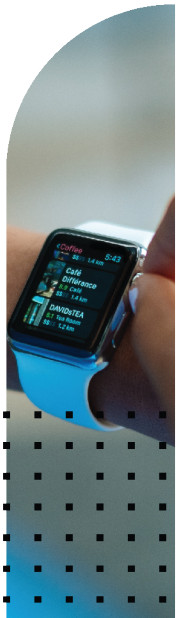
Cloud Deployment Guide

FortiAnalyzer 7.2.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

February 2nd, 2026
FortiAnalyzer 7.2.x Cloud Deployment Guide
05-72x-843405-20260202

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
Access FortiAnalyzer Cloud through FortiCloud 14
Viewing information about instances 16
Upgrading firmware from the portal 17
Using FortiAnalyzer Cloud **19**
Enabling managed SOC service from FortiAnalyzer Cloud 19
Configure log buffer cache size 20
Upgrading firmware from System Settings 21
Using account services **23**
Adding a secondary account 23
Modifying a secondary account 25
Supporting IAM users and IAM API users 25
Adding IAM users 25
Adding API users 27
Supporting external IdP users 28

Change Log

Date	Change Description
2023-03-08	Initial release.
2023-06-28	Updated Using account services on page 23.
2023-12-18	Updated Deploying a FortiAnalyzer Cloud instance on page 8.
2024-04-22	Updated Requirements on page 5.
2024-09-03	Release of FortiAnalyzer Cloud 7.2.7.
2024-10-18	Release of FortiAnalyzer Cloud 7.2.8.
2025-01-31	Release of FortiAnalyzer Cloud 7.2.9.
2025-03-06	Release of FortiAnalyzer Cloud 7.2.10.
2025-04-15	Updated Introduction on page 5.
2025-07-24	Updated Enabling managed SOC service from FortiAnalyzer Cloud on page 19.
2025-08-05	Updated Supporting external IdP users on page 28.
2025-10-01	Release of FortiAnalyzer 7.2.11.
2026-01-02	Updated Adding API users on page 27.
2026-02-02	Release of FortiAnalyzer Cloud 7.2.12.

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.

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 23.

  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 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.

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:
   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 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 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 23.

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

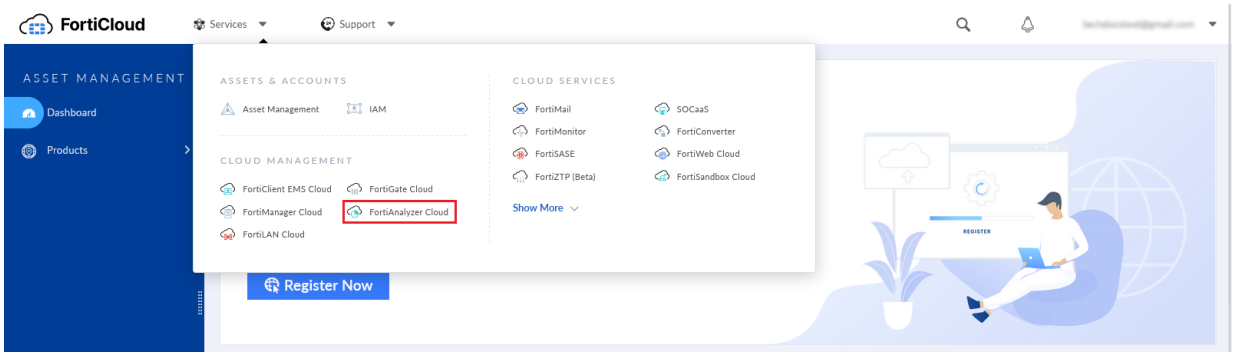
Only one FortiAnalyzer Cloud instance can be created per FortiCloud account.

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.

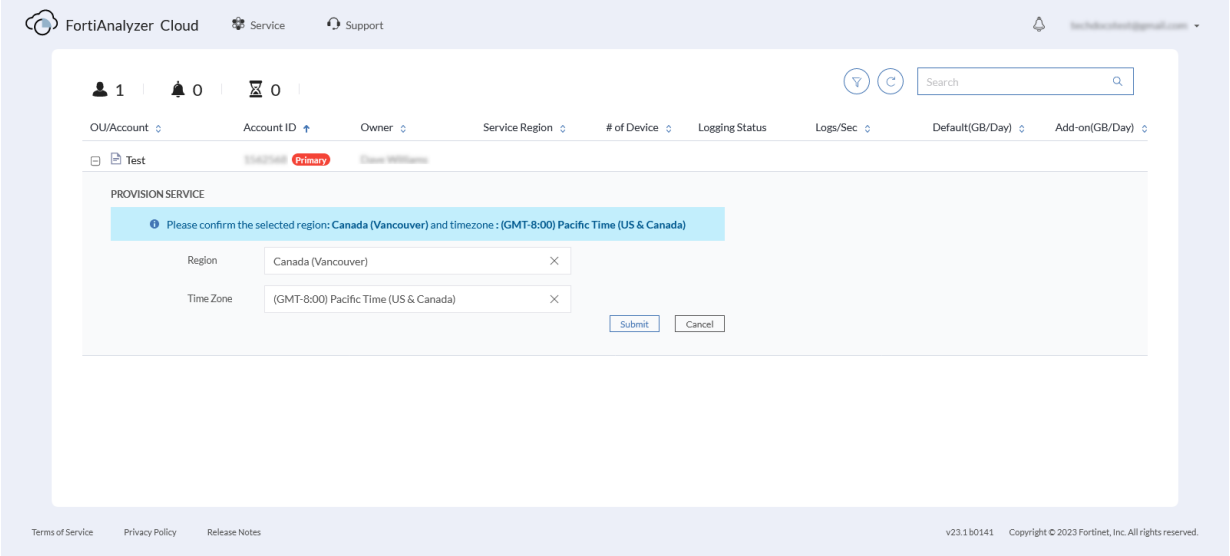
To deploy a FortiAnalyzer Cloud instance:

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*.



