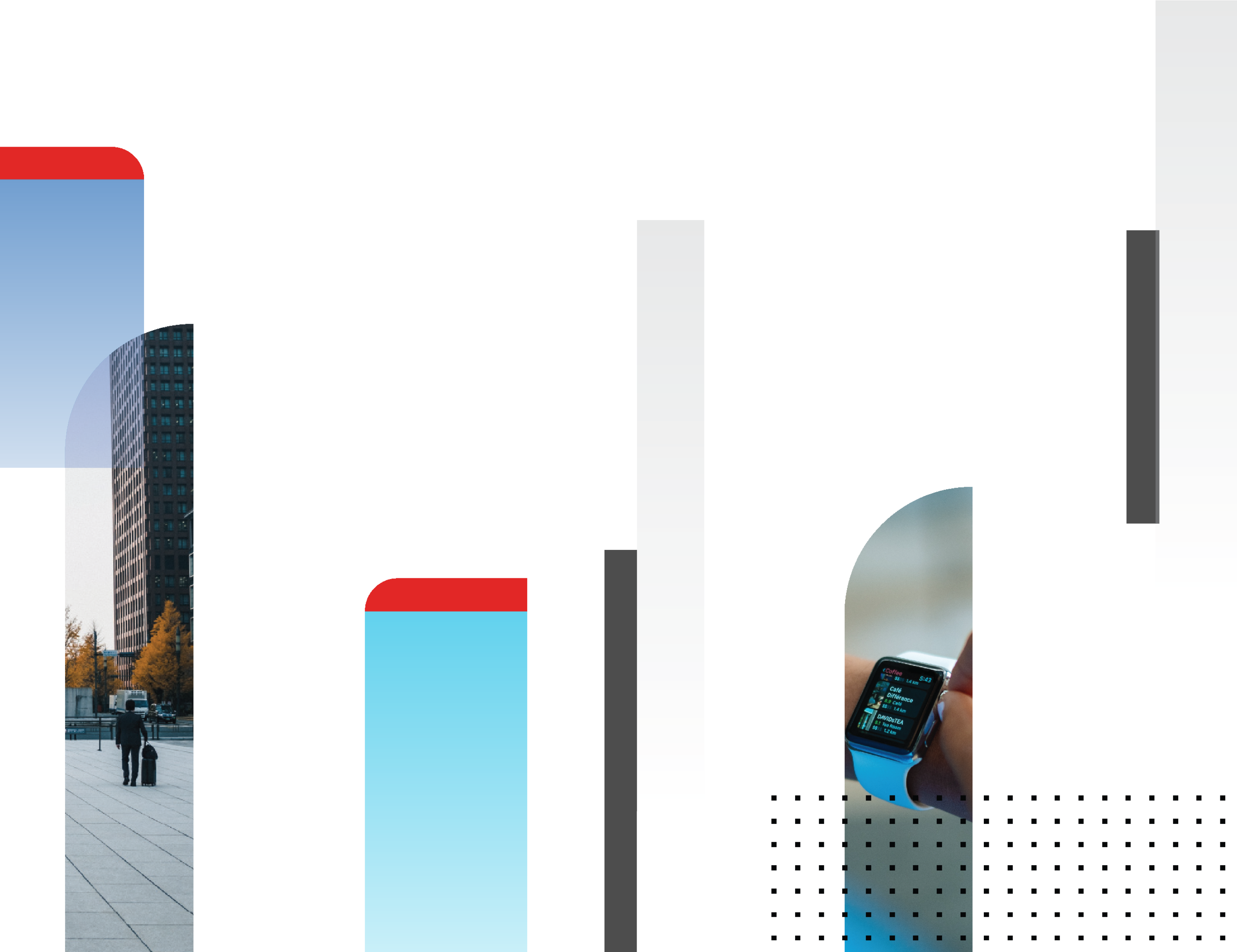
Cloud Deployment Guide

FortiAnalyzer 7.0.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

November 14th, 2025
FortiAnalyzer 7.0.x Cloud Deployment Guide
05-70x-743811-20251114

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-09-09	Initial release.
2021-10-13	Updated to remove mention of 360 Bundle.
2022-01-07	Added Adding IAM users on page 23.
2022-02-25	Added Adding API users on page 25.
2022-03-02	Added support for logging from FortiMail. See Configuring FortiMail on page 11.
2022-08-30	Release of 7.0.4 r1 and updated Requirements on page 5 and Licensing on page 6.
2023-12-18	Updated Checking requirements and licenses on page 7.
2024-04-22	Updated Requirements on page 5.
2025-07-03	Initial release of FortiAnalyzer Cloud 7.0.14.
2025-11-14	Initial release of FortiAnalyzer Cloud 7.0.15.

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 6.4.4 and later can receive Traffic, UTM, and other logs from FortiGates running firmware version 6.4.1 or later.

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 21.

  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

Form Factor	FortiGate Model	Total daily log limit for FortiAnalyzer-VM v6.4 and later
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. On FortiCloud, check requirements and licenses. 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.

   By default, FortiAnalyzer Cloud version 7.0.x is deployed. You can upgrade to later versions. See Upgrading firmware from the portal on page 17.
3. On FortiOS or FortiMail, enable logging to FortiAnalyzer Cloud:
   - For FortiOS, see Configuring FortiOS on page 10.
   - For FortiMail, see Configuring FortiMail on page 11.

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 21.

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

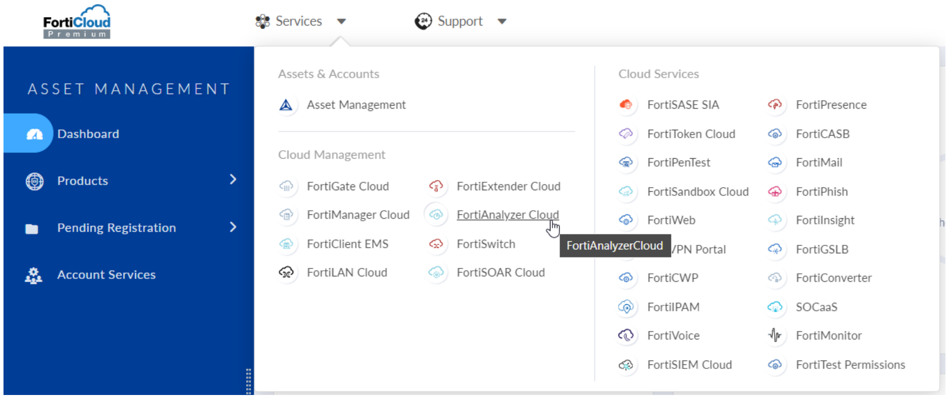
Only one FortiAnalyzer Cloud instance can be created per FortiCloud account.

