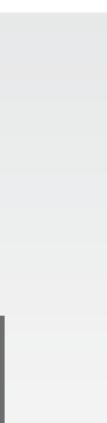
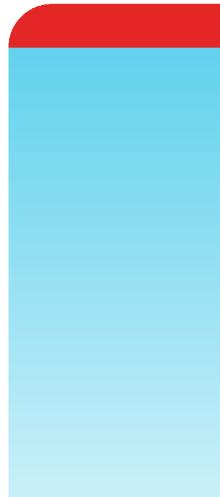


# Cloud Deployment Guide

**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](mailto:techdoc@fortinet.com)



October 1, 2024

FortiManager 7.4.x Cloud Deployment Guide

02-74-843404-20241001

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Requirements .....	5
Licensing .....	6
<b>Deploying FortiManager Cloud</b> .....	<b>7</b>
Checking requirements and licenses .....	7
Deploying a FortiManager Cloud instance .....	8
Configuring FortiOS .....	10
<b>Using FortiManager Cloud</b> .....	<b>12</b>
Accessing your FortiManager Cloud instance .....	12
Access FortiManager Cloud through FortiCloud .....	12
Upgrading firmware from the instance .....	13
Using the FortiManager Cloud toolbar .....	13
Service .....	14
Support .....	14
Notifications .....	14
Account .....	15
Privacy and notification preferences .....	15
Access Settings .....	16
Email Notifications .....	17
Updating the ADOM version .....	18
Enabling the FortiManager Cloud connector on FortiGate .....	19
Using FortiZTP with FortiManager Cloud .....	20
<b>Using the FortiManager Cloud &amp; Service portal</b> .....	<b>22</b>
Viewing the FortiManager Cloud portal .....	22
Providing feedback .....	24
<b>Using account services</b> .....	<b>25</b>
Adding a secondary account .....	25
Modifying a secondary account .....	27
Supporting IAM users and IAM API users .....	27
Adding IAM users .....	27
Adding API users .....	29
Supporting external IdP users .....	29
Using multiple roles with external IdP users .....	29

# Change Log

Date	Change Description
2023-09-19	Initial release.
2023-10-17	Updated <a href="#">Using FortiZTP with FortiManager Cloud on page 20</a> .
2023-01-30	Initial release of FortiManager Cloud 7.4.2.
2024-02-28	Updated <a href="#">Introduction on page 5</a> and <a href="#">Accessing your FortiManager Cloud instance on page 12</a> .
2024-06-06	Initial release of FortiManager Cloud 7.4.3.
2024-06-28	Added <a href="#">Privacy and notification preferences on page 15</a>
2024-07-02	Added <a href="#">Using multiple roles with external IdP users on page 29</a> .
2024-09-27	Initial release of FortiManager Cloud 7.4.4.

# 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 your FortiManager Cloud instance 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.

## To deploy FortiManager Cloud:

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 8](#).
3. (Optional) Upgrade FortiManager Cloud to the latest available cloud version. See [Upgrading firmware from the instance on page 13](#).
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 8](#).

## 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.



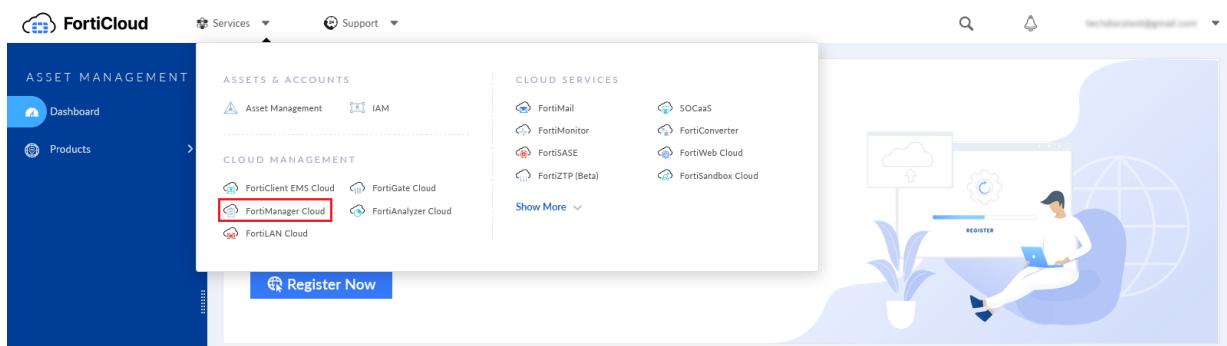
For support of FortiGates devices on earlier firmware versions, you can change the FortiManager Cloud ADOM version to match the firmware version of the FortiGates.

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 18](#).

### To deploy a FortiManager Cloud instance:

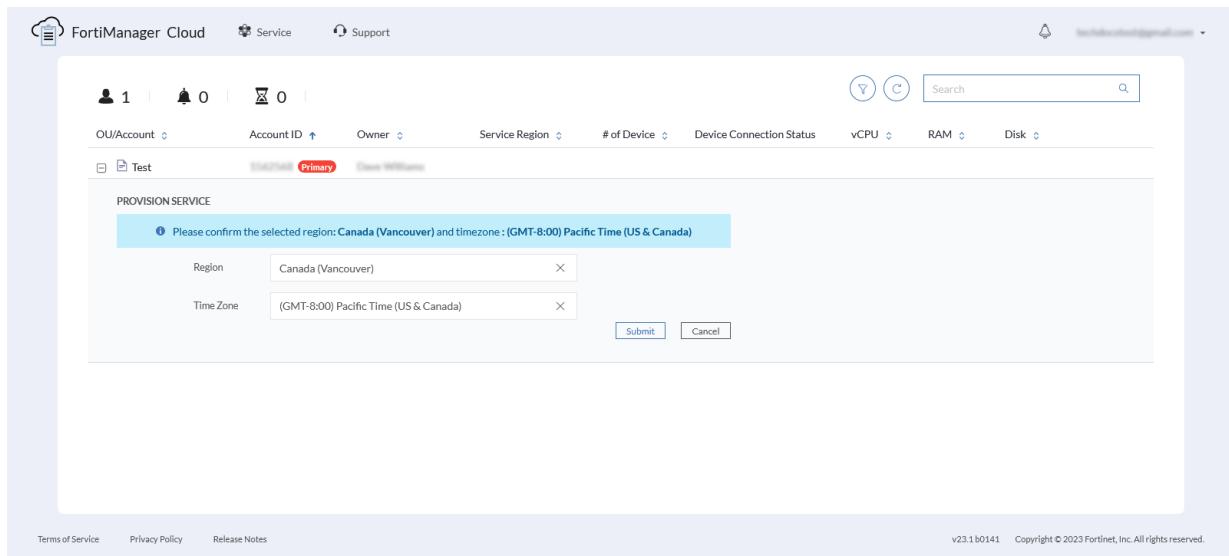
1. If not done already, go to FortiCloud (<https://support.fortinet.com/>), and use your FortiCloud account credentials to log in.  
The FortiCloud portal is displayed.
2. From the *Services* menu, select *FortiManager Cloud*.



The *FortiManager Cloud & Service* portal is displayed.

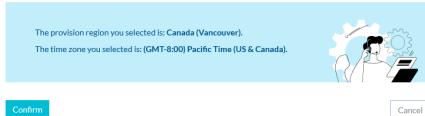
3. On the *FortiManager Cloud & Service* portal:
  - a. Select a *Region* for the FortiManager Cloud instance. In this example, the region is *Canada (Vancouver)*.
  - b. Select a *Time Zone* for the FortiManager Cloud instance.
4. Click *Submit*.

## Deploying FortiManager Cloud



The screenshot shows the FortiManager Cloud interface. At the top, there are navigation links for 'Service' and 'Support'. The main area shows a list of accounts with 'Test' selected. A modal window titled 'PROVISION SERVICE' is open, asking for confirmation of the selected region and time zone. The modal contains fields for 'Region' (set to 'Canada (Vancouver)') and 'Time Zone' (set to '(GMT-8:00) Pacific Time (US & Canada)'). It includes 'Submit' and 'Cancel' buttons. The bottom of the screen shows standard footer links for 'Terms of Service', 'Privacy Policy', and 'Release Notes', along with a copyright notice for Fortinet, Inc.