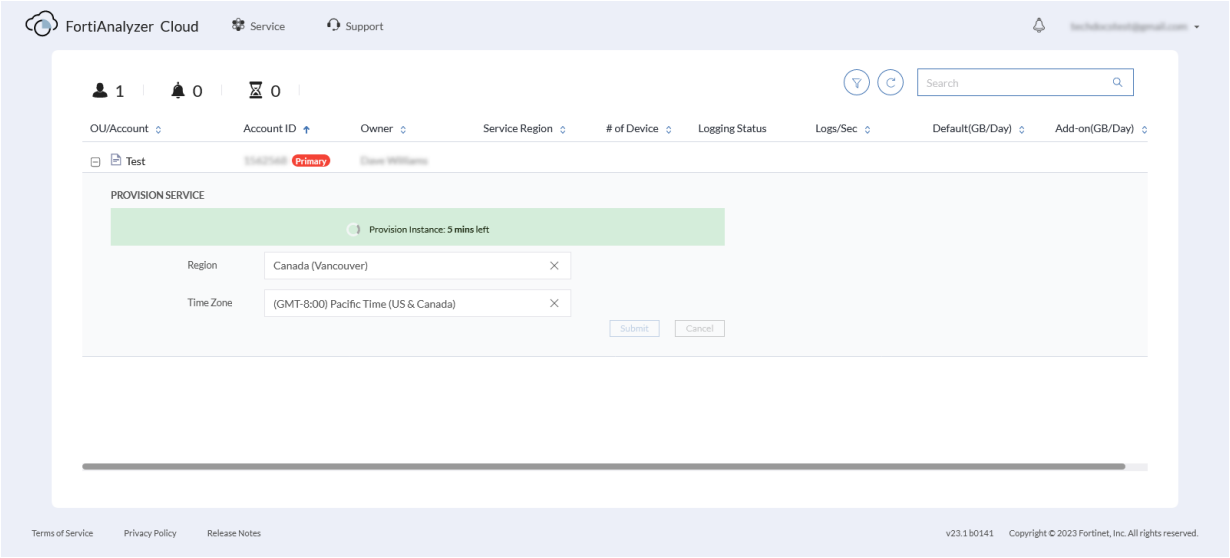
   The *FortiAnalyzer Cloud & Service* portal is displayed.
3. On the *FortiAnalyzer Cloud & Service* portal:
   a. Select a *Region* for the FortiAnalyzer Cloud instance. In this example, the region is *Canada (Vancouver)*.
   b. Select a *Time Zone* for the FortiAnalyzer Cloud instance.

4. Click *Submit*.

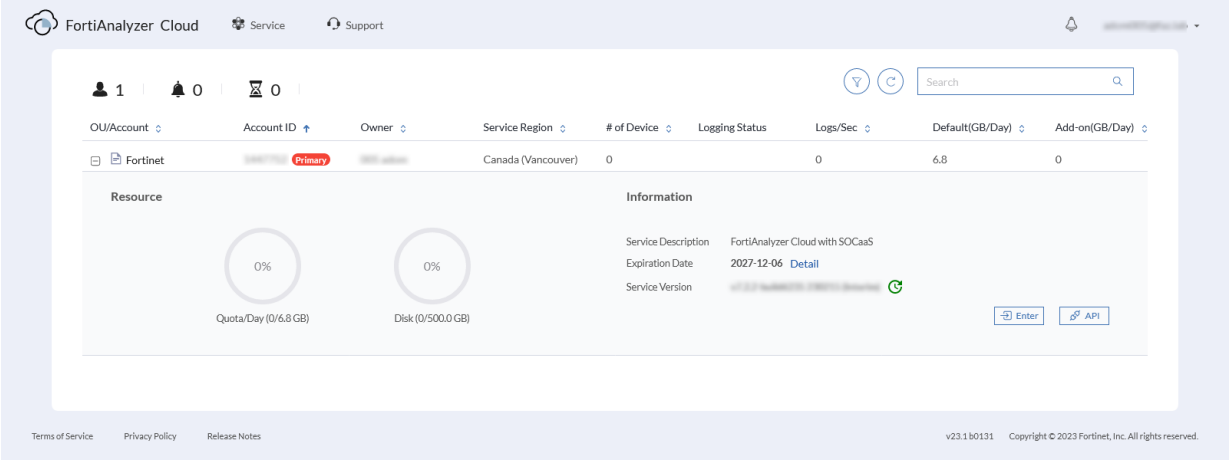


5. A message asking you to confirm your selected region and time zone is displayed.
   a. Click *Confirm* to provision in the FortiAnalyzer Cloud instance.
   b. Click *Cancel* to stop provisioning the instance, and change the region.

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



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



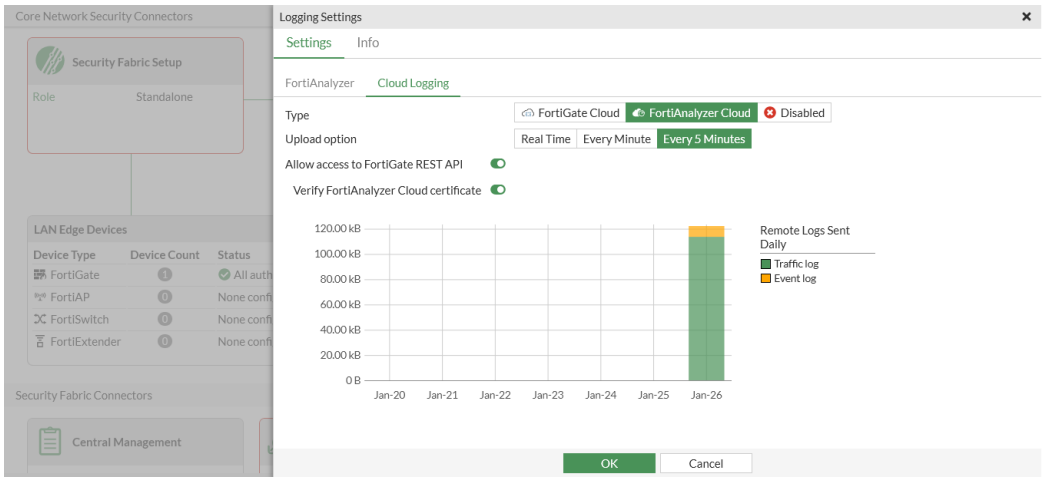
8. (Optional) Upgrade FortiAnalyzer Cloud to 7.2.x. See Upgrading firmware from the portal on page 17.
9. Configure FortiOS to work with FortiAnalyzer Cloud. See Configuring FortiOS on page 10.