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

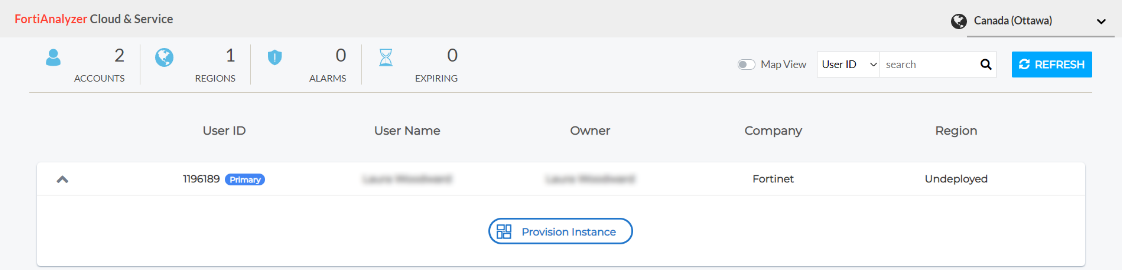
Check the latest FortiAnalyzer Cloud Deployment Guide to see the current FortiAnalyzer Cloud versions available for deployment.

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*.

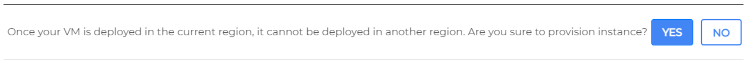


   The *FortiAnalyzer Cloud & Service* portal is displayed.
3. On the *FortiAnalyzer Cloud & Service* portal, select a region for the FortiAnalyzer Cloud instance from the top-right corner.
   In the examples in this section, the *Canada (Vancouver)* region is selected.
4. Expand the primary account that includes the FortiAnalyzer Cloud entitlement, and click *Provision Instance*.
   The User ID on *FortiAnalyzer Cloud & Service* portal represents the dedicated instance.



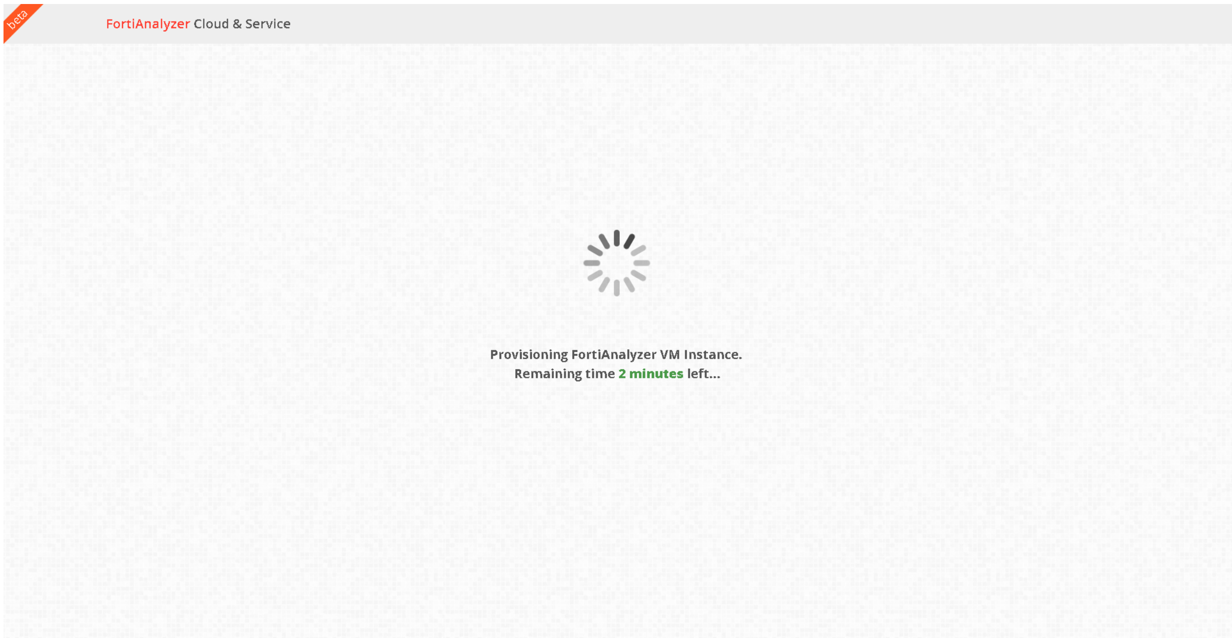
User ID	User Name	Owner	Company	Region
1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed

A message about the selected region is displayed.



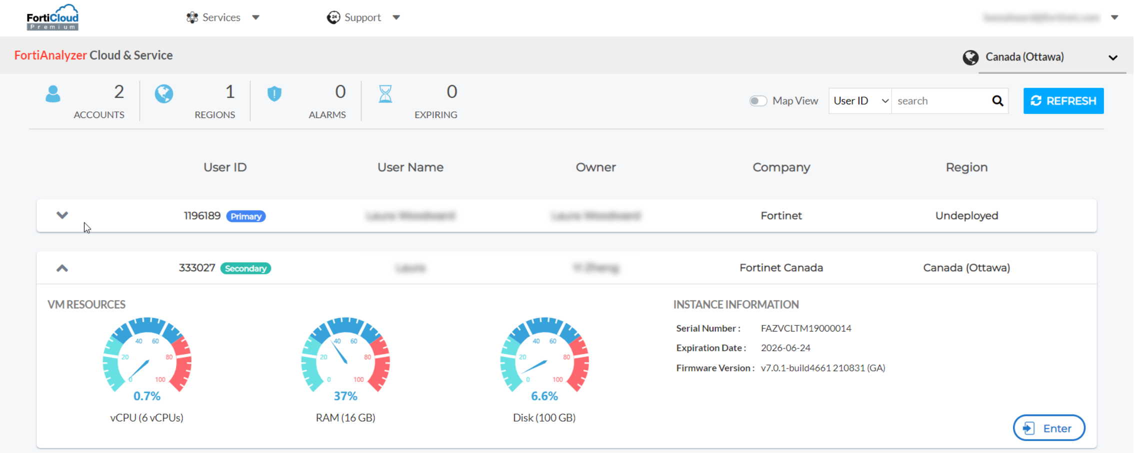
Once your VM is deployed in the current region, it cannot be deployed in another region. Are you sure to provision instance?

