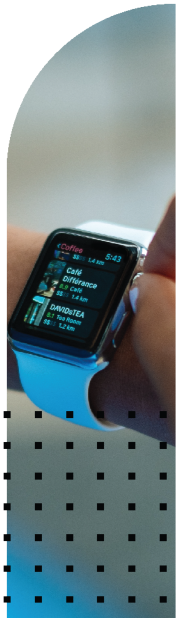
Cloud Deployment Guide

FortiManager 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

February 28th, 2024
FortiManager 7.4.x Cloud Deployment Guide
02-74-843404-20240228

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-09-19	Initial release.
2023-10-17	Updated Using FortiZTP with FortiManager Cloud on page 22.
2023-01-30	Initial release of FortiManager Cloud 7.4.2.
2024-02-28	Updated Introduction on page 5 and Accessing the portal and instances on page 12.

Introduction

FortiManager Cloud is a cloud-based management platform based on FortiManager.

Once a FortiManager Cloud entitlement has been added to your FortiCloud account, a FortiManager Cloud instance can be started. See Accessing the portal and instances on page 12 and Deploying FortiManager Cloud on page 7.

When a FortiGate device is registered to the same FortiCloud account, the FortiGate will automatically detect that your account includes a valid FortiManager Cloud entitlement, and the FortiGate GUI will allow you to select FortiManager Cloud for Central Management.

Central Management using FortiManager Cloud can also be configured from the FortiGate CLI using the following commands:

```
config system central-management
   set type fortimanager
   set fmg fortimanager.forticloud.com
end
```

Once Central Management has been configured, a FGFM tunnel is established between your FortiGate device and your FortiManager Cloud instance. After the FGFM tunnel is established, you can execute usual FortiManager functions from the FortiManager Cloud instance.

This section includes the following topics:

- Requirements on page 5
- Licensing on page 6

Requirements

The following items are required before you can initialize FortiManager 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 FortiManager Cloud. A primary FortiCloud account can invite other users to launch FortiManager Cloud as sub users. See Adding a secondary account on page 25.

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

See Licensing on page 6 for further license details.

Licensing

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

FortiManager Cloud requires one of the following licenses:

- **Cloud-based Central Management & Orchestration Service:**

Subscription for 3 devices/VDOMs managed by FortiManager Cloud.	FC0-10-MVCLD-227-01-DD
Subscription for 10 devices/VDOMs managed by FortiManager Cloud.	FC1-10-MVCLD-227-01-DD
Subscription for 100 devices/VDOMs managed by FortiManager Cloud.	FC2-10-MVCLD-227-01-DD
Subscription for 1000 devices/VDOMs managed by FortiManager Cloud.	FC3-10-MVCLD-227-01-DD

Deploying FortiManager Cloud

The section describes how to deploy FortiManager 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 FortiManager Cloud instance. See Deploying a FortiManager Cloud instance on page 7.
3. (Optional) Upgrade FortiManager Cloud to the latest available cloud version. See Upgrading firmware from the portal on page 15.
4. On FortiOS, enable management by FortiManager Cloud. See Configuring FortiOS on page 10.

At the time of the 7.4 release, FortiManager Cloud supports new deployments in version 7.0 and upgrades to version 7.2 and 7.4.

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

Checking requirements and licenses

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

To check for requirements and license for FortiManager 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 FortiManager Cloud entitlement is registered to your FortiCloud account.
   a. In the *Asset Management* portal, go to *Account Services*.
   b. Verify that FortiManager Cloud is listed.
   c. Optionally, click on the FortiManager Cloud serial number to view additional information.

   Some legacy licenses can instead be viewed by going to the Product List, expanding the *FortiGate* category and clicking on a device to view its details, and then confirming that the device *Entitlement* includes FortiManager Cloud.

3. Deploy the FortiManager Cloud instance. See Deploying a FortiManager Cloud instance on page 7.

Deploying a FortiManager Cloud instance

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

A primary FortiCloud account is required to deploy FortiManager Cloud. A primary FortiCloud account can invite other users to launch FortiManager Cloud as sub users. See Adding a secondary account on page 25.

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

At the time of the 7.4 release, FortiManager Cloud supports new deployments in version 7.0 and upgrades to version 7.2 and 7.4.

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

For support of FortiGates devices on earlier firmware versions, you can change the FortiManager Cloud ADOM version to match the firmware version of the FortiGates.

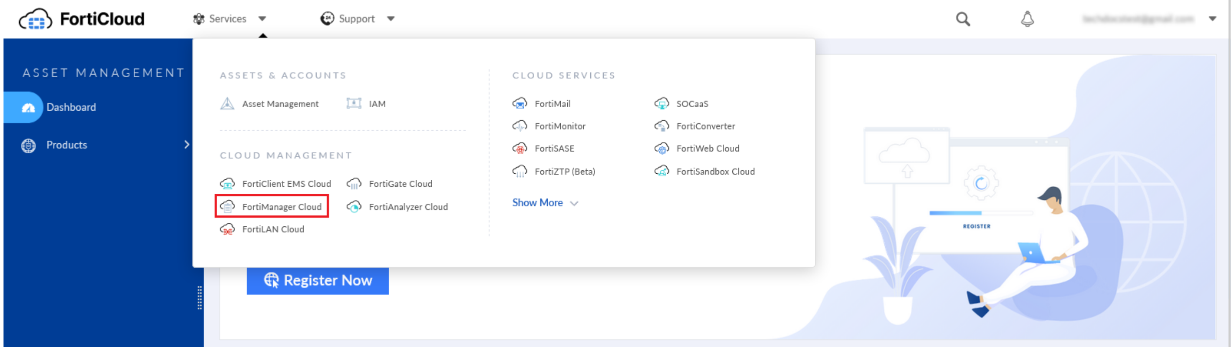
Check the FortiManager/FortiOS Compatibility Guide to see which FortiOS versions are supported by each FortiManager release.

For more information on changing the ADOM version, see Updating the ADOM version on page 20.

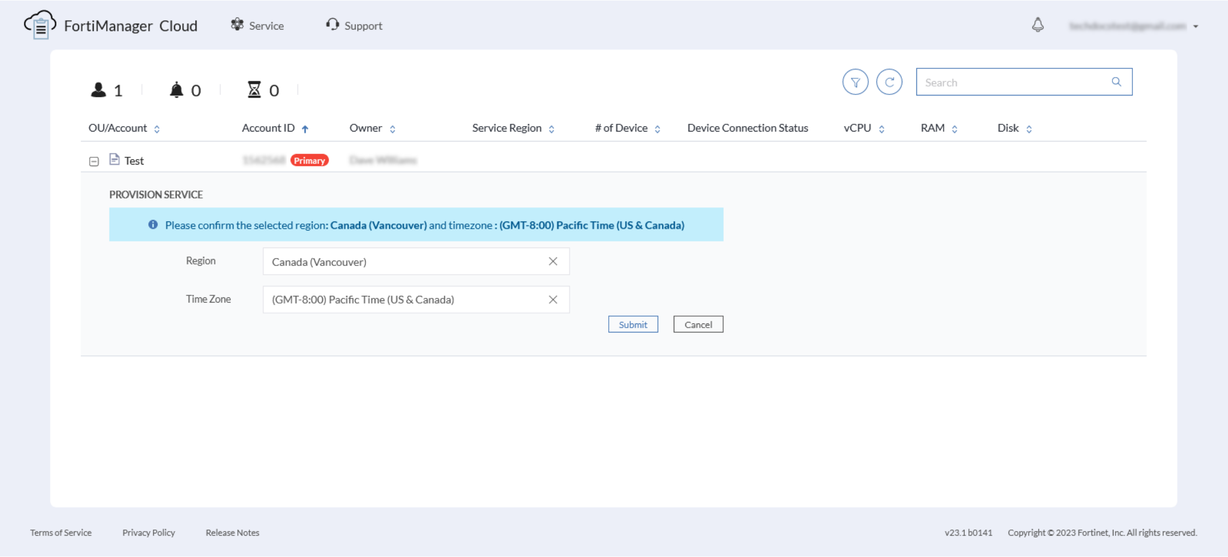
To deploy a FortiManager Cloud instance:

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 *FortiManager Cloud*.