Configuring FortiOS

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

To configure FortiOS:

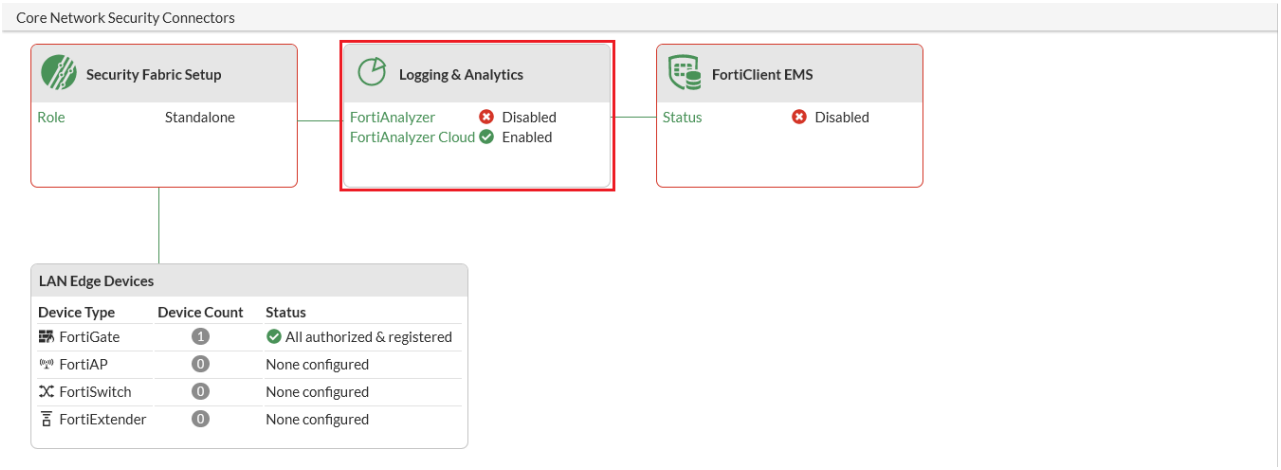
1. In FortiOS, enable FortiAnalyzer Cloud.
   a. Go to *Security Fabric* > *Fabric Connectors*, and edit the *Logging and Analytics* card.
   b. Select the *Cloud Logging* tab, and set the *Type* to FortiAnalyzerCloud.
   c. Configure the remaining settings to your preference, and click *OK*.



2. In the FortiAnalyzer Cloud instance, go to *Device Manager* and authorize the FortiGate.
   In some cases, FortiAnalyzer automatically authorizes the FortiGate, and you can skip this step. For example, FortiAnalyzer can automatically authorize a FortiGate when both devices are part of the same FortiCloud account, and the FortiAnalyzer API can verify the serial number and entitlement for the FortiGate

with FortiCare. FortiAnalyzer cannot automatically authorize a FortiGate in an HA cluster or in a Security Fabric.