5. Click *Yes* to provision in the FortiAnalyzer Cloud instance in the selected region.
   Click *No* to stop provisioning the instance, and change the region.
   FortiAnalyzer Cloud instance is provisioned in a few minutes.



Provisioning FortiAnalyzer VM Instance.
Remaining time 2 minutes left...

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



User ID	User Name	Owner	Company	Region
1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed
333027 Secondary	[redacted]	[redacted]	Fortinet Canada	Canada (Ottawa)

INSTANCE INFORMATION

Serial Number : FAZVCLTM19000014
Expiration Date : 2026-06-24
Firmware Version : v7.0.1-build4661 210831 (GA)

7. (Optional) Upgrade FortiAnalyzer Cloud to 7.0.x. See Upgrading firmware from the portal on page 17.

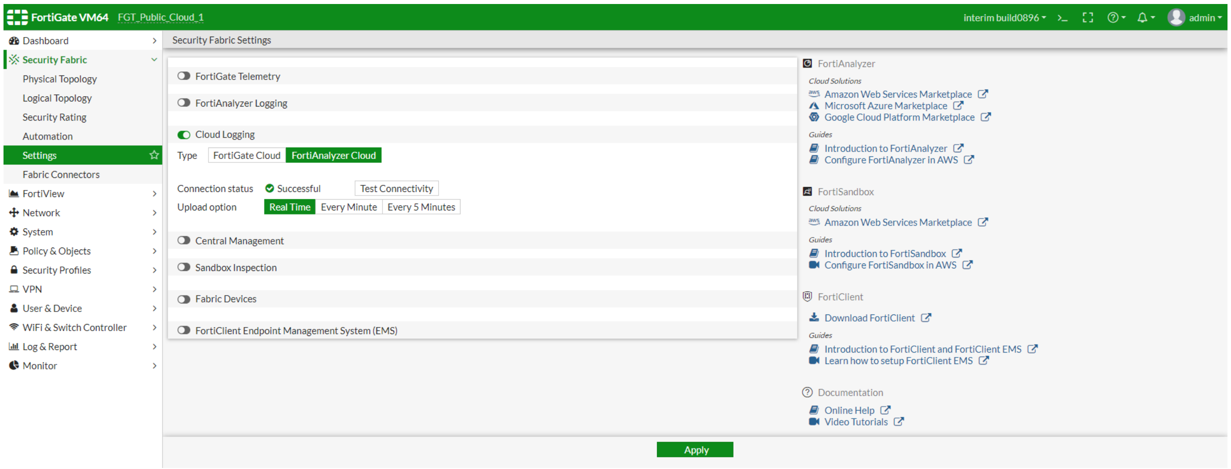
8. Configure FortiOS to work with FortiAnalyzer Cloud. See Configuring FortiOS on page 10.

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 > Settings*, and enable *Cloud Logging*.
   b. Click FortiAnalyzer Cloud, and then *Apply*.
   The *FortiAnalyzer Cloud* button is only available when you have a FortiAnalyzer Cloud product entitlement; the *FortiAnalyzer Cloud* button is not available without a FortiAnalyzer Cloud product entitlement.



Security Fabric Settings

○ FortiGate Telemetry

○ FortiAnalyzer Logging

● Cloud Logging

Type: FortiGate Cloud [✓ FortiAnalyzer Cloud]

Connection status: ✓ Successful

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

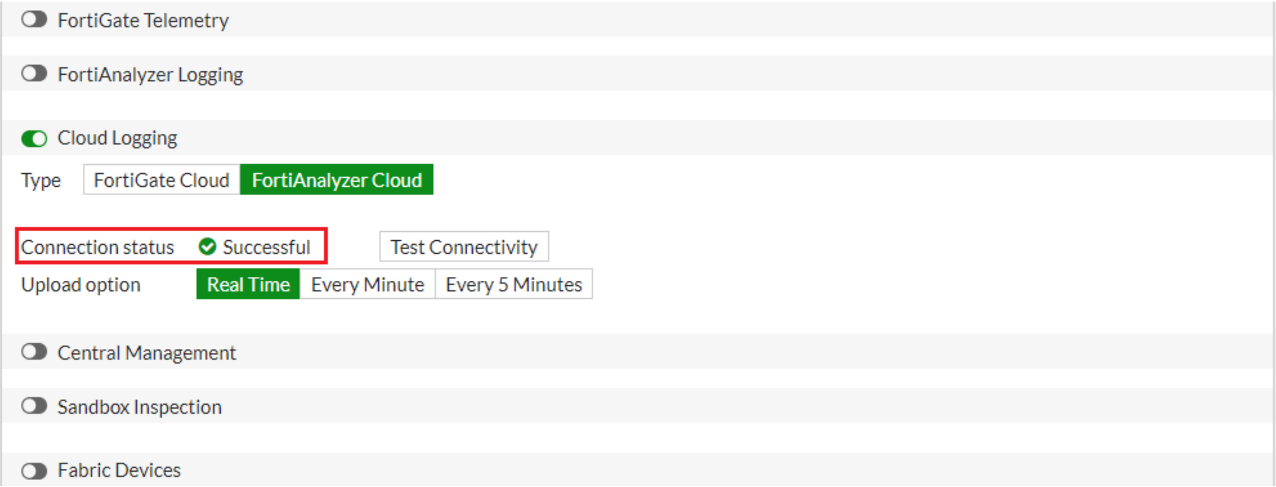
○ Central Management

○ Sandbox Inspection

○ Fabric Devices

○ FortiClient Endpoint Management System (EMS)

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 using FortiGate to enable FortiAnalyzer Cloud, the FortiGate device appears as an unauthorized device.
   When successfully authorized, the cloud logging status displays as *Successful*.



