Cloud Deployment Guide

FortiManager 7.2.x

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-08	Initial release.
2023-06-28	Updated Using account services on page 24.
2023-07-05	Updated Using FortiZTP with FortiManager Cloud on page 22.
2023-07-19	Updated Licensing on page 7.
2023-10-17	Updated Using FortiZTP with FortiManager Cloud on page 22.
2023-12-18	Updated Deploying a FortiManager Cloud instance on page 9. Updated Updating the ADOM version on page 19.
2024-09-03	Release of FortiManager Cloud 7.2.7.
2024-10-18	Release of FortiManager Cloud 7.2.8.
2025-01-31	Release of FortiManager Cloud 7.2.9.
2025-03-06	Release of FortiManager Cloud 7.2.10.
2025-04-15	Updated Introduction on page 5.
2025-08-05	Updated Supporting external IdP users on page 29.
2025-10-01	Release of FortiManager 7.2.11.
2025-10-09	Updated Licensing on page 7.
2026-01-02	Updated Adding API users on page 28.
2026-02-02	Release of FortiManager Cloud 7.2.12.

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 14 and Deploying FortiManager Cloud on page 8.

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.

> SSL inspection for `*.forticloud.com` must be disabled on any upstream FortiGates in order to reach FortiManager Cloud.

This section includes the following topics:

- Requirements on page 5
- Licensing on page 7

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 24.

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

See Licensing on page 7 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

When adding a FortiGate Security Fabric (CSF) to FortiManager Cloud, your subscription license must include enough device support for each FortiGate in the Fabric. This also applies to FortiGate devices operating in an HA cluster.

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 8.
2. On FortiCloud, deploy a FortiManager Cloud instance. See Deploying a FortiManager Cloud instance on page 9.
3. (Optional) Upgrade FortiManager Cloud to the latest available cloud version. See Upgrading firmware from the portal on page 18.
4. On FortiOS, enable management by FortiManager Cloud. See Configuring FortiOS on page 11.

> 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 9.

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 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 24.

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 19.
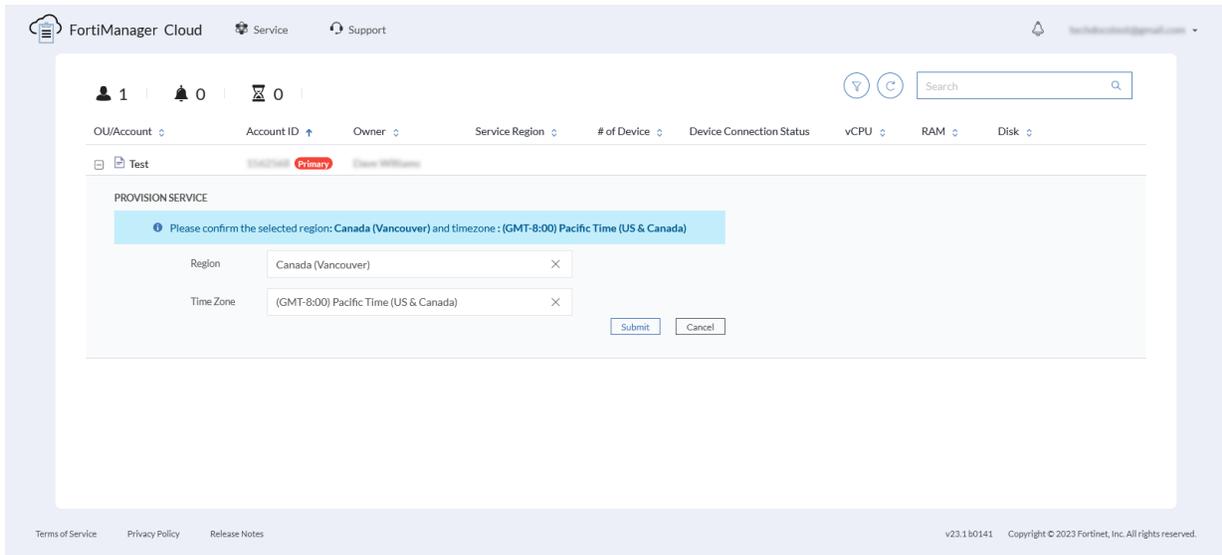
To deploy a FortiManager Cloud instance:

