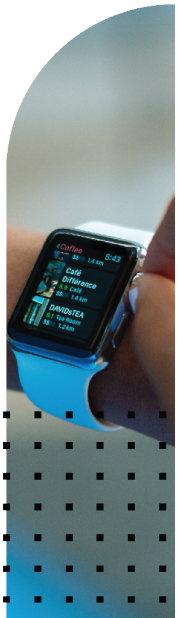
Cloud Deployment Guide

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

May 13th, 2026
FortiAnalyzer 7.4.x Cloud Deployment Guide
05-74-843405-20260513

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-09-19	Initial release.
2023-01-30	Initial release of FortiAnalyzer Cloud 7.4.2.
2024-02-28	Updated Introduction on page 5 and Accessing your FortiAnalyzer Cloud instance on page 20.
2024-04-22	Updated Requirements on page 5.
2024-06-06	Initial release of FortiAnalyzer Cloud 7.4.3.
2024-06-28	Added Privacy and notification preferences on page 23
2024-07-02	Added Using multiple roles with external IdP users on page 35.
2024-09-27	Initial release of FortiAnalyzer Cloud 7.4.4.
2024-10-18	Initial release of FortiAnalyzer Cloud 7.4.5.
2025-01-24	Initial release of FortiAnalyzer Cloud 7.4.6.
2025-04-15	Updated Introduction on page 5.
2025-06-16	Initial release of FortiAnalyzer Cloud 7.4.7.
2025-07-24	Updated Enabling managed SOC service from FortiAnalyzer Cloud on page 26.
2025-08-05	Updated Supporting external IdP users on page 35.
2025-10-14	Initial release of FortiAnalyzer Cloud 7.4.8.
2026-01-02	Updated Adding API users on page 34.
2026-02-02	Initial release of FortiAnalyzer Cloud 7.4.10.
2026-03-10	Updated Configuring FortiClient EMS/FortiEndpoint on page 12.
2026-05-13	Initial release of FortiAnalyzer Cloud 7.4.11.

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.

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

You can visit the FortiCloud status page to find and subscribe to status information for FortiAnalyzer Cloud.

This section includes the following topics:

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 29.

  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 and FortiMail

Additional storage may also be added as required for FortiGate, FortiEndpoint, and FortiWeb 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 and FortiMail 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 a number of licensed features including *OT Security Service* and *Attack Surface Rating and Compliance*.

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 8.
2. On FortiCloud, deploy a FortiAnalyzer Cloud instance. See Deploying a FortiAnalyzer Cloud instance on page 9.
3. (Optional) Upgrade FortiAnalyzer Cloud to the latest available cloud version. See Upgrading firmware from the instance on page 21.
4. On FortiOS or FortiMail, enable logging to FortiAnalyzer Cloud:
   - For FortiOS, see Configuring FortiOS on page 11.
   - For FortiClient EMS and FortiEndpoint, see Configuring FortiClient EMS/FortiEndpoint on page 12.
   - For FortiMail, see Configuring FortiMail on page 14.
   - For FortiWeb, see Configuring FortiWeb on page 15.

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:
   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 9.

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 29.

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.

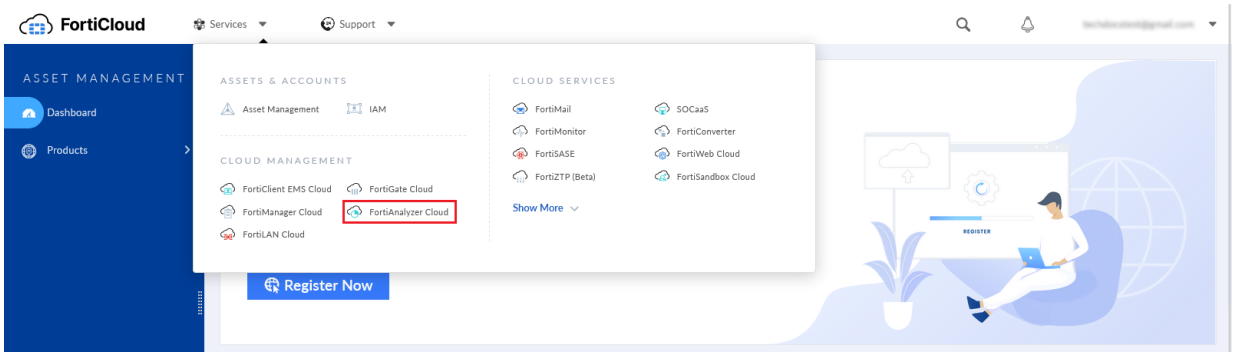
At the time of the 7.4 release, FortiAnalyzer Cloud supports new deployments in version 7.2 and upgrades to version 7.4.

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

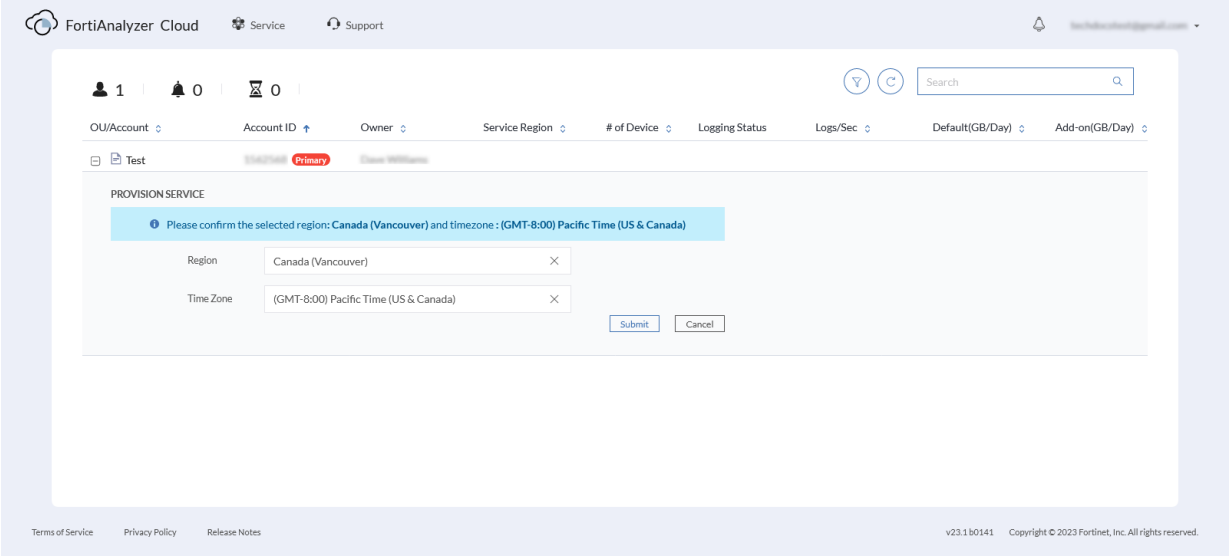
To deploy a FortiAnalyzer Cloud instance:

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*.

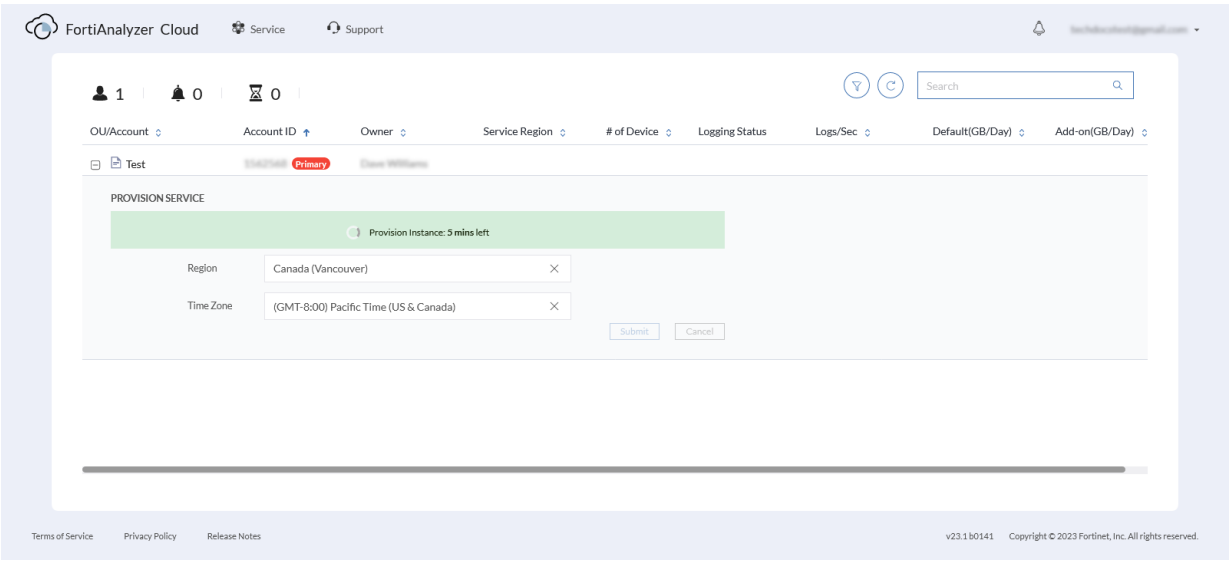


   The *FortiAnalyzer Cloud & Service* portal is displayed.
3. On the *FortiAnalyzer Cloud & Service* portal:
   a. Select a *Region* for the FortiAnalyzer Cloud instance. In this example, the region is *Canada (Vancouver)*.
   b. Select a *Time Zone* for the FortiAnalyzer Cloud instance.
4. Click *Submit*.

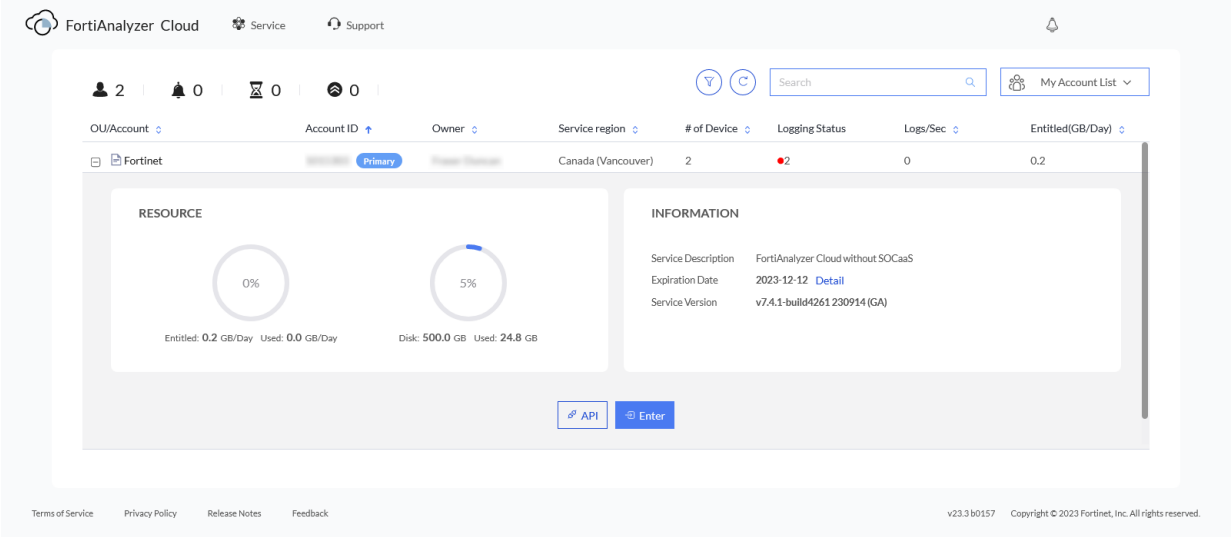


5. Confirm your selected region and time zone.

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 23.
8. FortiAnalyzer Cloud instance is provisioned in a few minutes.



