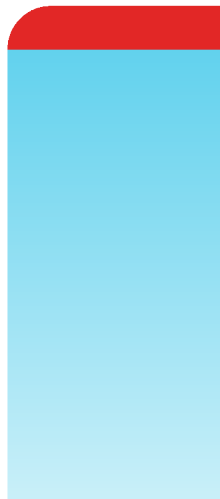


Cloud Deployment Guide

FortiManager 7.0.x



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



July 19, 2023

FortiManager 7.0.x Cloud Deployment Guide

02-70x-743809-20230719

TABLE OF CONTENTS

Change Log	4
Introduction	5
Requirements	5
Licensing	5
Deploying FortiManager Cloud	7
Checking requirements and licenses	7
Deploying a FortiManager Cloud instance	7
Configuring FortiOS	9
Using the FortiManager Cloud & Service portal	12
Accessing the portal and instances	12
Using Map View	14
Viewing information about instances	15
Upgrading firmware from the portal	16
Using FortiManager Cloud	18
Upgrading firmware from System Settings	18
Identifying the public IP address	18
Updating the ADOM version	19
Enabling the FortiManager Cloud connector on FortiGate	20
Using FortiZTP with FortiManager Cloud	21
Using account services	23
Adding a secondary account	23
Modifying a secondary account	25
Supporting IAM users and IAM API users	25
Adding IAM users	25
Adding API users	27

Change Log

Date	Change Description
2021-09-09	Initial release.
2021-10-13	Updated to remove mention of 360 Bundle.
2021-11-30	Added Enabling the FortiManager Cloud connector on FortiGate on page 20 .
2022-01-07	Added Adding IAM users on page 25 .
2022-02-25	Added Adding API users on page 27 .
2022-02-28	Added support for FortiZTP. See Using FortiZTP with FortiManager Cloud on page 21 .
2022-11-17	Updated Requirements on page 5 and Licensing on page 5 .
2023-07-19	Updated Licensing on page 5 .
2023-12-18	Updated Checking requirements and licenses on page 7 . Updated Updating the ADOM version on page 19 .

Introduction

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

Once FortiGate has acquired the required license, FortiCloud can be used to create a FortiManager instance under the user account. You can launch the portal for the cloud-based FortiManager from FortiCloud, and its URL starts with the User ID.

You can use a FortiGate with a required license to configure central management by using the FQDN of *FortiManager.forticloud.com*. A FortiGate-FortiManager tunnel is established between FortiGate and the FortiManager instance.

After the tunnel is established, you can execute FortiManager functions from the cloud-based FortiManager instance.

This section includes the following topics:

- [Requirements on page 5](#)
- [Licensing on page 5](#)

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 23](#).



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

See [Licensing on page 5](#) 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:

- FortiManager Cloud: Cloud-based Central Management & Orchestration Service.

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. On FortiCloud, check requirements and licenses. 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](#).

By default, FortiManager Cloud version 7.0.x is deployed. You can upgrade to later versions. See [Upgrading firmware from the portal on page 16](#).

3. On FortiOS, enable management by FortiManager Cloud. See [Configuring FortiOS on page 9](#).



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 license for the registered FortiGate units include a FortiManager Cloud entitlement:
 - a. Go to *Products > Product List*.
 - b. In the *View Options menu*, select *Group by Category*, and click *Apply*. The *Product List* is displayed by categories, such as *FortiGate*.
 - c. Expand the *FortiGate* category to confirm that its license 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 23](#).

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.



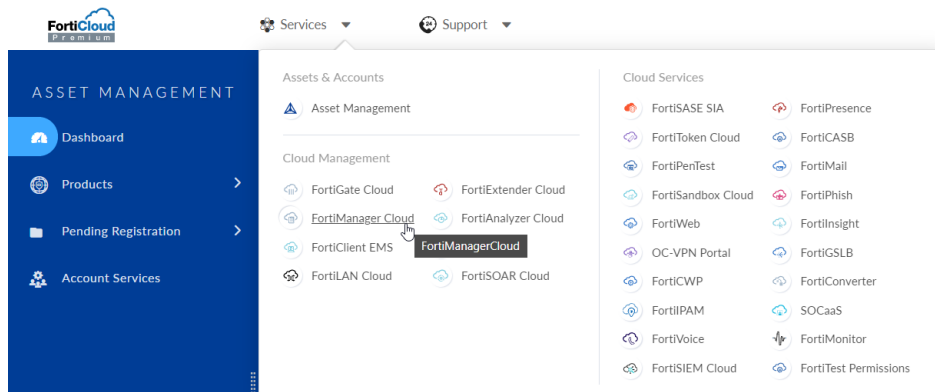
For support of FortiGate devices on earlier firmware versions, you can change the FortiManager Cloud ADOM version to match the firmware version of the FortiGates.

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 19](#).

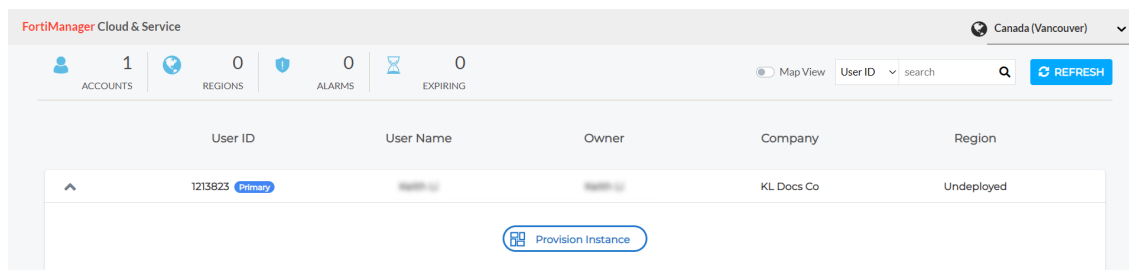
To deploy a FortiManager Cloud instance:

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.