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

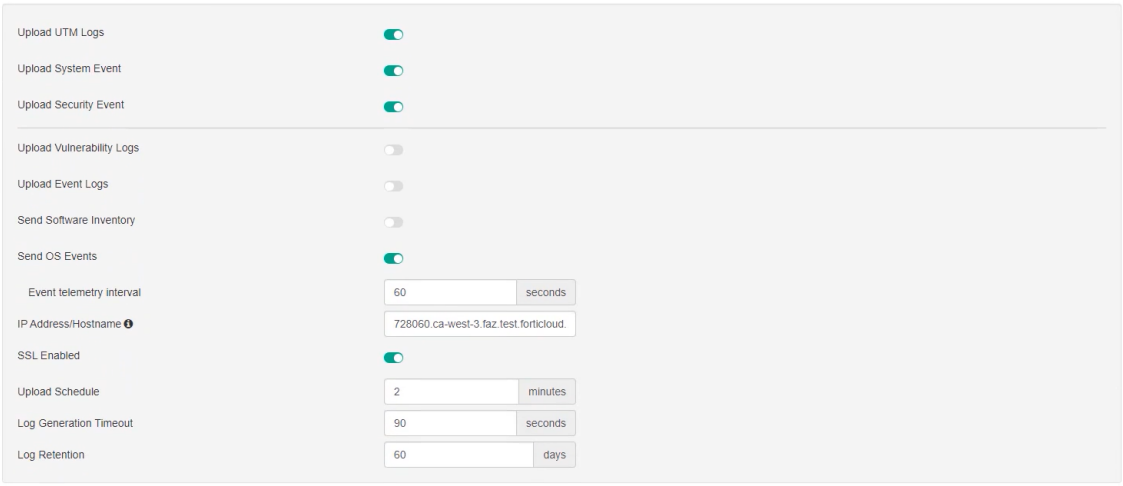


Configuring FortiClient EMS

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

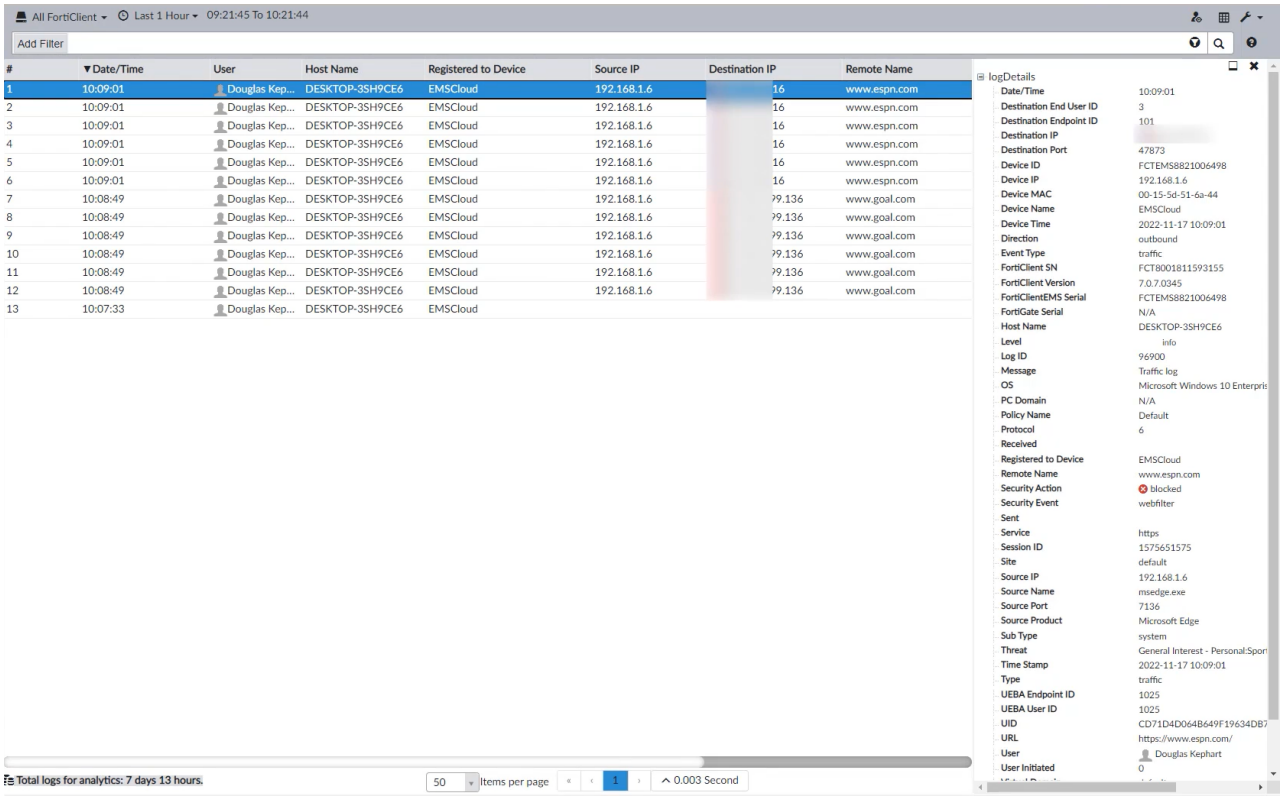
To configure FortiClient EMS:

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



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.

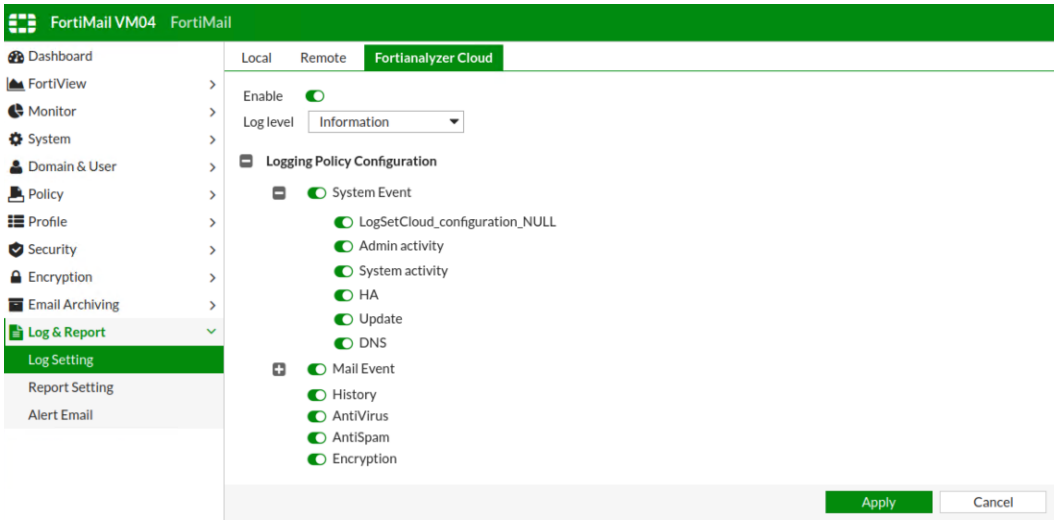


Configuring FortiMail

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

To configure FortiMail:

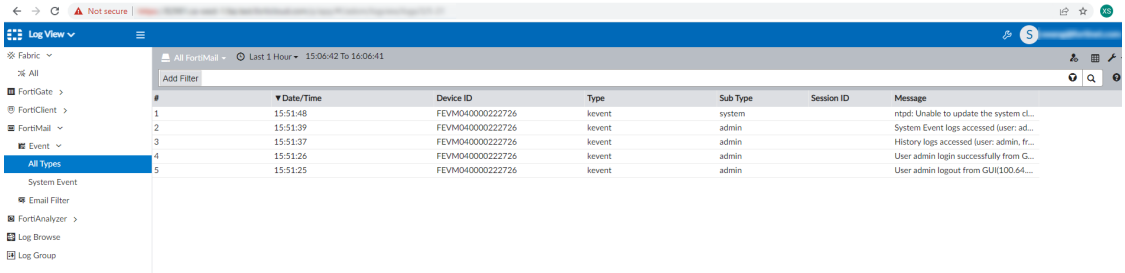
1. In FortiMail, enable logging to FortiAnalyzer Cloud.
   a. Go to *Log & Report* > *Log Setting*.
   b. On the *FortiAnalyzer Cloud* tab, toggle on the *Enable* option, and click *Apply*.
   As long as FortiMail has the correct license registered with FortiCare, a connection is established with FortiAnalyzer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



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

Accessing the portal and instances

After deploying one or more FortiAnalyzer Cloud instances, you can access the instances.

You can access FortiAnalyzer Cloud portal through one of the methods below:

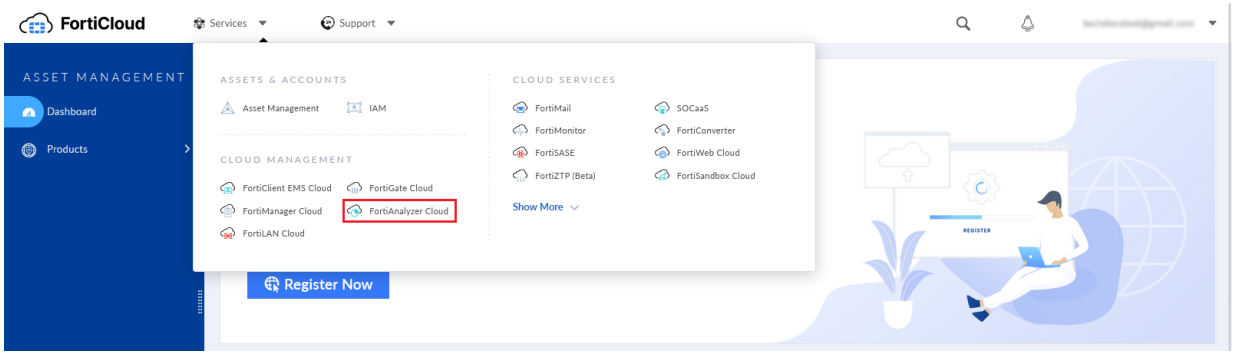
1. Select *FortiAnalyzer Cloud* from the list of available *Services* in the FortiCloud Portal. See Access FortiAnalyzer Cloud through FortiCloud on page 14.
2. Go to https://fortianalyzer.forticloud.com. After authentication, you are redirected to your own FortiAnalyzer Cloud instance.
3. Go directly 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.

