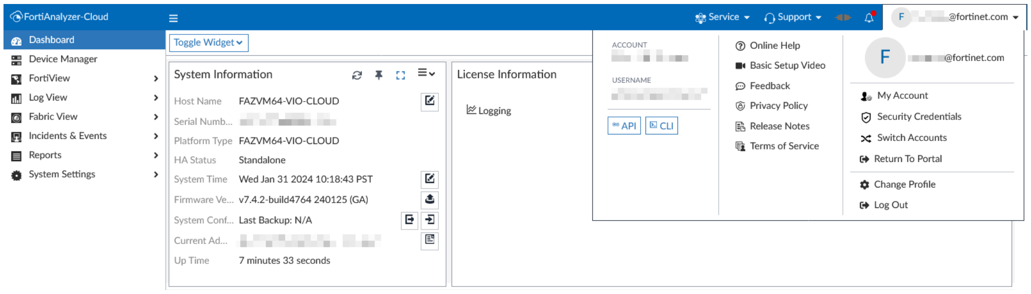
Cloud Service Notification Cloud Service

Your cloud instance image upgrade task completed.

Account

The account dropdown includes links and services related to your FortiCloud account and the FortiAnalyzer portal. 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.



System Information

Host Name FAZVM64-VIO-CLOUD
Serial Numb... [redacted]
Platform Type FAZVM64-VIO-CLOUD
HA Status Standalone
System Time Wed Jan 31 2024 10:18:43 PST
Firmware Ve... v7.4.2-build4764 240125 (GA)
System Conf... Last Backup: N/A
Current Ad... [redacted]
Up Time 7 minutes 33 seconds

ACCOUNT [redacted]
USERNAME [redacted]
[redacted]@fortinet.com

Enabling managed SOC service

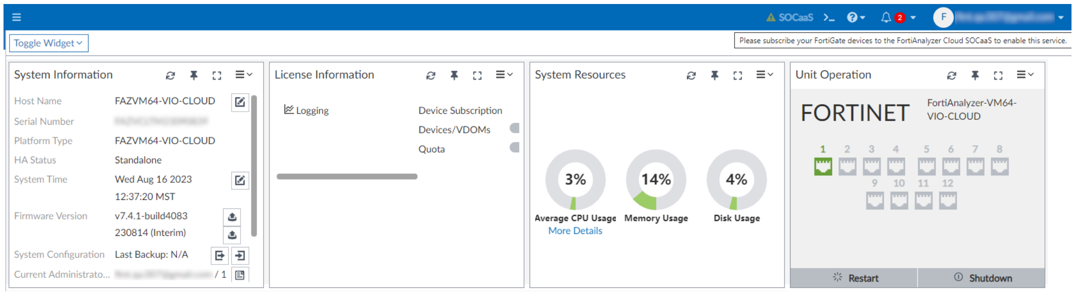
With a valid license, you can enable the *Managed SOC Service* option in FortiAnalyzer Cloud. When enabling the service, you are redirected to the SOCaaS Portal where you can complete the onboarding process.

For more information about onboarding the service from the SOCaaS portal, see the SOCaaS User Guide

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

To configure FortiAnalyzer Cloud:

1. Log in to FortiAnalyzer Cloud.
2. Click on the *SOCaaS* button 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.

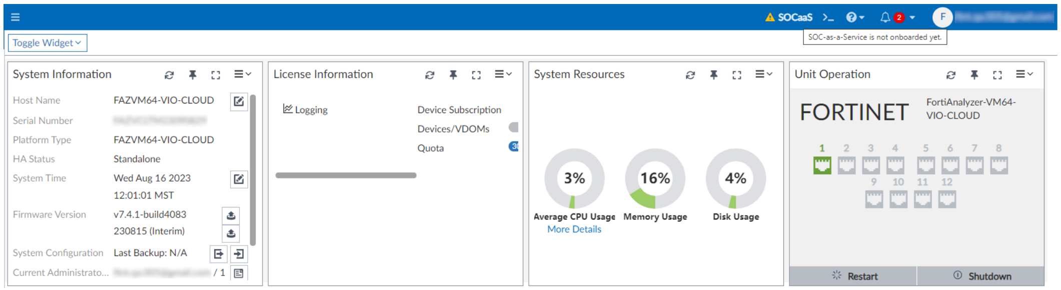


Please subscribe your FortiGate devices to the FortiAnalyzer Cloud SOCaaS to enable this service.