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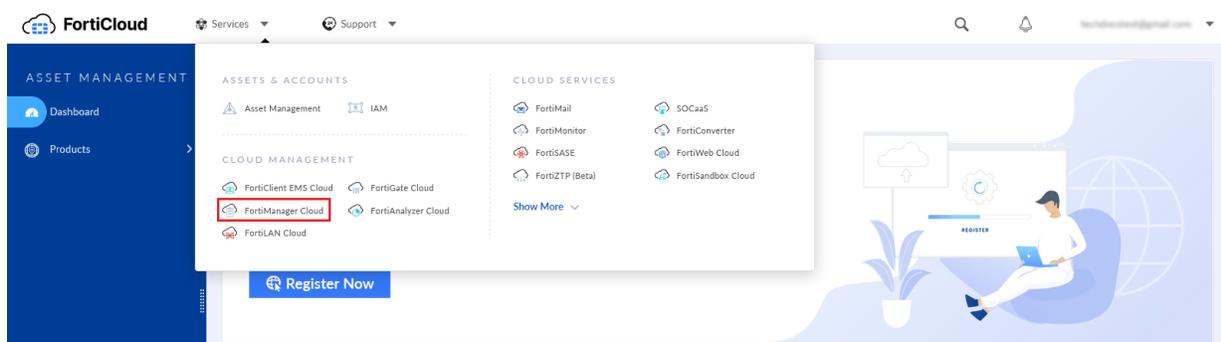
The *FortiManager Cloud & Service* portal is displayed.
3. On the *FortiManager Cloud & Service* portal:
   a. Select a *Region* for the FortiManager Cloud instance. In this example, the region is *Canada (Vancouver)*.
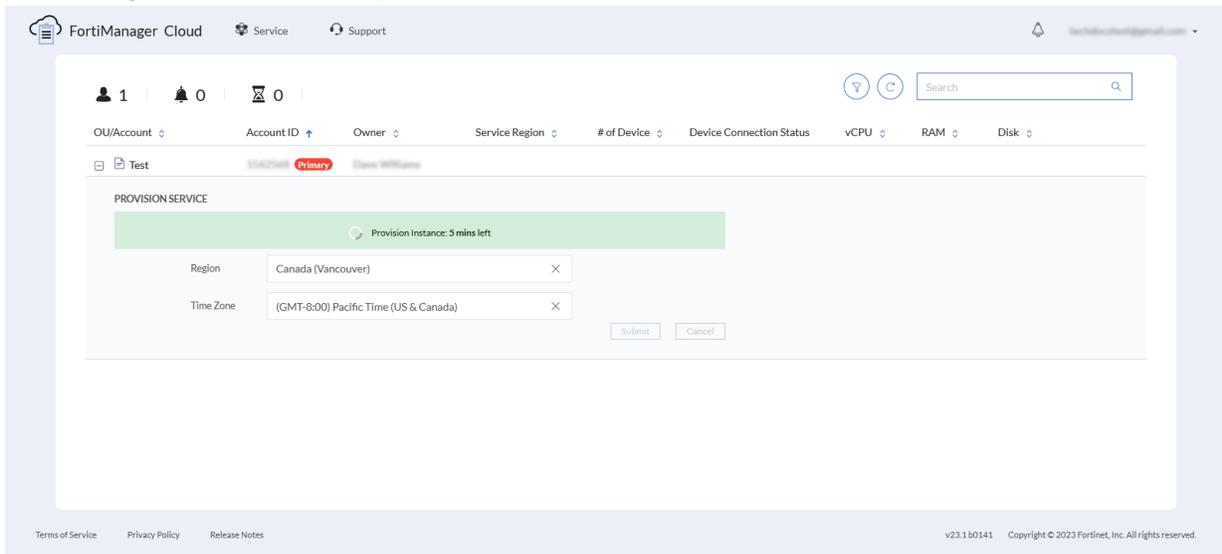   b. Select a *Time Zone* for the FortiManager Cloud instance.