Access FortiAnalyzer Cloud through FortiCloud

To access FortiAnalyzer Cloud through FortiCloud:

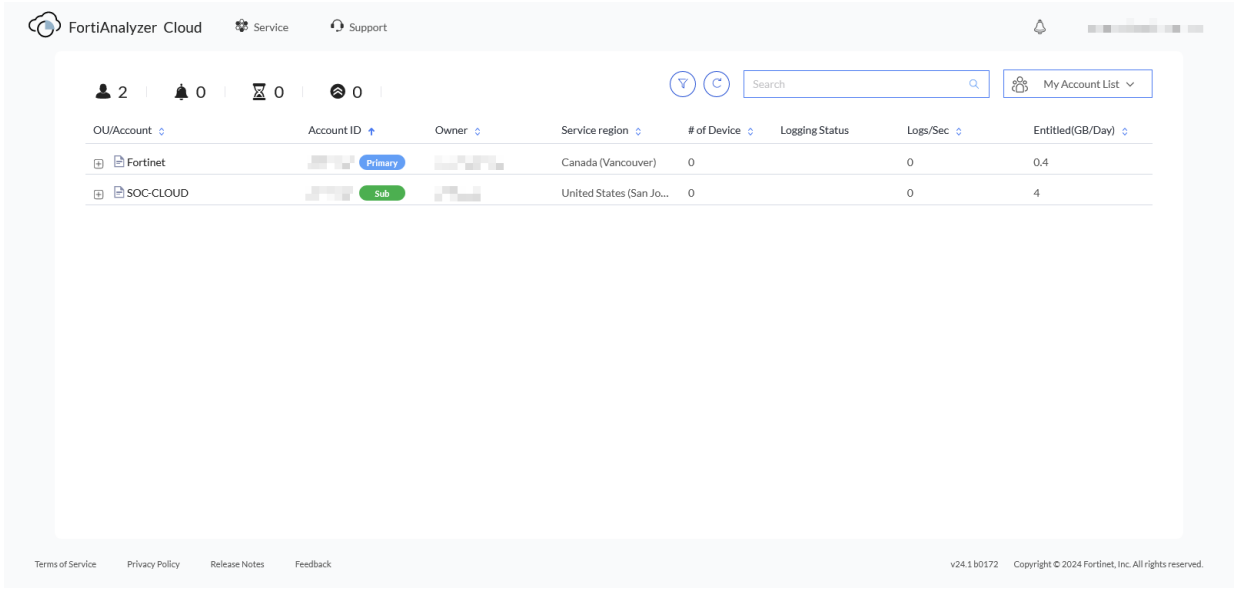
1. Go to FortiCloud (https://support.fortinet.com/), and use your FortiCloud account credentials to log in. The FortiCloud portal is displayed.

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



You are automatically logged in to your FortiAnalyzer instance.

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.



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.

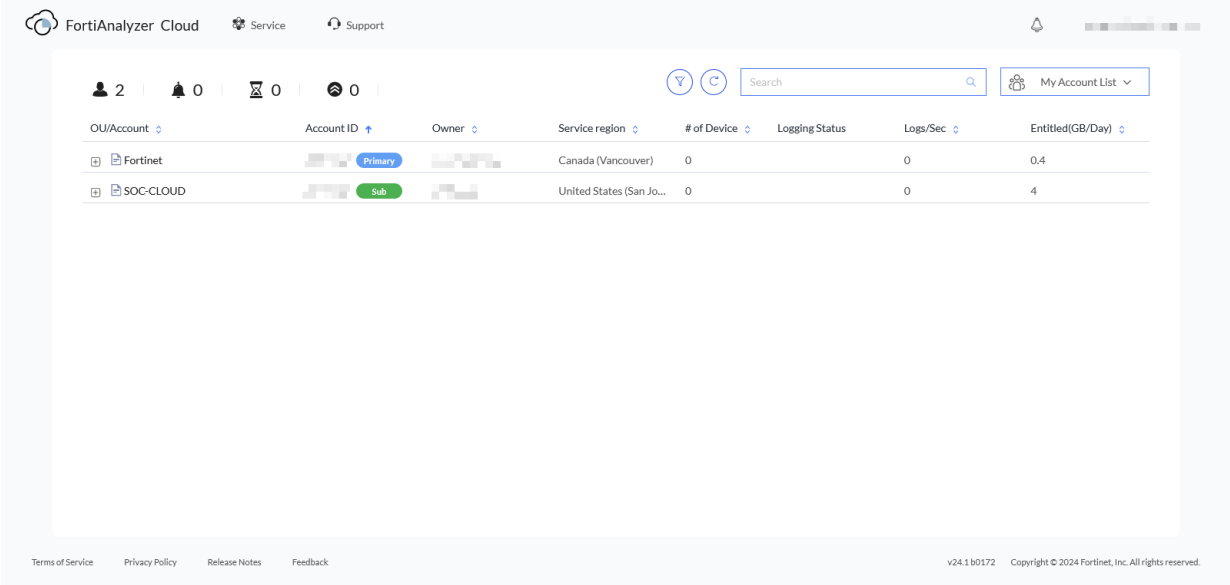
Accounts summary in table view	Each account displays as a row with the following columns: • *OU/Account*: The OU/Account this instance is configured for. • *Account ID*: The account ID. • *Owner*: The name of the owner. • *Service Region*: The region where the instance is deployed. • *# of Device*: The 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