System Information

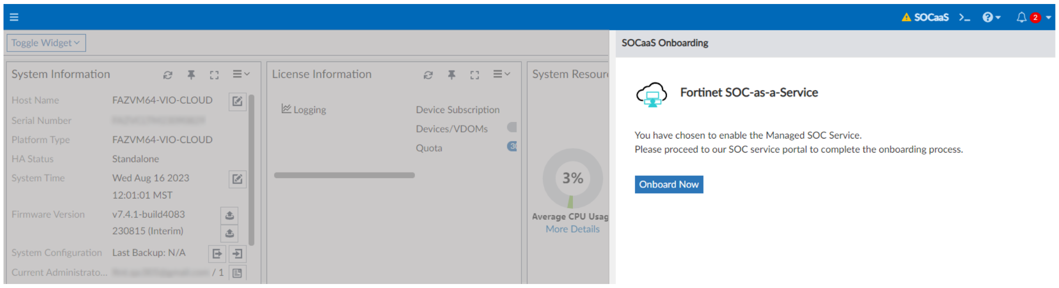
Host Name FAZVM64-VIO-CLOUD
Serial Number [redacted]
Platform Type FAZVM64-VIO-CLOUD
HA Status Standalone
System Time Wed Aug 16 2023 12:37:20 MST
Firmware Version v7.4.1-build4083 230814 (Interim)
System Configuration Last Backup: N/A
Current Administrato... [redacted] / 1

   b. With the correct entitlement, the SOCaaS Onboarding window opens. Can click *Onboard Now* to be redirected to the SOCaaS portal where you can complete your onboarding. See the SOCaaS User Guide.



SOC-as-a-Service is not onboarded yet.

Host Name	FAZVM64-VIO-CLOUD
Serial Number	[redacted]
Platform Type	FAZVM64-VIO-CLOUD
HA Status	Standalone
System Time	Wed Aug 16 2023 12:01:01 MST
Firmware Version	v7.4.1-build4083 230815 (Interim)
System Configuration	Last Backup: N/A
Current Administrato...	[redacted] / 1



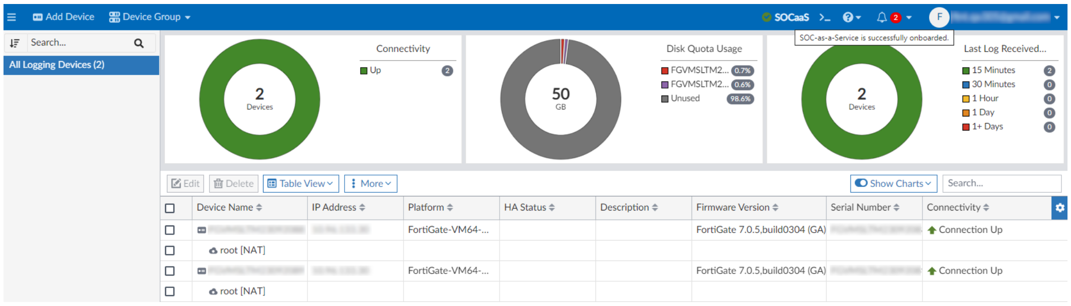
Host Name	FAZVM64-VIO-CLOUD
Serial Number	[redacted]
Platform Type	FAZVM64-VIO-CLOUD
HA Status	Standalone
System Time	Wed Aug 16 2023 12:01:01 MST
Firmware Version	v7.4.1-build4083 230815 (Interim)
System Configuration	Last Backup: N/A
Current Administrato...	[redacted] / 1

Fortinet SOC-as-a-Service

You have chosen to enable the Managed SOC Service.
Please proceed to our SOC service portal to complete the onboarding process.

Onboard Now

3. Once onboarded to SOCaaS, the FortiAnalyzer Cloud SOCaaS button is no longer clickable and is displayed with a green check mark.



SOC-as-a-Service is successfully onboarded.

	Device Name	IP Address	Platform	HA Status	Description	Firmware Version	Serial Number	Connectivity
□	[redacted]	[redacted]	FortiGate-VM64-...			FortiGate 7.0.5,build0304 (GA)	[redacted]	Connection Up
□	root [NAT]							
□	[redacted]	[redacted]	FortiGate-VM64-...			FortiGate 7.0.5,build0304 (GA)	[redacted]	Connection Up
□	root [NAT]							

Using account services

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

- Adding a secondary account on page 24
- Modifying a secondary account on page 26
- Supporting IAM users and IAM API users on page 26

For information about using FortiCloud portal, see the FortiCloud Account Services page on the Fortinet Document Library.