4. Click *Submit*.

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.

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

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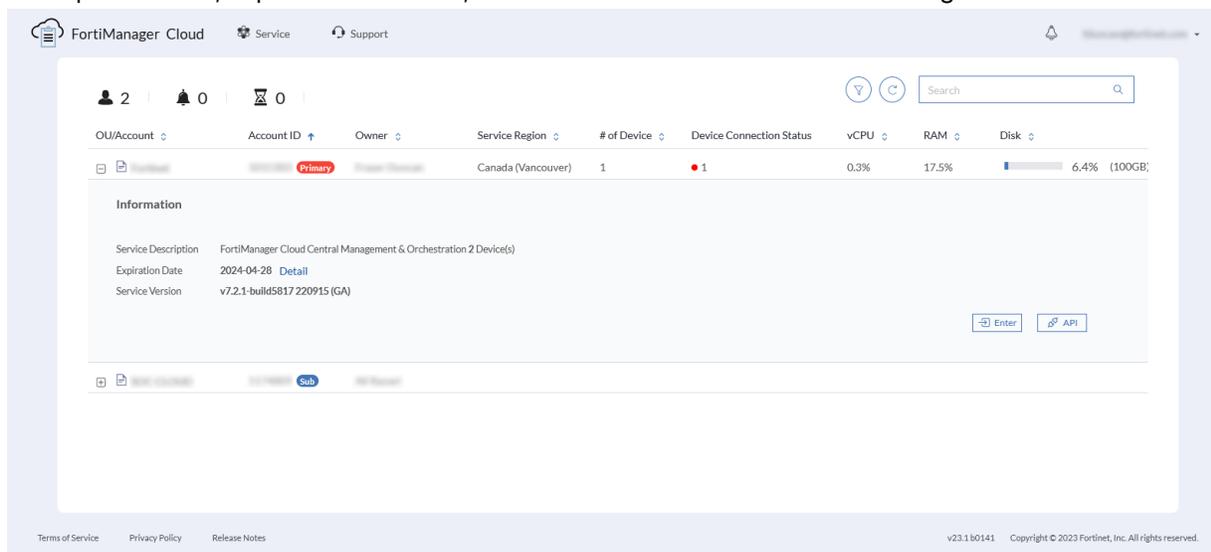

8. (Optional) Upgrade FortiManager Cloud to 7.2.x. See Upgrading firmware from the portal on page 18.