FortiGate Telemetry

FortiAnalyzer Logging

Cloud Logging

Type: FortiGate Cloud | **FortiAnalyzer Cloud**

Connection status ✓ Successful

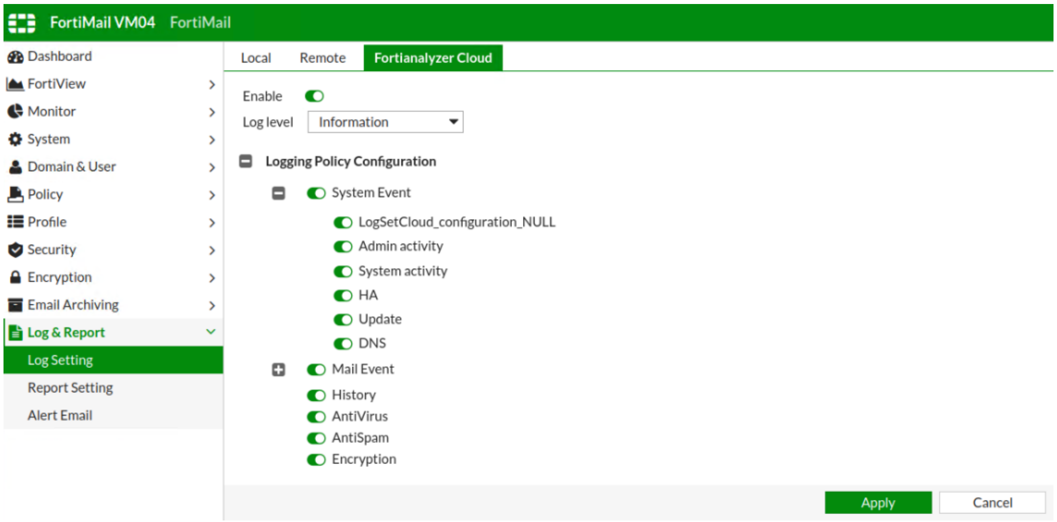
Upload option: **Real Time** | Every Minute | Every 5 Minutes

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.

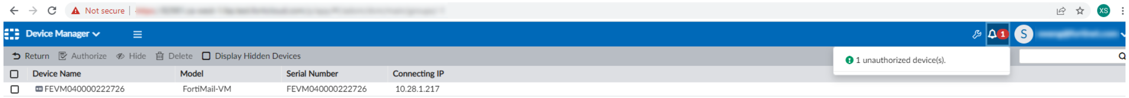


Enable: on

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.

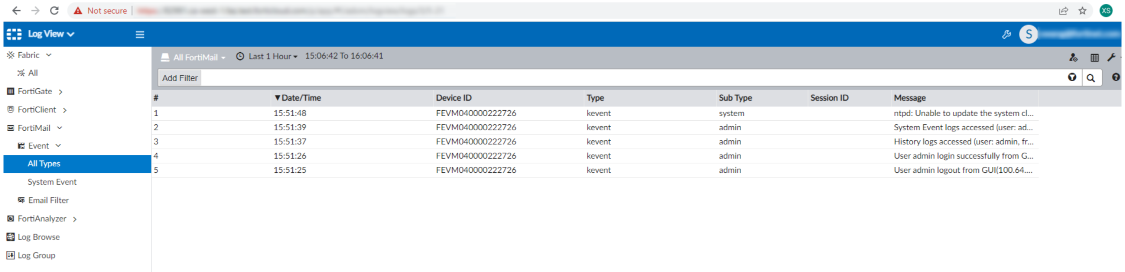


1 unauthorized device(s).

□	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 13
- Using Map View on page 15
- 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:

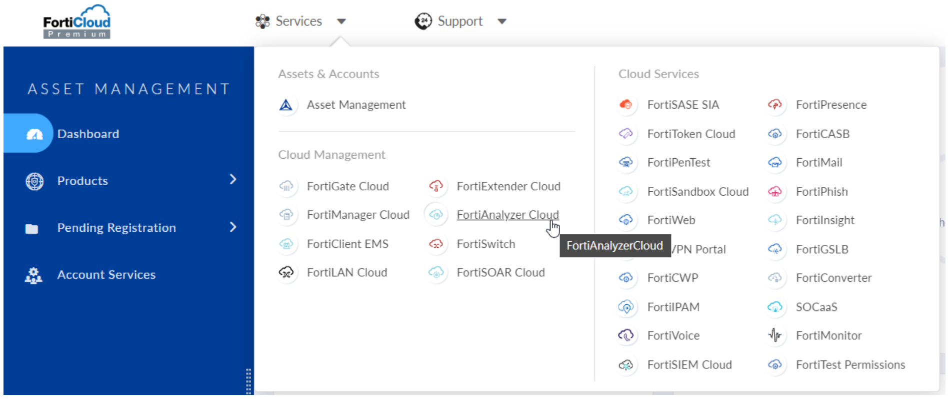
1. Select *FortiAnalyzer Cloud* from the list of available *Services* in the FortiCloud Portal. See Access FortiAnalyzer Cloud through FortiCloud on page 13.
2. Go to https://fortianalyzer.forticloud.com. After authentication, you are redirected to your own FortiAnalyzer Cloud instance.
3. Go directly 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:

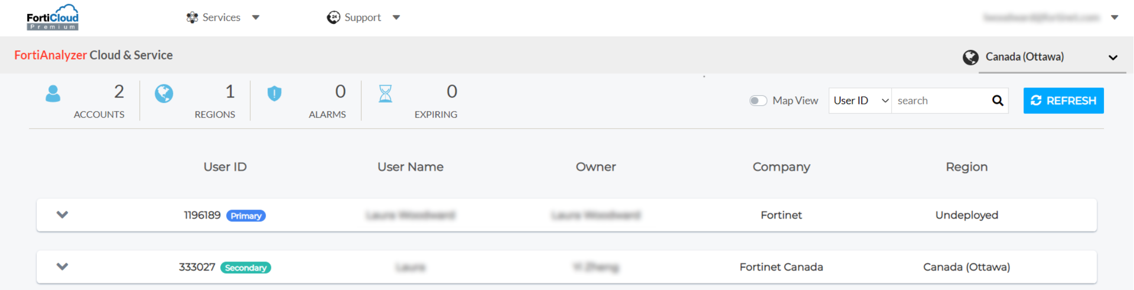
1. Go to FortiCloud (https://support.fortinet.com/), and use your FortiCloud account credentials to log in.
   The FortiCloud portal is displayed.