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



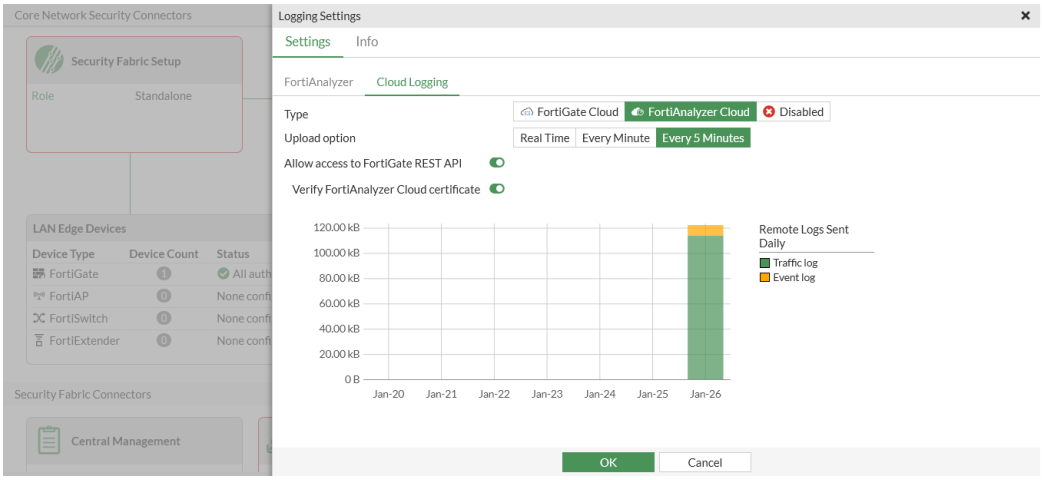
10. (Optional) Upgrade FortiAnalyzer Cloud to 7.4.x. See Upgrading firmware from the instance on page 21.
11. Configure FortiOS to work with FortiAnalyzer Cloud. See Configuring FortiOS on page 11.

Configuring FortiOS

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

To configure FortiOS:

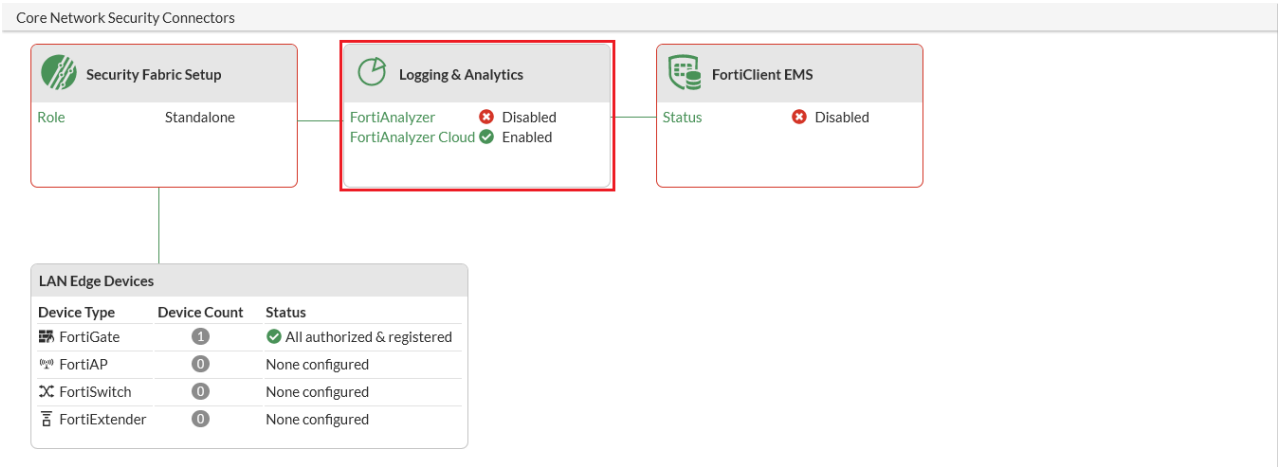
1. In FortiOS, enable FortiAnalyzer Cloud.
   a. Go to *Security Fabric* > *Fabric Connectors*, and edit the *Logging and Analytics* card.
   b. Select the *Cloud Logging* tab, and set the *Type* to FortiAnalyzerCloud.
   c. Configure the remaining settings to your preference, and click *OK*.



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*.

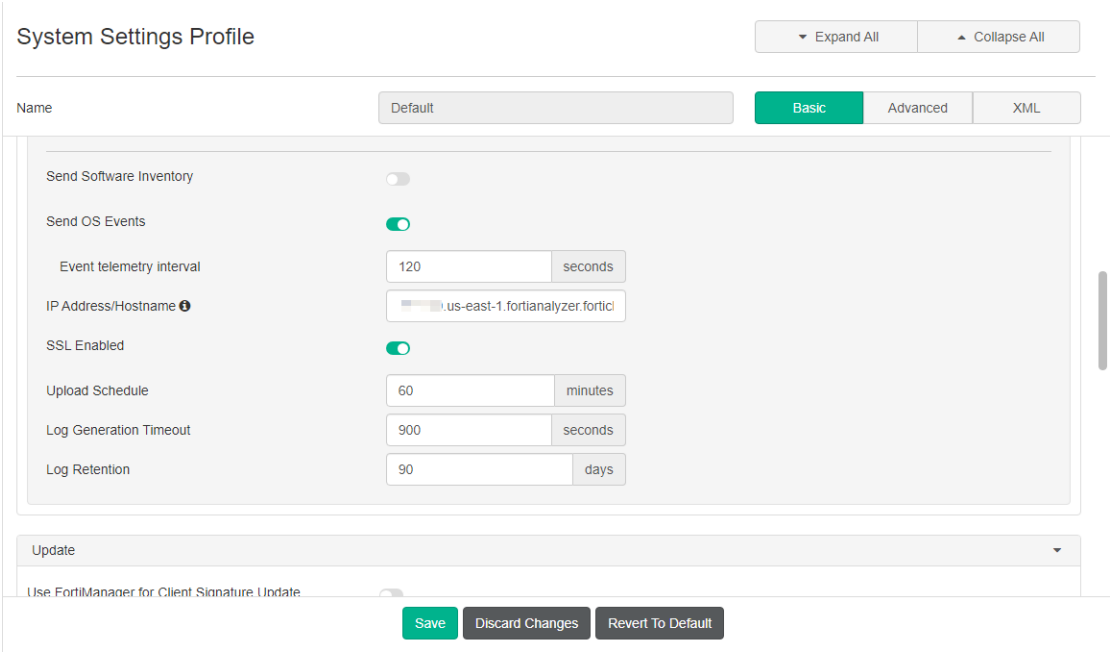


Configuring FortiClient EMS/FortiEndpoint

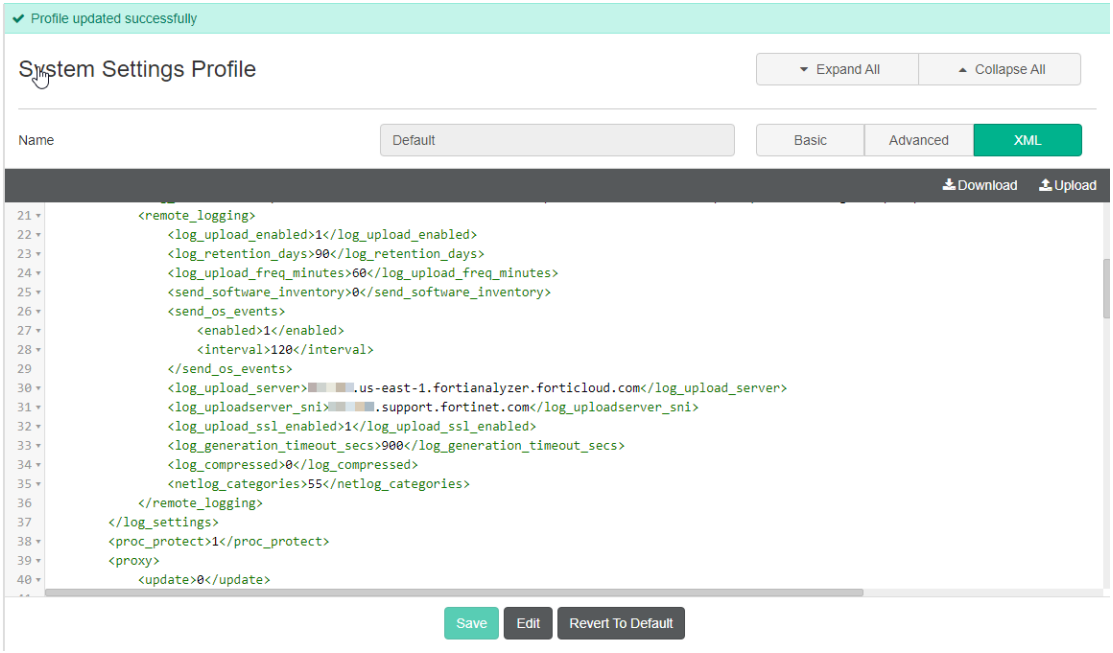
This section explains how to enable FortiClient EMS 7.0.3 and later and FortiEndpoint to send logs to FortiAnalyzer Cloud.

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.

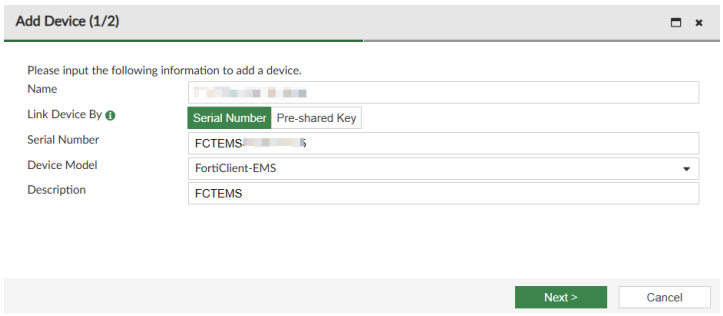


e. Configure the SNI for FortiAnalyzer Cloud by switching to the *XML* view and adding the `<log_uploadserver_sni>` tag with the FortiAnalyzer Cloud SNI. See the FortiClient EMS XML Reference Guide for more information.



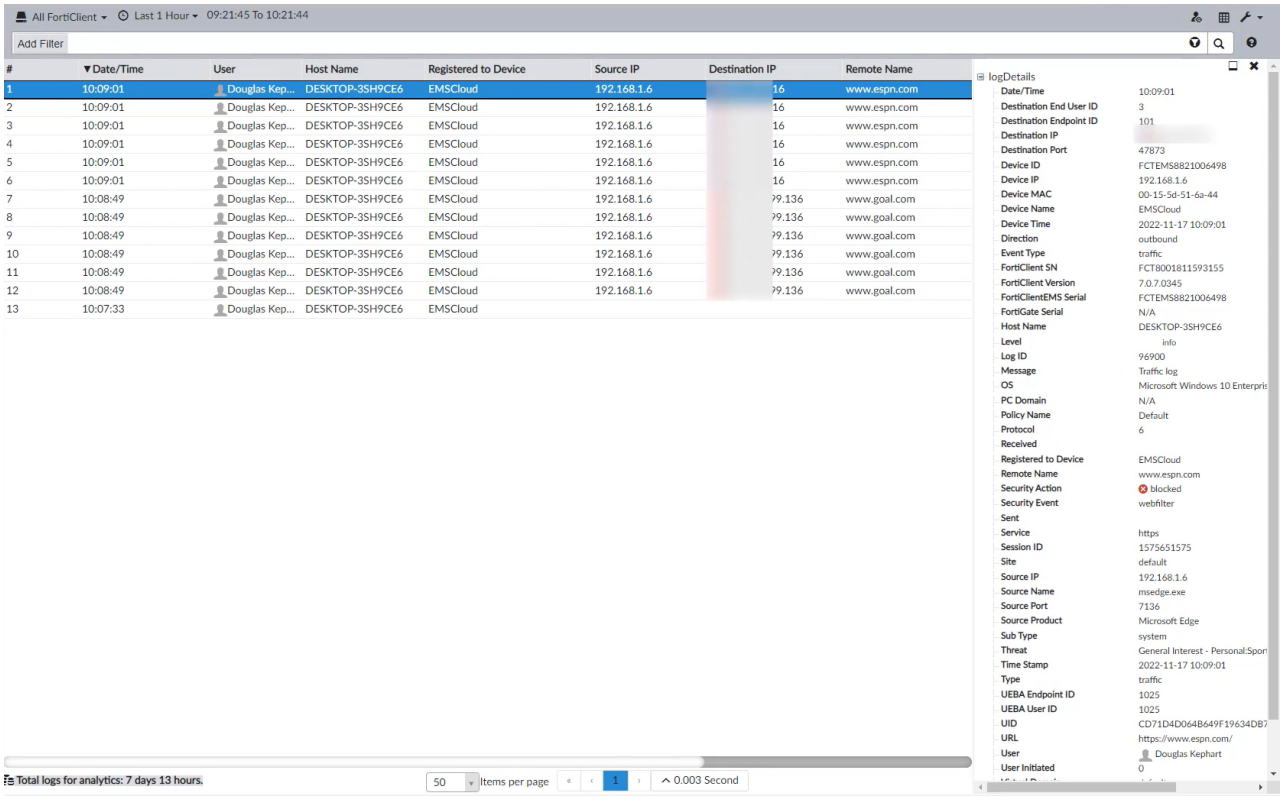
f. Configure other fields as desired, and save the profile.