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



OU/Account	Account ID	Owner	Service Region	# of Device	Device Connection Status	vCPU	RAM	Disk
Test	[redacted] Primary	[redacted]						

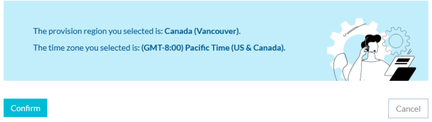
PROVISION SERVICE

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

Region: Canada (Vancouver)

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

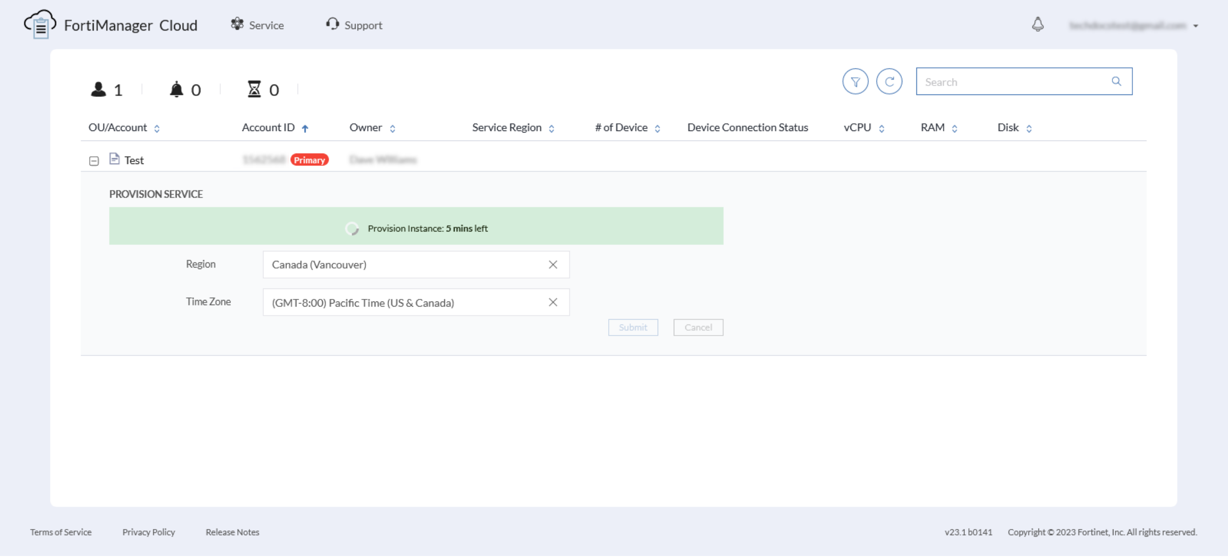
5. A message asking you to confirm your selected region and time zone is displayed.
   a. Click *Confirm* to provision in the FortiManager Cloud instance.
   b. Click *Cancel* to stop provisioning the instance, and change the region.



The provision region you selected is: **Canada (Vancouver).**

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

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



OU/Account	Account ID	Owner	Service Region	# of Device	Device Connection Status	vCPU	RAM	Disk
Test	[redacted] Primary	[redacted]						

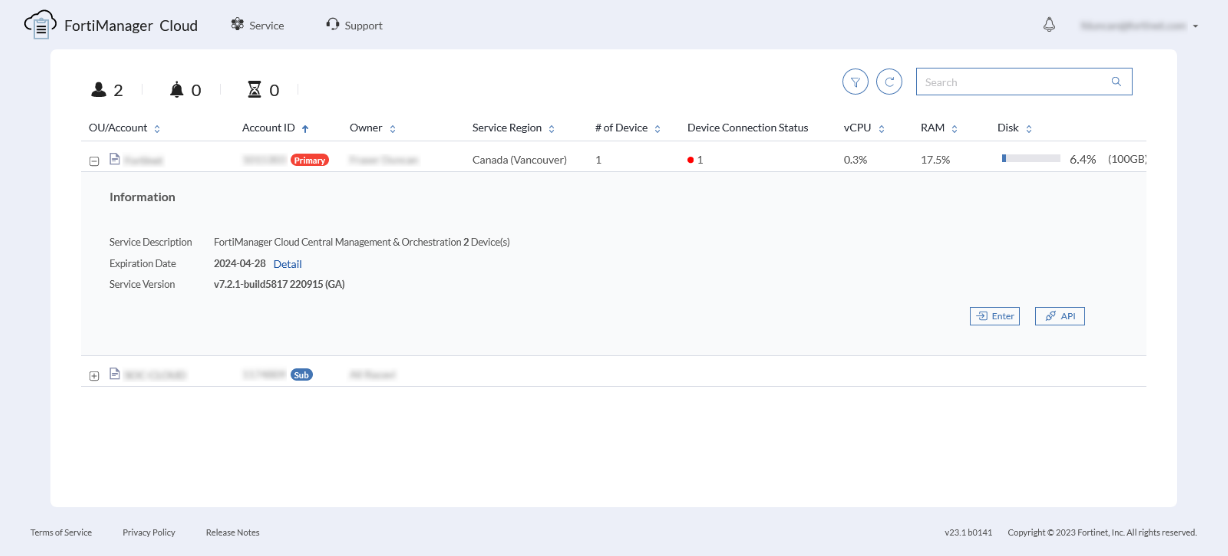
PROVISION SERVICE

Provision Instance: **5 mins left**

Region: Canada (Vancouver)

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

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



FortiManager Cloud · Service · Support · [redacted]

👤 2 | 🔔 0 | ⌛ 0

OU/Account	Account ID	Owner	Service Region	# of Device	Device Connection Status	vCPU	RAM	Disk
⊟ [redacted]	[redacted] Primary	[redacted]	Canada (Vancouver)	1	● 1	0.3%	17.5%	6.4% (100GB)
⊞ [redacted]	[redacted] Sub	[redacted]						

Information

Service Description FortiManager Cloud Central Management & Orchestration 2 Device(s)
Expiration Date 2024-04-28 Detail
Service Version v7.2.1-build5817 220915 (GA)

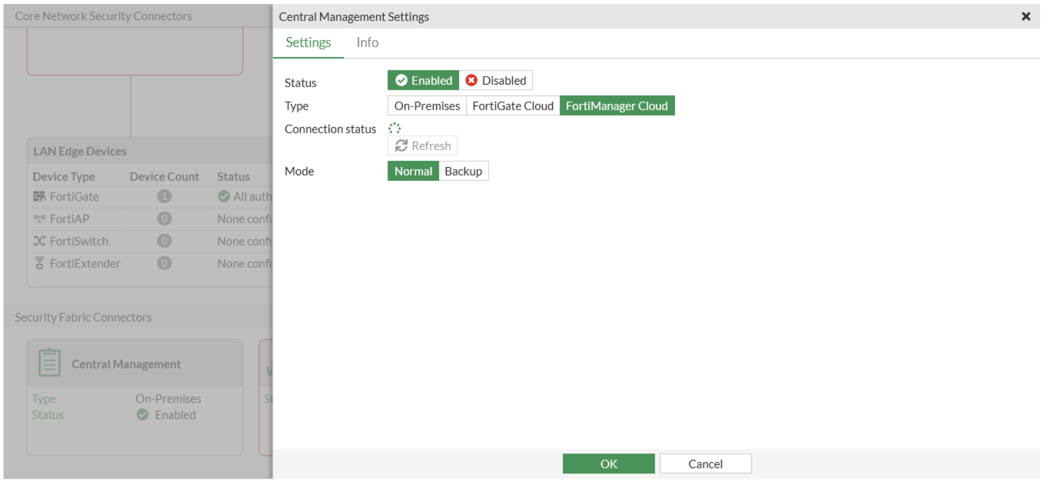
8. (Optional) Upgrade FortiManager Cloud to 7.4.x. See Upgrading firmware from the portal on page 15.
9. Configure FortiOS to work with FortiManager Cloud. See Configuring FortiOS on page 10.

Configuring FortiOS

This section explains how to enable management of FortiGate by FortiManager Cloud.

To configure FortiOS:

1. In FortiOS, enable FortiManager Cloud.
   a. Go to *Security Fabric > Fabric Connectors*, and edit the *Central Management* card.
   b. Select the *Settings* tab, and set the *Status* to *Enabled*.
   c. Click *FortiManager Cloud*, and click *OK*.

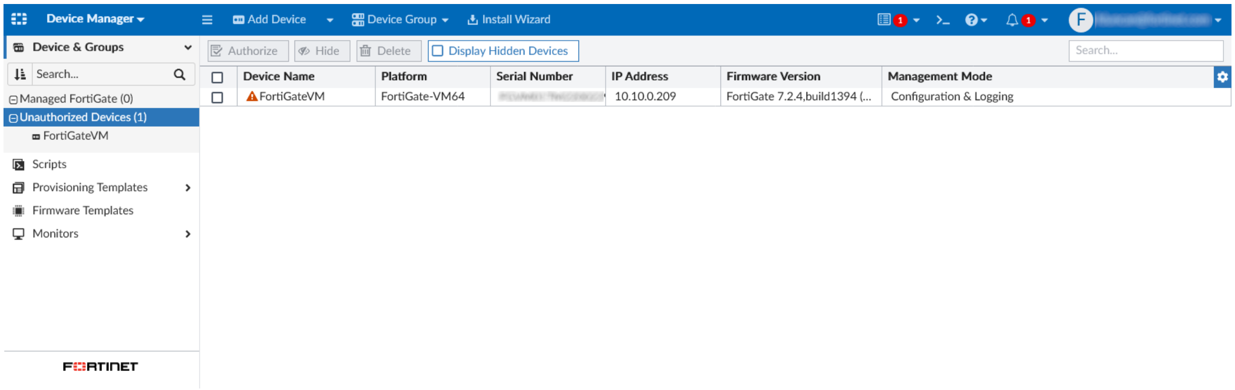


Central Management Settings

Settings | Info

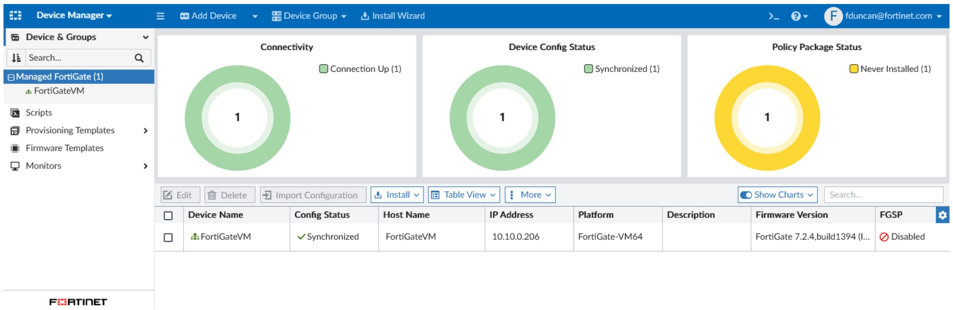
Status: Enabled
Type: FortiManager Cloud
Connection status
Mode: Normal