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.



User ID	User Name	Owner	Company	Region
1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed
333027 Secondary	[redacted]	[redacted]	Fortinet Canada	Canada (Ottawa)

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.

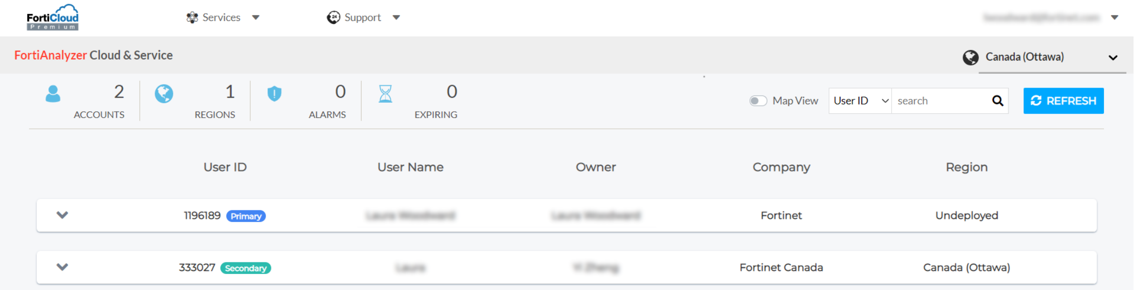
See also Viewing information about instances on page 16 and Upgrading firmware from the portal on page 17.

Using Map View

After accessing the FortiAnalyzer Cloud & Service portal, you can display deployed instances on a map.

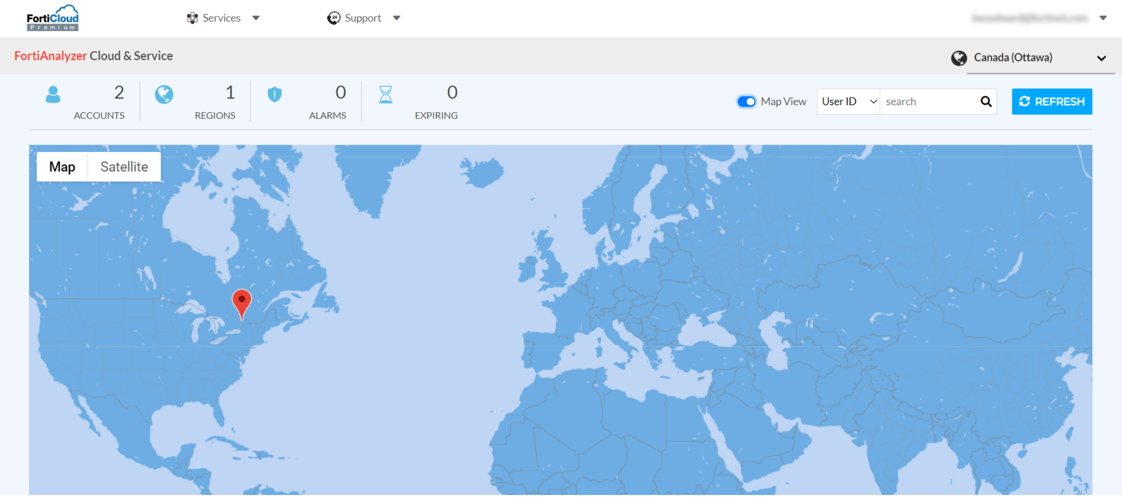
To use Map View:

1. Access the portal. See Accessing the portal and instances on page 13.
   The FortiAnalyzer Cloud & Service portal is displayed.

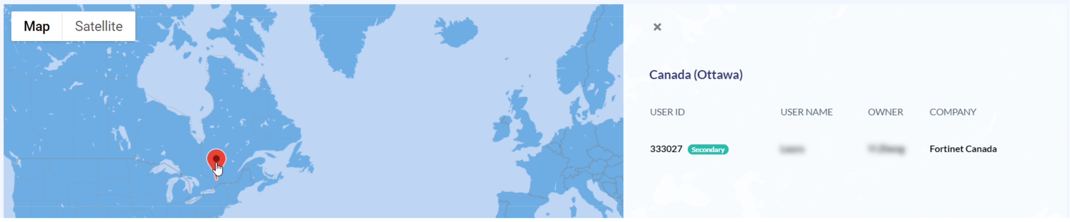


	User ID	User Name	Owner	Company	Region
⌄	1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed
⌄	333027 Secondary	[redacted]	[redacted]	Fortinet Canada	Canada (Ottawa)

2. From the top-right corner, select a region, such as *Canada*.
   Notice that the URL for the FortiAnalyzer & Service portal changes.
3. Toggle *Map View* on.
   The Map View is displayed.



4. Click the location to display information about the instance.
   Details about the instance are displayed on the right-hand pane. Click *X* to close the right-hand pane.