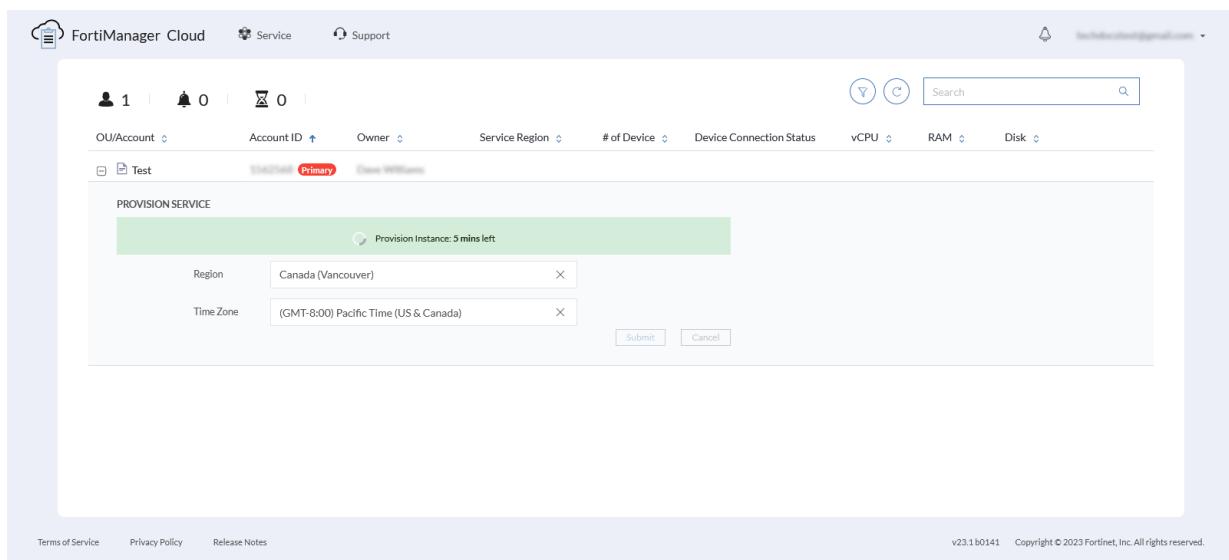
**5. Confirm your selected region and time zone.**



**6. Click *Submit*.**

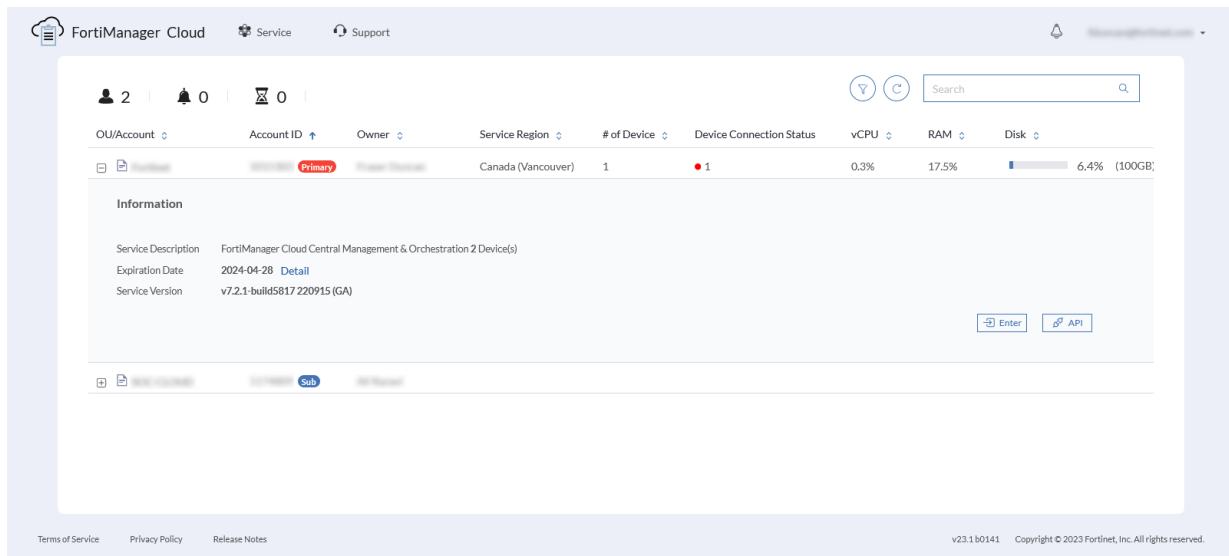
**7. Review and accept the *Terms of Service* and *Privacy Policy*. Privacy settings can be configured in the instance. See [Privacy and notification preferences on page 15](#).**

**8. FortiManager Cloud instance is provisioned in a few minutes.**



The screenshot shows the FortiManager Cloud interface. A modal window titled 'PROVISION SERVICE' is open, showing a green progress bar with the text 'Provision Instance: 5 mins left'. The modal contains fields for 'Region' (set to 'Canada (Vancouver)') and 'Time Zone' (set to '(GMT-8:00) Pacific Time (US & Canada)'). It includes 'Submit' and 'Cancel' buttons. The background shows a list of accounts with 'Test' selected.

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



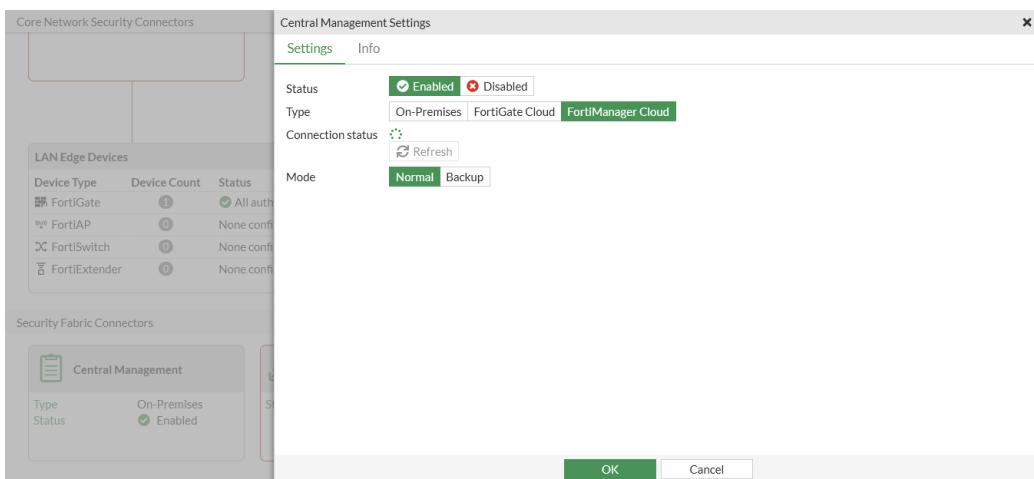
10. (Optional) Upgrade FortiManager Cloud to 7.4.x. See [Upgrading firmware from the instance on page 13](#).
11. Configure FortiOS to work with FortiManager Cloud. See [Configuring FortiOS on page 10](#).

## 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*.



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

## Deploying FortiManager Cloud

Device Manager

Device & Groups

Unauthorized Devices (1)

- FortiGateVM

Scripts

Provisioning Templates

Firmware Templates

Monitors

Search...

Authorize Hide Delete Display Hidden Devices

Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode
FortiGateVM	FortiGate-VM64	XXXXXXXXXX	10.10.0.209	FortiGate 7.2.4.build1394 (...	Configuration & Logging

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

Device Manager

Device & Groups

Managed FortiGate (1)

- FortiGateVM

Scripts

Provisioning Templates

Firmware Templates

Monitors

Search...

Edit Delete Import Configuration Install Table View More Show Charts Search...