2. In the FortiManager Cloud instance, go to *Device Manager* and authorize the FortiGate.



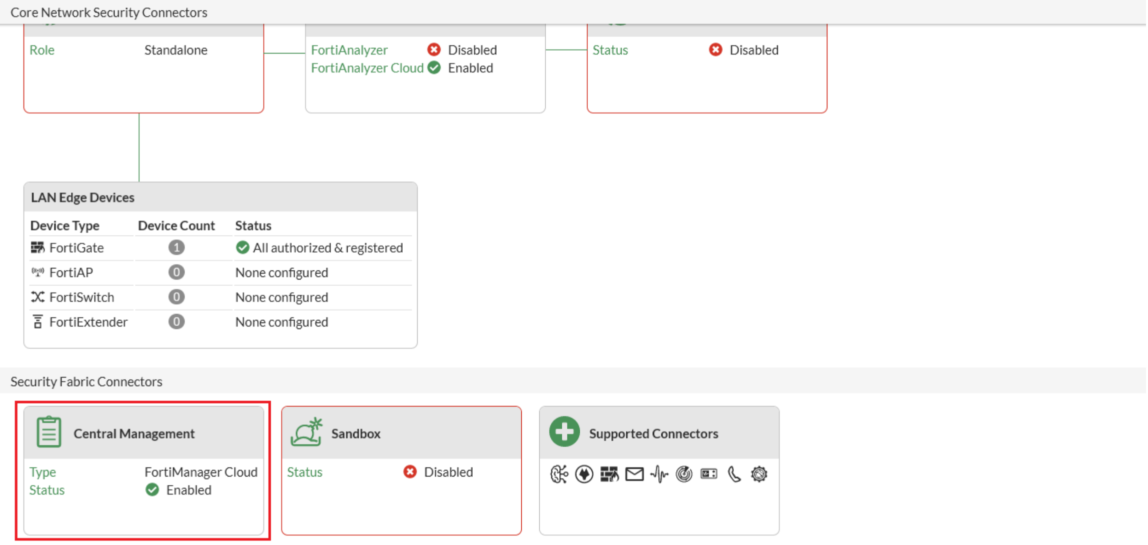
☐	Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode
☐	FortiGateVM	FortiGate-VM64	[redacted]	10.10.0.209	FortiGate 7.2.4,build1394 (...	Configuration & Logging

After authorizing the FortiGate, the FortiGate becomes a managed device.



☐	Device Name	Config Status	Host Name	IP Address	Platform	Description	Firmware Version	FGSP
☐	FortiGateVM	✓ Synchronized	FortiGateVM	10.10.0.206	FortiGate-VM64		FortiGate 7.2.4,build1394 (I...	Disabled

When successfully authorized, the central management status displays as *Enabled on FortiManager*.


Core Network Security Connectors

Role	Standalone

FortiAnalyzer	✗ Disabled
FortiAnalyzer Cloud	✓ Enabled

Status	✗ Disabled

LAN Edge Devices

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

Security Fabric Connectors

Central Management

Type	FortiManager Cloud
Status	✓ Enabled

Sandbox

Status	✗ Disabled

Supported Connectors

Using the FortiManager Cloud & Service portal

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

This section includes the following procedures about using the portal:

- Accessing the portal and instances on page 12
- Viewing information about instances on page 14
- Upgrading firmware from the portal on page 15
- Providing feedback on page 16

Accessing the portal and instances

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

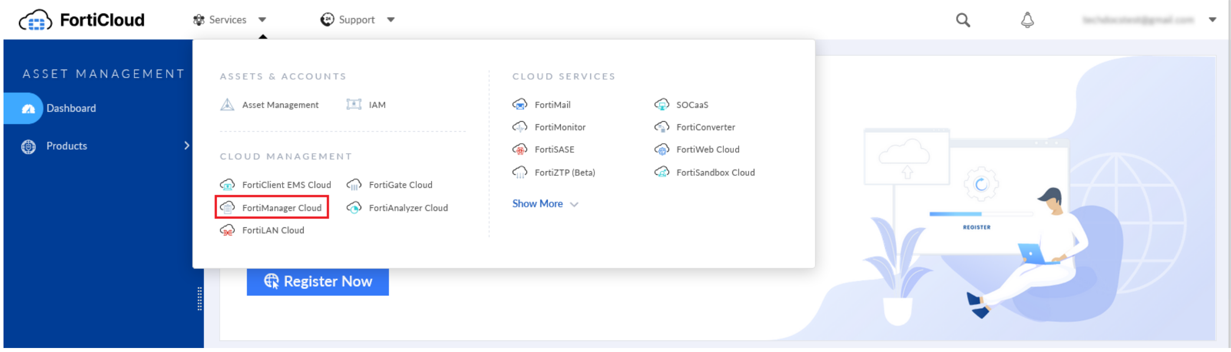
You can access FortiManager Cloud portal through one of the methods below:

1. Select *FortiManager Cloud* from the list of available *Services* in the FortiCloud Portal. See Access FortiManager Cloud through FortiCloud on page 12.
2. Go to https://fortimanager.forticloud.com. After authentication, you are redirected to your own FortiManager Cloud instance.
3. Go directly to your instance using the specific URL for your instance (e.g. `https:://{account_id}.{region}.fortimanager.forticloud.com`). You can obtain your instance's URL from your browser's address bar once you have accessed FortiManager Cloud through one of the previous methods.

Access FortiManager Cloud through FortiCloud

To access FortiManager Cloud through FortiCloud:

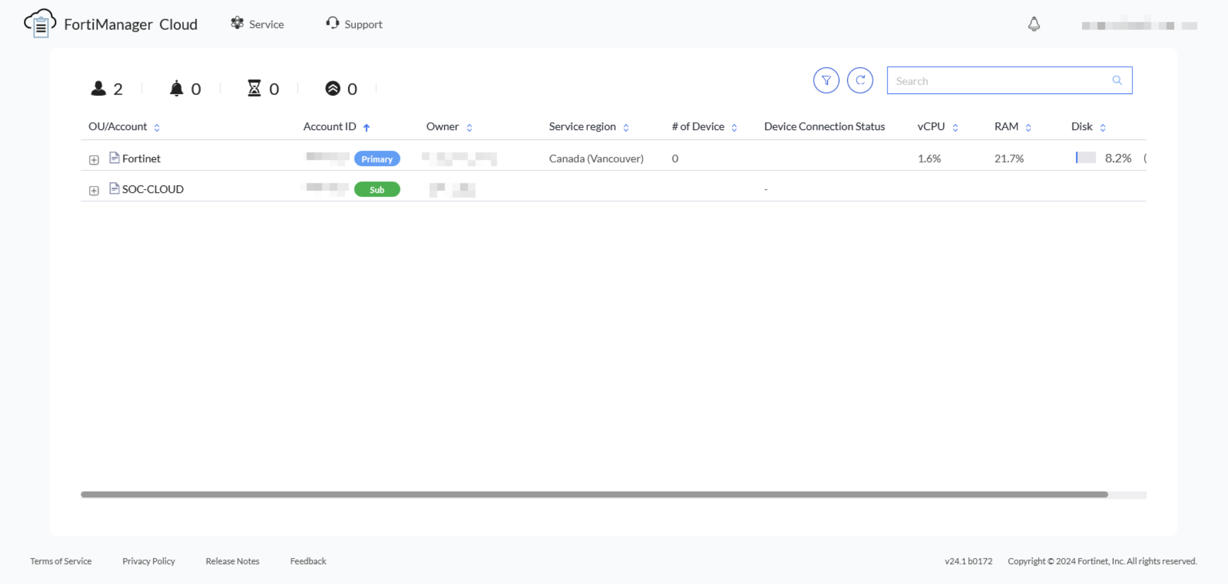
1. Go to FortiCloud (https://support.fortinet.com/), and use your FortiCloud account credentials to log in.
   The FortiCloud portal is displayed.
2. From the *Services* menu, select *FortiManager Cloud* under *Cloud Management*.