9. Configure FortiOS to work with FortiManager Cloud. See Configuring FortiOS on page 11.

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*.
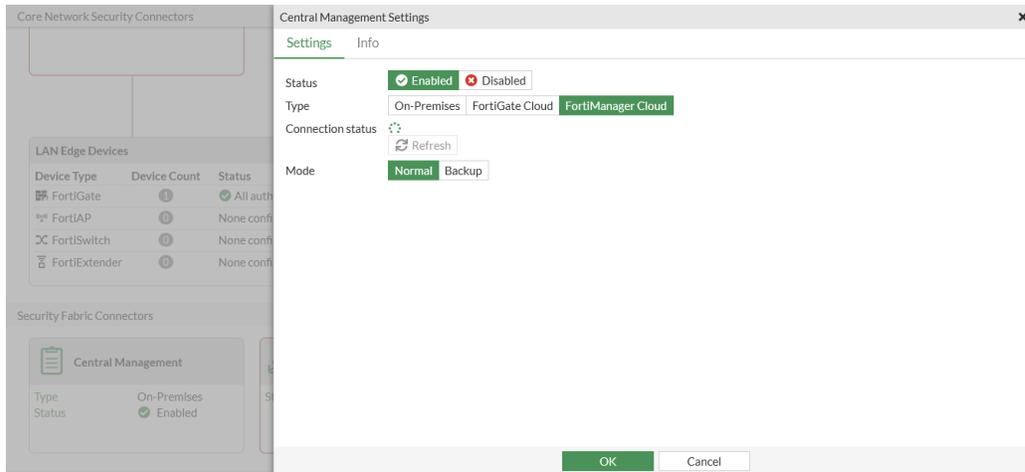
2. In the FortiManager Cloud instance, go to *Device Manager* and authorize the FortiGate.
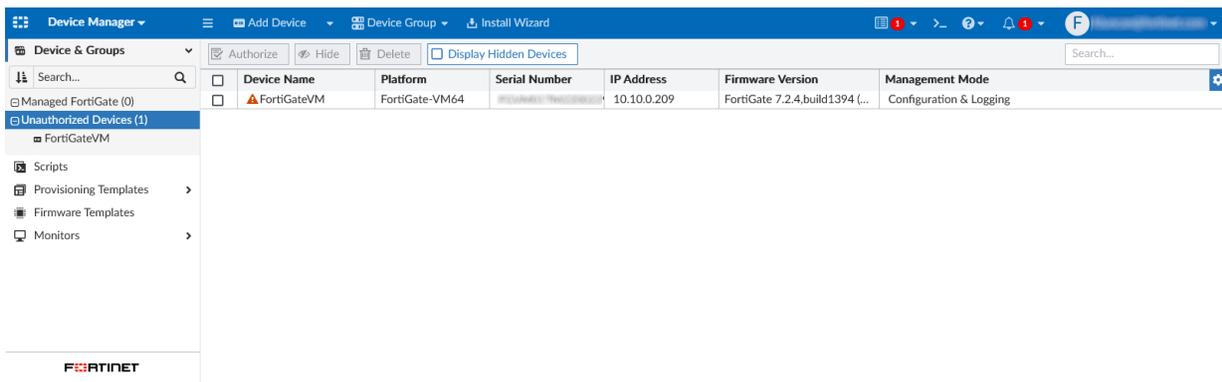
After authorizing the FortiGate, the FortiGate becomes a managed device.
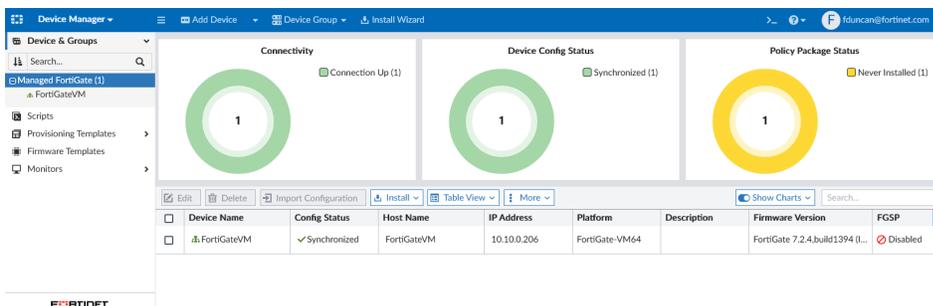
When successfully authorized, the central management status displays as *Enabled on FortiManager*.

Core Network Security Connectors

Role	Standalone	FortiAnalyzer ❌ Disabled	Status	❌ Disabled
		FortiAnalyzer Cloud ✅ 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	❌ Disabled	
Status	✅ Enabled			