Adding a secondary account

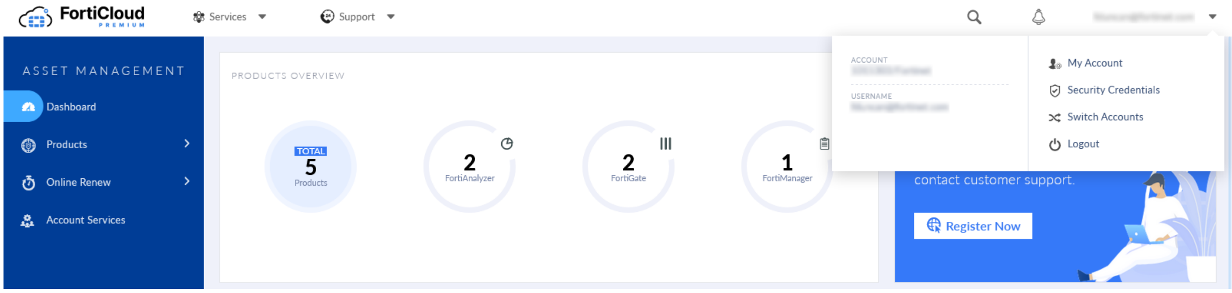
Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. Be default, the secondary account holder is assigned the default administrator profile named *Restricted_User*. However, the primary account holder can modify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

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

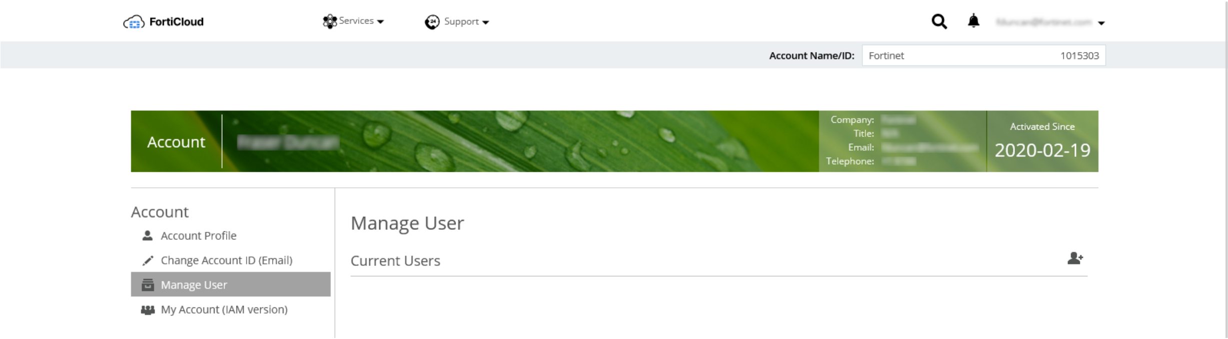
With FortiAnalyzer Cloud 7.0.x and later, you can use the Identity and Access Management (IAM) portal, and you can migrate secondary accounts to the IAM portal. In IAM portal, secondary accounts are called sub users. For information about migrating sub users, see the *Identity & Access Management Guide*.

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.



FortiCloud Services ▾ Support ▾ [redacted] ▾

Account Name/ID: Fortinet 1015303

Account [redacted]

Company: [redacted]
Title: [redacted]
Email: [redacted]
Telephone: [redacted]