You are automatically logged in to your FortiManager instance.

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

> In FortiManager Cloud 7.4.2 and later, you can navigate between accounts or return to the FortiManager Cloud portal using the options in the FortiManager Cloud toolbar. See Using the FortiManager Cloud toolbar on page 18.



OU/Account	Account ID	Owner	Service region	# of Device	Device Connection Status	vCPU	RAM	Disk
Fortinet	[redacted] Primary	[redacted]	Canada (Vancouver)	0		1.6%	21.7%	8.2% (
SOC-CLOUD	[redacted] Sub	[redacted]			-			

The following options are displayed:

Dashboard	The top-left includes a dashboard summary of the accounts displayed on the pane: • *Accounts*: Displays the number of accounts you can access. • *Alarms*: Displays the number of notifications or alarms that need your attention. Notifications and alarms display in the banner. For alarms, you can also scroll down through the accounts to find an alarm icon on affected accounts. • *Expiring*: Displays the number of licenses that will expire soon.
Filter	Click to view options to filter by license status and quota/storage alarm.
Refresh	Click to manually retrieve the latest license information from FortiCare and refresh the pane. Information from FortiCare is also automatically retrieved on a regular interval.
Account Search	Use to search for accounts. In the *Search* box, type search criteria, and press *Enter*. Delete the search criteria, and press *Enter* to display all accounts again.
Accounts summary in table view	Each account displays as a row with the following columns: • *OU/Account*: The OU/Account this instance is configured for. • *Account ID*: The account ID. • *Owner*: The name of the owner. • *Service Region*: The region where the instance is deployed. • *# of Device*: The number of devices connected to the instance. • *Device Connection Status*: The status of connected devices.

- *vCPU*
- *RAM*
- *Disk*

Expand the pane to view additional information:

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

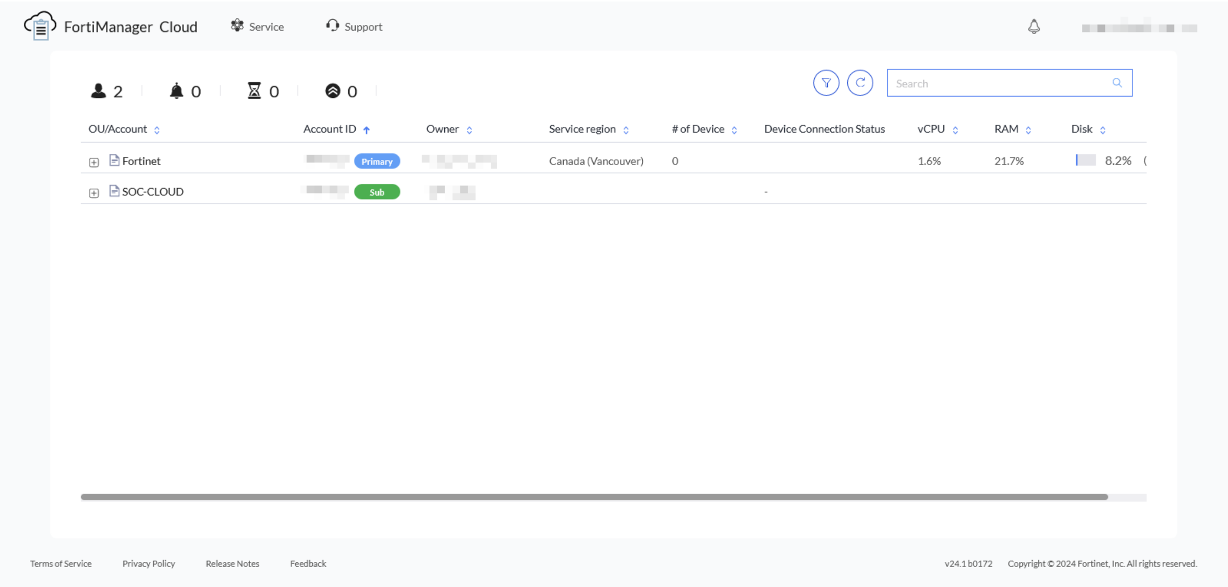
See also Viewing information about instances on page 14 and Upgrading firmware from the portal on page 15.

Viewing information about instances

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

To view information about instances:

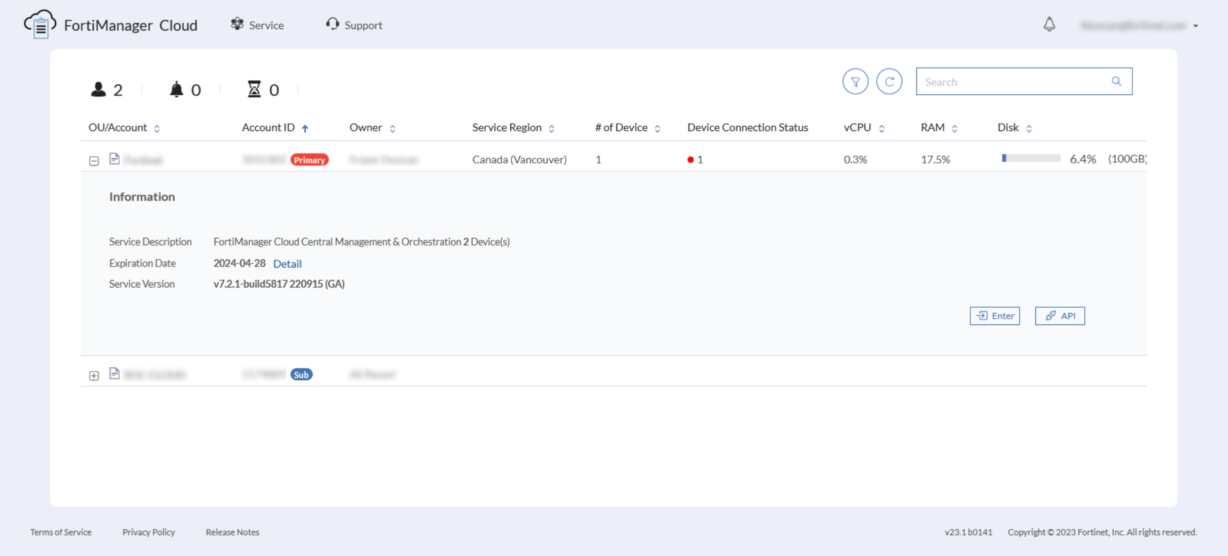
1. Access the portal. See Accessing the portal and instances on page 12.
   The FortiManager Cloud & Service portal is displayed.



OU/Account	Account ID	Owner	Service region	# of Device	Device Connection Status	vCPU	RAM	Disk	
Fortinet	[redacted] Primary	[redacted]	Canada (Vancouver)	0		1.6%	21.7%	8.2%	(
SOC-CLOUD	[redacted] Sub	[redacted]			-				

2. Expand an account with no instances deployed.
   The account details are displayed. If it is a primary account, you can provision a new instance. See Deploying a FortiManager Cloud instance on page 7.
3. Expand an account with deployed instances.
   Information about the VM resources and the instance is displayed.

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



OU/Account	Account ID	Owner	Service Region	# of Device	Device Connection Status	vCPU	RAM	Disk
[redacted]	[redacted] Primary	[redacted]	Canada (Vancouver)	1	● 1	0.3%	17.5%	6.4% (100GB)

Information

Service Description FortiManager Cloud Central Management & Orchestration 2 Device(s)
Expiration Date 2024-04-28 Detail
Service Version v7.2.1-build5817 220915 (GA)

OU/Account	Account ID	Owner
[redacted]	[redacted] Sub	[redacted]

Upgrading firmware from the portal

FortiManager Cloud firmware can be upgraded. The FortiManager 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 FortiManager Cloud & Service portal.

See also Upgrading firmware from the instance on page 17.

To upgrade firmware from the portal:

1. Access the portal. See Accessing the portal and instances on page 12.

   The FortiManager 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 FortiManager Cloud.

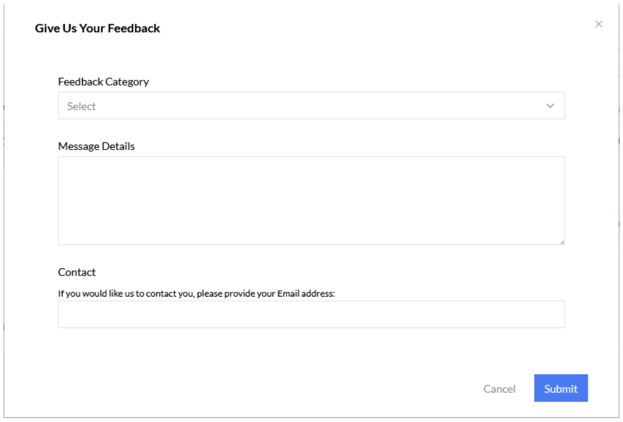
Providing feedback

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

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

- The footer on the *FortiManager* Cloud & Service portal.
- The FortiManager Cloud portal account dropdown inside the FortiManager Cloud instance. See Using the FortiManager Cloud toolbar on page 18.