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 (...	Disabled

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

Core Network Security Connectors

Role	Standalone	FortiAnalyzer	Status
		FortiAnalyzer Cloud	Disabled
			Enabled

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	Sandbox	Supported Connectors
Type: FortiManager Cloud Status: Enabled	Status: Disabled	

# 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:

- [Accessing your FortiManager Cloud instance on page 12](#)
- [Upgrading firmware from the instance on page 13](#)
- [Using the FortiManager Cloud toolbar on page 13](#)
- [Updating the ADOM version on page 18](#)
- [Enabling the FortiManager Cloud connector on FortiGate on page 19](#)
- [Using FortiZTP with FortiManager Cloud on page 20](#)

## Accessing your FortiManager Cloud instance

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

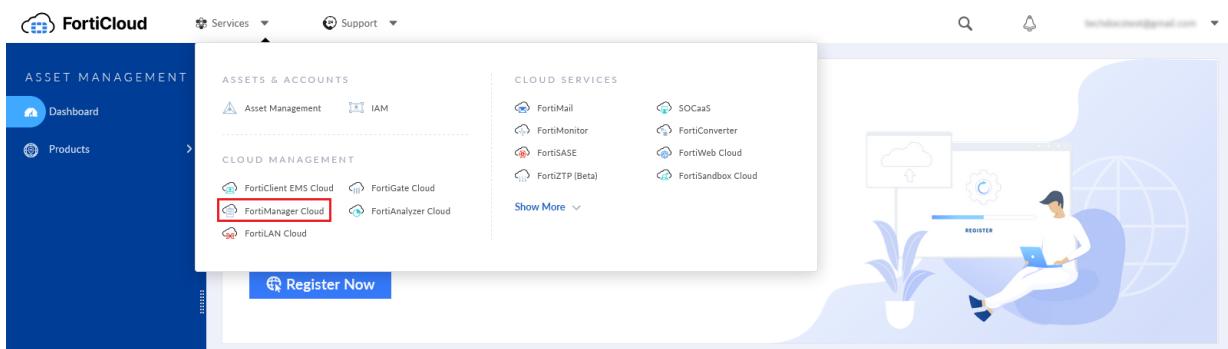
1. Go to <https://fortimanager.forticloud.com>. After authentication, you are redirected to your own FortiManager Cloud instance.
2. Go directly to your instance using the specific URL for your instance (e.g. `https://:{account_id}.{region}.fortimanager.forticloud.com`). You can obtain your instance's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

## Access FortiManager Cloud through FortiCloud

**To access FortiManager Cloud through FortiCloud:**

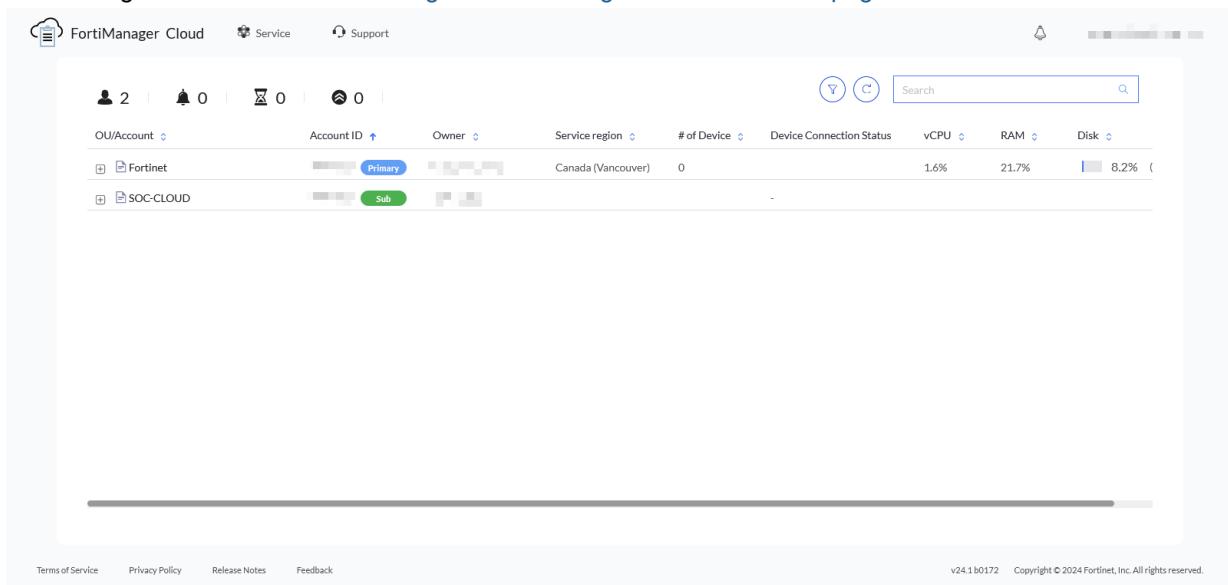
1. Go to FortiCloud (<https://support.fortinet.com/>), and use your FortiCloud account credentials to log in. The FortiCloud portal is displayed.

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



You are automatically logged in to your FortiManager instance.

3. 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 13](#).



## Upgrading firmware from the instance

For information about upgrading firmware, see the [FortiManager Cloud Release Notes](#).

## 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:

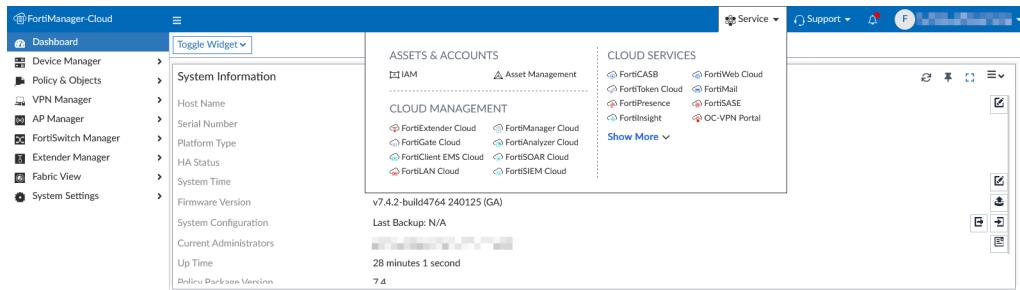
- [Service on page 14](#)
- [Support on page 14](#)

## Using FortiManager Cloud

- [Notifications on page 14](#)
- [Account on page 15](#)

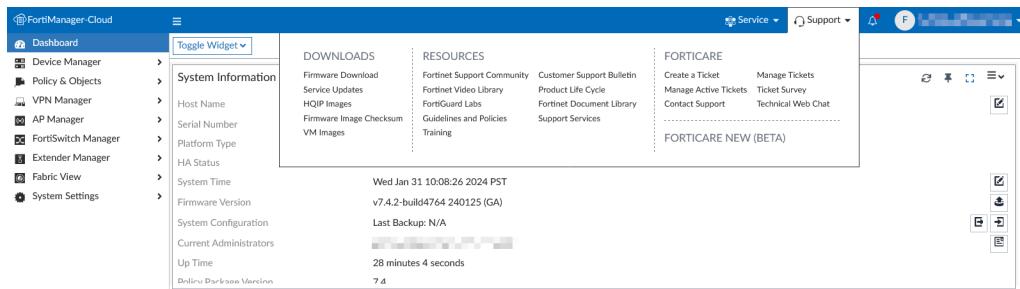
## Service

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



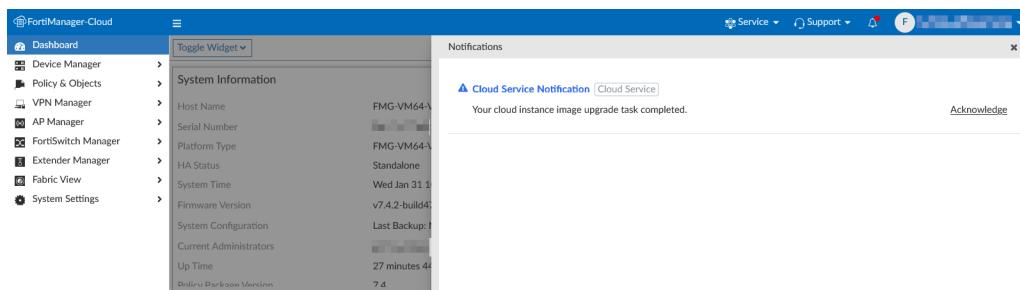
## Support

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



## Notifications

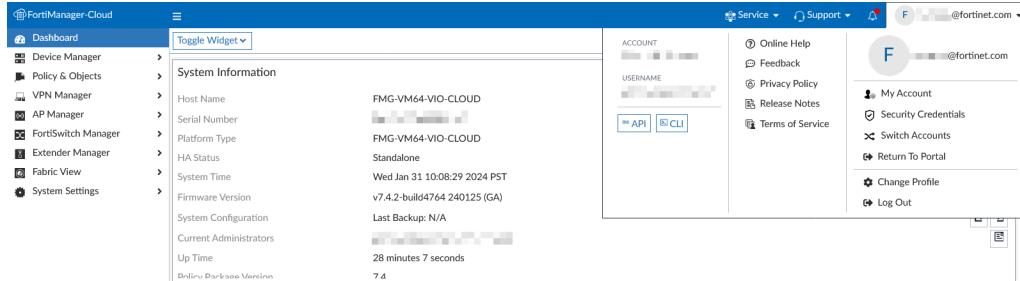
Click the notification icon  to open the notification drawer and view and interact with notifications for FortiManager Cloud.