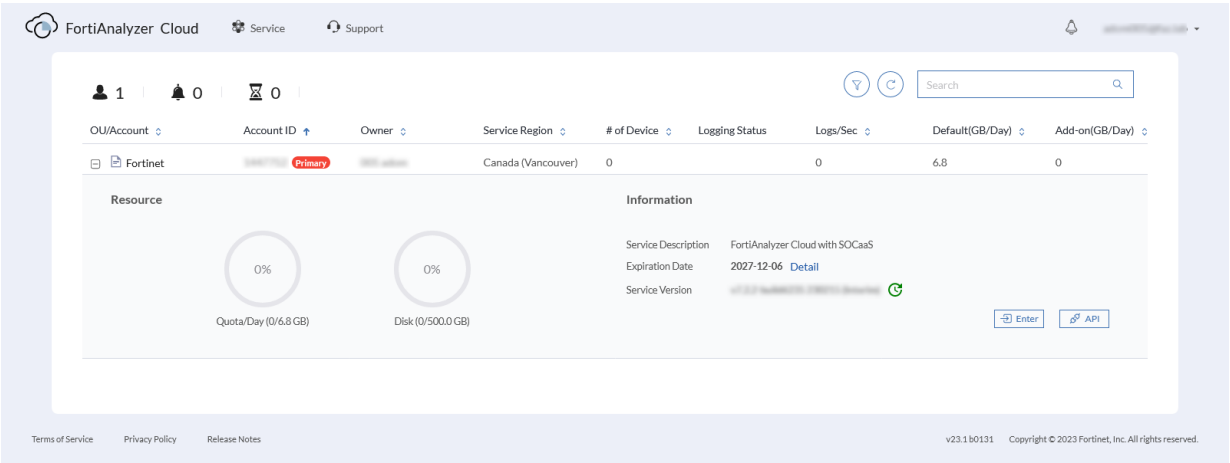
After accessing the FortiAnalyzer Cloud & Service portal, you can expand each account and view information about the account and any deployed instances.

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.



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.



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 System Settings on page 21.

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.

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 System Settings on page 21
- Enabling managed SOC service from FortiAnalyzer Cloud on page 19

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.

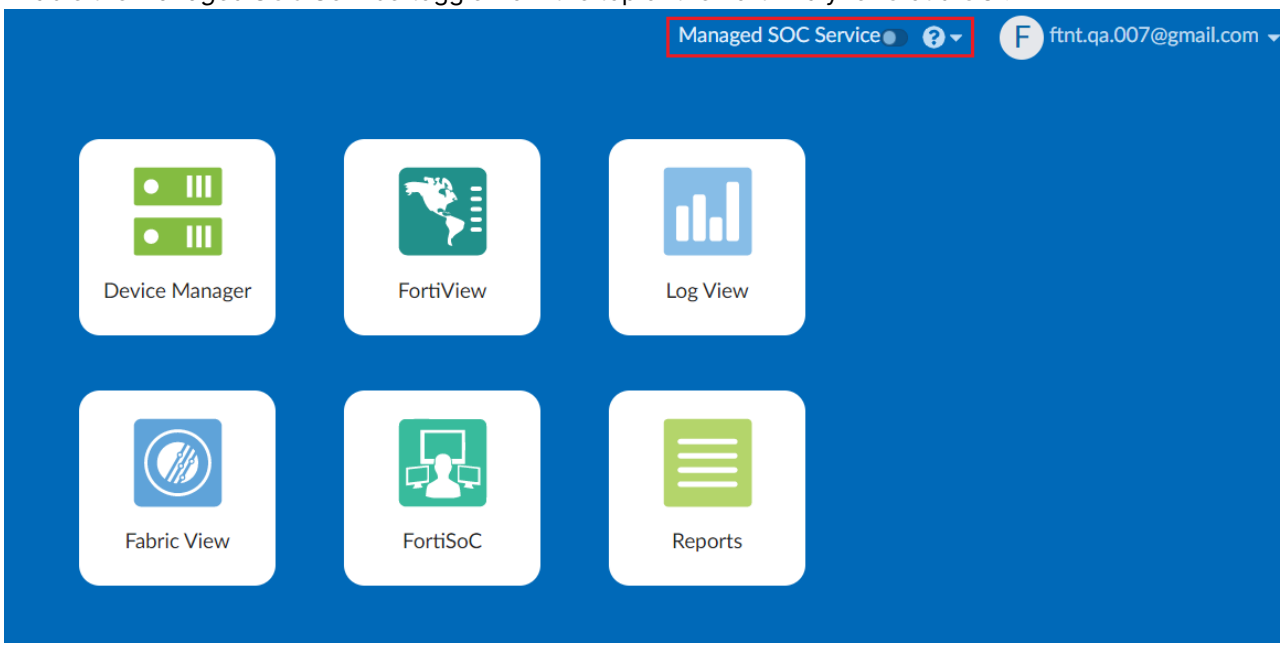
Prerequisites

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

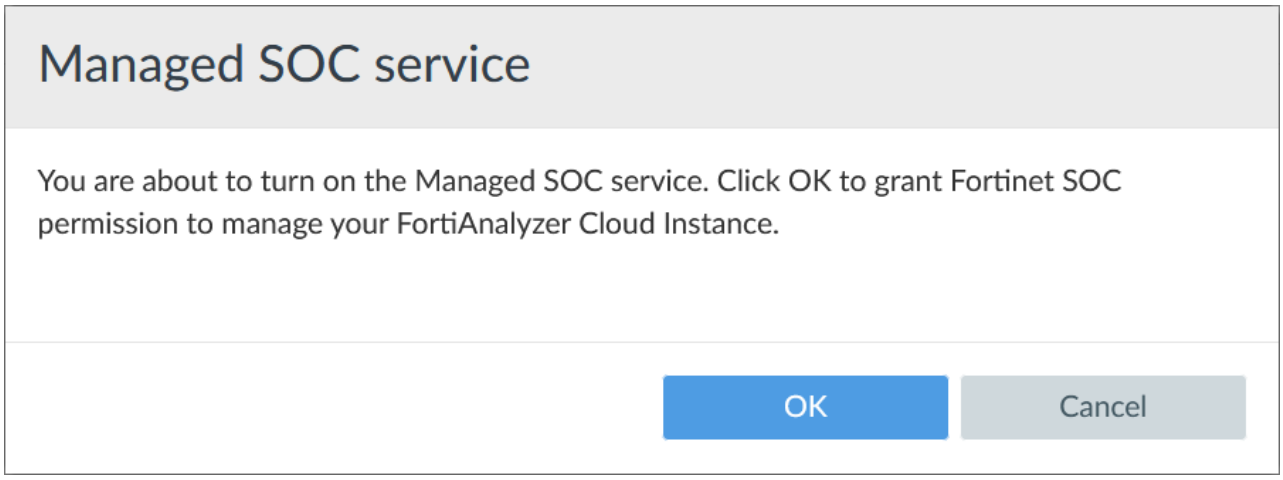
1. You have provisioned the FortiAnalyzer Cloud instance on the region of your choice. See Deploying a FortiAnalyzer Cloud instance on page 8.
2. You have configured the FortiGate to send the entitled device logs to the SOCaaS collection point (FortiAnalyzer Cloud) that will forward the logs. See Configuring FortiOS on page 10.