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



Give Us Your Feedback

Feedback Category

Select

Message Details

Contact

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

Using FortiManager Cloud

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

For information about using FortiManager and FortiManager Cloud, see the FortiManager 7.2.1 Administration Guide.

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

- Upgrading firmware from the instance on page 17
- Identifying the public IP address on page 17
- Using the FortiManager Cloud toolbar on page 18
- Updating the ADOM version on page 20
- Enabling the FortiManager Cloud connector on FortiGate on page 21
- Using FortiZTP with FortiManager Cloud on page 22

Upgrading firmware from the instance

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

For information about upgrading firmware from the FortiManager & Service portal, see Upgrading firmware from the portal on page 15.

Before you can use FortiManager Cloud 7.4.x, you must upgrade all FortiGates to FortiOS 7.0.0 or later.

To upgrade firmware from the instance:

1. Access the instance. See Accessing the portal and instances on page 12.
2. In FortiManager Cloud, go to *Dashboard*.
3. In the *System Information* widget, click the *Upgrade Firmware* button beside *Firmware Version*.

   The *Firmware Management* dialog box is displayed.
4. From the *Select Firmware* list, select the firmware version, and click *OK*.

Identifying the public IP address

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

To determine the public IP address:

1. Access the instance. See Accessing the portal and instances on page 12.
2. Open the CLI console by clicking the CLI option from the FortiManager Cloud toolbar. See Using the FortiManager Cloud toolbar on page 18.
3. In the CLI console, run the following commands:

```
FMG-VM64-VIO-CLOUD # config system admin setting
set shell-access enable
Enter new password: <password>
Confirm new password: <password>
End
FMG-VM64-VIO-CLOUD # execute shell
Enter password:
bash$
bash$ curl ifconfig.me
173.243.137.11
```

In this example, the public IP address for FortiManager 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 FortiManager Cloud toolbar

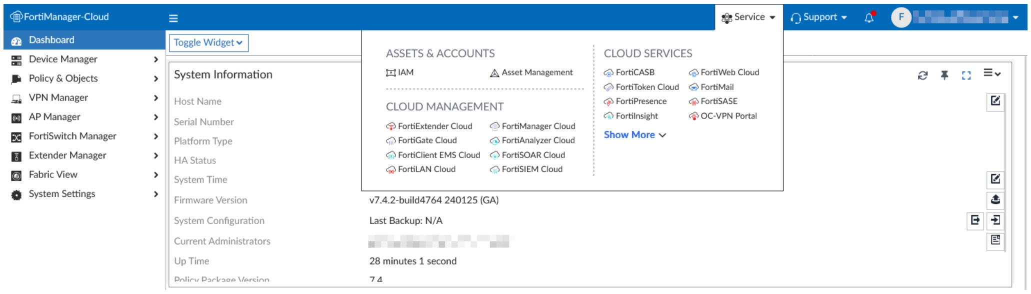
You can access FortiCloud services and support links from the FortiManager Cloud toolbar.

The FortiManager toolbar includes the following dropdown menus:

- Service on page 18
- Support on page 19
- Notifications on page 19
- Account on page 19

Service

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

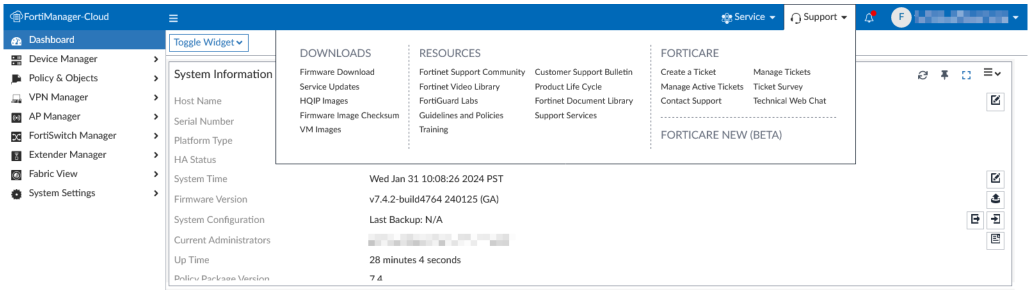


System Information

Host Name
Serial Number
Platform Type
HA Status
System Time
Firmware Version v7.4.2-build4764 240125 (GA)
System Configuration Last Backup: N/A
Current Administrators [redacted]
Up Time 28 minutes 1 second
Policy Package Version 7.4

Support

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



System Information

Host Name

Serial Number

Platform Type

HA Status

System Time Wed Jan 31 10:08:26 2024 PST

Firmware Version v7.4.2-build4764 240125 (GA)

System Configuration Last Backup: N/A

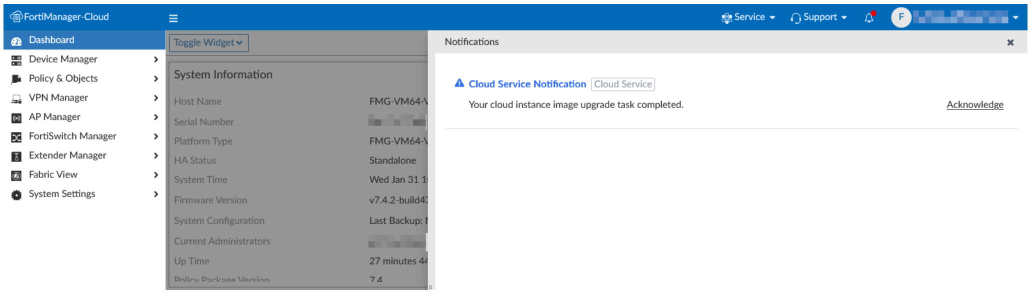
Current Administrators [redacted]

Up Time 28 minutes 4 seconds

Policy Package Version 7.4

Notifications

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



System Information

Host Name FMG-VM64-V

Serial Number [redacted]

Platform Type FMG-VM64-V

HA Status Standalone

System Time Wed Jan 31 1

Firmware Version v7.4.2-build47

System Configuration Last Backup: N

Current Administrators [redacted]

Up Time 27 minutes 44

Policy Package Version 7.4

Cloud Service Notification Cloud Service

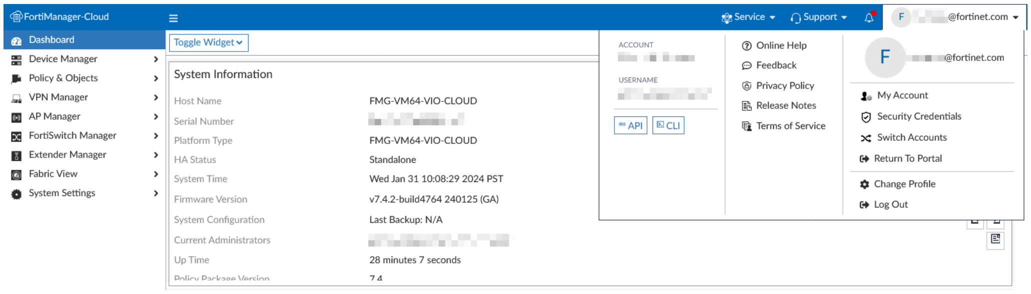
Your cloud instance image upgrade task completed.

Account

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

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

Security Credentials	Go to the FortiCloud Security Credentials page.
Switch Accounts	Switch between available accounts.
Return to Portal	Return to the FortiManager Cloud portal. See Using the FortiManager Cloud & Service portal on page 12.
Change Profile	Change FortiManager Cloud profile options including avatar and theme.
Log Out	Log out of FortiManager Cloud.



System Information

Host Name FMG-VM64-VIO-CLOUD
Serial Number [redacted]
Platform Type FMG-VM64-VIO-CLOUD
HA Status Standalone
System Time Wed Jan 31 10:08:29 2024 PST
Firmware Version v7.4.2-build4764 240125 (GA)
System Configuration Last Backup: N/A
Current Administrators [redacted]
Up Time 28 minutes 7 seconds
Policy Package Version 7.4

ACCOUNT [redacted]
USERNAME [redacted]

F [redacted]@fortinet.com

Updating the ADOM version

FortiManager Cloud supports one ADOM and version. With FortiManager Cloud 7.4.x, the ADOM can be any of the following versions: 7.0, 7.2 or 7.4.

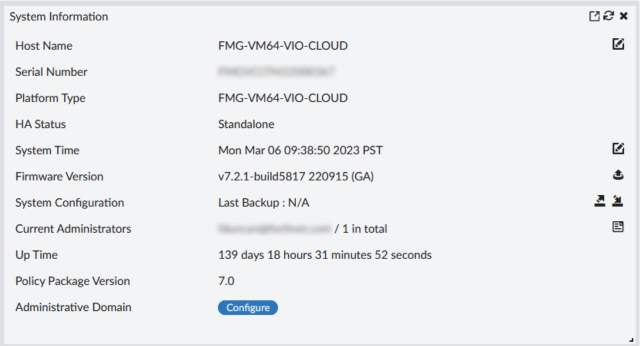
You can view the ADOM version on the *System Settings > Dashboard* pane in the *System Information* widget.