2. In the FortiAnalyzer Cloud instance, go to *Device Manager*, and click *Add Device* to add the 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.



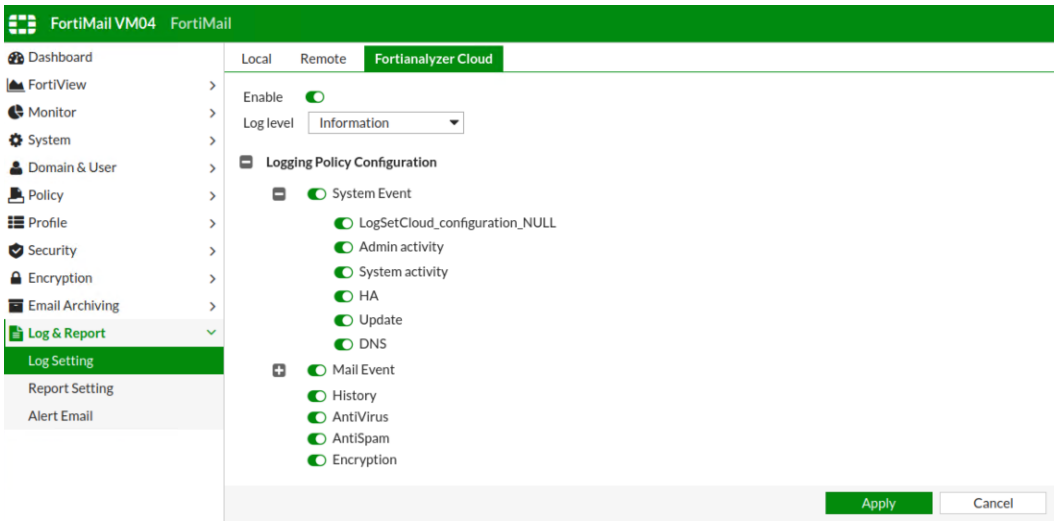
Configuring FortiMail

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

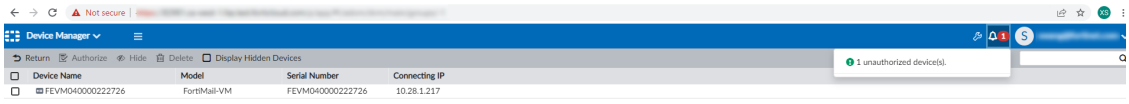
To configure FortiMail:

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.

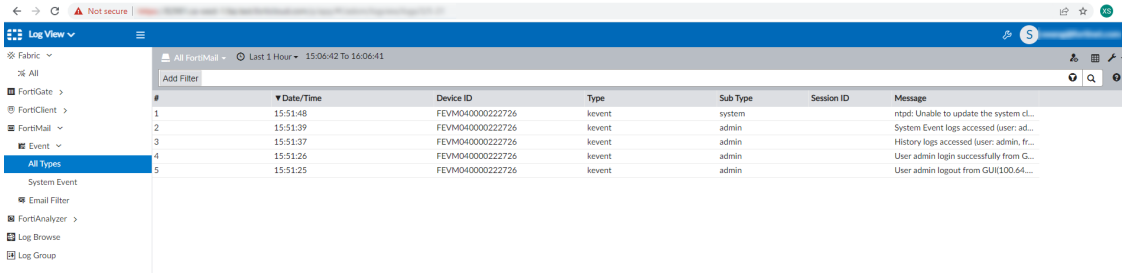


2. In the FortiAnalyzer Cloud instance, go to *Device Manager*, and authorize FortiMail.



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.

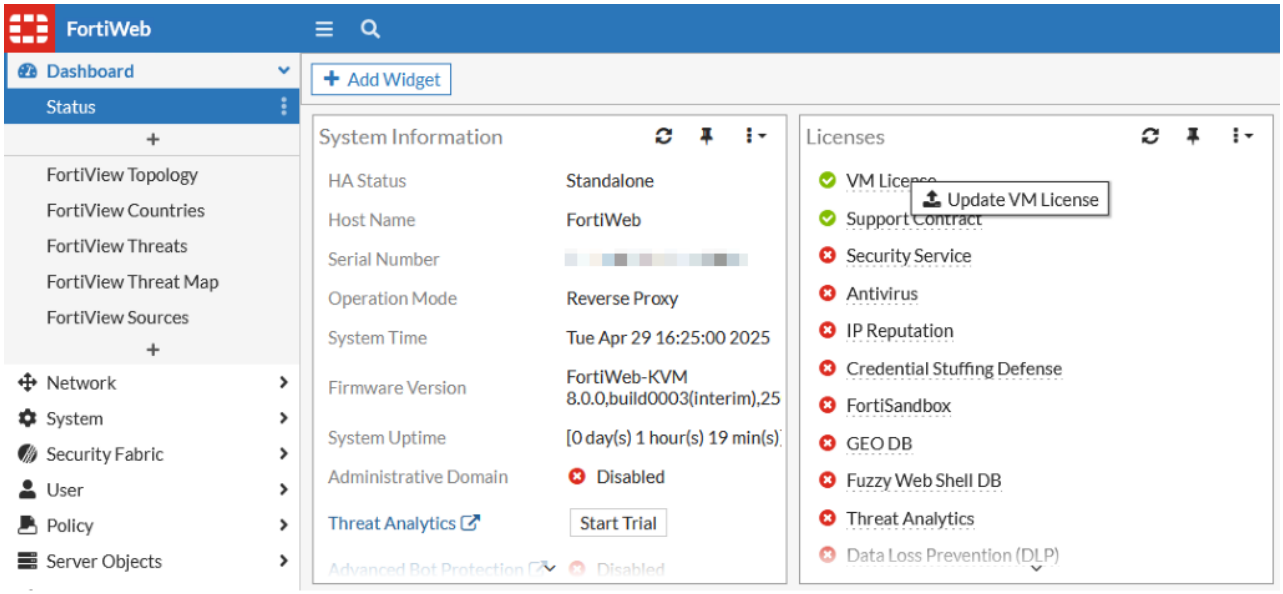
Before configuring FortiAnalyzer Cloud on FortiWeb, verify that the FortiAnalyzer Cloud license is active to ensure proper connectivity and log forwarding. You can check the license status directly from the FortiWeb Dashboard to confirm whether the service is enabled and valid.

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

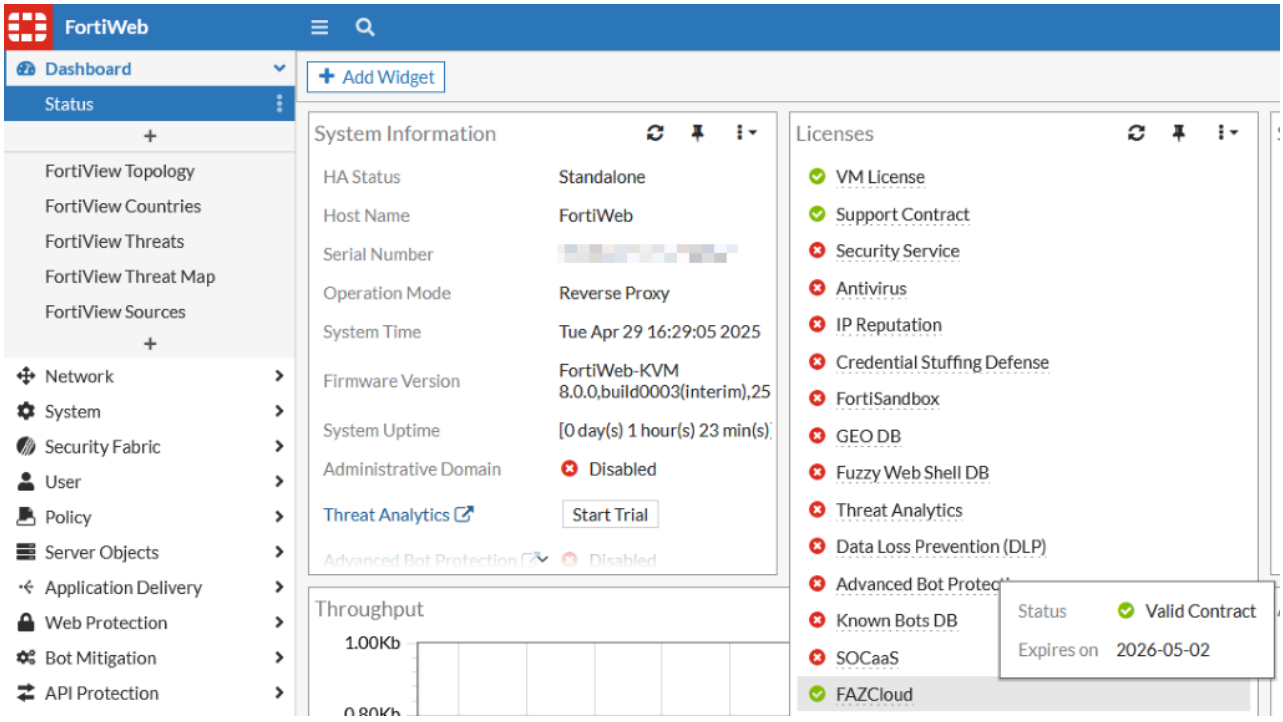
For more information on enabling logging from FortiWeb, see the FortiWeb Administration Guide.

To configure FortiWeb logging to FortiAnalyzer Cloud:

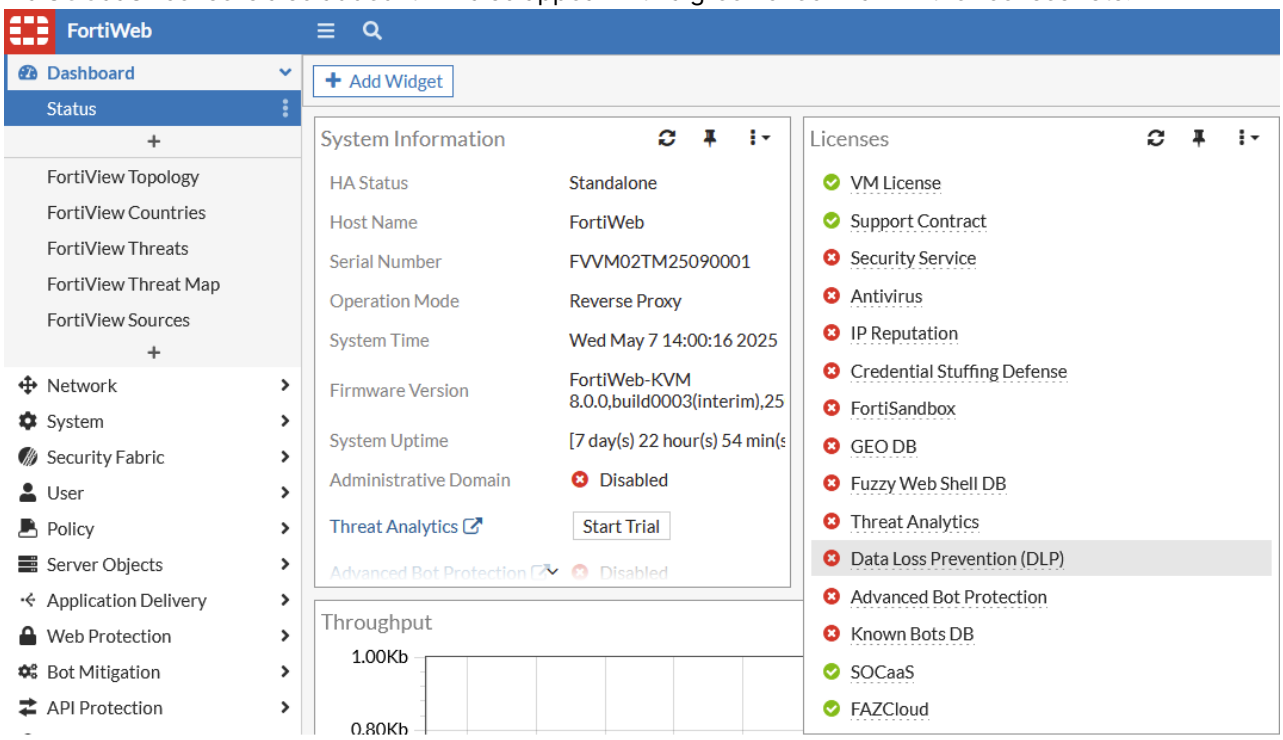
1. On the FortiWeb *Dashboard* > *Status* page, upload the license file which includes the FortiAnalyzer Cloud entitlement.
   Once the license file is uploaded, FortiWeb will reboot.