To configure FortiAnalyzer Cloud:

1. Log in to FortiAnalyzer Cloud.
2. Enable the *Managed SOC Service* toggle from the top of the FortiAnalyzer Cloud GUI.



3. The Managed SOC Service dialog box is displayed. Click *OK*.



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 20.

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 *System Settings* > *Dashboard*.
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.

Upgrading firmware from System Settings

The primary and secondary account holders can upgrade firmware from the *System Settings* 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 System Settings:

1. Access the instance. See Accessing the portal and instances on page 14.
2. In FortiAnalyzer Cloud, go to *System Settings*.
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*.

Using account services

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

- Adding a secondary account on page 23
- Modifying a secondary account on page 25
- Supporting IAM users and IAM API users on page 25

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

Adding a secondary account

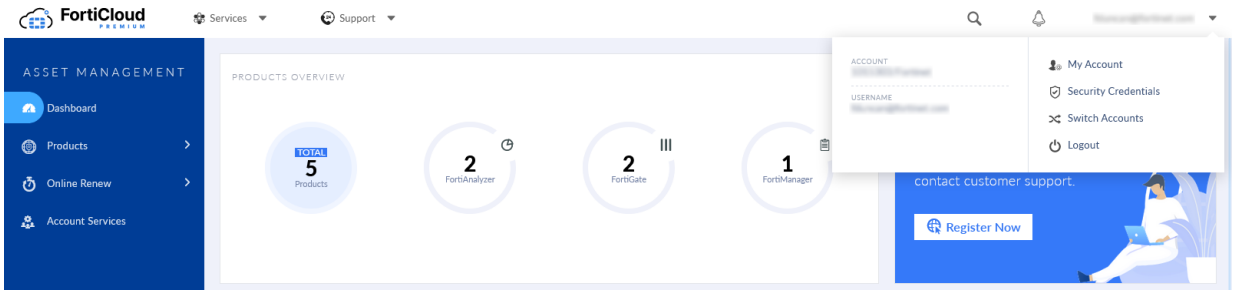
Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. Be default, the secondary account holder is assigned the default administrator profile named *Restricted_User*. However, the primary account holder can modify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

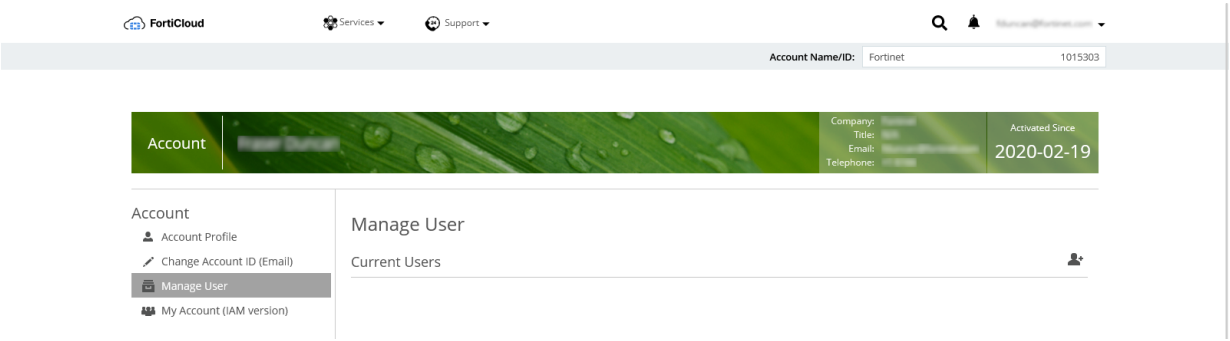
To add a secondary account:

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*.

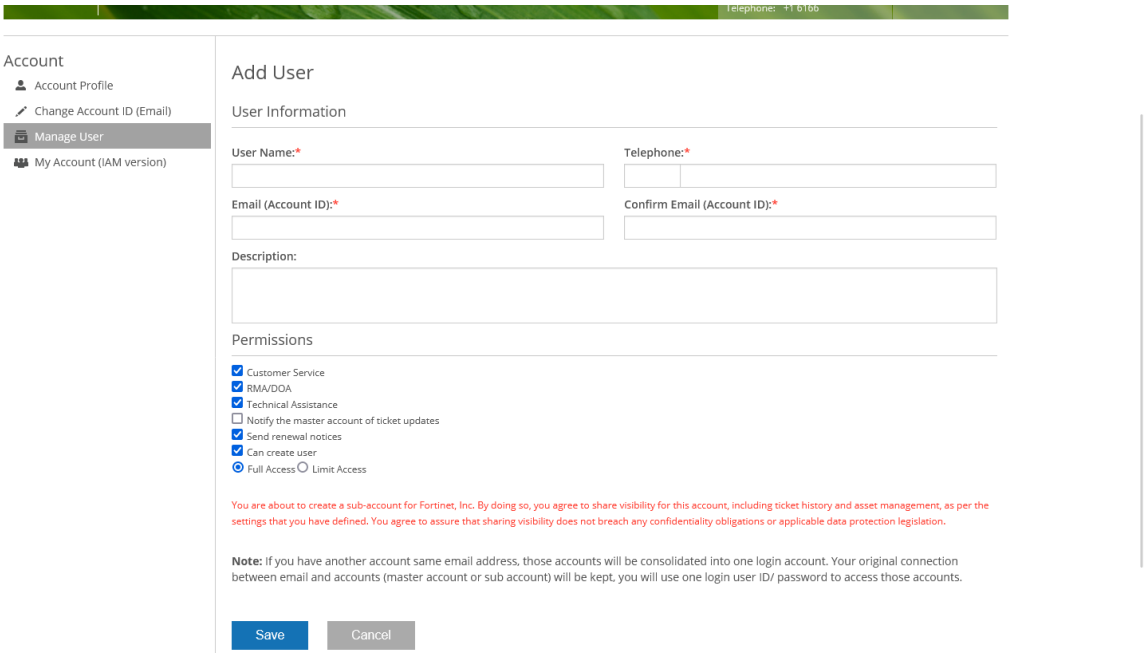


3. Click *Manage User*.

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 25.