Before you can upgrade an ADOM to a higher version, you must upgrade firmware for all managed FortiGates to a version that is supported on the new ADOM.

You can only upgrade one ADOM version at a time. For example, if you are using a 7.0 ADOM and want to upgrade to a 7.4 ADOM, you must upgrade from 7.0 to 7.2, and then you can upgrade from 7.2 to 7.4.

To upgrade the ADOM version:

1. Access FortiManager Cloud. See Accessing the portal and instances on page 12.
2. In FortiManager Cloud, ensure that all managed FortiGates are running a FortiOS version that is supported by the new ADOM version. For more information on firmware versions supported in each ADOM, see the FortiManager Administration Guide.
3. Go to *System Settings > Dashboard*. The *Dashboard* is displayed.



System Information

Host Name	FMG-VM64-VIO-CLOUD
Serial Number	[redacted]
Platform Type	FMG-VM64-VIO-CLOUD
HA Status	Standalone
System Time	Mon Mar 06 09:38:50 2023 PST
Firmware Version	v7.2.1-build5817 220915 (GA)
System Configuration	Last Backup : N/A
Current Administrators	[redacted] / 1 in total
Up Time	139 days 18 hours 31 minutes 52 seconds
Policy Package Version	7.0
Administrative Domain	Configure

4. In the *System Information* widget, click *Configure* beside *Administrative Domain* option.
   The *Edit ADOM* dialog box is displayed.
5. In the *Type* field select a version, such as *7.4*.
6. Click *OK*, and the ADOM is upgraded to the selected version.

To downgrade the ADOM version:

1. Access FortiManager Cloud. See Accessing the portal and instances on page 12.
2. Open the FortiManager CLI from the toolbar, and enter the following command:
   ```
   execute reset adom 3 <version> <major release number>
   ```
   For example, to change the ADOM to version 7.0, you can enter the following command:
   ```
   execute reset adom 3 7 0
   ```
3. Log in to the user portal again following reboot, and the ADOM is downgraded to the selected version.
   You can see the current ADOM versions at *System Settings > Dashboard*.

Enabling the FortiManager Cloud connector on FortiGate

When you enable the FortiManager Cloud connector on FortiGate, you can enable management of the FortiGate by FortiManager Cloud.

This topic describes how to enable the FortiManager Cloud connector by using FortiGate. It also provides an example of how to use the FortiManager Cloud connector on FortiGate to support FortiGate-VM PAYG/ONDEMAND when both devices are registered to the same FortiCloud account.

The FortiGate-VM PAYG/ONDEMAND model is only supported with a FortiManager Cloud account subscription. FortiGate licenses for ondemand models are not available for purchase.

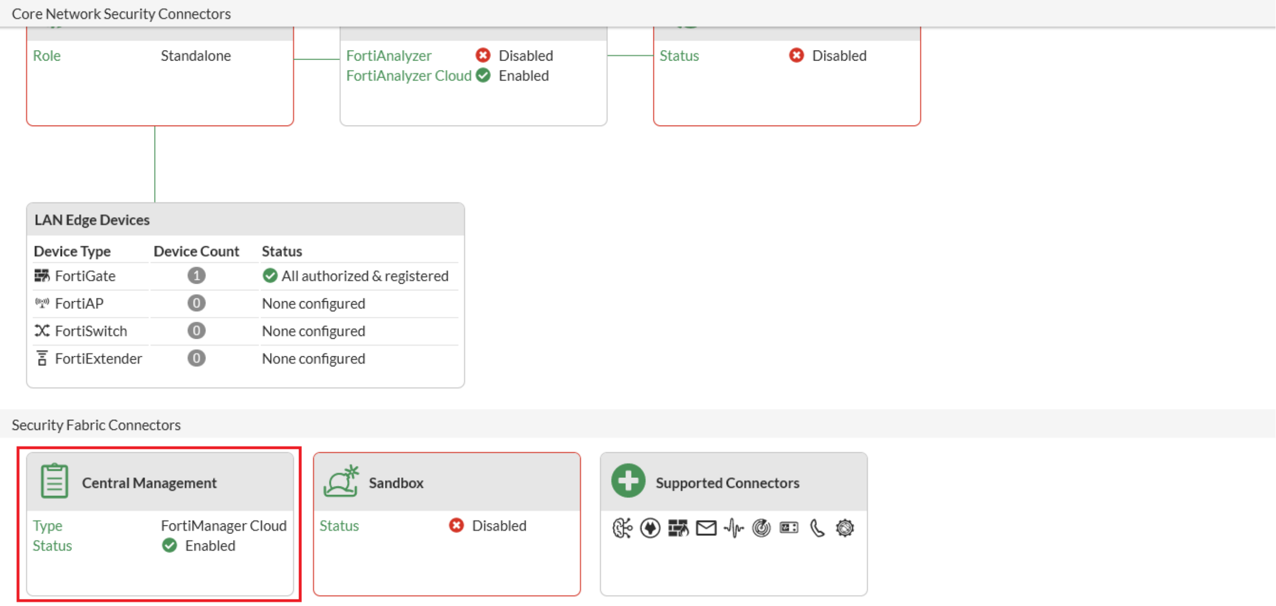
To enable the FortiManager Cloud connector in FortiGate:

1. Register FortiManager Cloud with FortiCloud.
2. Verify the per-device FortiManager entitlement was added to the account.
   a. In *Asset Management*, go to *Products List*, and find the FortiManager Cloud device.
   b. In the *Entitlement* widget, click *Show Contracts*.
   c. In the *Registered Support Contract(S)* pane, the *SKU* column will contain `FC<#>-10-MVCLD-227-01-12`.

3. Register the FortiGate device with the same FortiCloud account.
4. In the FortiGate device, use the CLI console to verify the User ID was updated by FortiGuard.

```
diag test update info
...
Support contract: pending_registration=255 got-contract info=1
   accoutn_id=[user_email] company=[company_name] industry=[instustry_name]
User ID: <user_id>
```

5. In the FortiGate device GUI, go to *Security Fabric > Fabric Connectors*. The FortiManager option is enabled.



Core Network Security Connectors

Role Standalone

FortiAnalyzer ✗ Disabled
FortiAnalyzer Cloud ✓ Enabled

Status ✗ Disabled

LAN Edge Devices

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

Security Fabric Connectors

Central Management
Type FortiManager Cloud
Status ✓ Enabled

Sandbox
Status ✗ Disabled

Supported Connectors

Please allow 2-4 hours for FortiGate to enable the FortiManager Cloud option in the connector.

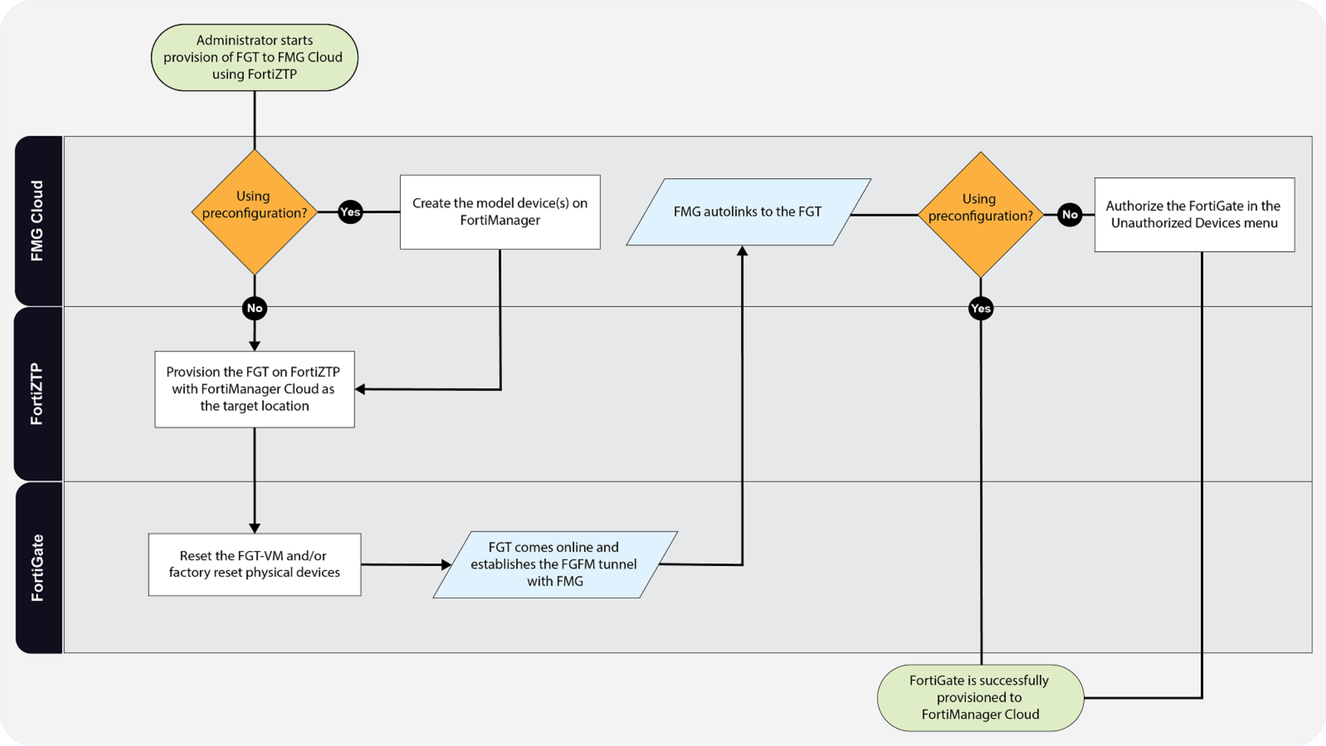
Using FortiZTP with FortiManager Cloud

FortiZTP is a centralized zero-touch provisioning platform for FortiCloud cloud product services. The service supports individual or bulk device provisioning to the target on-premise or cloud services, including FortiManager Cloud.