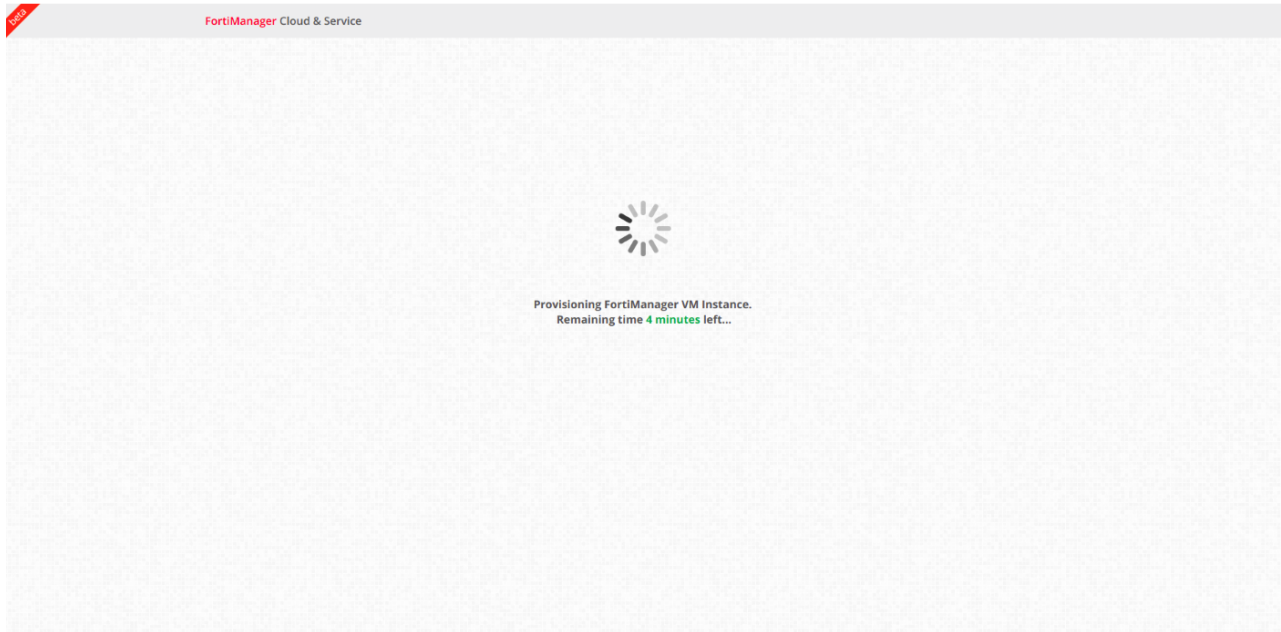
3. On the *FortiManager Cloud & Service* portal, select a region for the FortiManager Cloud instance from the top-right corner.
In the examples in this section, the *Canada (Vancouver)* region is selected.
4. Expand the primary account that includes the FortiManager Cloud entitlement, and click *Provision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



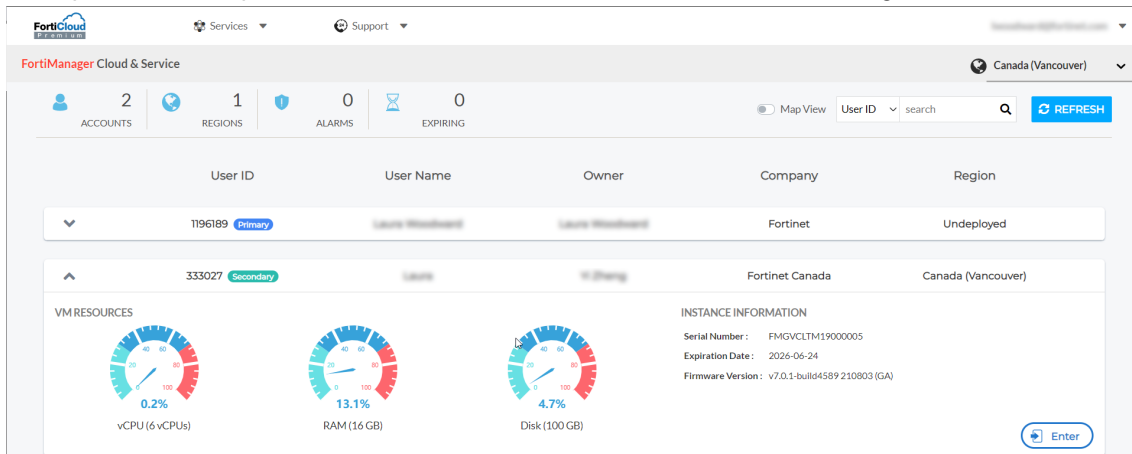
A message about the selected region is displayed.

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

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



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



- (Optional) Upgrade FortiManager Cloud to 7.0.x. See [Upgrading firmware from the portal on page 16](#).
- Configure FortiOS to work with FortiManager Cloud. See [Configuring FortiOS on page 9](#).