## Account

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

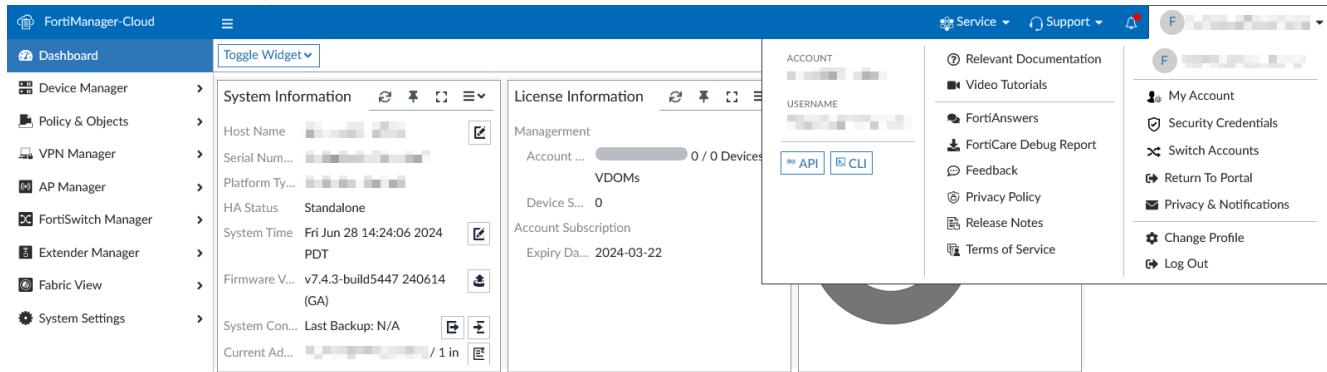
<b>Account</b>	Your account ID.
<b>Username</b>	Your current username.
<b>API and CLI</b>	Open the API User or CLI pane.
<b>Help Content</b>	Links for Online Help, Basic Setup Videos, Feedback, Privacy Policy, Release Notes, and Terms of Service.
<b>FortiCloud Account Links</b>	FortiCloud account links including My Account, Security Credentials, Subscriptions, Return to Portal, ChangeProfile, and Log Out.
<b>My Account</b>	Go to the FortiCloud Account Profile page.
<b>Security Credentials</b>	Go to the FortiCloud Security Credentials page.
<b>Switch Accounts</b>	Switch between available accounts.
<b>Return to Portal</b>	Return to the FortiManager Cloud portal.
<b>Change Profile</b>	Change FortiManager Cloud profile options including avatar and theme.
<b>Privacy &amp; Notifications</b>	Click to access the <i>Privacy &amp; Notification</i> menu where you can configure access settings for the FortiCloud team as well as email notification preferences. See <a href="#">Privacy and notification preferences on page 15</a> .
<b>Log Out</b>	Log out of FortiManager Cloud.



## Privacy and notification preferences

You can configure privacy and notification preferences from within the FortiManager Cloud instance.

To access your privacy and notification preferences, click your user account dropdown from the FortiManager Cloud toolbar and click *Privacy & Notification*.



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

- [Access Settings on page 16](#)
- [Email Notifications on page 17](#)

## Access Settings

Access settings determine what level of access Fortinet's cloud operation team has in order to diagnose and perform maintenance on your cloud instance. The following access levels are available:

A screenshot of the 'Privacy &amp; Notifications' page. The 'Access Settings' section contains three radio buttons: 'Service Maintenance (Recommended)', 'Full Access', and 'No Access'. Each option has a description below it. The 'Service Maintenance (Recommended)' option is selected. The 'Full Access' and 'No Access' options are also shown with their descriptions.

### Service Maintenance (Recommended)

Fortinet's cloud operation team can access diagnostic data and perform maintenance operations on your cloud instance. However, they only have access to system-level data and do not access personal data like logs, reports, or device configurations. This level ensures the smooth operation of services.

### Full Access

Fortinet personnel can access your account with full privileges for support services, including personal data such as logs, reports, and device configurations for troubleshooting.

### No Access

The most restrictive control, where Fortinet personnel has no access to your cloud instance. With no access, the cloud operation team cannot access diagnostic data or perform maintenance tasks, and the smooth operation of the service cannot be guaranteed when this level is selected.

### Full Access

Fortinet personnel can access your account with full privileges for support services, including personal data such as logs, reports, and device configurations for troubleshooting.

**No Access**

The most restrictive control, where Fortinet personnel has no access to your cloud instance. With no access, the cloud operation team cannot access diagnostic data or perform maintenance tasks, and the smooth operation of the service cannot be guaranteed when this level is selected.

Select your preferred access level and click **OK**.

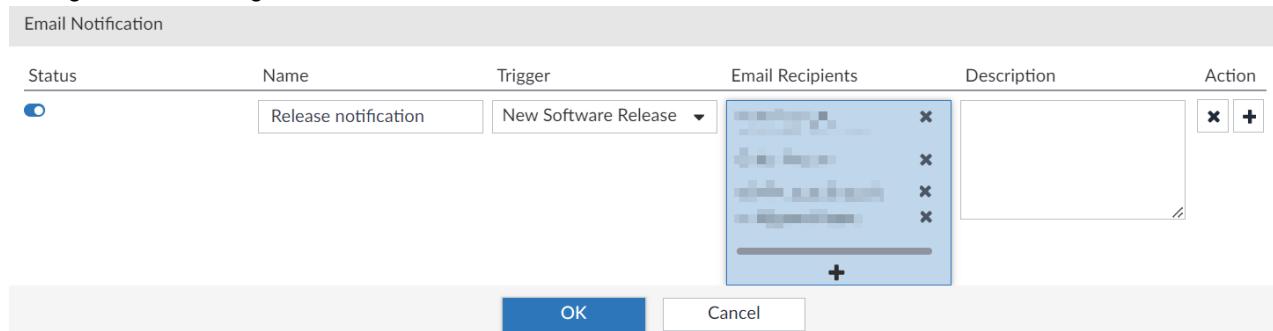
FortiManager Cloud records changes to access settings in the *Event Log*.

## Email Notifications

Email notification preferences can be configured through your FortiManager instance.

### To configure email notification preference:

1. Select your account dropdown from the FortiManager Cloud toolbar.
2. Select *Privacy & Notifications*.
3. Click the add icon in the *Email Notification* section to configure new email notification preferences.
4. Configure the following:



<b>Status</b>	Toggle the notification preference on or off. Notifications are only sent when the status of the notification preference is enabled.
<b>Name</b>	Enter a name for the notification preference.
<b>Trigger</b>	Select a trigger condition from the dropdown menu.
<b>Email Recipients</b>	Click to add at least one email recipient. You can select IAM/Sub users from the populated list or click the <i>Email Address</i> tab to add additional emails.
<b>Description</b>	Add an optional description.
<b>Action</b>	You can use the action field to delete a notification preference or create additional notifications preferences.