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.

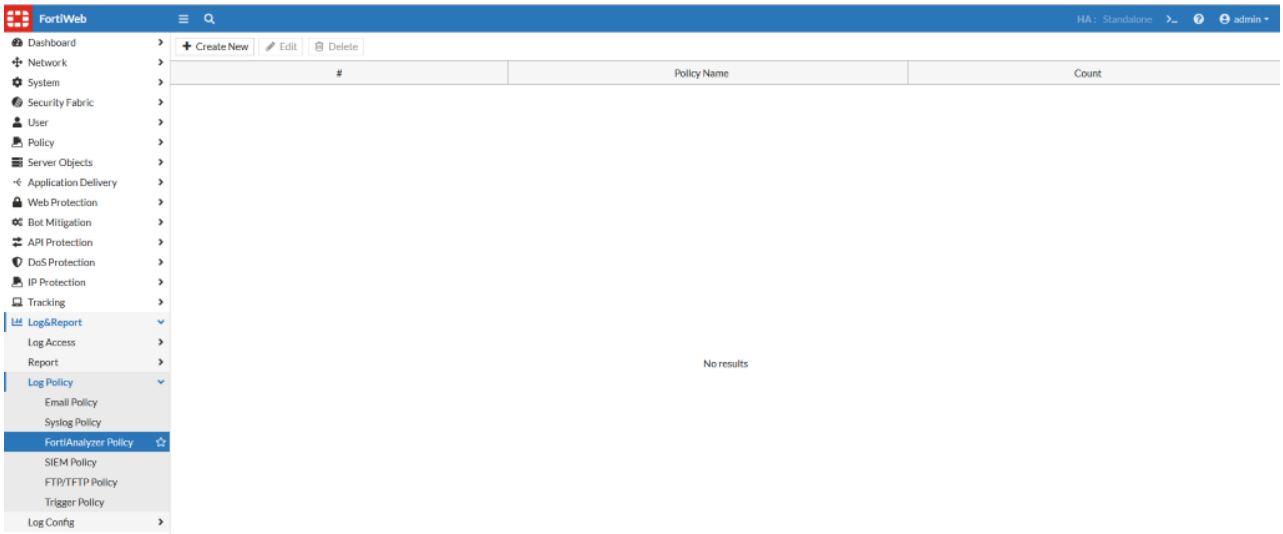


3. On FortiAnalyzer Cloud, go to Device Manager.

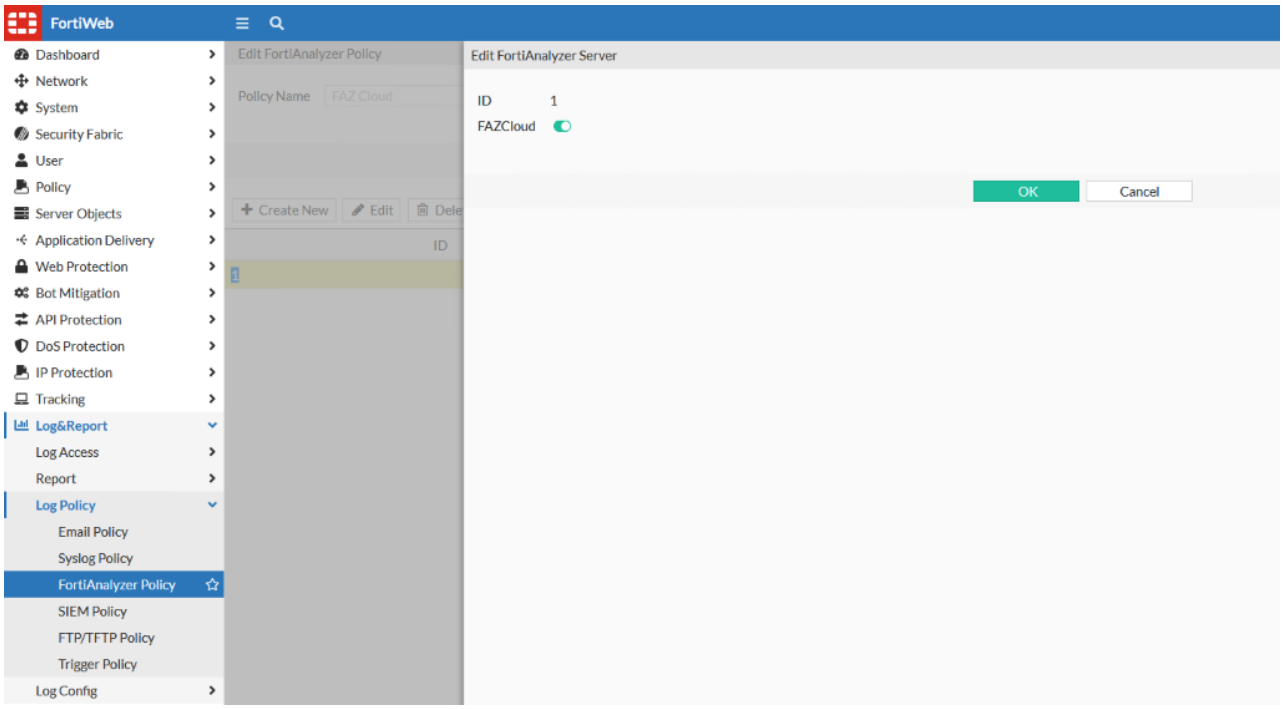
   FortiWeb will be automatically added and authenticated to FortiAnalyzer Cloud. You can alternatively manually add the FortiWeb device by entering its serial number in the *Add Device* wizard.

To configure a log policy on FortiWeb:

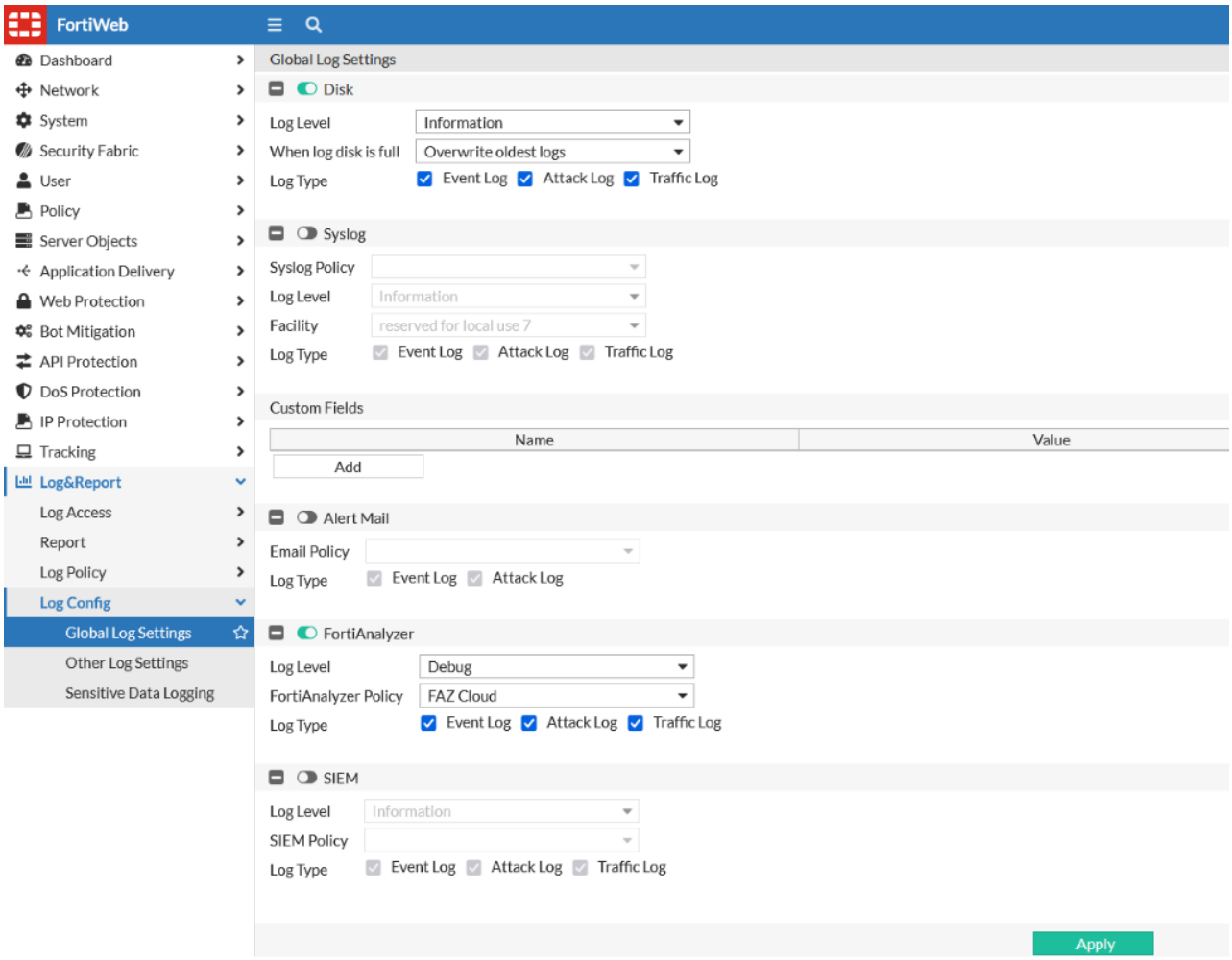
1. On FortiWeb, go to *Log&Report* > *Log Policy* > *FortiAnalyzer Policy*. Click *Create New*.



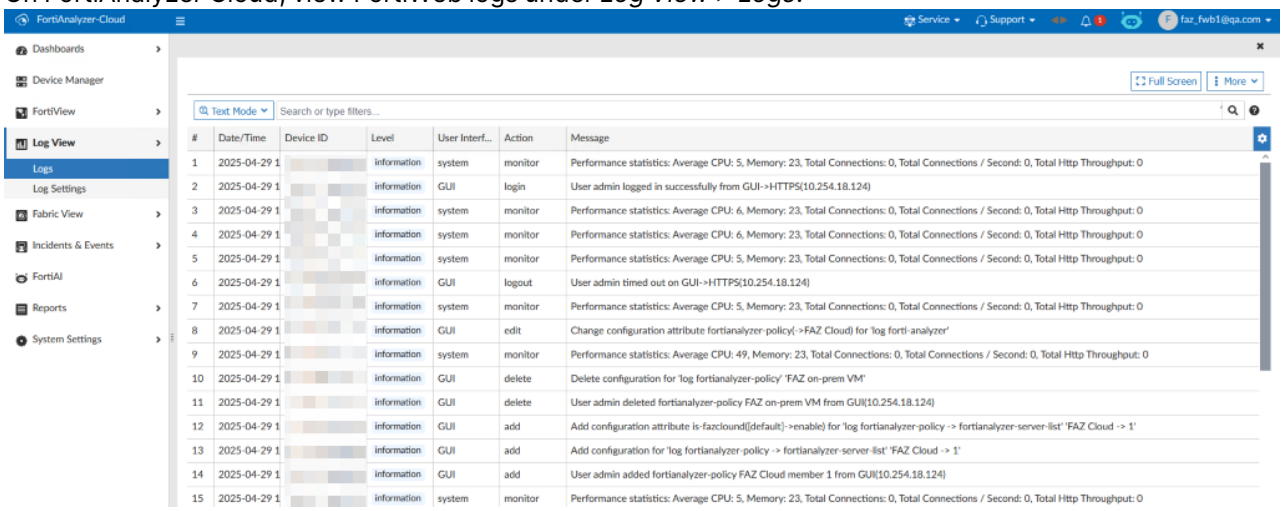
2. Enter a name for the policy and click *OK*.
3. Click *Create New* to open a slide window. Enable *FAZCloud*, and click *OK*.