Configuring FortiOS

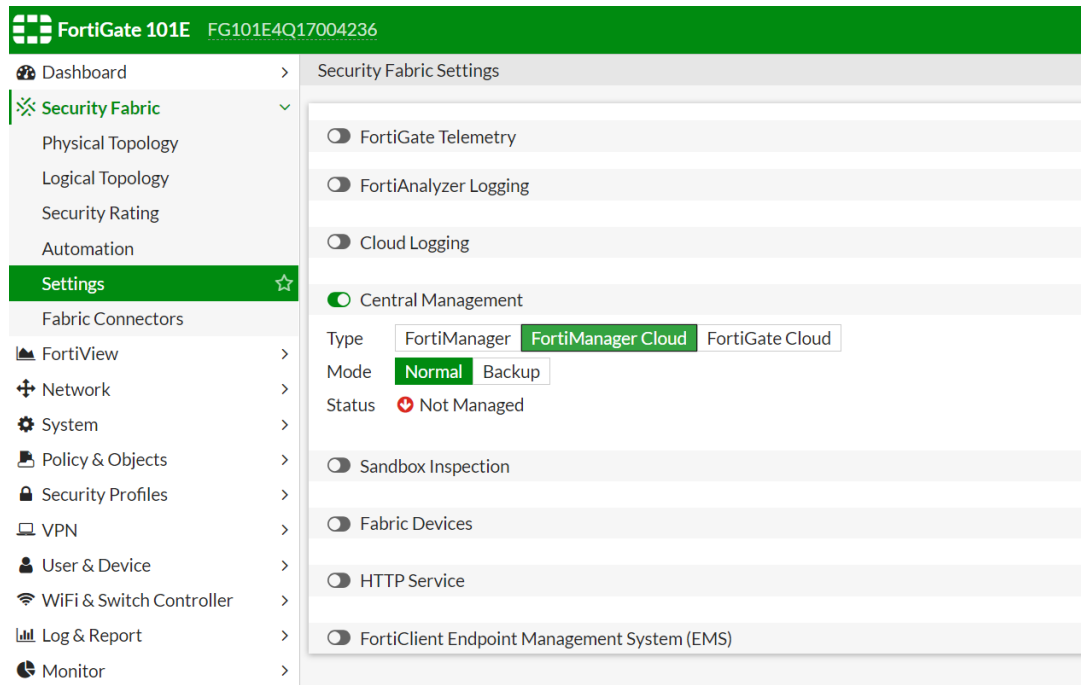
This section explains how to enable management of FortiGate by FortiManager Cloud.

To configure FortiOS:

1. In FortiOS, enable FortiManager Cloud.

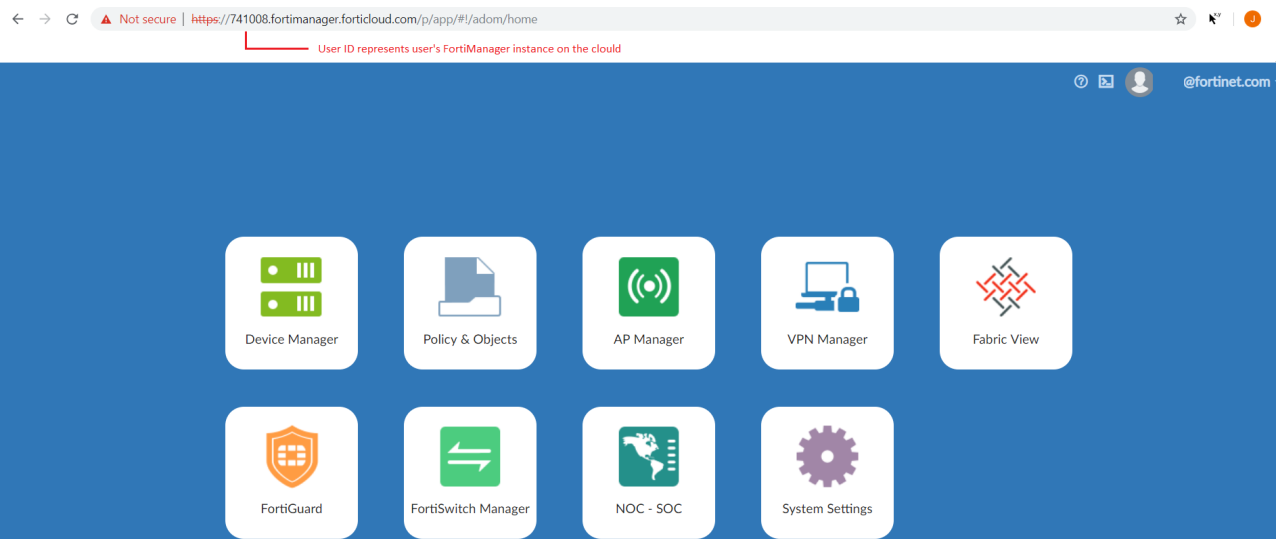
- a. Go to *Security Fabric > Settings*, and enable *Central Management*.
- b. Click *FortiManager Cloud*, and then *Apply*.

The *FortiManager Cloud* button is only available when you have a FortiManager Cloud product entitlement; the *FortiManager Cloud* button is not available without a FortiManager Cloud product entitlement.