Activated Since
2020-02-19

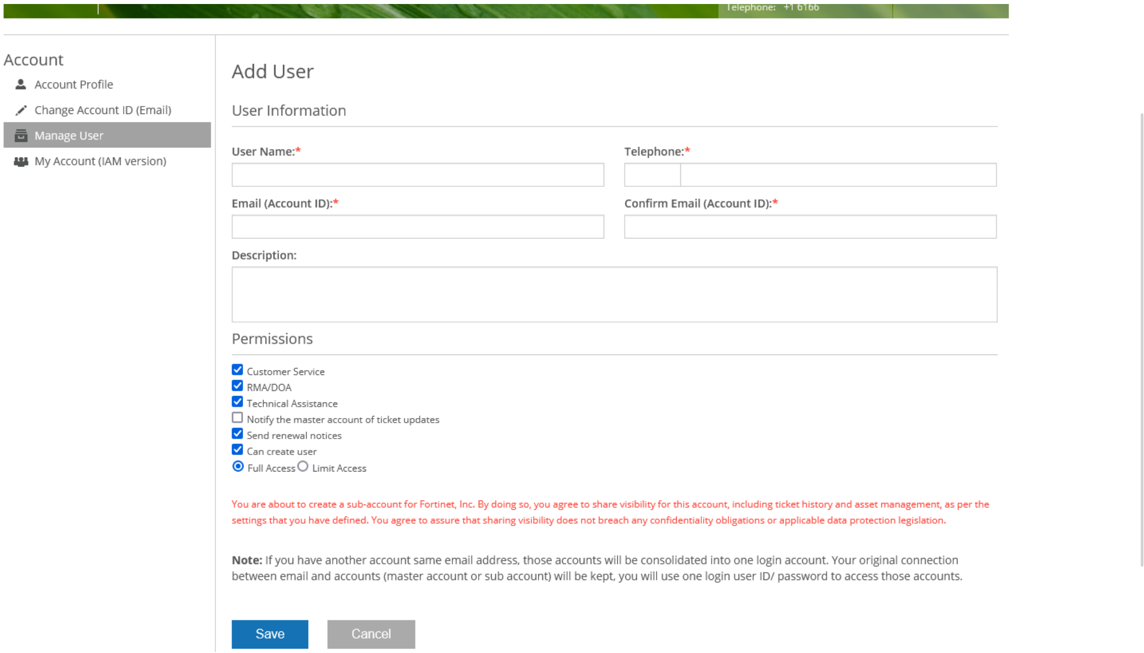
Account
- Account Profile
- Change Account ID (Email)
- Manage User
- My Account (IAM version)

Manage User

Current Users

5. 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.



Telephone: +1 6166

Account
- Account Profile
- Change Account ID (Email)
- Manage User
- My Account (IAM version)

Add User

User Information

User Name:*

Telephone:*

Email (Account ID):*

Confirm Email (Account ID):*

Description:

Permissions

☑ Customer Service
☑ RMA/DOA
☑ Technical Assistance
☐ Notify the master account of ticket updates
☑ Send renewal notices
☑ Can create user
● Full Access ○ Limit Access

You are about to create a sub-account for Fortinet, Inc. By doing so, you agree to share visibility for this account, including ticket history and asset management, as per the settings that you have defined. You agree to assure that sharing visibility does not breach any confidentiality obligations or applicable data protection legislation.

Note: If you have another account same email address, those accounts will be consolidated into one login account. Your original connection between email and accounts (master account or sub account) will be kept, you will use one login user ID/ password to access those accounts.

Save Cancel

6. Log in to the personal FortiCare portal. Under FortiAnalyzer Cloud section, you will see an account listed as a secondary member.
7. Click the entry to expand the view.
8. 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 26.

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 24.

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*.

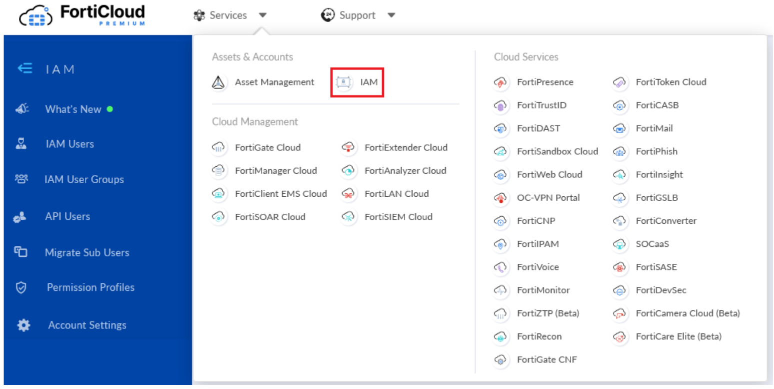
See also Adding IAM users on page 26 and Adding API users on page 28.

Adding IAM users

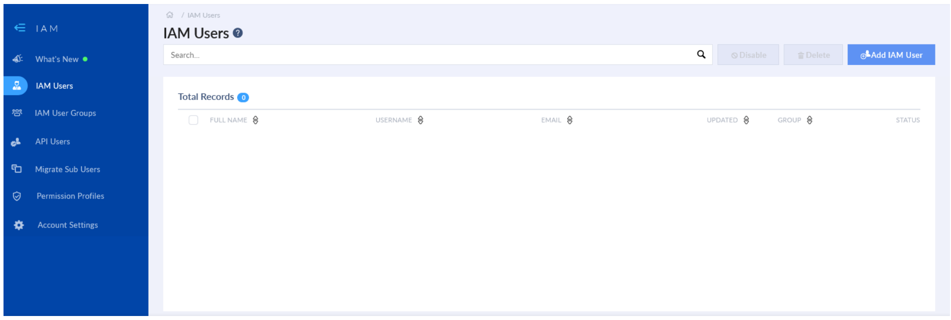
FortiAnalyzer Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiAnalyzer Cloud.