You can provision devices from FortiZTP with or without preconfiguration on FortiManager Cloud.

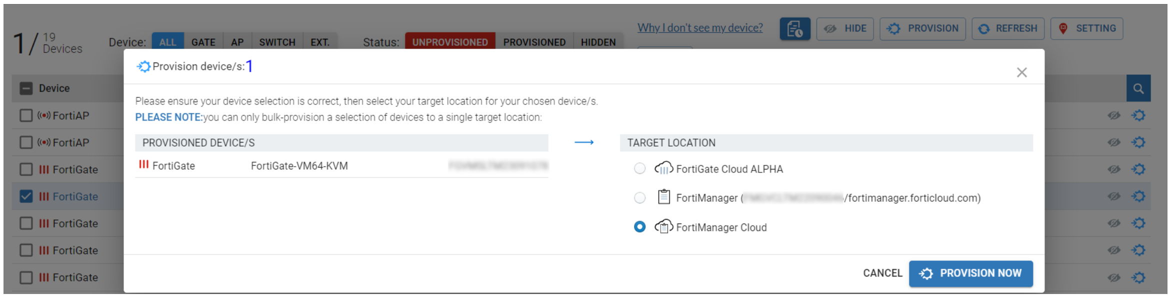
- With preconfiguration, you must create a model device in FortiManager Cloud before provisioning using FortiZTP. The provisioned FortiGate will auto-link to the model device.
- Without preconfiguration, you must manually authorize the FortiGate device from the unregistered list on FortiManager Cloud after provisioning from FortiZTP.

Below is an example diagram of the workflow for using FortiZTP with FortiManager Cloud:


Administrator starts provision of FGT to FMG Cloud using FortiZTP
FMG Cloud
FortiZTP
FortiGate
Using preconfiguration?
Yes
No
Create the model device(s) on FortiManager
FMG autolinks to the FGT
Using preconfiguration?
No
Yes
Authorize the FortiGate in the Unauthorized Devices menu
Provision the FGT on FortiZTP with FortiManager Cloud as the target location
Reset the FGT-VM and/or factory reset physical devices
FGT comes online and establishes the FGFM tunnel with FMG
FortiGate is successfully provisioned to FortiManager Cloud

To provision a FortiGate to FortiManager Cloud:

1. (Optional) Create the model device on FortiManager Cloud when using the preconfiguration method.
2. Provision the FortiGate using FortiZTP.
   a. Go to the FortiZTP portal.
   b. On the *UNPROVISIONED* tab, do the following:
      - To provision a single FortiGate, click the *Provision* icon.
      - To provision multiple FortiGates, select the checkboxes for the desired FortiGates, then click the *PROVISION* button.
   c. Under *TARGET LOCATION* in the *Provision devices* dialog, select *FortiManager Cloud*.
   d. Click *PROVISION NOW*.



Provision device/s: 1

Please ensure your device selection is correct, then select your target location for your chosen device/s.
PLEASE NOTE: you can only bulk-provision a selection of devices to a single target location:

PROVISIONED DEVICE/S → TARGET LOCATION

FortiGate FortiGate-VM64-KVM [redacted]

○ FortiGate Cloud ALPHA
○ FortiManager ([redacted]/fortimanager.forticloud.com)
● FortiManager Cloud

CANCEL PROVISION NOW

3. Reboot the FortiGate. For physical FortiGate devices, you must perform a factory reset.
4. Complete the onboarding of the managed device:
   When provisioning with preconfiguration:
   a. After the FortiGate comes online, the FGFM tunnel is established.
   b. The auto-link process is performed automatically, and the FortiGate is added as a managed device.

When provisioning without preconfiguration:

a. After the FortiGate comes online, FortiZTP will set the FortiManager Cloud serial number on the FortiGate to establish the FGFM tunnel. The FortiGate is added to the *Unauthorized Devices* menu on FortiManager Cloud.
b. Authorize the FortiGate to add it as a managed device.

For more information about the use of FortiZTP, see the FortiZTP Administration Guide.

Deprovisioning a device from the FortiZTP portal will not delete the device from FortiManager Cloud. The device must be manually deleted.

Using account services

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

- Adding a secondary account on page 25
- Modifying a secondary account on page 27
- Supporting IAM users and IAM API users on page 27

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

Adding a secondary account

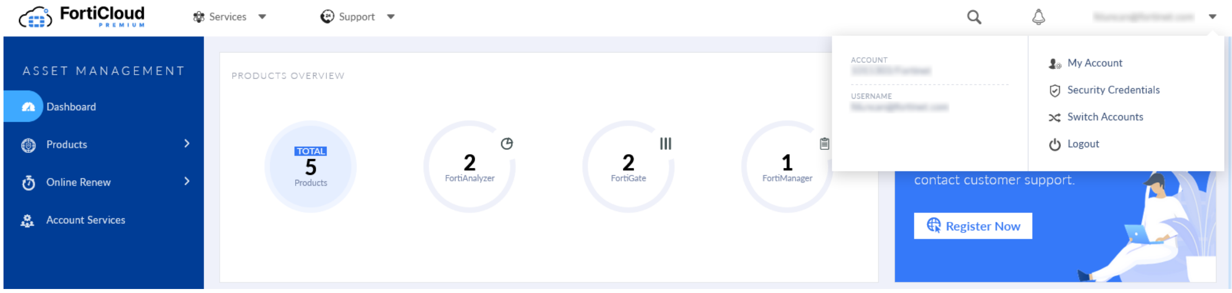
Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. Be default, the secondary account holder is assigned the default administrator profile named *Restricted_User*. However, the primary account holder can modify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

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

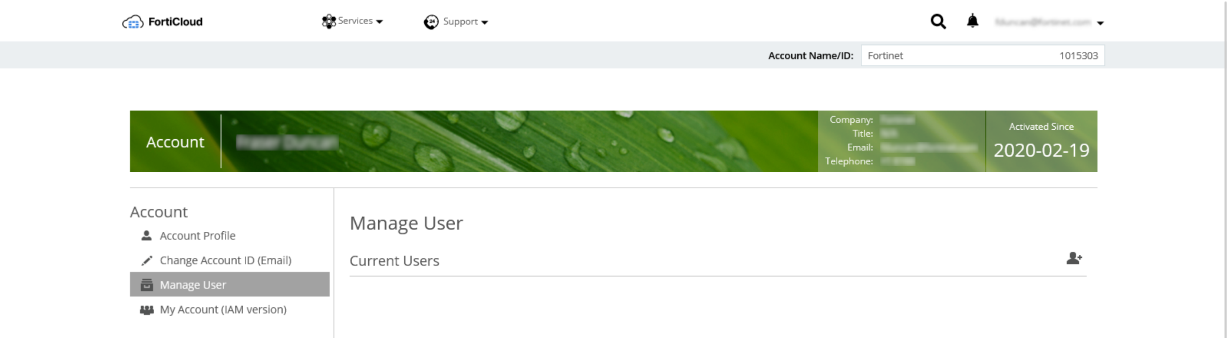
With FortiManager Cloud 7.0.x and later, you can use the Identity and Access Management (IAM) portal, and you can migrate secondary accounts to the IAM portal. In IAM portal, secondary accounts are called sub users. For information about migrating sub users, see the *Identity & Access Management Guide*.