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

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 14.
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*.
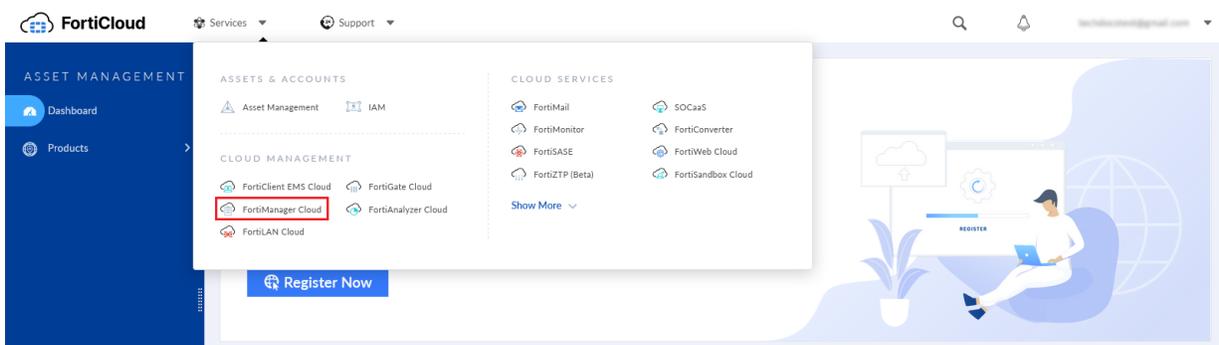
You are automatically logged in to your FortiManager instance.

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.
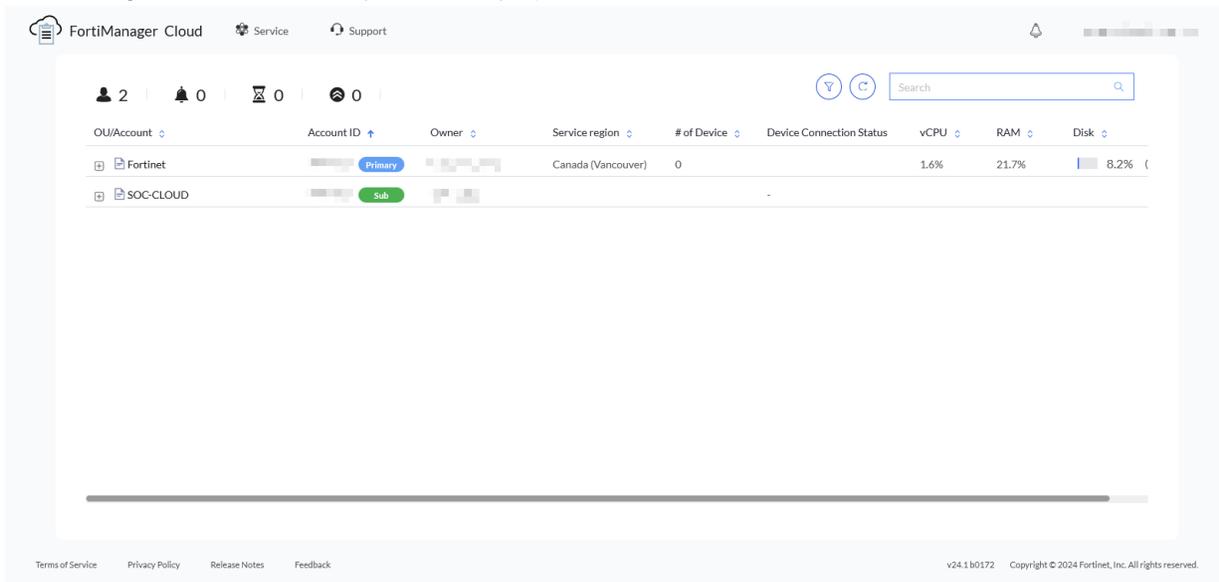
The following options are displayed:

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 16 and Upgrading firmware from the portal on page 18.