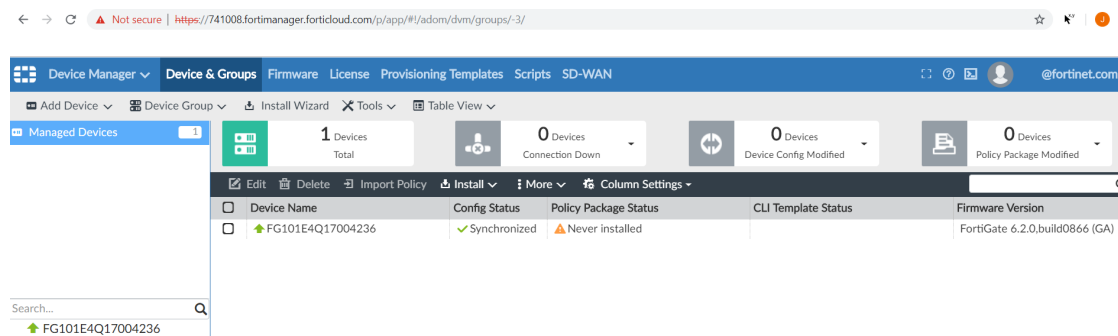


2. In the FortiManager Cloud instance, go to *Device Manager* and authorize the FortiGate.

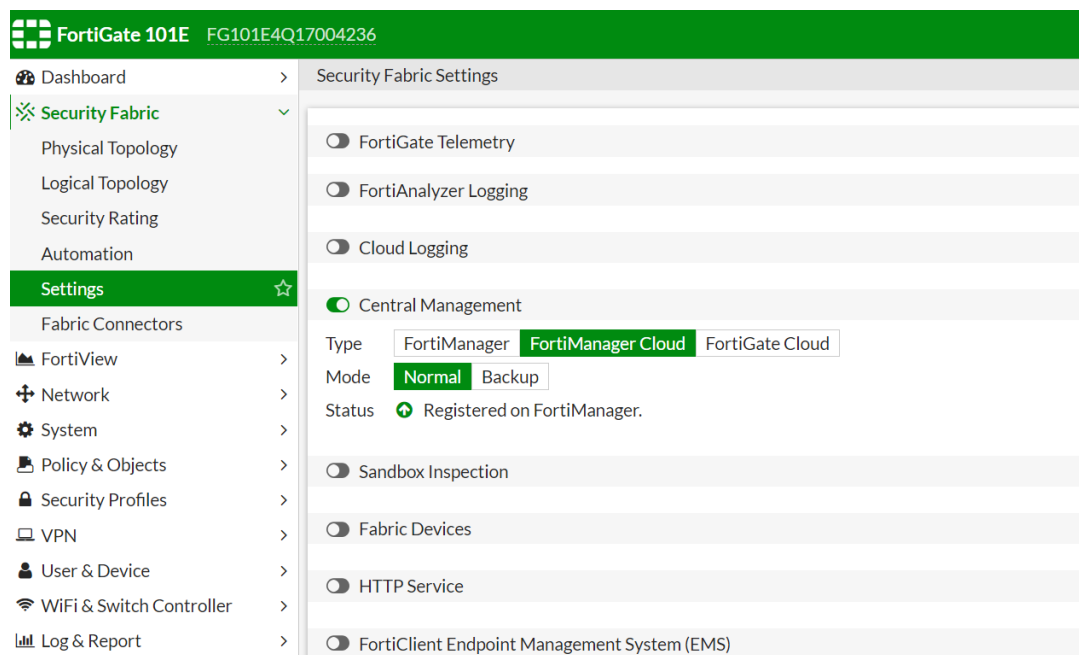
When using FortiGate to enable FortiManager Cloud, the FortiGate device appears as an unauthorized device.



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



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



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](#)
- [Using Map View on page 14](#)
- [Viewing information about instances on page 15](#)
- [Upgrading firmware from the portal on page 16](#)

Accessing the portal and instances

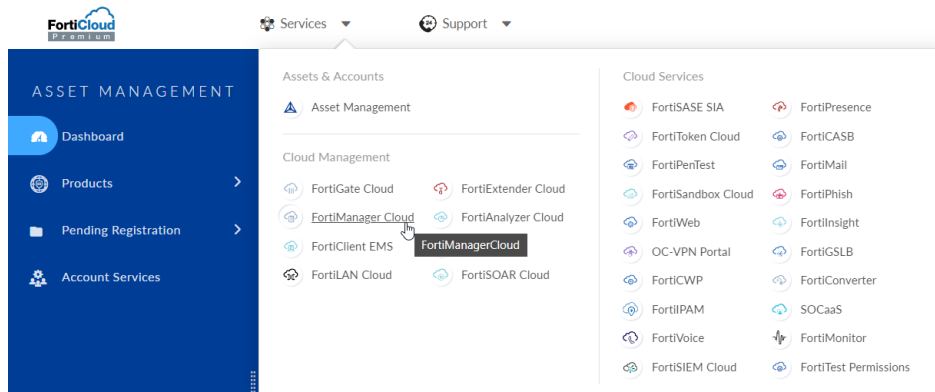
After deploying one or more FortiManager Cloud instances, you can access the instances from the FortiManager Cloud & Service portal.



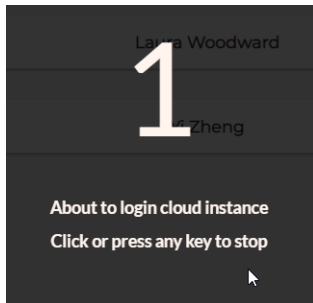
When you access the FortiManager Cloud & Service portal, an automatic instance login process begins, and a countdown is displayed. The process automatically logs you in to the last instance that you accessed. You can stop the automatic login process by clicking anywhere on the screen.

To access the portal and instances:

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**.



An automatic instance login process begins, and a countdown is displayed.

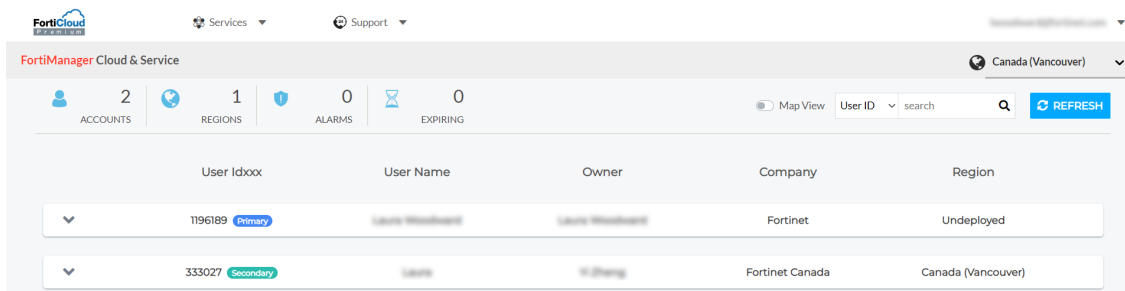


- Click any where on the screen to stop logging in to the FortiManager instance, and access the FortiManager Cloud & Service portal.



If you let the countdown complete, you are automatically logged in to the FortiManager instance. After logging in to the FortiManager instance, you can return to the portal. In the top-right corner, click your name and select *FortiManager Cloud*.

The *FortiManager Cloud & Service* portal is displayed.