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



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



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

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

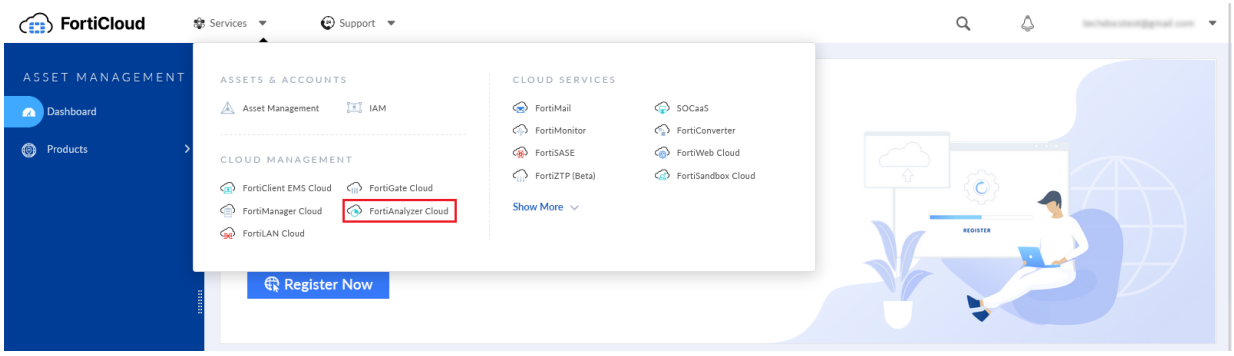
1. Go to https://fortianalyzer.forticloud.com. After authentication, you are redirected to your own FortiAnalyzer Cloud instance.
2. Go directly to your instance using the specific URL for your instance (e.g. `https://{account_id}.{region}.fortianalyzer.forticloud.com`). You can obtain your instance's 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 20.

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.

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



You are automatically logged in to your FortiAnalyzer instance.

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 20.
2. Open the CLI console by clicking the CLI option from the FortiAnalyzer Cloud toolbar. See Using the FortiAnalyzer Cloud toolbar on page 21.
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.

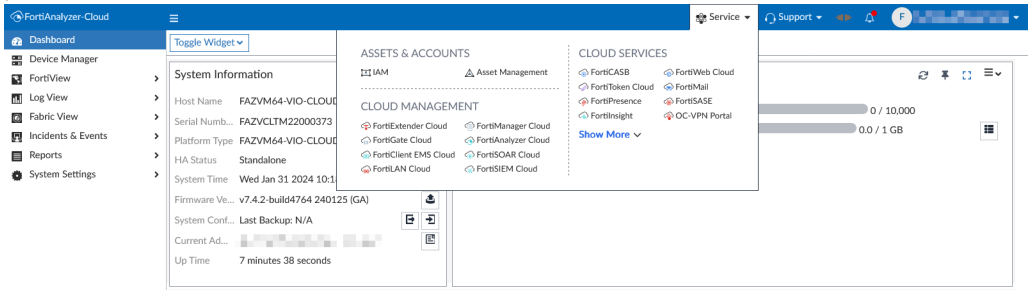
Using the FortiAnalyzer Cloud toolbar

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

The FortiAnalyzer toolbar includes the following dropdown menus:

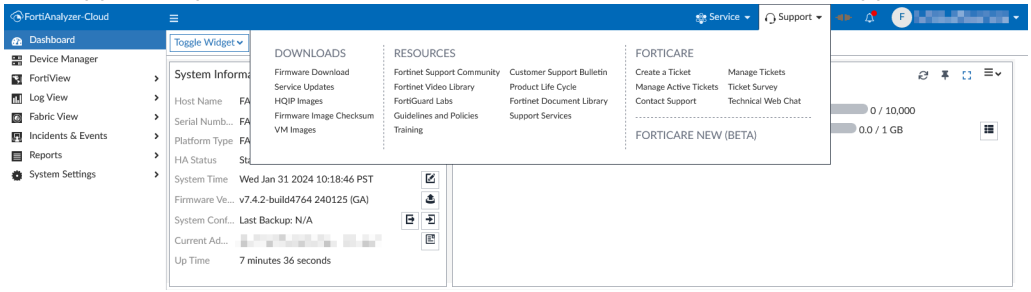
Service

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



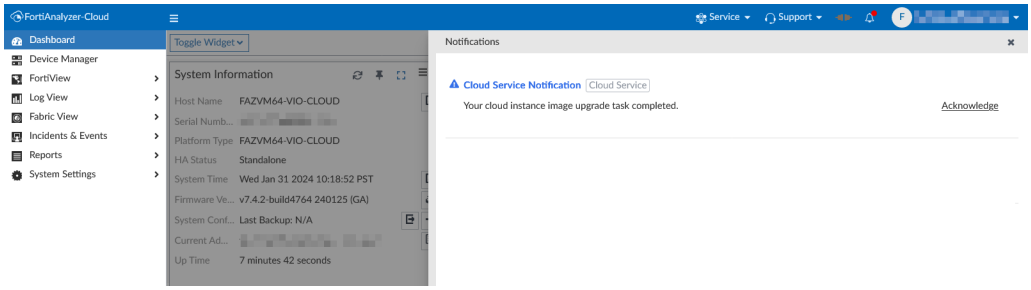
Support

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



Notifications

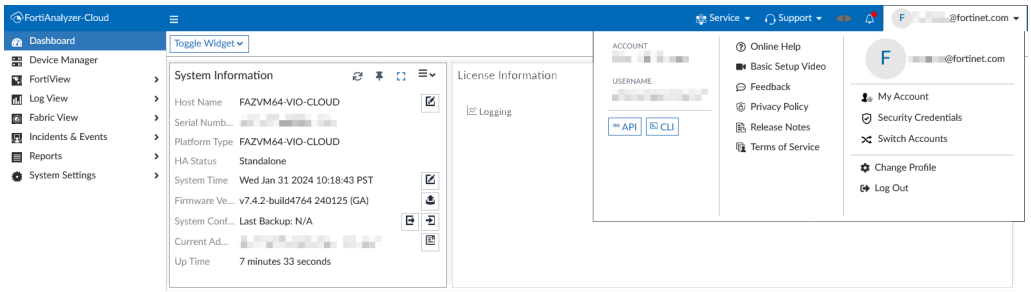
Click the notification icon  to open the notification drawer and view and interact with notifications for FortiAnalyzer Cloud.



Account

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

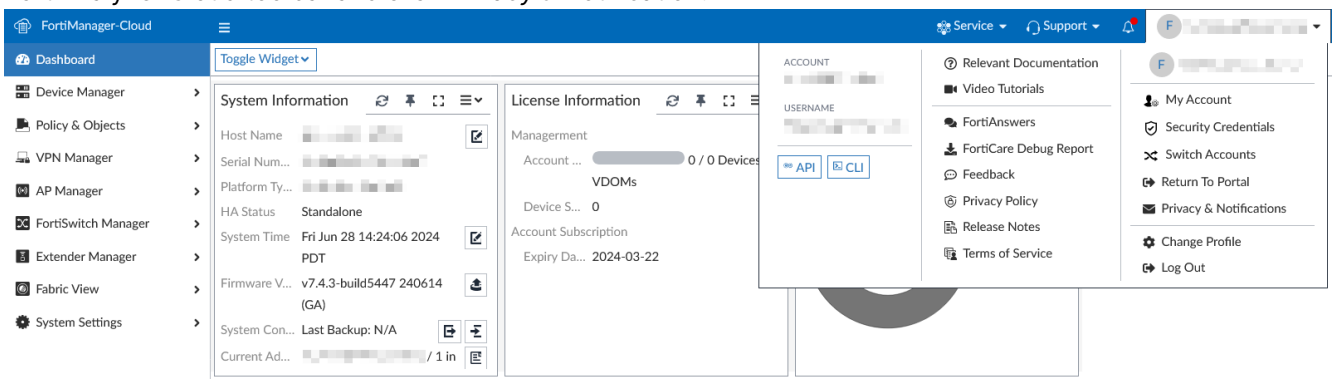
Account		Your account ID.
Username		Your current username.
API and CLI		Open the API User or CLI pane.
Help Content		Links for Online Help, Basic Setup Videos, Feedback, Privacy Policy, Release Notes, and Terms of Service.
FortiCloud Account Links		FortiCloud account links including My Account, Security Credentials, Subscriptions, 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.
	Change Profile	Change FortiAnalyzer Cloud profile options including avatar and theme.
	Privacy & Notifications	Click to access the *Privacy & Notification* menu where you can configure access settings for the FortiCloud team as well as email notification preferences. See Privacy and notification preferences on page 23.
	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*.

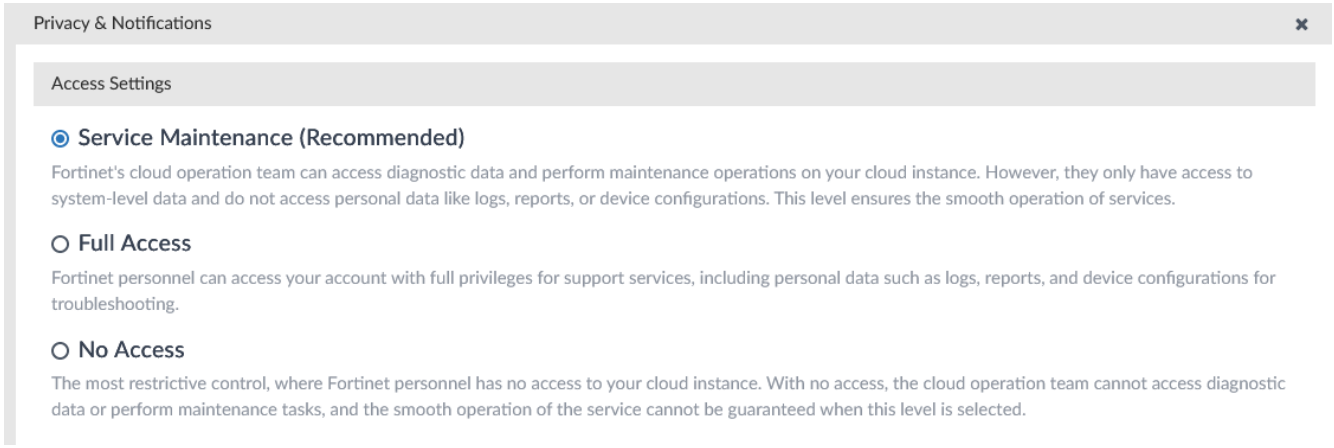


In *Privacy & Notifications*, you can configure the following:

- Access Settings on page 24
- Email Notifications on page 25

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:



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*.

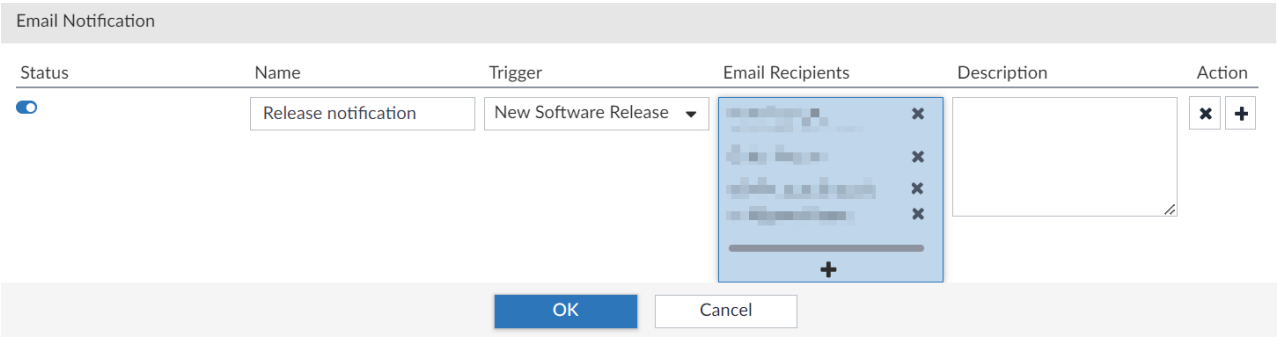
FortiAnalyzer Cloud records changes to access settings in the *Event Log*.

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. Click the add icon in the *Email Notification* section to configure new email notification preferences.
4. Configure the following:



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.
Email Recipients	Click to add at least one email recipient. You can select IAM/Sub users from the populated list or click the *Email Address* tab to add additional emails.
Description	Add an optional description.
Action	You can use the action field to delete a notification preference or create additional notifications preferences.

5. Click *OK*.

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

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.