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 23.

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*.

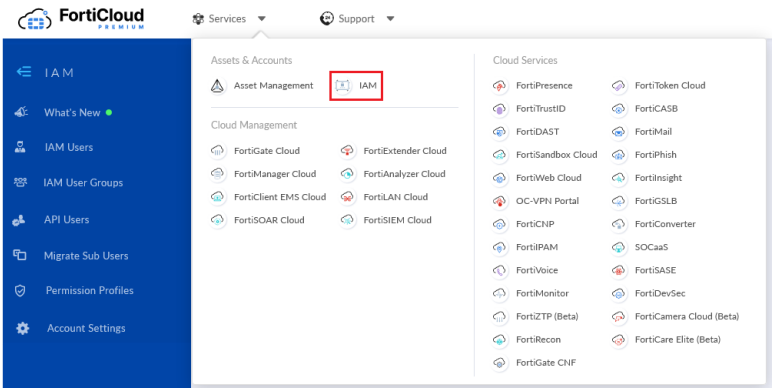
See also Adding IAM users on page 25 and Adding API users on page 27.

Adding IAM users

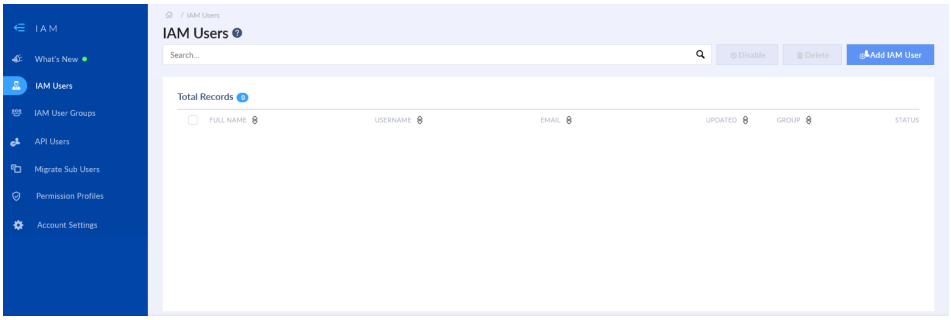
FortiAnalyzer Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiAnalyzer Cloud.

To add an IAM user:

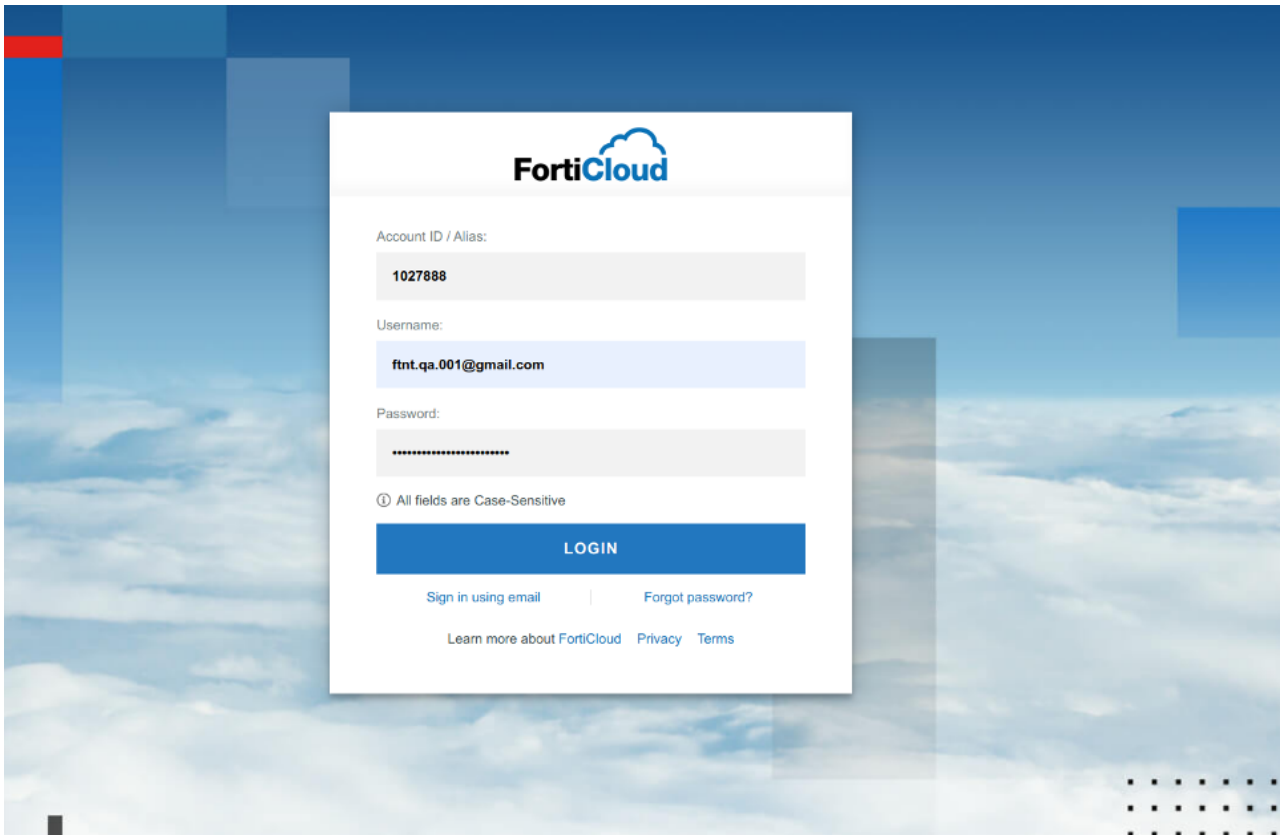
1. Go to FortiCloud (https://support.fortinet.com/), and log in.
2. From the *Services* menu, select *IAM* .



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.

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 users can 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.

www.fortinet.com