The following options are displayed:

Region list	The top-right corner displays the selected region. Click the region list to select another region. When you change the region, the URL for the FortiManager & Service portal changes. Before deploying an instance, select the region for deployment.
Dashboard	The top-left includes a dashboard summary of the accounts displayed on the pane: - Accounts: Displays the number of accounts you can access. - Regions: Displays the number of regions that contain deployed instances of FortiManager Cloud. - 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.
Map View	Toggle on to display a world map with locations of deployed instances. You can click each location for details about the instance. See Using Map View on page 14 . Toggle off to display a summary table of account information. Expand each account to view additional options and information.
Account Filters	Select one of the following filters to change how the list of accounts display: - User ID - Name

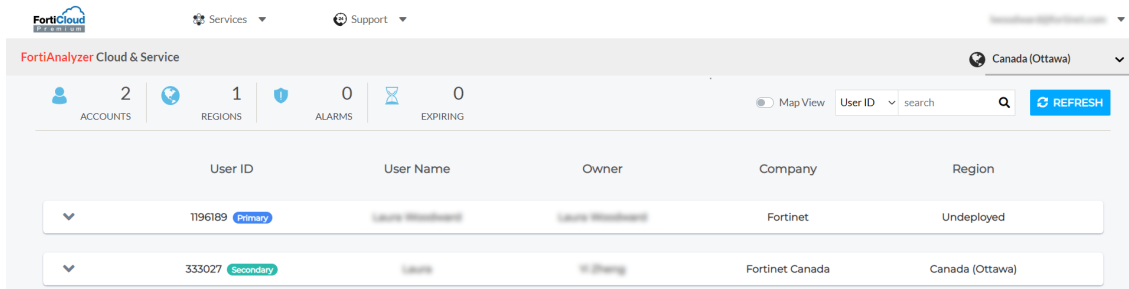
	• Owner • Company • Region
Account Search	Use to search for accounts. In the <i>Search</i> box, type search criteria, and press <i>Enter</i> . Delete the search criteria, and press <i>Enter</i> to display all accounts again.
Refresh	Click to manually retrieve the latest license information from FortiCare and refresh the pane. Information from FortiCare is also automatically retrieved on a regular interval.
Accounts summary in table view	Available when <i>Map View</i> is toggled off. Each account displays as a row with the following columns: • User ID: Displays the ID associated with the FortiCloud user and whether the user is a primary or secondary user. Primary users can deploy and upgrade FortiManager Cloud instances from the FortiManager Cloud & Service portal. Secondary users can enter FortiManager Cloud instances from the FortiManager Cloud & Service portal. • User Name: Displays the name of the user. • Owner: Displays the name of the primary account holder. • Company: Displays the name of the company for the user. • Region: Displays the name of the region where the instance is deployed. Expand the account to access more information and options: • Provision Instance: Displays for primary accounts without a deployed instance that meet requirements for deployment. • Enter: Displays for primary and secondary accounts with deployed instances to let you enter the instance. • Upgrade: Displays for primary accounts when a firmware version is available for upgrade. See also Viewing information about instances on page 15 and Upgrading firmware from the portal on page 16.

Using Map View

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

To use Map View:

1. Access the portal. See [Accessing the portal and instances on page 12](#).
The FortiManager Cloud & Service portal is displayed.



- From the top-right corner, select a region, such as *Canada*.
Notice that the URL for the FortiManager & Service portal changes.
- Toggle *Map View* on.
The Map View is displayed.
- Click the location to display information about the instance.
Details about the instance are displayed on the right-hand pane. Click X to close the right-hand pane.



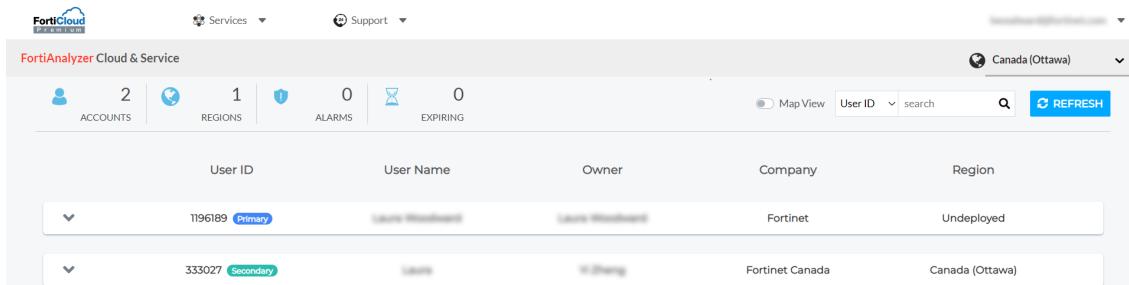
- At the bottom-right of the map, click the + button to zoom in to the map, and click the - button to zoom out of the map.
- Toggle *Map View* off to exit the map and display the list of accounts in table view.

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:

- Access the portal. See [Accessing the portal and instances on page 12](#).
The FortiManager Cloud & Service portal is displayed.

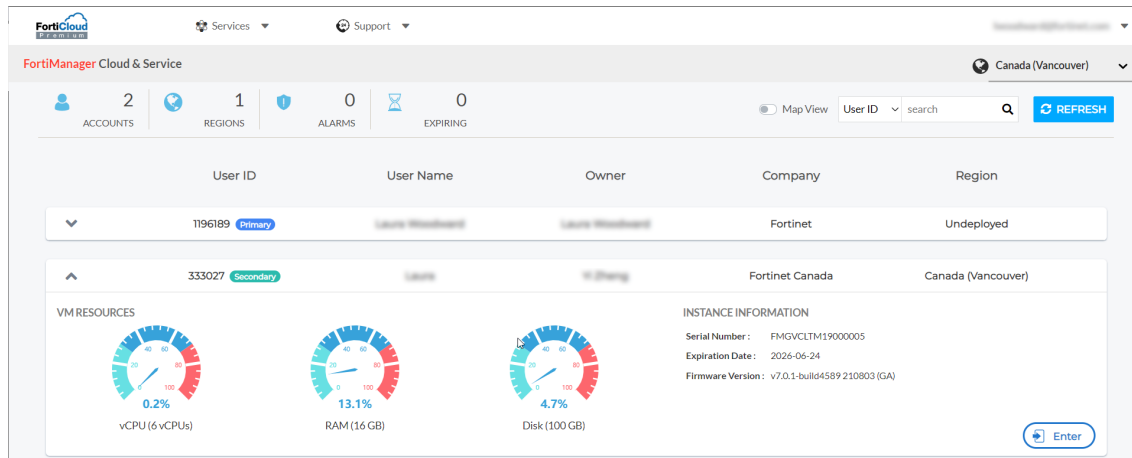


- Expand an account with no instances deployed.
The account details are displayed. If it is a primary account, you can click *Provision Instance* to provision a FortiManager Cloud instance.