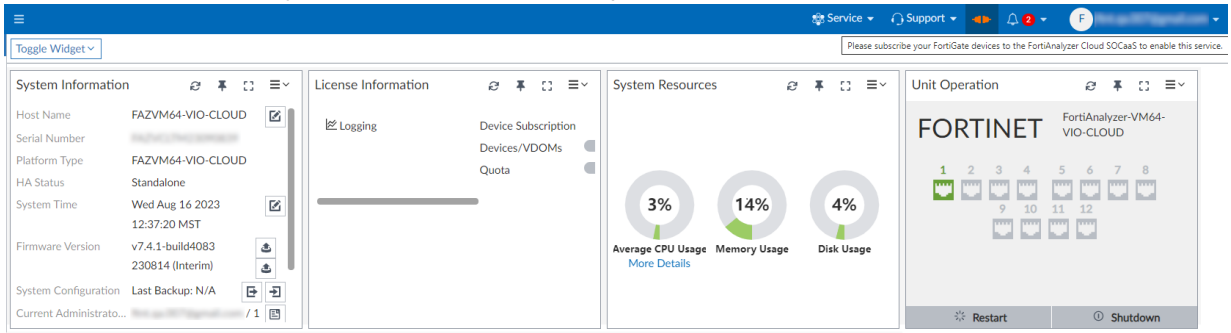
Prerequisites

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

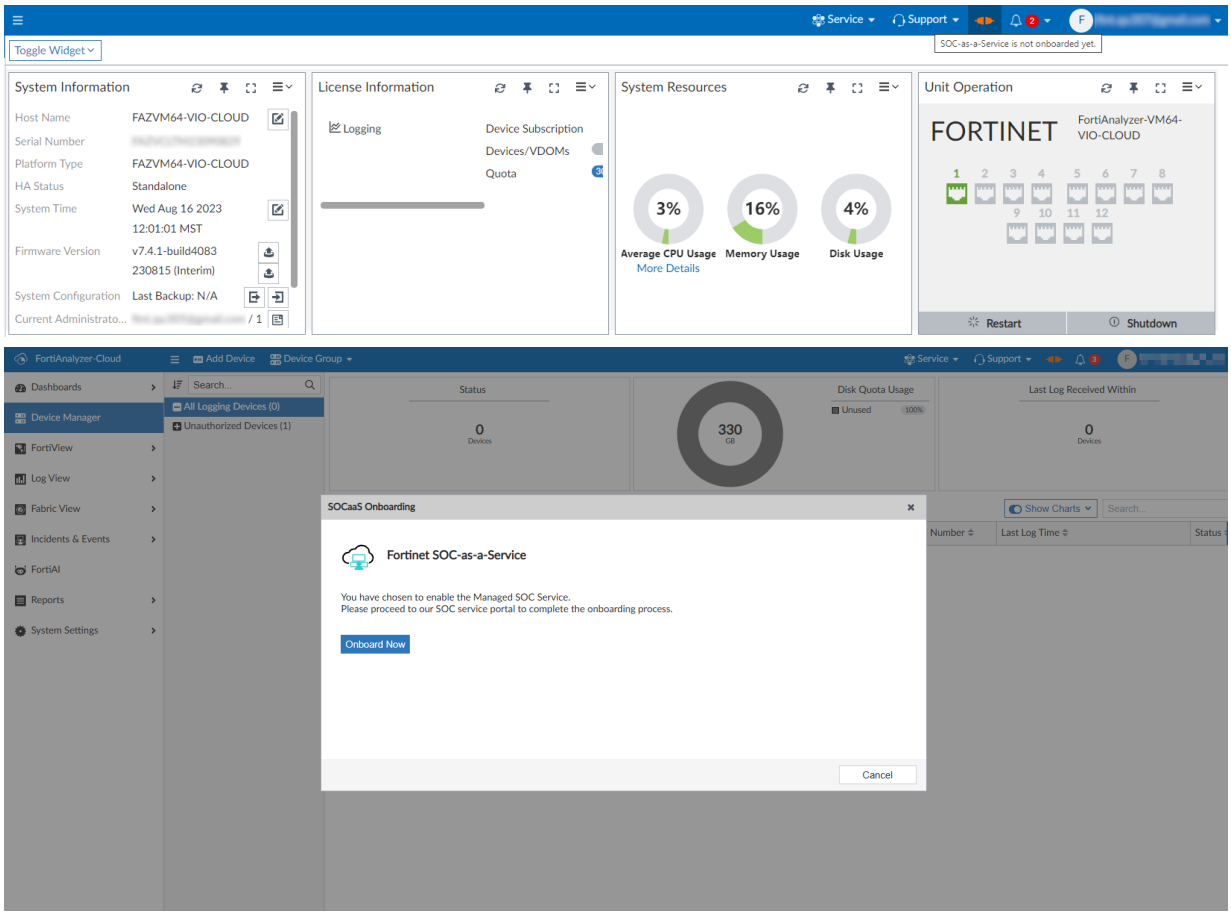
1. You have provisioned the FortiAnalyzer Cloud instance on the region of your choice. See Deploying a FortiAnalyzer Cloud instance on page 9.
2. You have configured the FortiGate to send the entitled device logs to the SOCaaS collection point (FortiAnalyzer Cloud) that will forward the logs. See Configuring FortiOS on page 11.

To configure FortiAnalyzer Cloud:

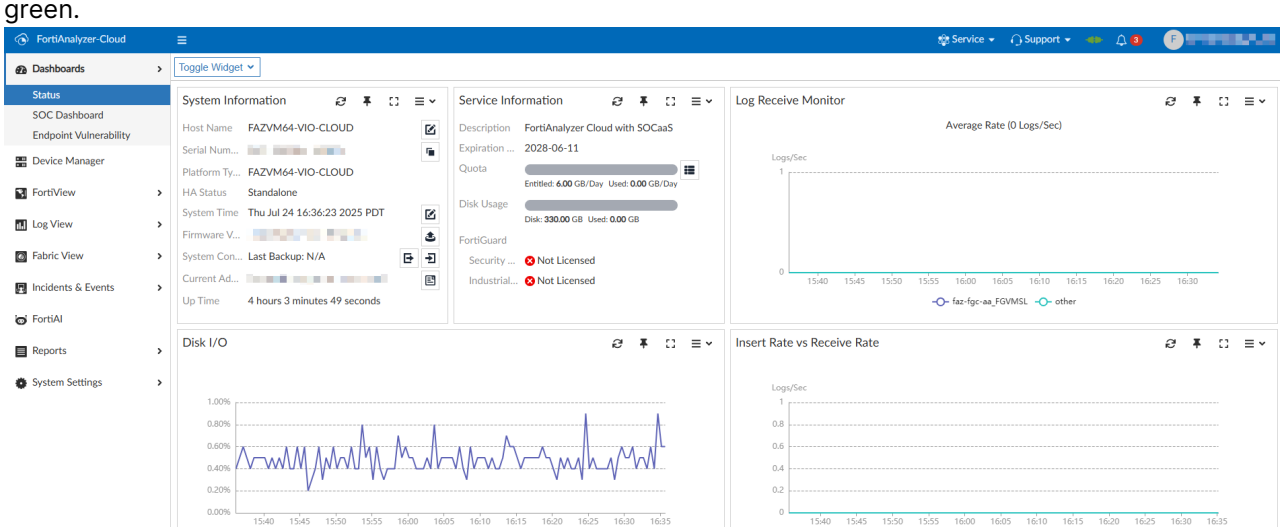
1. Log in to FortiAnalyzer Cloud.
2. Click on the *SOCaaS* connection icon at the top of the GUI. A SOCaaS entitlement is required to enable the service.
   a. Without the correct entitlement, a message is displayed advising you to subscribe your FortiGate devices to the FortiAnalyzer Cloud SOCaaS subscription.



   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.



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



4. 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 28.

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:

`Average Lograte * 200 * seconds in 1 day (86400) * 1.2 = 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 account services

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

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

Adding a secondary account

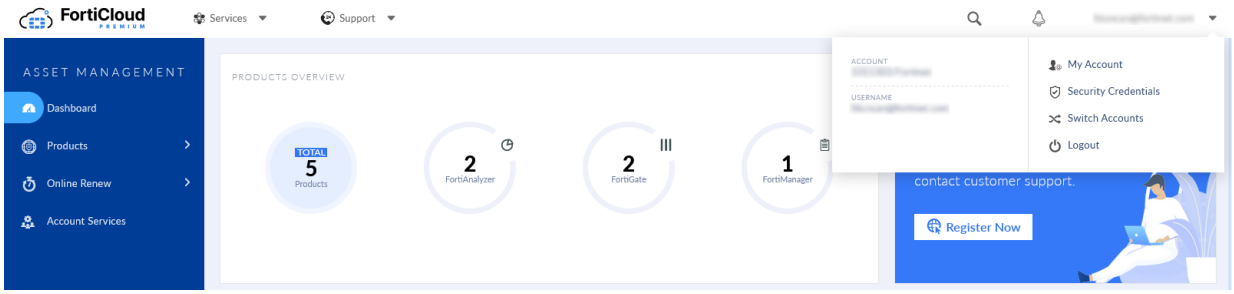
Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. Be default, the secondary account holder is assigned the default administrator profile named *Restricted_User*. However, the primary account holder can modify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

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

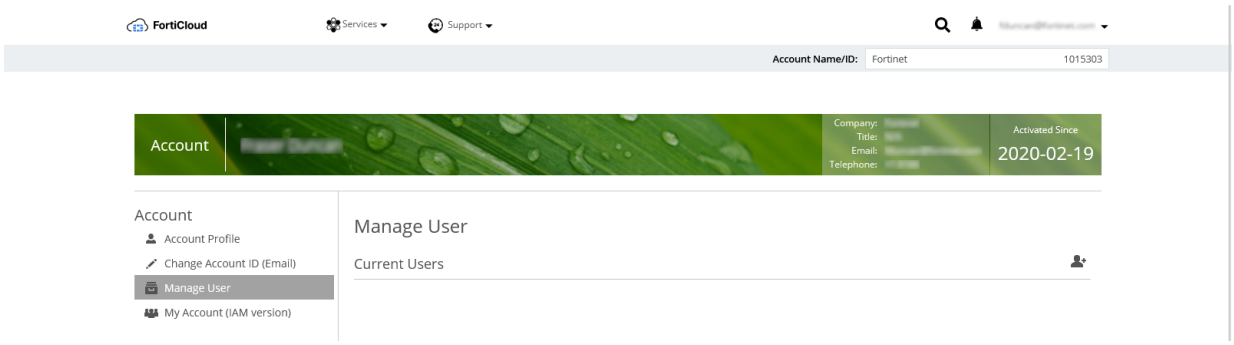
With FortiAnalyzer Cloud 7.0.x and later, you can use the Identity and Access Management (IAM) portal, and you can migrate secondary accounts to the IAM portal. In IAM portal, secondary accounts are called sub users. For information about migrating sub users, see the *Identity & Access Management Guide*.

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*.

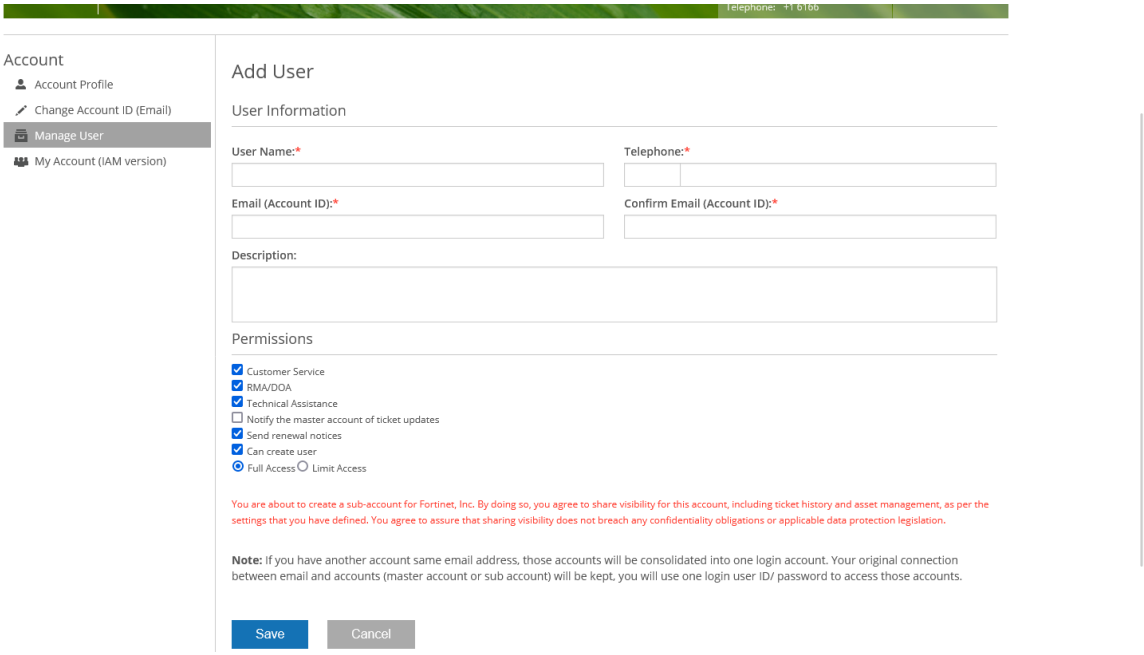


3. Click *Manage User*.
4. Click the new user icon to add a new user.



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.