Canada (Ottawa)

USER ID	USER NAME	OWNER	COMPANY
333027 Secondary	[redacted]	[redacted]	Fortinet Canada

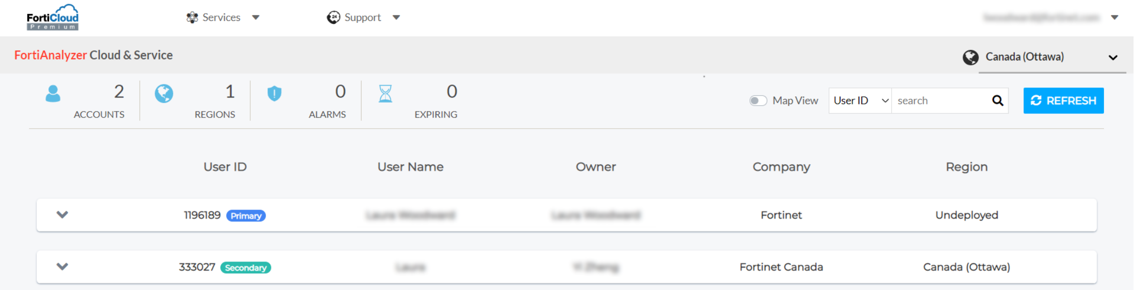
5. At the bottom-right of the map, click the + button to zoom in to the map, and click the - button to zoom out of the map.
6. Toggle *Map View* off to exit the map and display the list of accounts in table view.

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.

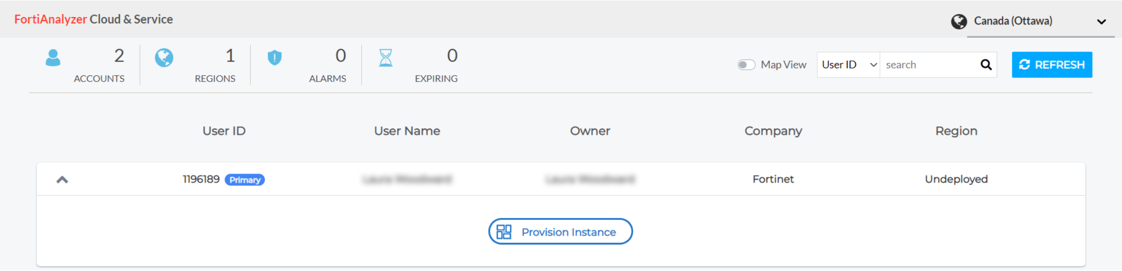
To view information about instances:

1. Access the portal. See Accessing the portal and instances on page 13.
   The FortiAnalyzer Cloud & Service portal is displayed.



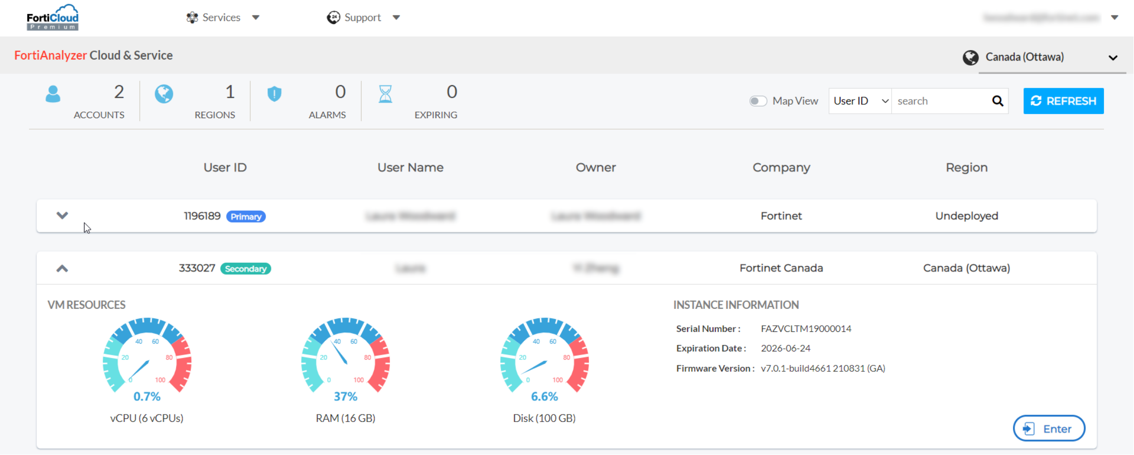
	User ID	User Name	Owner	Company	Region
⌄	1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed
⌄	333027 Secondary	[redacted]	[redacted]	Fortinet Canada	Canada (Ottawa)

2. Expand an account with no instances deployed.
   The account details are displayed. If it is a primary account, you can click *Provision Instance* to provision a FortiAnalyzer Cloud instance.



User ID	User Name	Owner	Company	Region
1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed

3. Expand an account with deployed instances.
   Information about the VM resources and the instance is displayed. If a firmware upgrade is available, a message is displayed, and you can upgrade now or later. You can also click *Enter* to access the instance.
   When a firmware upgrade is available, information about the firmware upgrade is also displayed.



User ID	User Name	Owner	Company	Region
1196189 Primary	[redacted]	[redacted]	Fortinet	Undeployed
333027 Secondary	[redacted]	[redacted]	Fortinet Canada	Canada (Ottawa)

INSTANCE INFORMATION

Serial Number : FAZVCLTM19000014
Expiration Date : 2026-06-24
Firmware Version : v7.0.1-build4661 210831 (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 System Settings on page 20.

To upgrade firmware from the portal:

1. Access the portal. See Accessing the portal and instances on page 13.
   The FortiAnalyzer Cloud & Service portal is displayed.
2. Expand your account.
3. Click *Upgrade Now* to update the firmware immediately, or click *Upgrade Later* to schedule upgrade of the firmware for a later date.
4. Click *OK*.
5. 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 7.0.1 Administration Guide.