3. Expand an account with deployed instances.

Information about the VM resources and the instance is displayed. If a firmware upgrade is available, a message is displayed, and you can upgrade now or later. You can also click *Enter* to access the instance.

When a firmware upgrade is available, information about the firmware upgrade is also displayed.



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 System Settings on page 18](#).



Before you can use FortiManager Cloud 7.0.x, you must upgrade all FortiGates to FortiOS 6.2.0 or later.

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 *Upgrade Now* to update the firmware immediately, or click *Upgrade Later* to schedule upgrade of the firmware for a later date.

4. Click *OK*.
5. Click *Enter* to open FortiManager Cloud.

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 7.0.1 Administration Guide](#).

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

- [Upgrading firmware from System Settings on page 18](#)
- [Identifying the public IP address on page 18](#)
- [Updating the ADOM version on page 19](#)
- [Enabling the FortiManager Cloud connector on FortiGate on page 20](#)
- [Using FortiZTP with FortiManager Cloud on page 21](#)

Upgrading firmware from System Settings

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

For information about upgrading firmware from the FortiManager & Service portal, see [Upgrading firmware from the portal on page 16](#).



Before you can use FortiManager Cloud 7.0.x, you must upgrade all FortiGates to FortiOS 6.2.0 or later.

To upgrade firmware from System Settings:

1. Access the instance. See [Accessing the portal and instances on page 12](#).
2. In FortiManager Cloud, go to *System Settings*.
3. In the *System Information* widget, click the *Upgrade Firmware* button beside *Firmware Version*. The *Firmware Management* dialog box is displayed.
4. From the *Select Firmware* list, select the firmware version, and click *OK*.

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



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

```
FMG-VM64-VIO-CLOUD # Config sys admin setting
Set shell enable
End
FMG-VM64-VIO-CLOUD # execute shell
Enter password:
bash$
bash$ curl ifconfig.me
173.243.137.11
```

In this example, the public IP address for 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.

Updating the ADOM version

FortiManager Cloud supports one ADOM and version. With FortiManager Cloud 7.0.x, the ADOM can be any of the following versions: 6.2, 6.4 and 7.0.

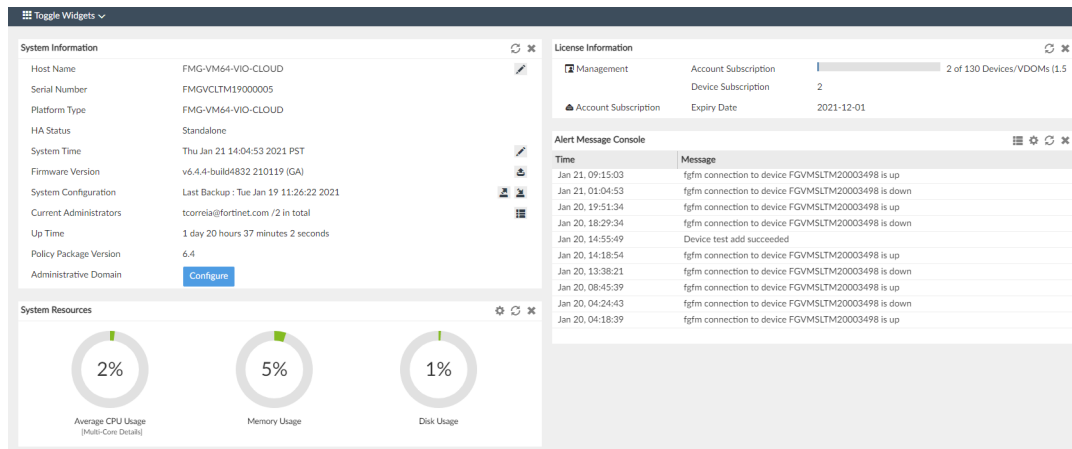
You can view the ADOM version on the *System Settings > Dashboard* pane in the *System Information* widget.

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 6.2 ADOM and want to upgrade to a 7.0 ADOM, you must upgrade from 6.2 to 6.4, and then you can upgrade from 6.4 to 7.0.

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.



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 7.0.
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 6.4, you can enter the following command:

```
execute reset adom 3 6 4
```



All devices (including unauthorized devices) must be deleted from the ADOM prior to performing the ADOM reset.

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
```

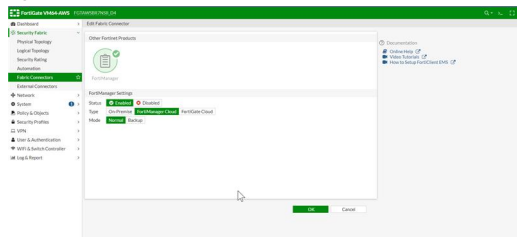
```
...
```

```
Support contract: pending_registration=255 got-contract info=1
```

```
  accountn_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*, and select the connector. The FortiManager option is enabled.



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.