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 31.

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 29.

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*.

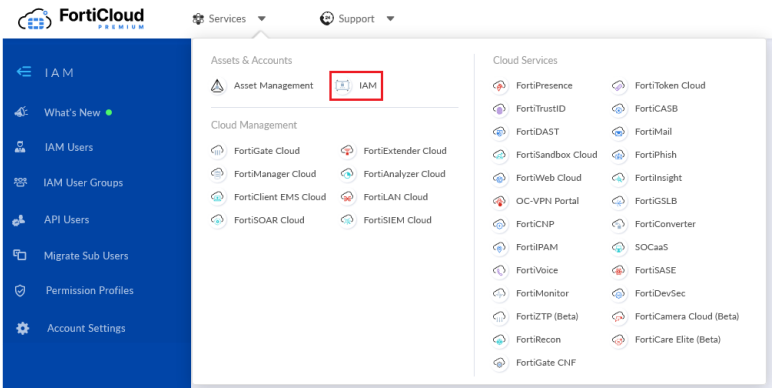
See also Adding IAM users on page 31 and Adding API users on page 34.

Adding IAM users

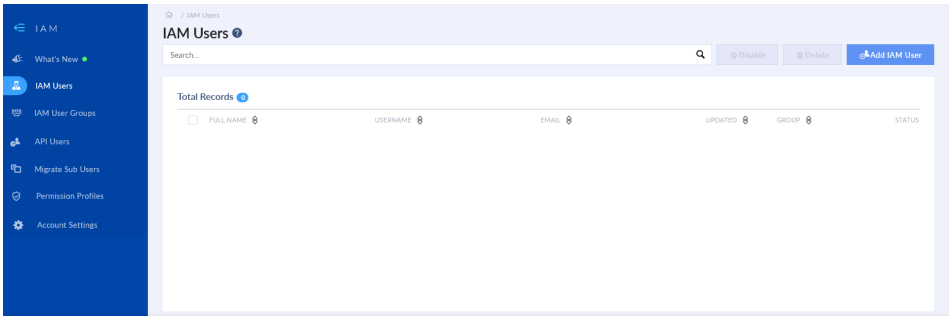
FortiAnalyzer Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiAnalyzer Cloud.

To add an IAM user:

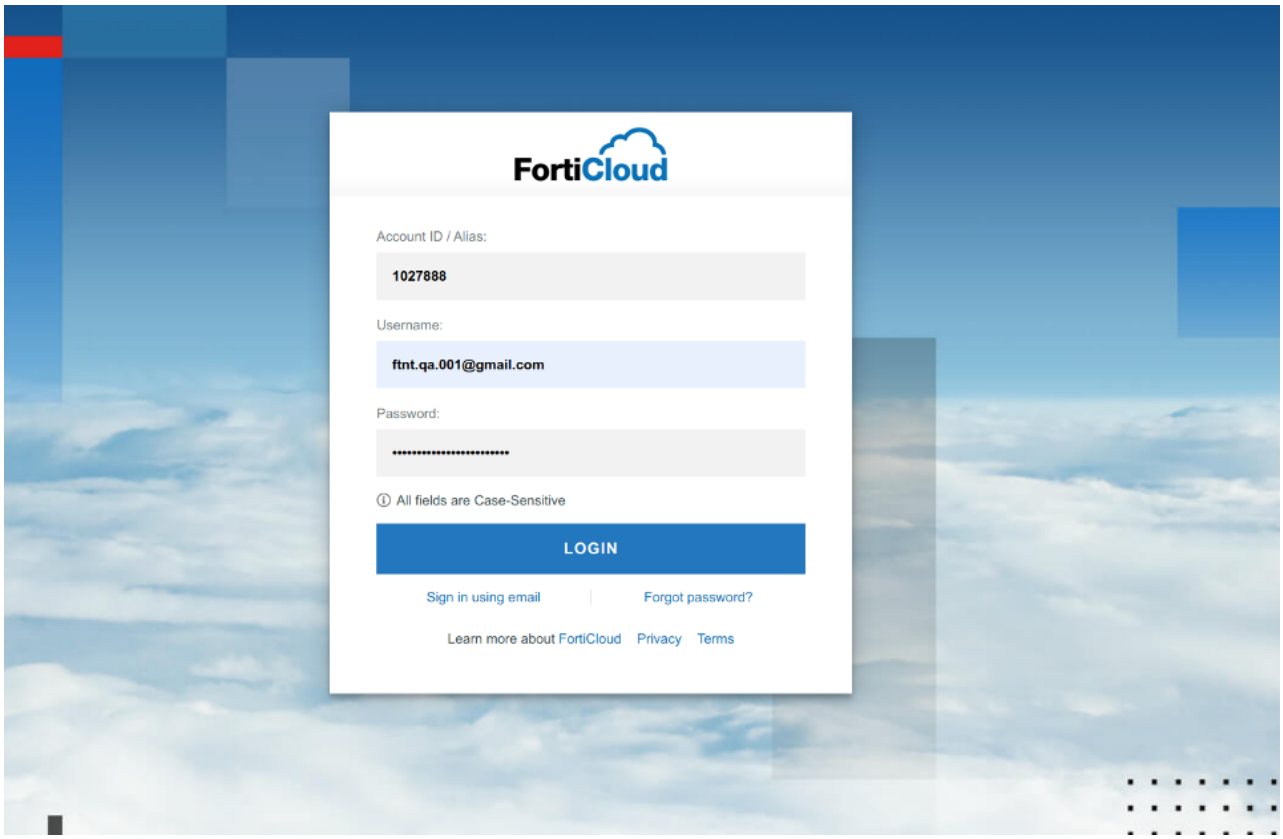
1. Go to FortiCloud (https://support.fortinet.com/), and log in.
2. From the *Services* menu, select *IAM* .



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 *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, 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	`https://<FortiAnalyzer_cloud_url>/p/forticloud_jsonrpc_login/`

Request Body	`{`
	`  "access_token": "<access token obtained in step 2>"`
	`}`

Response example	`{`
	`  "session": "ykF3W6G8CfZv+xecsZBC00n6P0TEbsO*****"`
	`}`

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	`https://<FortiAnalyzer_cloud_url>/jsonrpc`

Request Body	`{`
	`  "method": "get",`
	`  "params": [`
	`  {`
	`  "url": "/sys/status"`
	`  }`
	`  ],`
	`  "id": 1,`
	`  "verbose": 1,`
	`  "session": "ykF3W6G8CfZv+xecsZBC00n6P0TEbsO*****",`
	`}`

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.

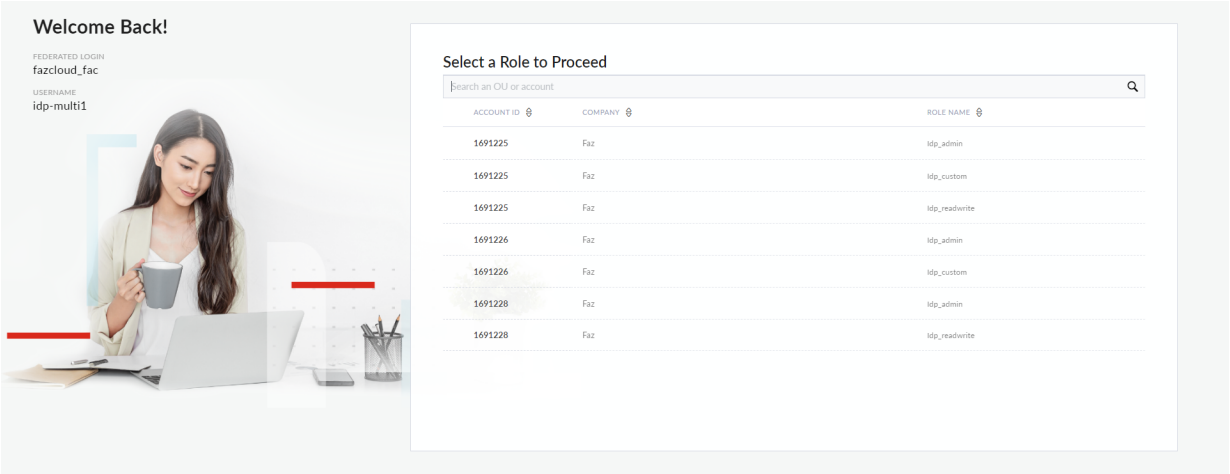
For more information on managing external IdP roles and users for cloud products, see the FortiCloud Identity & Access Management (IAM) user guide.

Using multiple roles with external IdP users

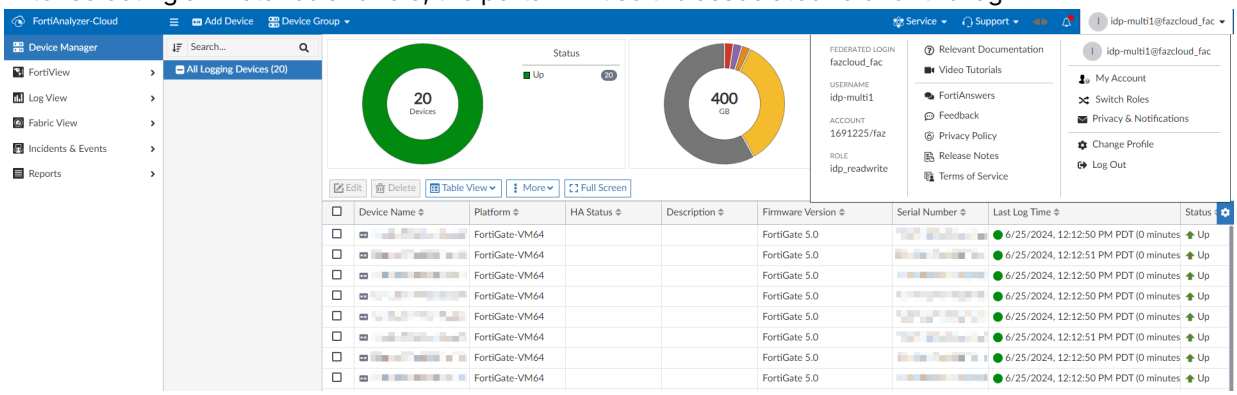
For more information on external IdP users for FortiCloud, see External IdP roles.

Logging in as an external IdP user with multiple roles:

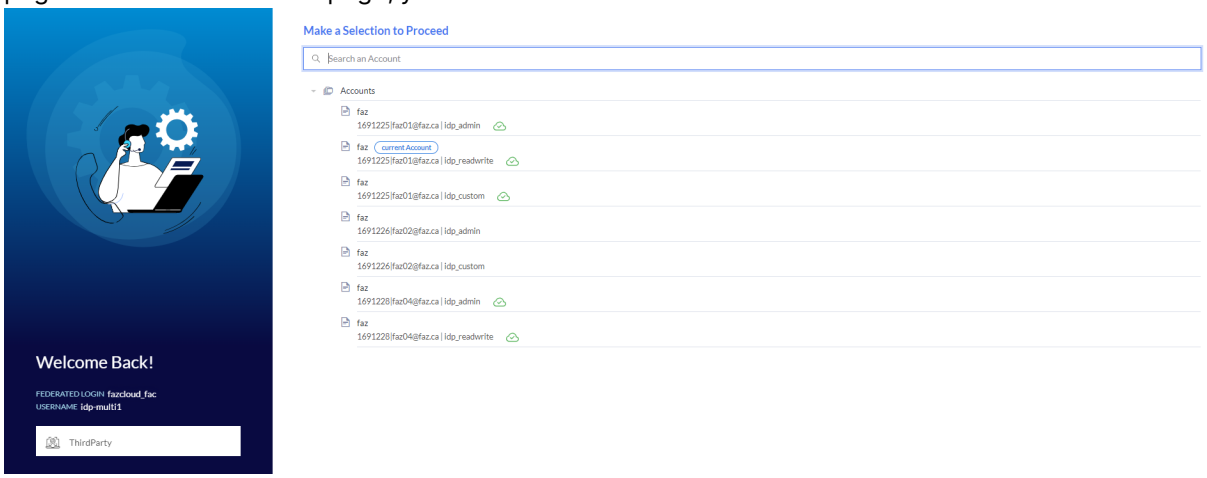
1. When logging in as an IdP user that has multiple roles, the account selection page is displayed allowing users to select which instance to access.
   External IdP users can have multiple roles assigned to a single FortiAnalyzer Cloud instance.