5. Click **OK**.

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

## 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.

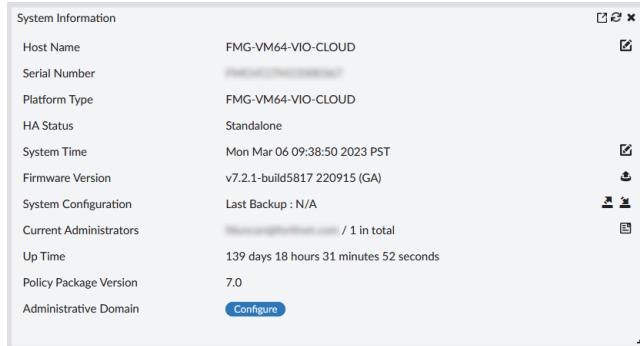
You can view the ADOM version on the *System Settings > Dashboard* pane in the *System Information* widget.

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 your FortiManager Cloud instance 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.



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 your FortiManager Cloud instance 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
  account_id=[user_email] company=[company_name] industry=[industry_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	Status
	FortiAnalyzer FortiAnalyzer Cloud <span style="color: green;">Enabled</span>	<span style="color: red;">✖</span> Disabled

**LAN Edge Devices**

Device Type	Device Count	Status
FortiGate	1	<span style="color: green;">✓</span> All authorized & registered
FortiAP	0	None configured
FortiSwitch	0	None configured
FortiExtender	0	None configured

**Security Fabric Connectors**

Central Management	Sandbox	Supported Connectors
Type Status	FortiManager Cloud <span style="color: green;">✓</span> Enabled	<span style="color: red;">✖</span> Disabled



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

## Using FortiZTP with FortiManager Cloud

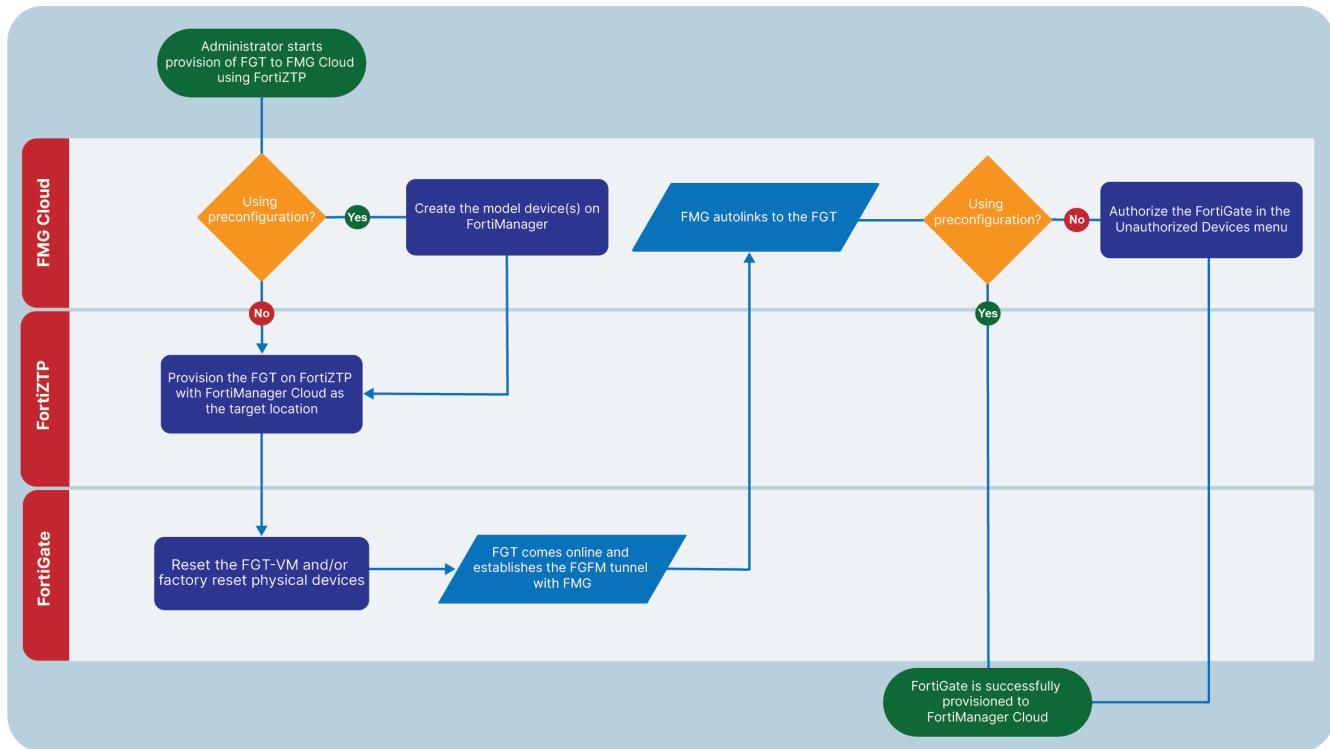
FortiZTP is a centralized zero-touch provisioning platform for FortiCloud cloud product services. The service supports individual or bulk device provisioning to the target on-premise or cloud services, including FortiManager Cloud.

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:

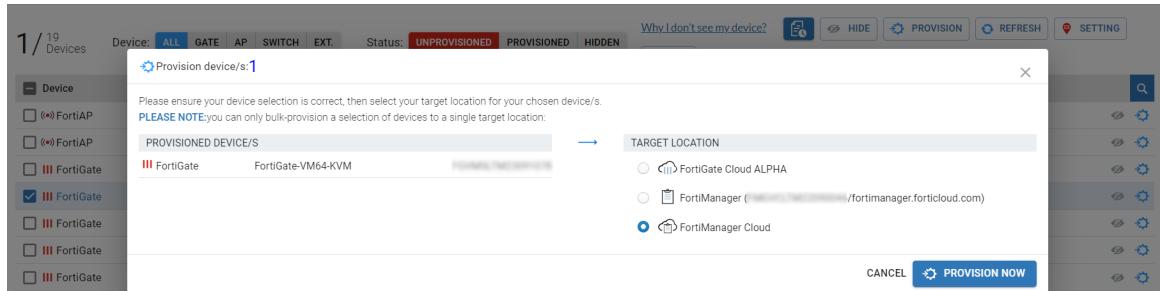
Workflow diagram for using FortiZTP with FortiManager Cloud



### To provision a FortiGate to FortiManager Cloud:

- (Optional) Create the model device on FortiManager Cloud when using the preconfiguration method.
- 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*.



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 the FortiManager Cloud & Service portal

After deploying a FortiManager Cloud instance, you can use the FortiManager Cloud & Service portal to view and navigate between instances.

- [Viewing the FortiManager Cloud portal on page 22](#)
- [Providing feedback on page 24](#)

## Viewing the FortiManager Cloud portal

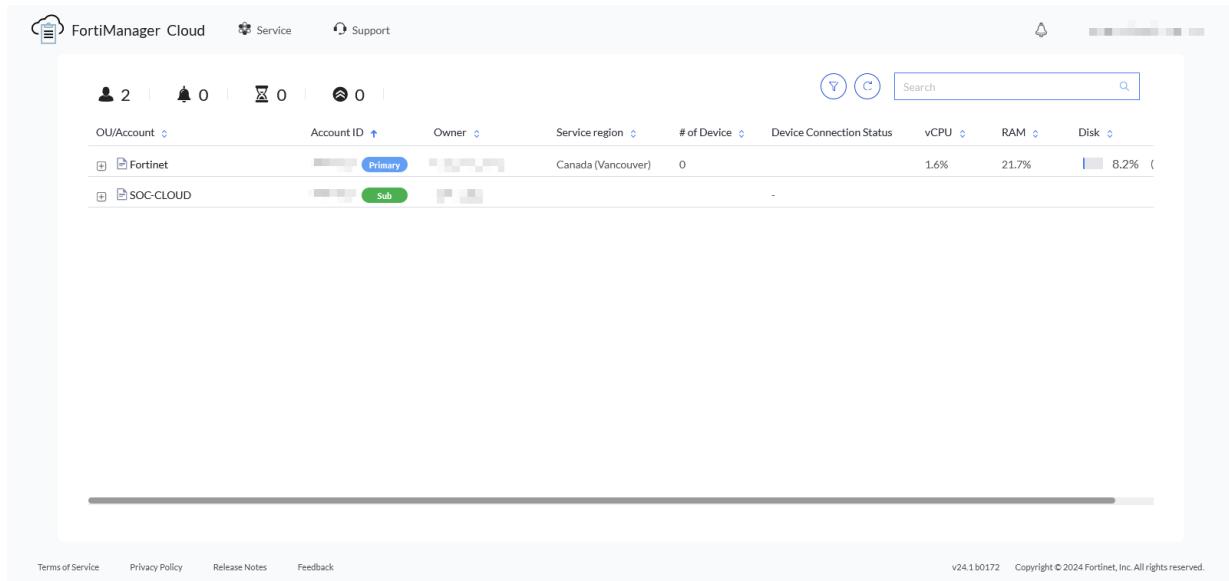
After accessing your FortiManager Cloud instance, you can navigate to the FortiManager Cloud portal by opening the toolbar and choosing *Return to Portal*. See [Using the FortiManager Cloud toolbar on page 13](#).