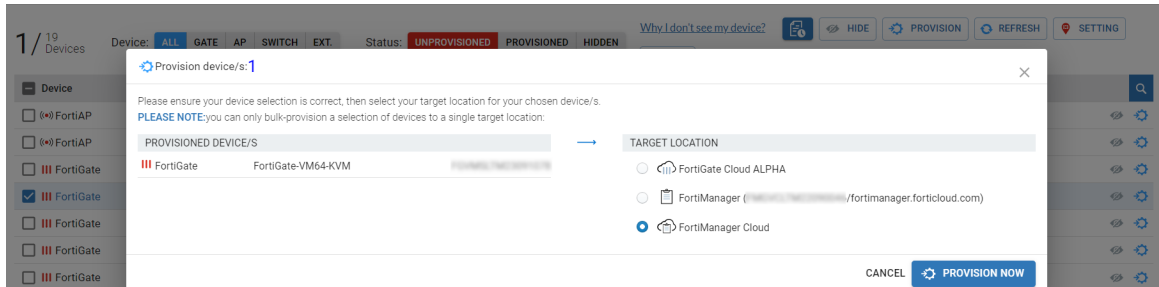
You can provision devices from FortiZTP with or without preconfiguration on FortiManager Cloud.

- 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.

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.
- Under *TARGET LOCATION* in the *Provision devices* dialog, select *FortiManager Cloud*.
 - Click *PROVISION NOW*.



- Reboot the FortiGate. For physical FortiGate devices, you must perform a factory reset.
- Complete the onboarding of the managed device:
 - When provisioning with preconfiguration:**
 - After the FortiGate comes online, the FGFM tunnel is established.
 - The auto-link process is performed automatically, and the FortiGate is added as a managed device.
 - When provisioning without preconfiguration:**
 - 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.
 - 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 23](#)
- [Modifying a secondary account on page 25](#)
- [Supporting IAM users and IAM API users on page 25](#)

For information about using FortiCloud portal, see the [FortiCloud Account Services](#) page on the [Fortinet Document Library](#).

Adding a secondary account

Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance. 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.

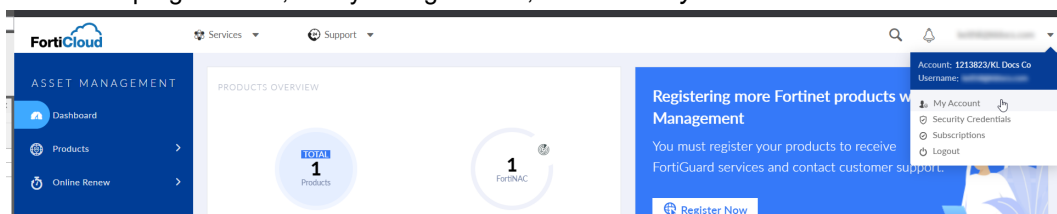
A secondary account allows the Fortinet support team to troubleshoot the FortiManager Cloud deployment.



With FortiManager Cloud 6.4.5 and later, you can use the Identity and Access Management (IAM) portal, and you can migrate secondary accounts to the IAM portal. In IAM portal, secondary accounts are called sub users. For information about migrating sub users, see the [Identity & Access Management Guide](#).

To add a secondary account:

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



3. Click *Manage User*.

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

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

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

6. Log in to the personal FortiCare portal. Under FortiManager Cloud section, you will see an account listed as a secondary member.
7. 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.
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 25](#).



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 23](#).

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](#).

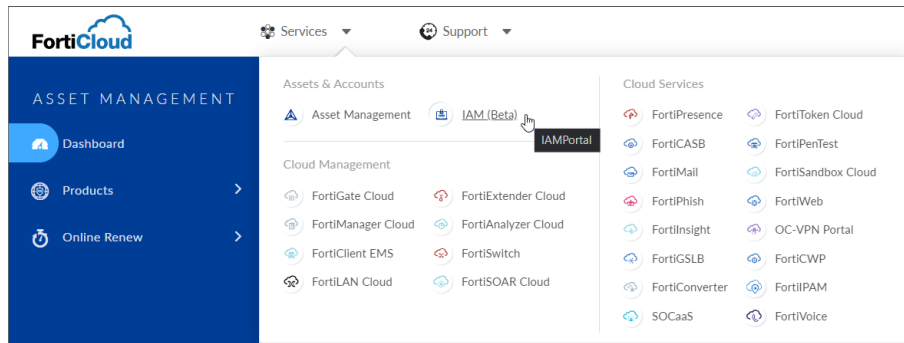
See also [Adding IAM users on page 25](#) and [Adding API users on page 27](#).

Adding IAM users

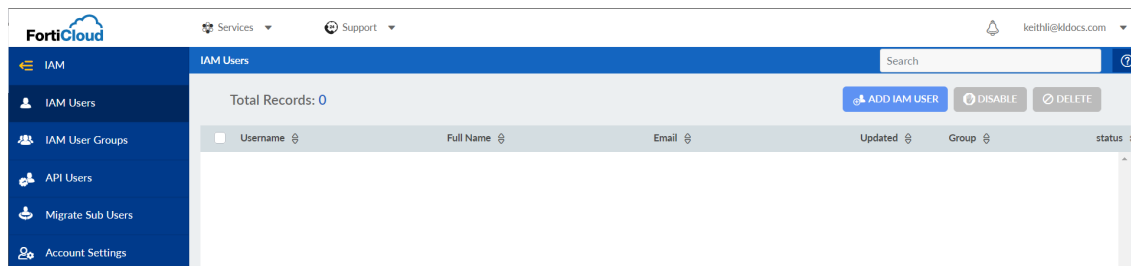
FortiManager Cloud supports FortiCloud Identity and Access Management (IAM). You can use the FortiCloud portal to manage users, authentication credentials, and access permissions for FortiManager Cloud.