To add an IAM user:

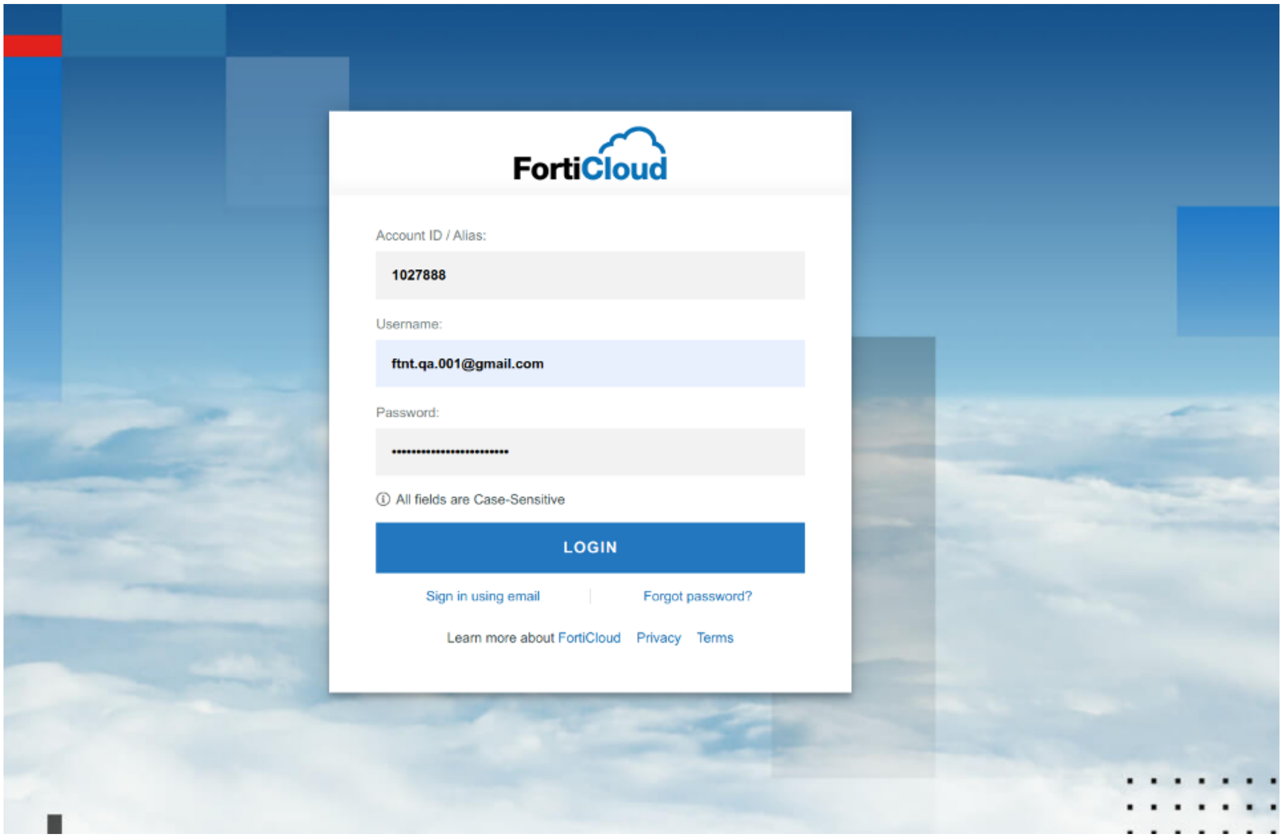
1. Go to FortiCloud (https://support.fortinet.com/), and log in.
2. From the *Services* menu, select *IAM* .



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.



Account ID / Alias: 1027888

Username: ftnt.qa.001@gmail.com

Password: ••••••••••••••••••••••••

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 *Super_User* admin profile.
Read-Write	Assigned to the *Standard_User* admin profile.
Read-Only	Assigned to the *Restricted_User* admin profile.
Custom	*Custom* users are assigned to the *Restricted_User* admin profile the first time they log in. A *Super_User* 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 through the API. API users can only use OAuth 2.0 for authentication.

See Adding an API user in the FortiCloud Account Services documentation for instructions on how to add API users.

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.

External IdP support is currently a *limited beta* feature in FortiCloud. If you require external IdP support for your FortiAnalyzer Cloud instance, please contact FortiCare Support.

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

www.fortinet.com