In the FortiManager Cloud 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 your FortiManager Cloud instance on page 12](#).

The FortiManager Cloud & Service portal is displayed.



The screenshot shows the FortiManager Cloud & Service portal interface. At the top, there are three tabs: 'FortiManager Cloud' (selected), 'Service', and 'Support'. Below the tabs, there are four status indicators: 'OU/Account 2', 'Account ID 0', 'Owner 0', and 'Service region 0'. To the right of these are 'Device Connection Status', 'vCPU 1.6%', 'RAM 21.7%', and 'Disk 8.2%'. A search bar with a magnifying glass icon is positioned above the main table. The main table has columns for 'OU/Account', 'Account ID', 'Owner', 'Service region', 'Device Connection Status', 'vCPU', 'RAM', and 'Disk'. It lists two accounts: 'Fortinet' (Primary) and 'SOC-CLOUD' (Sub). The 'Fortinet' account is located in 'Canada (Vancouver)' with 0 devices. The 'SOC-CLOUD' account is also in 'Canada (Vancouver)' with 0 devices. At the bottom of the page, there are links for 'Terms of Service', 'Privacy Policy', 'Release Notes', and 'Feedback', along with a copyright notice: 'v24.1b0172 Copyright © 2024 Fortinet, Inc. All rights reserved.'

2. Expand an account with no instances deployed.

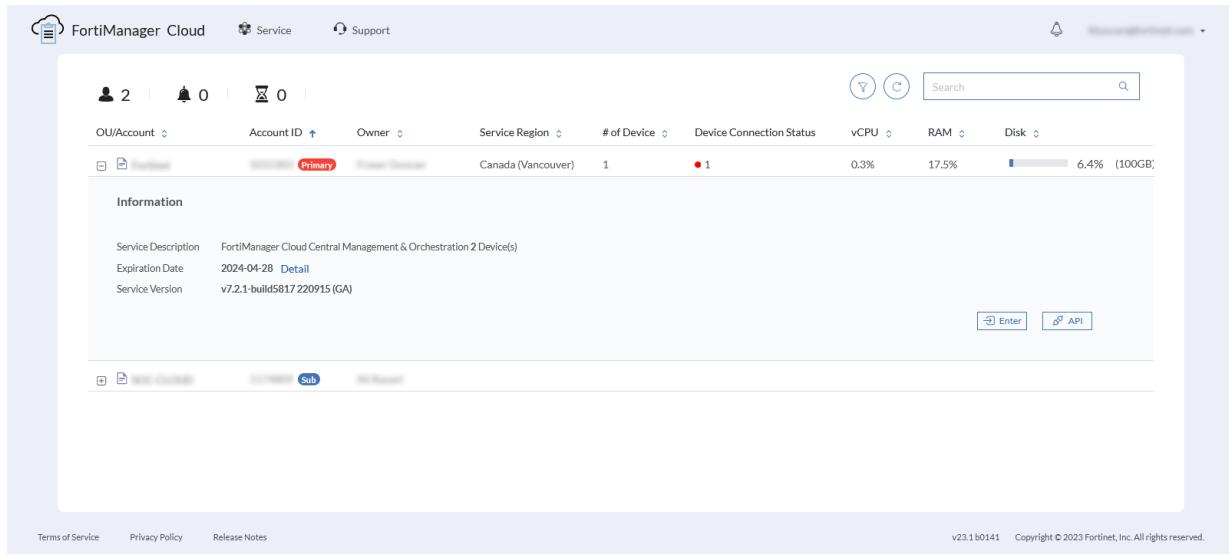
The account details are displayed. If it is a primary account, you can provision a new instance. See [Deploying a FortiManager Cloud instance on page 8](#).

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.



The following options are displayed:

<b>Dashboard</b>	The top-left includes a dashboard summary of the accounts displayed on the pane: <ul style="list-style-type: none"> <li><b>Accounts:</b> Displays the number of accounts you can access.</li> <li><b>Alarms:</b> 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.</li> <li><b>Expiring:</b> Displays the number of licenses that will expire soon.</li> </ul>
<b>Filter</b>	Click to view options to filter by license status and quota/storage alarm.
<b>Refresh</b>	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.
<b>Account Search</b>	Use to search for accounts. In the <i>Search</i> box, type search criteria, and press <i>Enter</i> . Delete the search criteria, and press <i>Enter</i> to display all accounts again.
<b>Accounts summary in table view</b>	Each account displays as a row with the following columns: <ul style="list-style-type: none"> <li><b>OU/Account:</b> The OU/Account this instance is configured for.</li> <li><b>Account ID:</b> The account ID.</li> <li><b>Owner:</b> The name of the owner.</li> <li><b>Service Region:</b> The region where the instance is deployed.</li> <li><b># of Device:</b> The number of devices connected to the instance.</li> <li><b>Device Connection Status:</b> The status of connected devices.</li> <li><b>vCPU</b></li> <li><b>RAM</b></li> <li><b>Disk</b></li> </ul> Expand the pane to view additional information: <ul style="list-style-type: none"> <li><b>Service Description:</b> A short description of the FortiManager Cloud service.</li> <li><b>Expiration Date:</b> The license expiration date.</li> </ul>

- **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 the FortiManager Cloud portal on page 22](#).

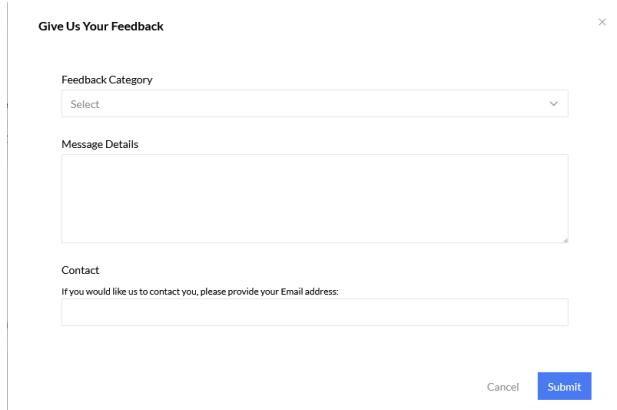
## Providing feedback

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 13](#).

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:

Cancel Submit

# 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. By 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.

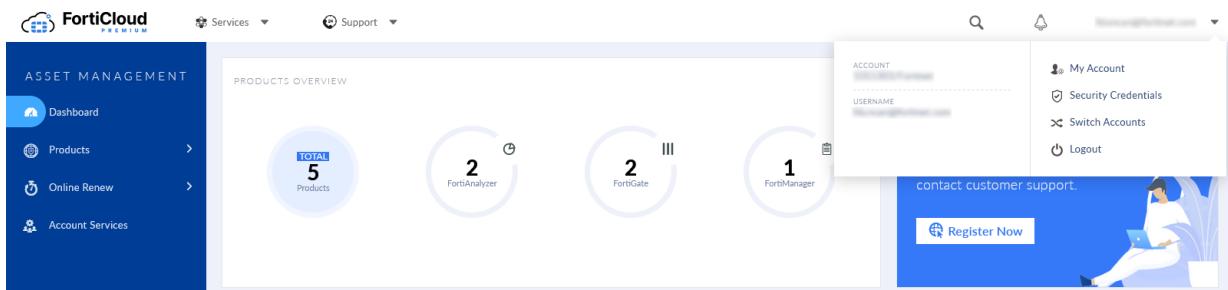
A secondary account allows the Fortinet support team to troubleshoot the FortiManager Cloud deployment.