To add an IAM user:

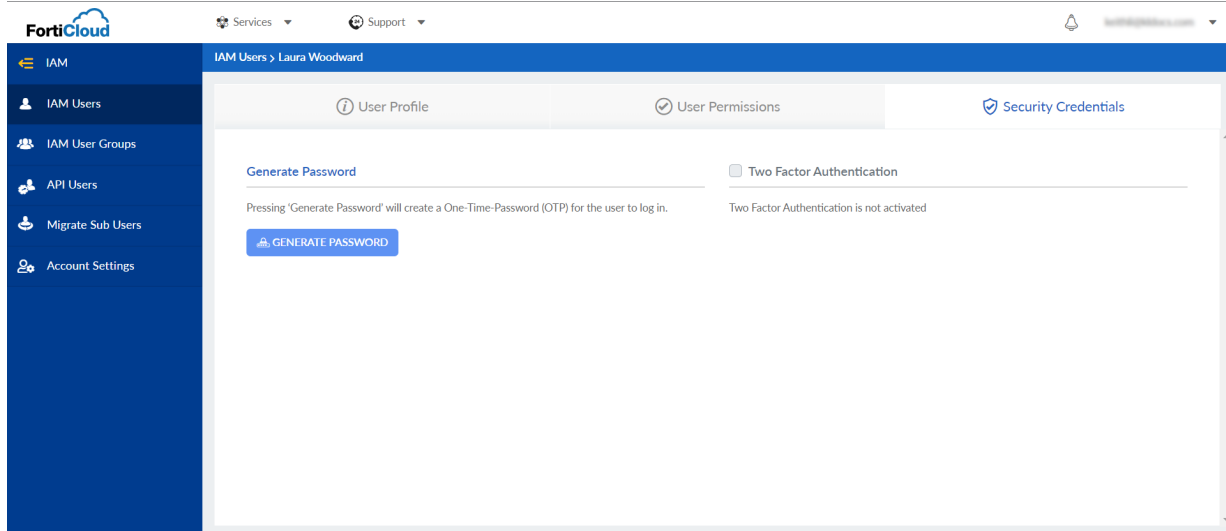
1. Go to FortiCloud (<https://support.fortinet.com/>), and log in.
2. From the **Services** menu, select **IAM**.



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.
 - a. Go to *IAM Users*, and click the full name of the user. The *User Profile* tab is displayed.
 - b. Go to the *Security Credentials* tab, and click *Generate Password*.

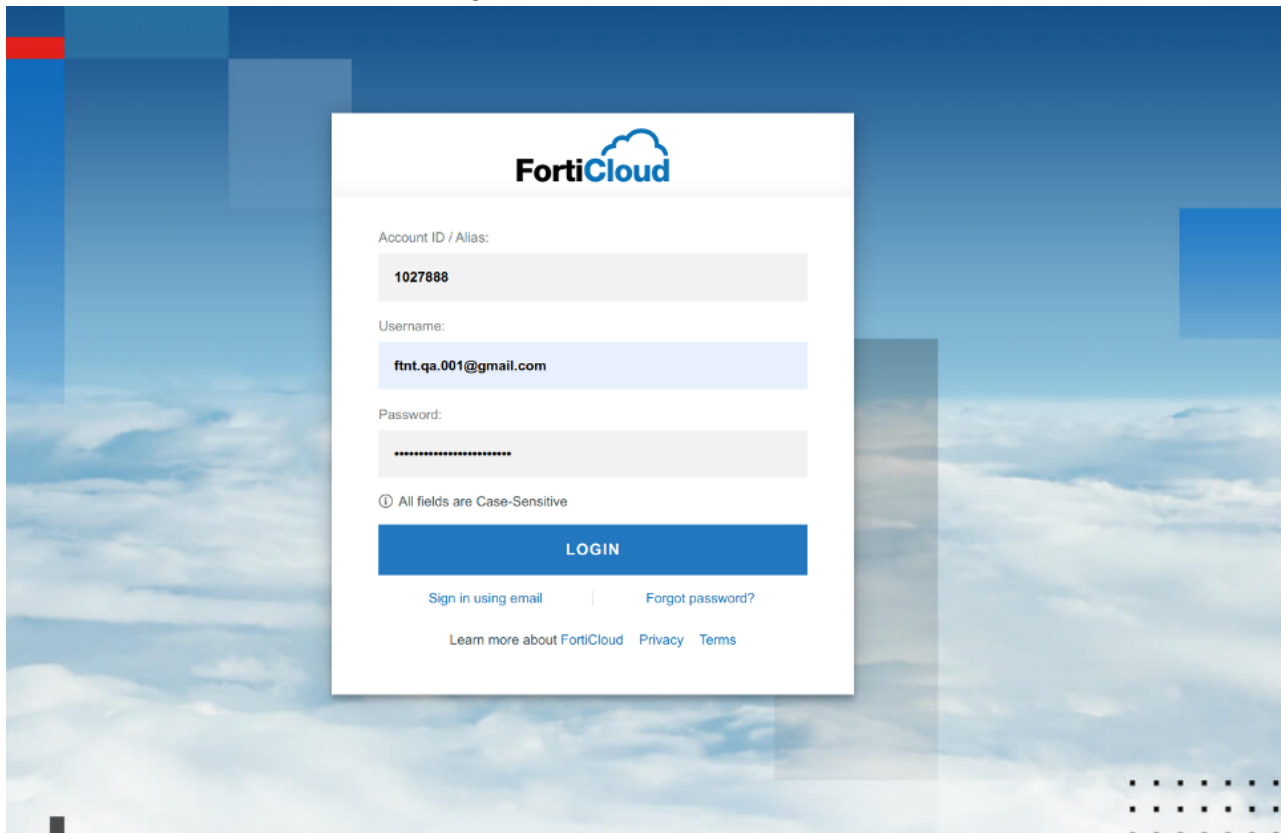


The *Generate Password* dialog box is displayed.

- c. Click *Proceed*. A file of credentials in csv format is generated and downloaded to your computer.
- d. Open the csv file to view the credentials for the IAM user.

A	B	C	D	E	F
Account ID	Alias	Username	Name	Email	Password
1027888	1027888	ftnt.qa.001@gmail.com	ftnt.qa.001	ftnt.qa.001@gmail.com	671815c831eab448aebb11Aa

- e. Share the credentials with the IAM user.
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.

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.



www.fortinet.com

Copyright© 2023 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 General Counsel, 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.