To add a secondary account:

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



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



FortiCloud

[redacted]

Account Name/ID: Fortinet 1015303

Account [redacted]

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

Activated Since
2020-02-19

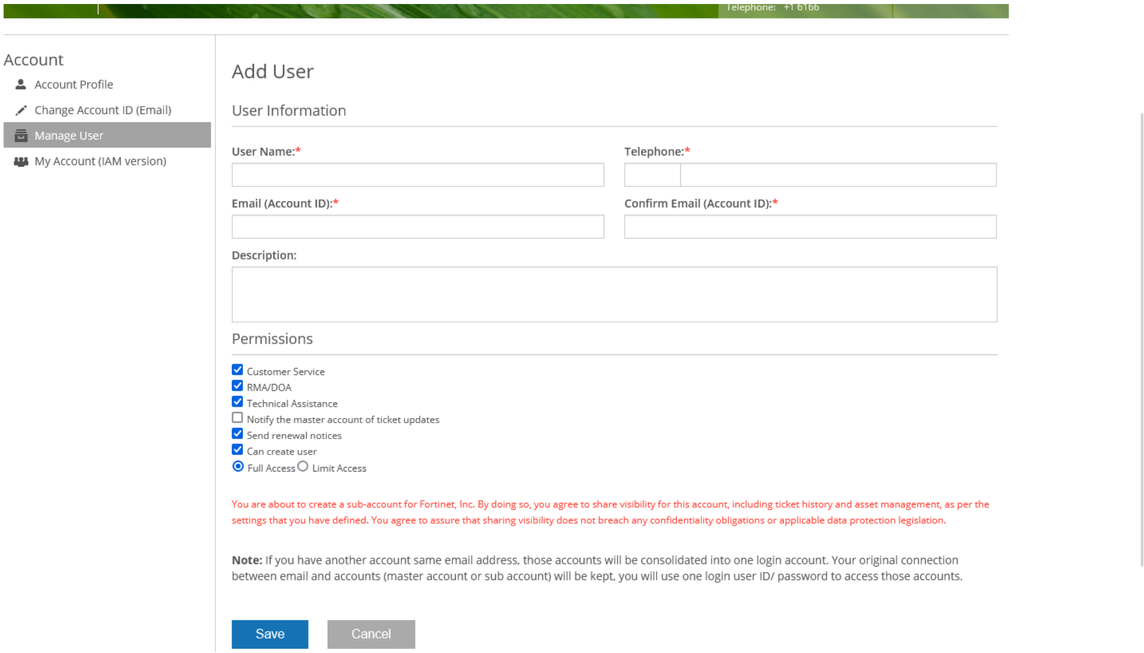
Account
- Account Profile
- Change Account ID (Email)
- Manage User
- My Account (IAM version)

Manage User

Current Users

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

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



Telephone: +1 6166

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

Add User

User Information

User Name:*

Telephone:*

Email (Account ID):*

Confirm Email (Account ID):*

Description:

Permissions

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

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

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

6. Log in to the personal FortiCare portal. Under FortiManager Cloud section, you will see an account listed as a secondary member.
7. Click the entry to expand the view.
   a. Click *Enter* to access the system via HTTPS.
   b. (Optional) Click *Download New Image* to get the latest firmware version.
8. Ask the new user to log in to FortiManager Cloud.

   After the new user logs in to FortiManager Cloud, the user is displayed on the *FortiManager* Cloud instance, and the administrator can modify the account. See Modifying a secondary account on page 27.

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

Modifying a secondary account

The new user must log in to FortiManager Cloud for the account to be displayed in the FortiManager 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 25.

To modify a secondary account:

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

Supporting IAM users and IAM API users

FortiManager 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 FortiManager Cloud.

For more information about using the IAM portal, see the *Identity & Access Management Administration Guide*.

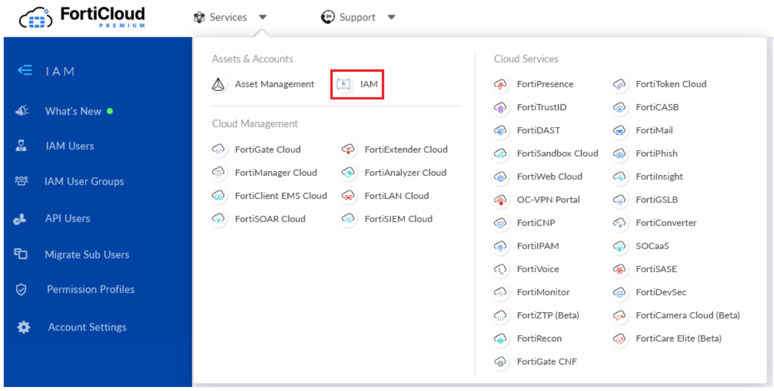
See also Adding IAM users on page 27 and Adding API users on page 29.

Adding IAM users

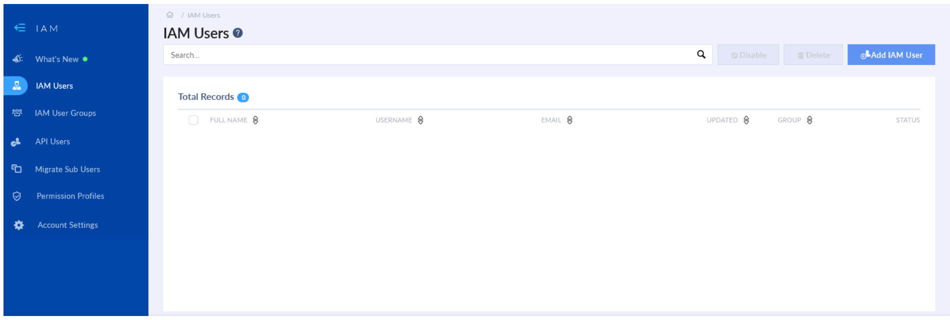
FortiManager Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiManager Cloud.

To add an IAM user:

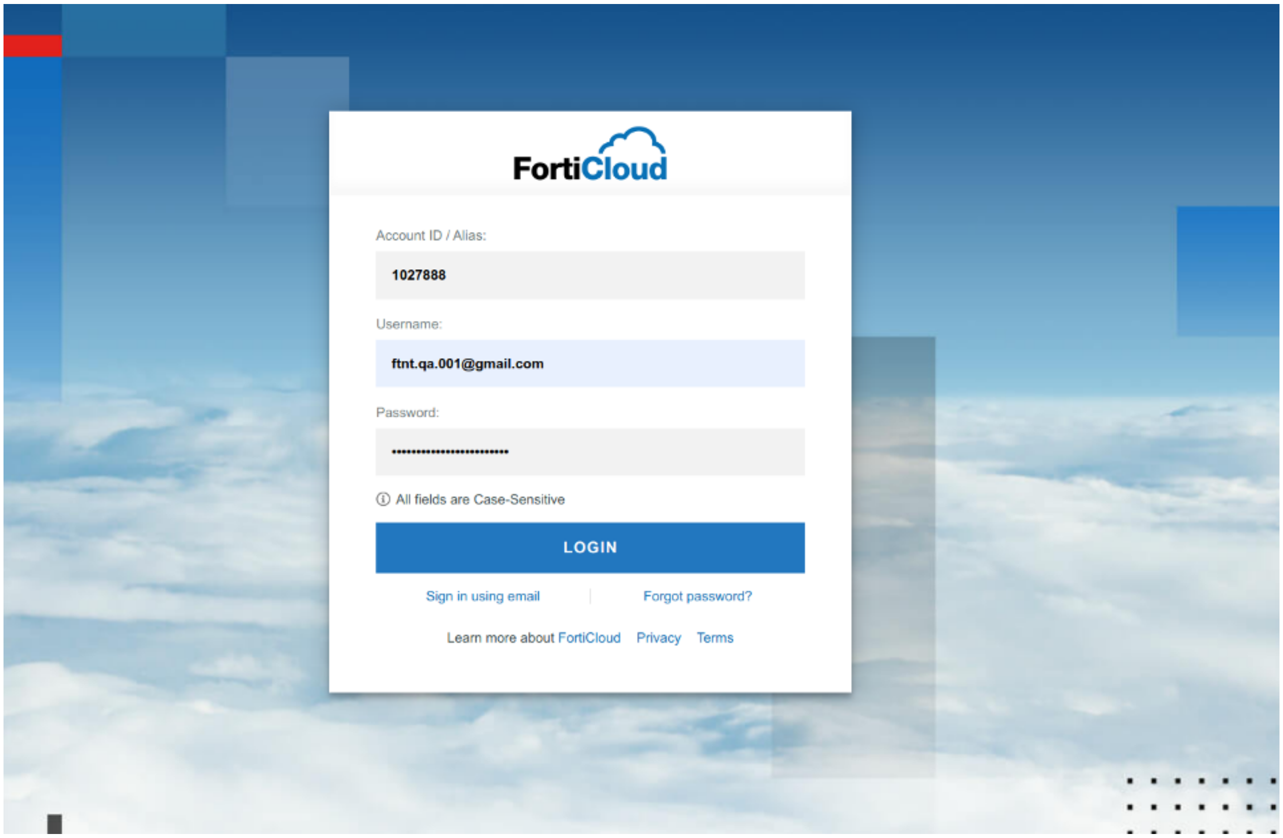
1. Go to FortiCloud (https://support.fortinet.com/), and log in.
2. From the *Services* menu, select *IAM* .



The *IAM portal* is displayed.



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



Account ID / Alias: 1027888

Username: ftnt.qa.001@gmail.com

Password: ••••••••••••••••••••••••

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

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

Adding API users

API users can access FortiCloud services through the API. API users can only use OAuth 2.0 for authentication.

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

Supporting external IdP users

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

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

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

www.fortinet.com