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.

The screenshot shows the FortiCloud account management interface. At the top, there are navigation links for 'Services' and 'Support', and a search bar. The main area is titled 'Manage User' and shows a list of 'Current Users'. On the left, a sidebar has 'Manage User' selected. At the top right, account details are displayed: Company: Fortinet, Title: Manager, Email: muncar@fortinet.com, Telephone: 1015303, and Activated Since: 2020-02-19.

- 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.

The screenshot shows the 'Add User' form. The left sidebar has 'Manage User' selected. The main form has 'User Information' and 'Permissions' sections. In the 'User Information' section, fields include 'User Name' (mandatory), 'Telephone' (mandatory), 'Email (Account ID)' (mandatory), and 'Confirm Email (Account ID)' (mandatory). In the 'Permissions' section, checkboxes are checked for 'Customer Service', 'RMA/DOA', and 'Technical Assistance', and 'Can create user'. A note at the bottom states: '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.' A note below that says: '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.' At the bottom are 'Save' and 'Cancel' buttons.

- Log in to the personal FortiCare portal. Under FortiManager Cloud section, you will see an account listed as a secondary member.
- Click the entry to expand the view.
  - Click *Enter* to access the system via HTTPS.
  - (Optional) Click *Download New Image* to get the latest firmware version.
- 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](#).

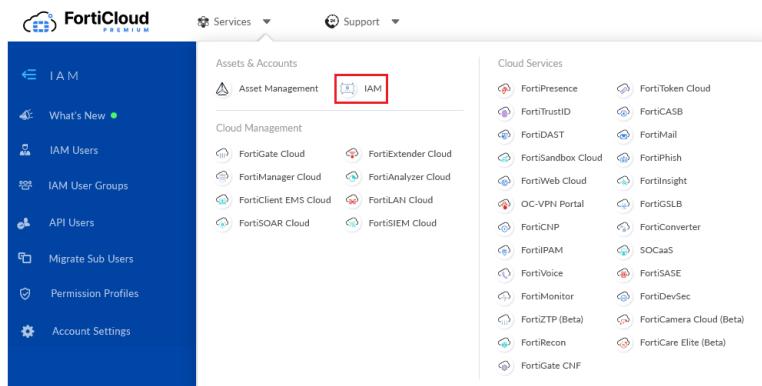
See also [Adding IAM users on page 27](#) and [Adding API users on page 29](#).

## Adding IAM users

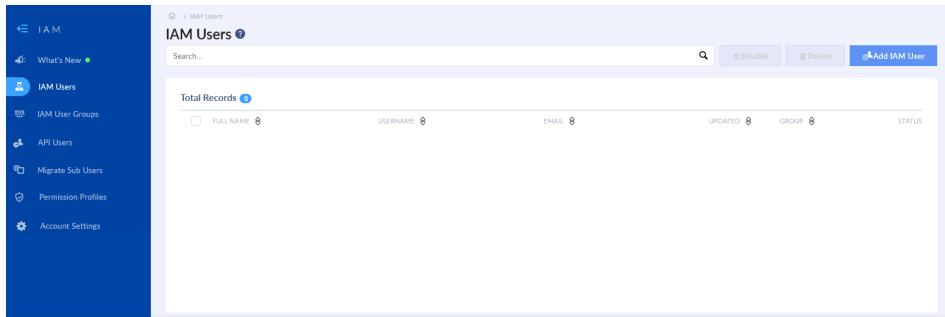
FortiManager Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiManager Cloud.

### 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.

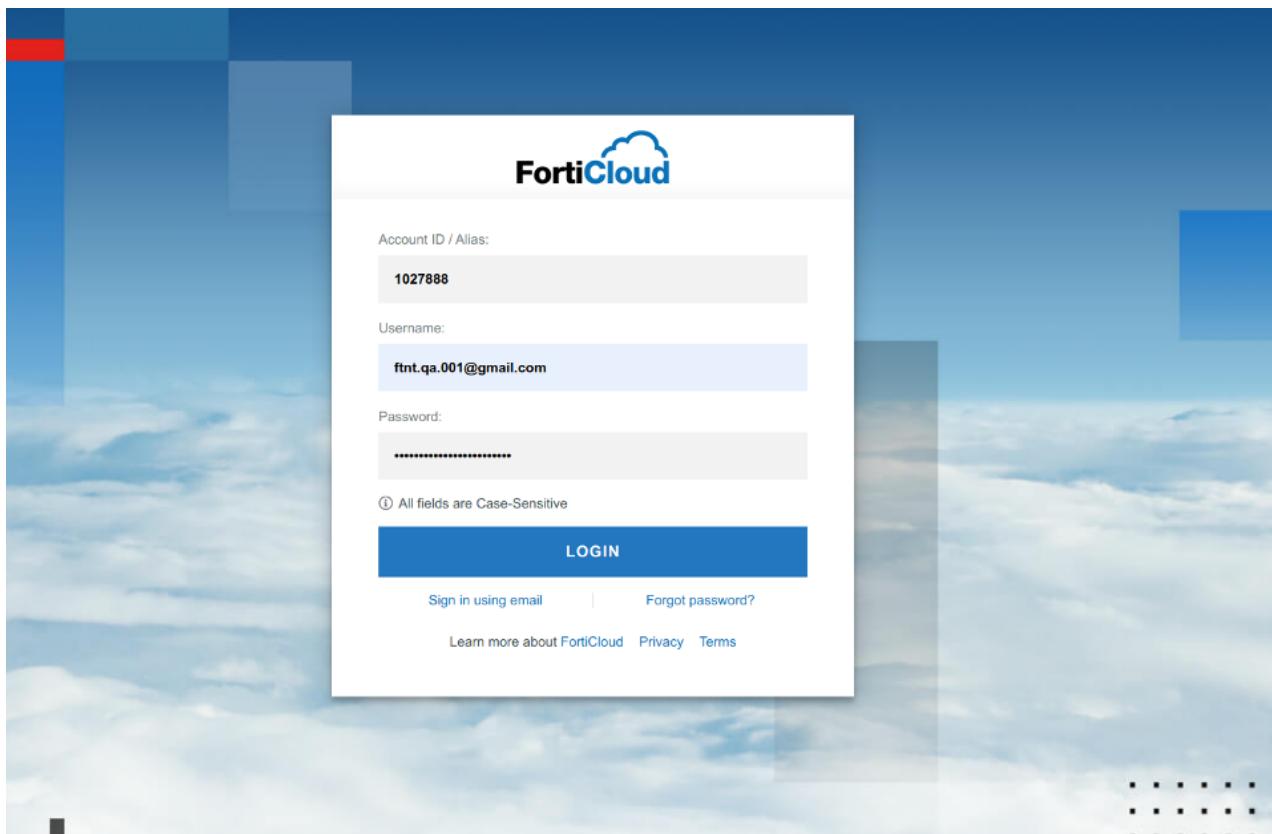
### 4. Add an IAM user group, and add the user to it.

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.



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
<b>Admin</b>	Assigned to the <i>Super_User</i> admin profile.
<b>Read-Write</b>	Assigned to the <i>Standard_User</i> admin profile.
<b>Read-Only</b>	Assigned to the <i>Restricted_User</i> admin profile.
<b>Custom</b>	<i>Custom</i> users are assigned to the <i>Restricted_User</i> admin profile the first time they log in. A <i>Super_User</i> 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.

## Using multiple roles with external IdP users

For more information on external IdP users for FortiCloud, see [External IdP roles](#).

### Logging in as an external IdP user with multiple roles:

1. When logging in as an IdP user that has multiple roles, the account selection page is displayed allowing users to select which instance to access.

## Using account services

External IdP users can have multiple roles assigned to a single FortiManager Cloud instance.

Welcome Back!