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

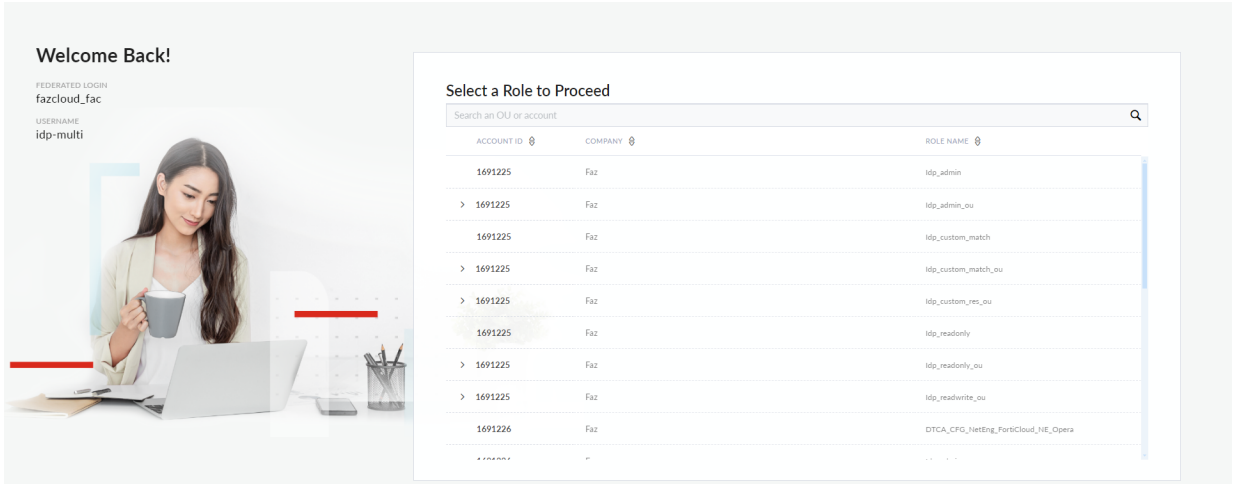


3. Click *Switch Roles* in the FortiAnalyzer Cloud toolbar to return to the FortiAnalyzer Cloud role selection page. On the role selection page, you can select another account and role.

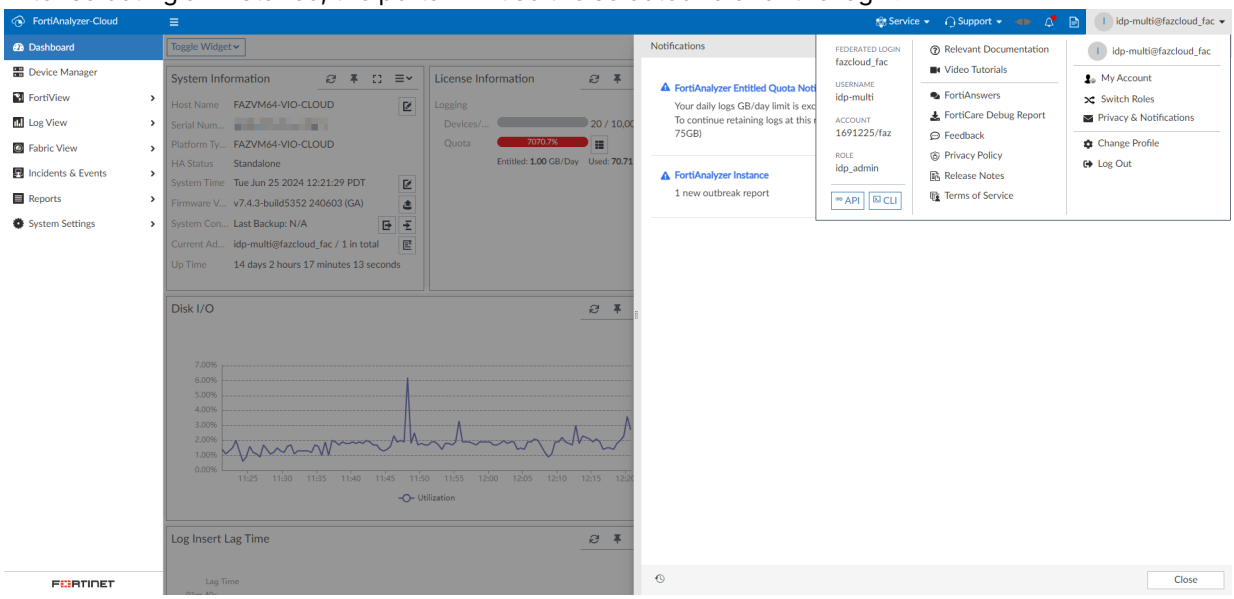


Logging in as an external IdP user with multiple roles in an Organizational Unit:

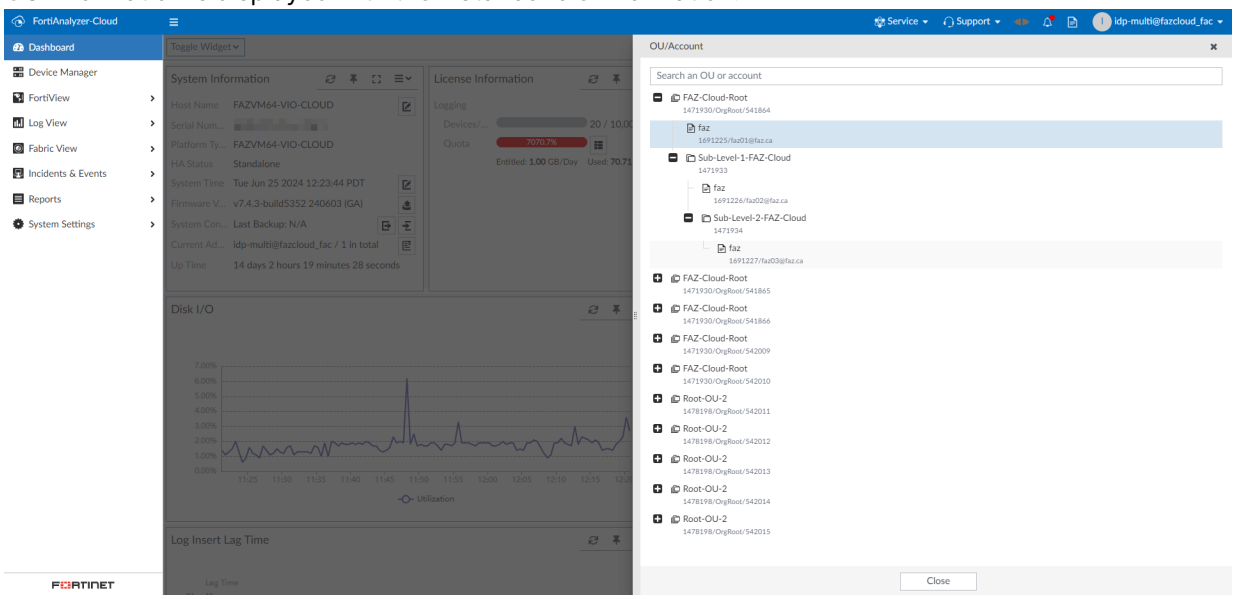
1. When logging in as an external IdP user with multiple roles in an Organizational Unit (OU), the account selection page is displayed allowing you to select an instance, role, and OU.



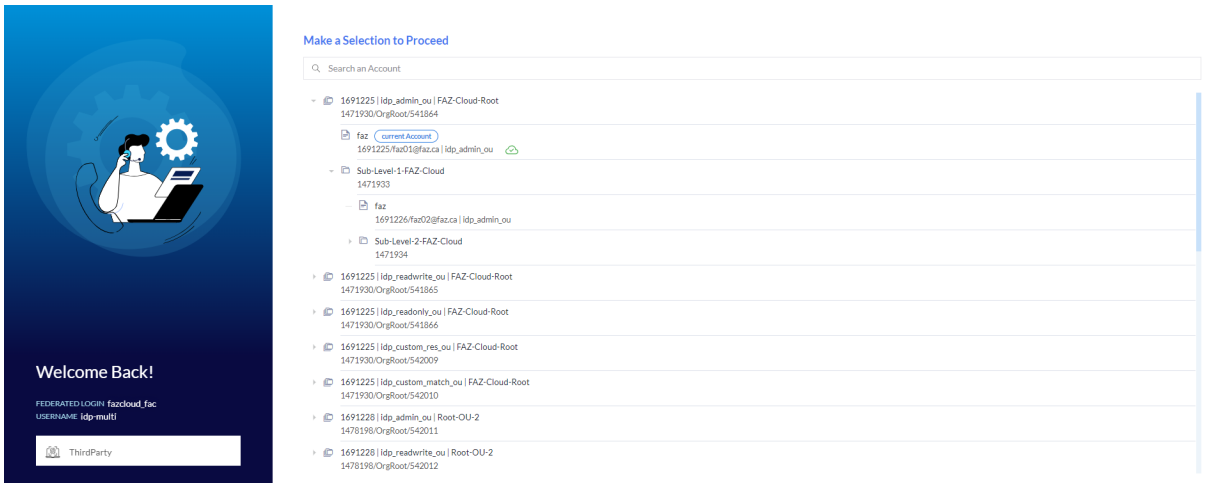
2. After selecting an instance, the portal will use the selected role for the login.



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



4. Click *Switch Roles* 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.


Welcome Back!
FEDERATED LOGIN fazcloud_fac
USERNAME idp-multi
ThirdParty
Make a Selection to Proceed
Search an Account
1691225 | idp_admin_ou | FAZ-Cloud-Root
1471930/OrgRoot/541864
faz
current Account
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

Providing feedback

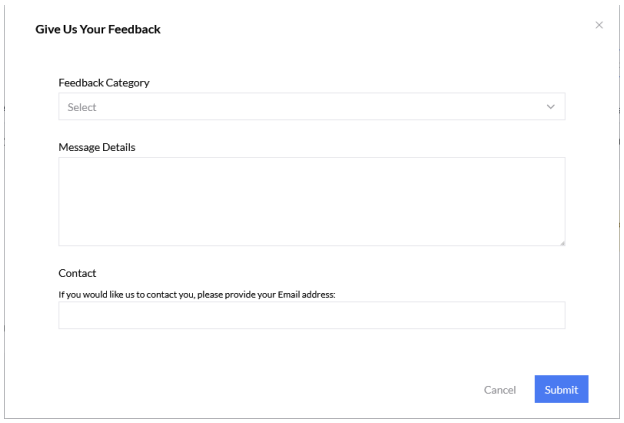
Feedback form

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

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

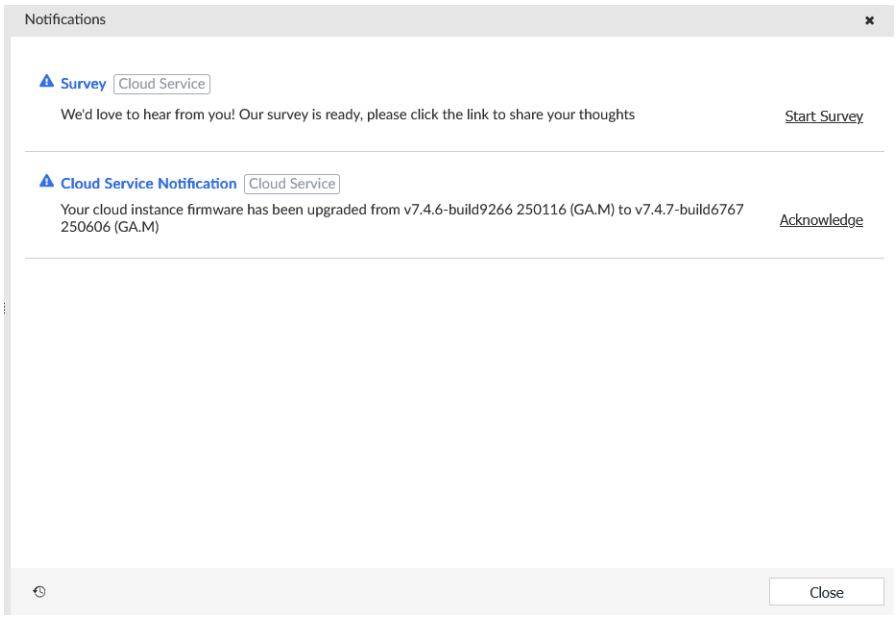
- The footer on the *FortiAnalyzer* Cloud & Service portal.
- The FortiAnalyzer Cloud portal account dropdown inside the FortiAnalyzer Cloud instance. See Using the FortiAnalyzer Cloud toolbar on page 21.

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

www.fortinet.com