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 14.
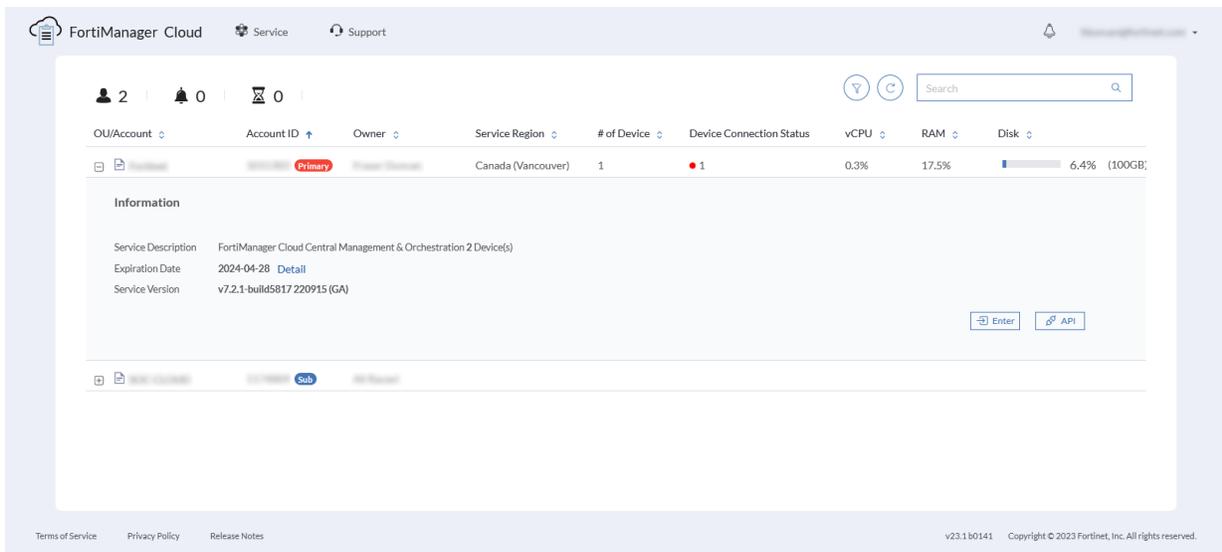   The FortiManager Cloud & Service portal is displayed.
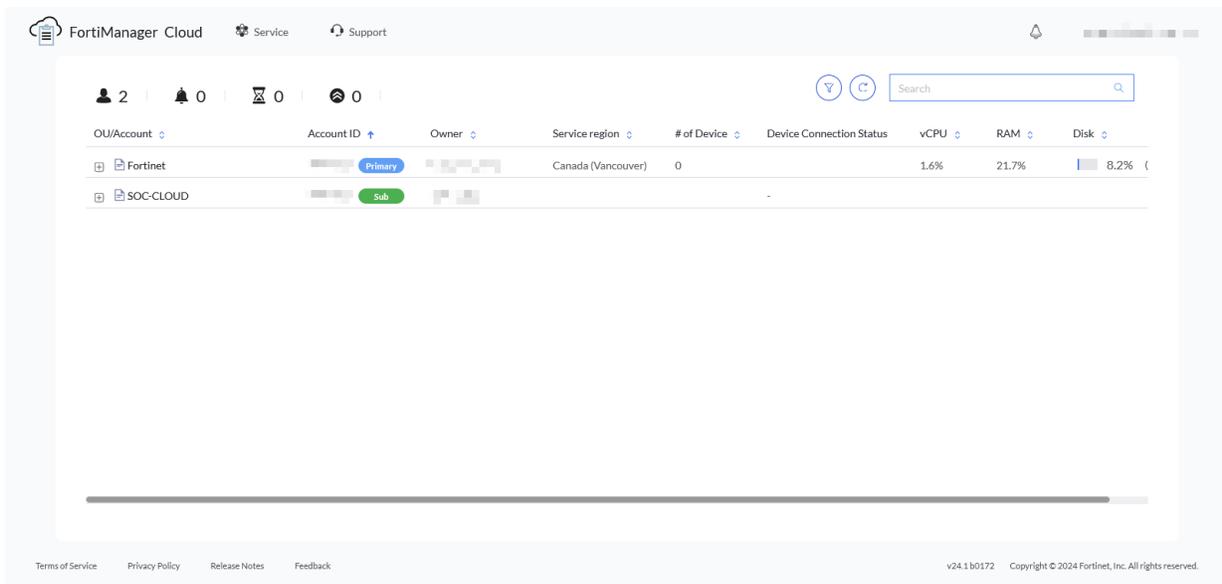
2. Expand an account with no instances deployed.
   The account details are displayed. If it is a primary account, you can provision a new instance. See Deploying a FortiManager Cloud instance on page 9.