FEDERATED LOGIN  
fazcloud\_fac

USERNAME  
idp-multi1



### Select a Role to Proceed

Search an OU or account

ACCOUNT ID	COMPANY	ROLE NAME
1691225	Faz	idp_admin
1691225	Faz	idp_custom
1691225	Faz	idp_readwrite
1691226	Faz	idp_admin
1691226	Faz	idp_custom
1691228	Faz	idp_admin
1691228	Faz	idp_readwrite

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

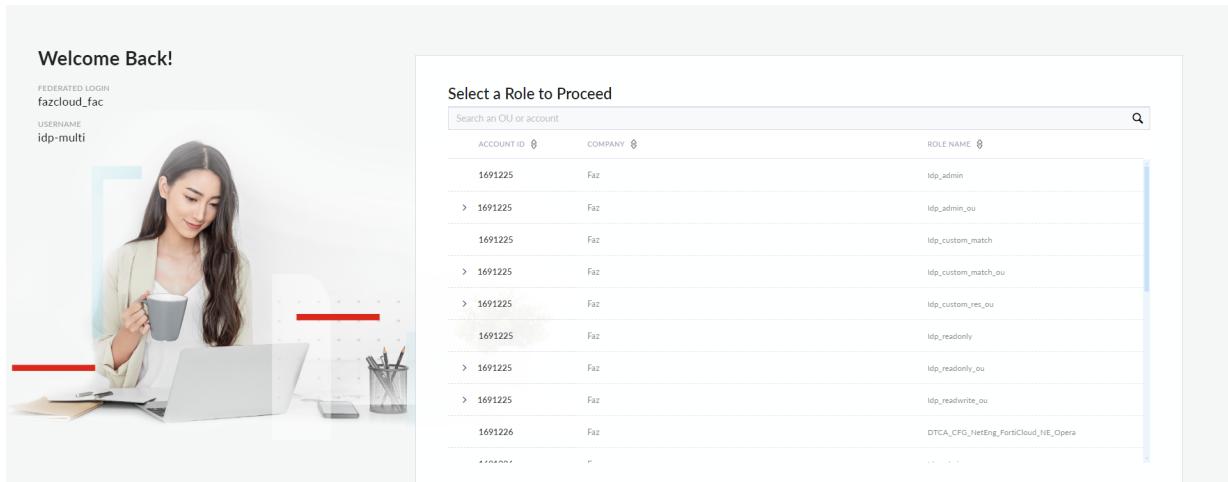
The screenshot shows the FortiAnalyzer-Cloud interface. The top navigation bar includes 'Add Device', 'Device Group', 'Service', 'Support', and a user dropdown for 'idp-multi1@fazcloud\_fac'. The left sidebar has sections for 'Device Manager', 'FortiView', 'Log View', 'Fabric View', 'Incidents & Events', and 'Reports'. The main content area displays a green circular status summary for '20 Devices' with 'Up' status and 20 entries. Below it is a grey circular summary for '400 GB' with a small red segment. A table lists 10 devices, all identified as 'FortiGate-VM64' with 'FortiGate 5.0' firmware, showing 'Up' status and '0 minutes' since the last log. The right sidebar provides links to 'Relevant Documentation', 'Video Tutorials', 'FortiAnswers', 'Feedback', 'Privacy Policy', 'Release Notes', and 'Terms of Service', along with account management options like 'My Account', 'Switch Roles', 'Return To Portal', 'Privacy & Notifications', 'Change Profile', and 'Log Out'.

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

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

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

## Using account services



Welcome Back!

FEDERATED LOGIN  
fazcloud\_fac

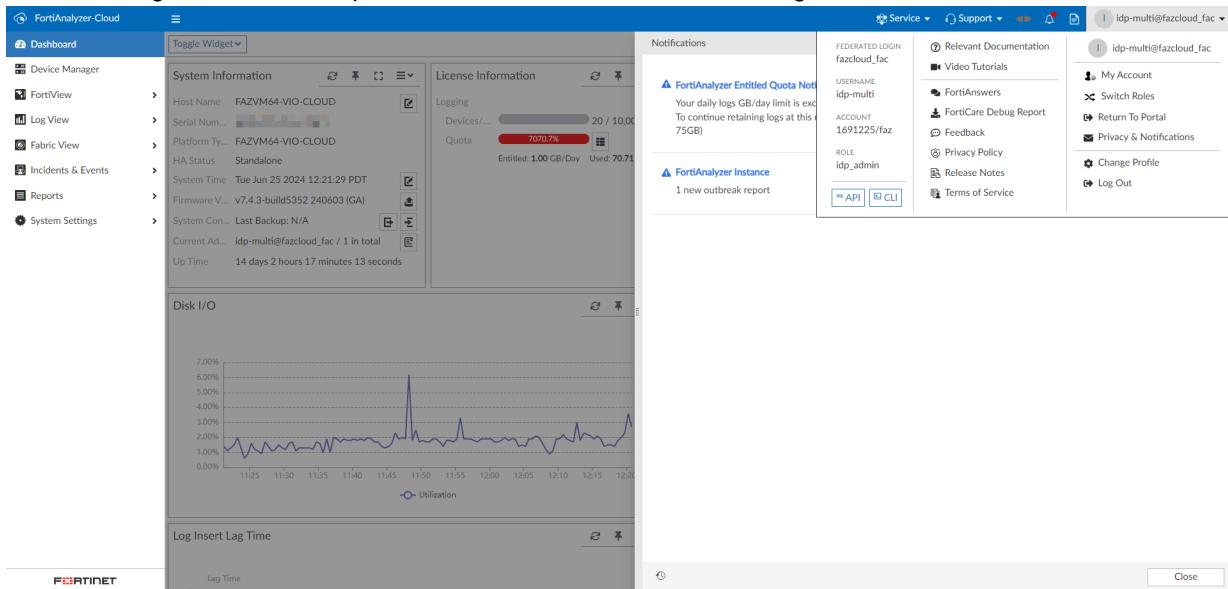
USERNAME  
idp-multi

Select a Role to Proceed

Search an OU or account

ACCOUNT ID	COMPANY	ROLE NAME
1691225	Faz	idp_admin
> 1691225	Faz	idp_admin_ou
1691225	Faz	idp_custom_match
> 1691225	Faz	idp_custom_match_ou
> 1691225	Faz	idp_custom_res_ou
1691225	Faz	idp_READONLY
> 1691225	Faz	idp_READONLY_ou
1691226	Faz	idp_readwrite
		DTCA_CFG_NetEng_FortiCloud_NF_Opera

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



FortiAnalyzer-Cloud

Dashboard

System Information

- Host Name: FAZVM64-VIO-CLOUD
- Serial Num.: [REDACTED]
- Platform Type: FAZVM64-VIO-CLOUD
- HA Status: Standalone
- System Time: Tue Jun 25 2024 12:21:29 PDT
- Firmware Ver.: v7.4.3-build5352 240603 (GA)
- System Configuration: Last Backup: N/A
- Current Adm.: idp-multi@fazcloud\_fac / 1 in total
- Up Time: 14 days 2 hours 17 minutes 13 seconds

License Information

Logging

Devices: 20 / 10.00

Quota: 7070.7% (Entitled: 1.00 GB/Day, Used: 70.71 GB)

Notifications

FortiAnalyzer Entitled Quota Note

Your daily logs GB/day limit is exceeded. To continue retaining logs at this rate, you must increase your quota (75GB).

FortiAnalyzer Instance

1 new outbreak report

FEDERATED LOGIN  
fazcloud\_fac

USERNAME  
idp-multi

ACCOUNT  
1691225/faz

ROLE  
idp\_admin

API CLI

Disk I/O

Log Insert Lag Time

Fortinet

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

The screenshot shows the FortiAnalyzer-Cloud dashboard with various monitoring and configuration panels. A modal window titled 'OU/Account' is open, showing a hierarchical list of OUs and accounts. The tree structure includes 'faz' and 'fazmulti' under the 'faz' OU, and several other OUs like 'FAZ-Cloud-Root' and 'Root-OU-2'.

### 4. Click *Switch Roles* or *Return To Portal* to return to the FortiManager Cloud role selection page. On the role selection page, you can select another role or OU to use for login.

The screenshot shows the FortiManager Cloud role selection page. The sidebar includes a user icon, the message 'Welcome Back!', and the text 'FEDERATED LOGIN fazcloud\_fac' and 'USER NAME: idp-multi'. The main panel is titled 'Make a Selection to Proceed' and contains a search bar and a list of accounts and OUs, including 'faz' and 'fazmulti' under 'faz'.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.