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

- Upgrading firmware from System Settings on page 20
- Identifying the public IP address on page 19
- Enabling managed SOC service on page 20

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 13.
2. In FortiAnalyzer Cloud, go to *System Settings > Dashboard*.
3. Click inside the CLI Console widget, and run the following commands:

   If the widget is not available, select *Toggle Widgets* from the toolbar to add the widget to the dashboard.

```
FMG-VM64-VIO-CLOUD # Config sys admin setting
Set shell enable
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.

Enabling managed SOC service

With a valid license, you can enable the *Managed SOC Service* option to give the Fortinet SOC service team permission to manage your instance of FortiAnalyzer Cloud. Once the service is enabled, Fortinet will configure your instance to enable the SOC team to monitor FortiGate logs for incident detection. For more information about enabling the service from FortiAnalyzer Cloud, see the SOCaaS User Guide.

You can continue configuring FortiAnalyzer after you enable the service. If you disable or delete a custom event handler with the prefix *SOCaaS*, the SOC service will not work as designed.

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

To enable SOC management:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, enable *Managed SOC Service*. The *Managed SOC Service* dialog is displayed.
3. Click *OK*.

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 13.
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 21
- Modifying a secondary account on page 23
- Supporting IAM users and IAM API users on page 23

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

Adding a secondary account

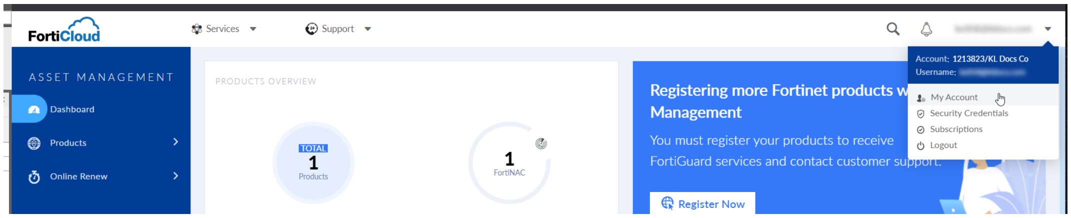
Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. Be default, the secondary account holder is assigned the default administrator profile named *Restricted_User*. However, the primary account holder can modify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

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

With FortiAnalyzer Cloud 6.4.5 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*.



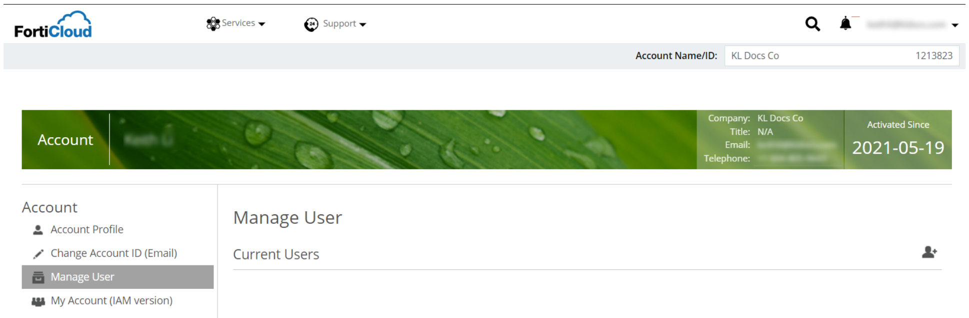
Account: 1213823/KL Docs Co
Username: [redacted]

Registering more Fortinet products w Management

You must register your products to receive FortiGuard services and contact customer support.

3. Click *Manage User*.

4. Click the new user icon to add a new user.

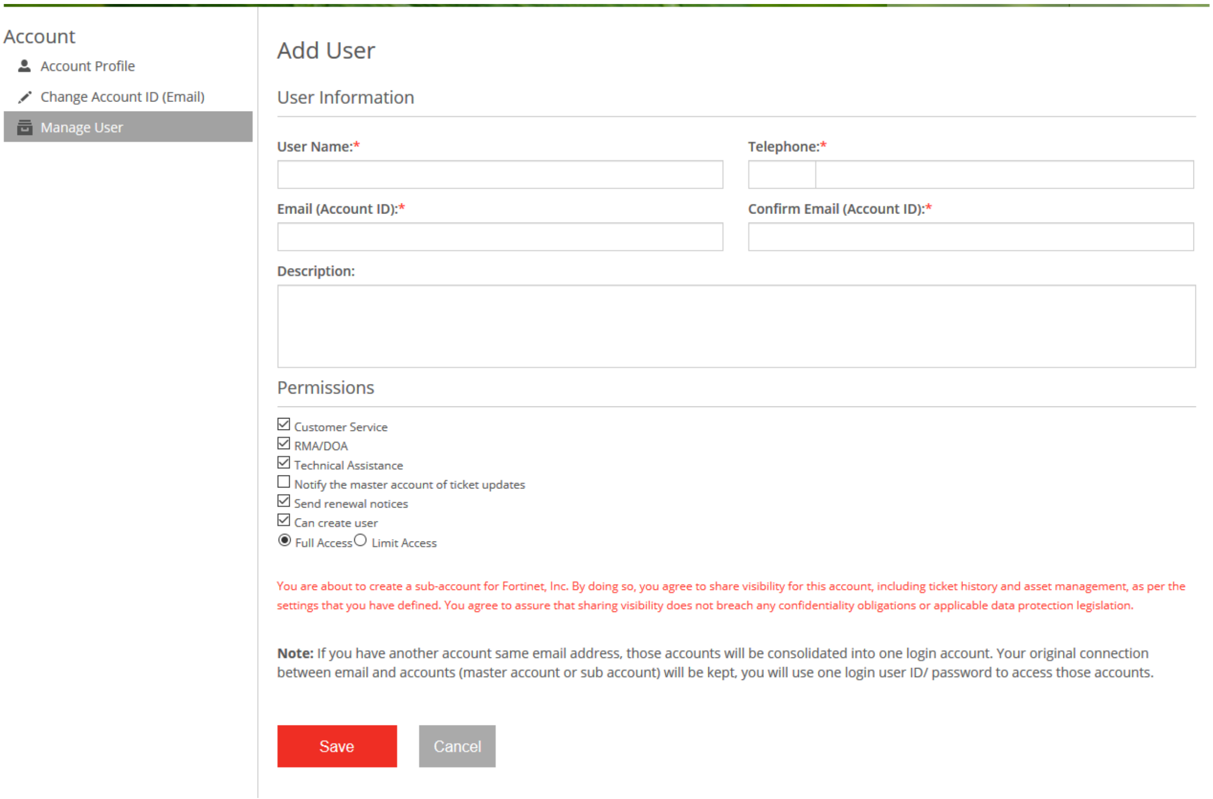


Account Name/ID: KL Docs Co 1213823

Company: KL Docs Co
Title: N/A
Email: [redacted]
Telephone: [redacted]

Activated Since
2021-05-19

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.



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.

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 23.

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 21.

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*.

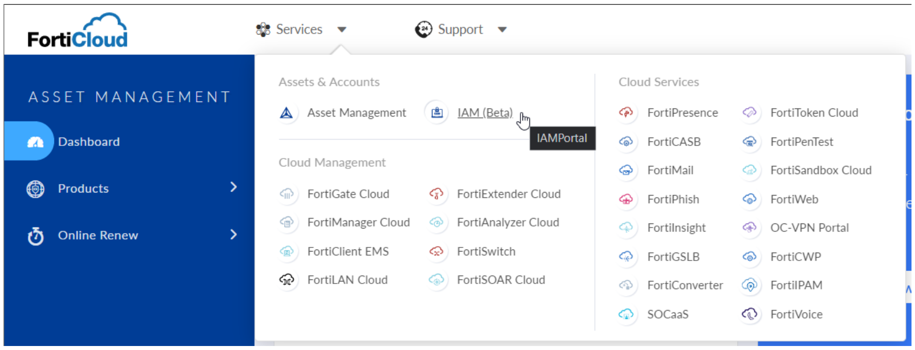
See also Adding IAM users on page 23 and Adding API users on page 25.

Adding IAM users

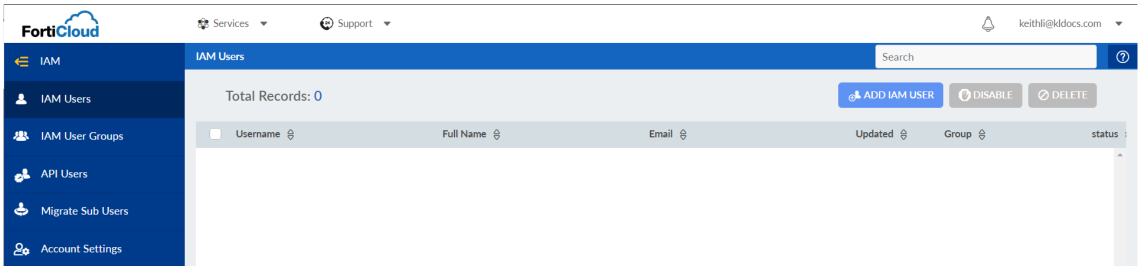
FortiAnalyzer Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiAnalyzer Cloud.

To add an IAM user:

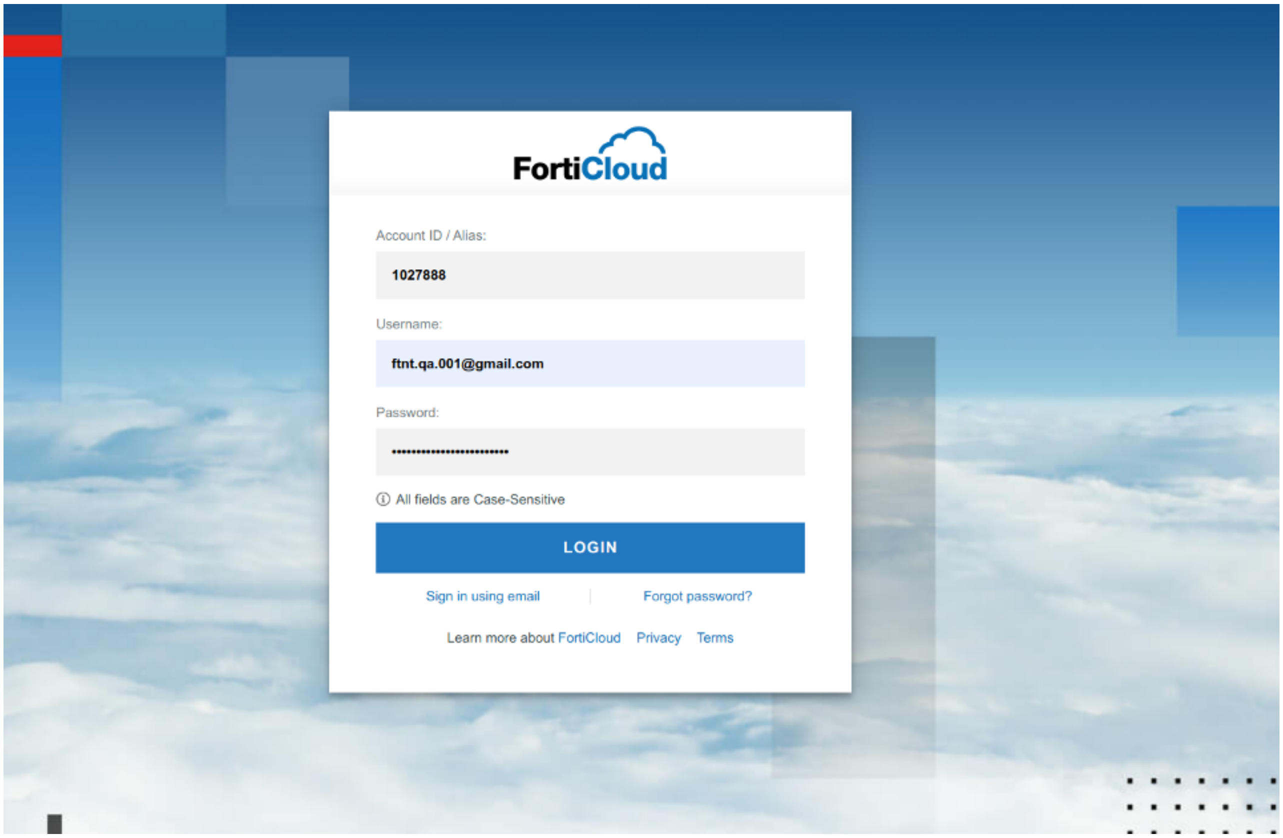
1. Go to FortiCloud (https://support.fortinet.com/), and log in.
2. From the *Services* menu, select *IAM* .



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.



FortiCloud

Account ID / Alias: 1027888

Username: ftnt.qa.001@gmail.com

Password: ••••••••••••••••••••••••

ⓘ All fields are Case-Sensitive

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 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.

FORTINET®

www.fortinet.com

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