3. Expand an account with deployed instances.
   Information about the VM resources and the instance is displayed.
   When a firmware upgrade is available, you can click the upgrade icon ⟳ to view additional information about the upgrade, choose upgrade immediately, or schedule an upgrade for later. You can also click *Enter* to access the instance.

Upgrading firmware from the portal

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 19.

> Before you can use FortiManager Cloud 7.2.x, you must upgrade all FortiGates to FortiOS 6.4.4 or later.

To upgrade firmware from the portal:

1. Access the portal. See Accessing the portal and instances on page 14.
   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.

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 System Settings on page 19
- Updating the ADOM version on page 19
- Enabling the FortiManager Cloud connector on FortiGate on page 21
- Using FortiZTP with FortiManager Cloud on page 22

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 18.

> Before you can use FortiManager Cloud 7.2.x, you must upgrade all FortiGates to FortiOS 6.4.4 or later.

To upgrade firmware from System Settings:

1. Access the instance. See Accessing the portal and instances on page 14.
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*.

Updating the ADOM version

FortiManager Cloud supports one ADOM and version. With FortiManager Cloud 7.2.x, the ADOM can be any of the following versions: 6.4, 7.0, or 7.2.

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 6.4 ADOM and want to upgrade to a 7.2 ADOM, you must upgrade from 6.4 to 7.0, and then you can upgrade from 7.0 to 7.2.

To upgrade the ADOM version:

1. Access FortiManager Cloud. See Accessing the portal and instances on page 14.
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.
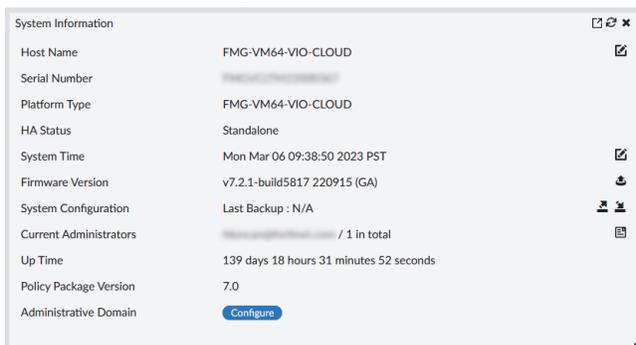
4. In the *System Information* widget, click *Configure* beside *Administrative Domain* option.
   The *Edit ADOM* dialog box is displayed.
5. In the *Type* field select a version, such as *7.2*.
6. Click *OK*, and the ADOM is upgraded to the selected version.

To downgrade the ADOM version:

1. Access FortiManager Cloud. See Accessing the portal and instances on page 14.
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
   ```

   > 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
        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.

> **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.

c. Under *TARGET LOCATION* in the *Provision devices* dialog, select *FortiManager Cloud*.

d. Click *PROVISION NOW*.
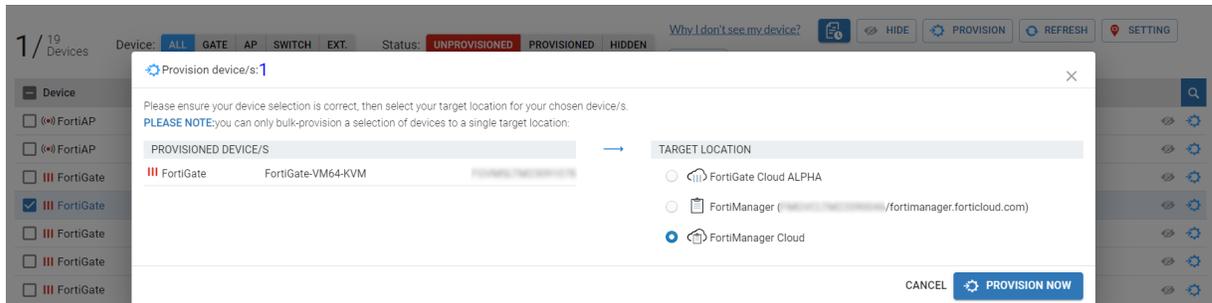
3. Reboot the FortiGate. For physical FortiGate devices, you must perform a factory reset.

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 account services

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

- Adding a secondary account on page 24
- Modifying a secondary account on page 26
- Supporting IAM users and IAM API users on page 26

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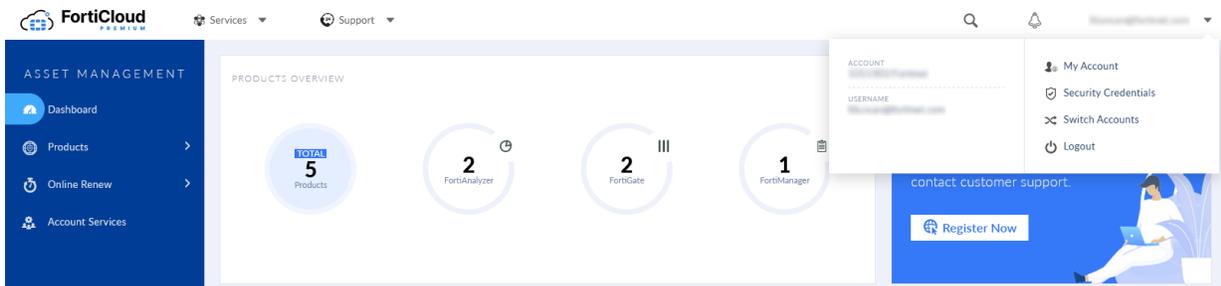
A secondary account allows the Fortinet support team to troubleshoot the FortiManager Cloud deployment.

> 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.

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.

    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 26.

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 24.

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 26 and Adding API users on page 28.
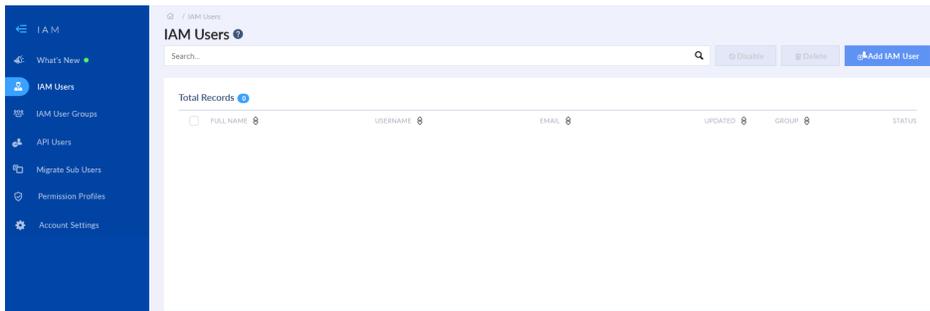
Adding IAM users

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* .
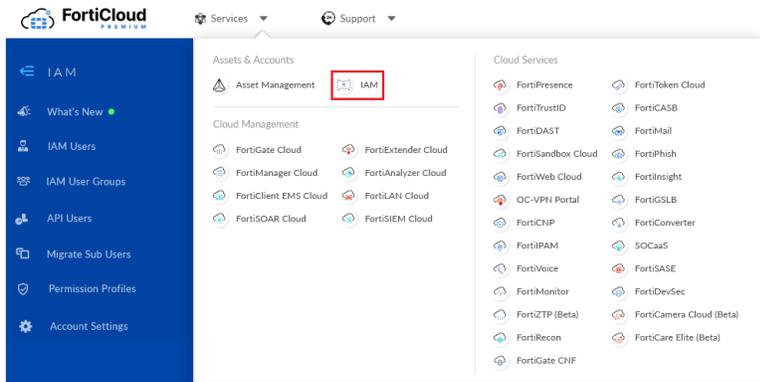
The *IAM portal* is displayed.

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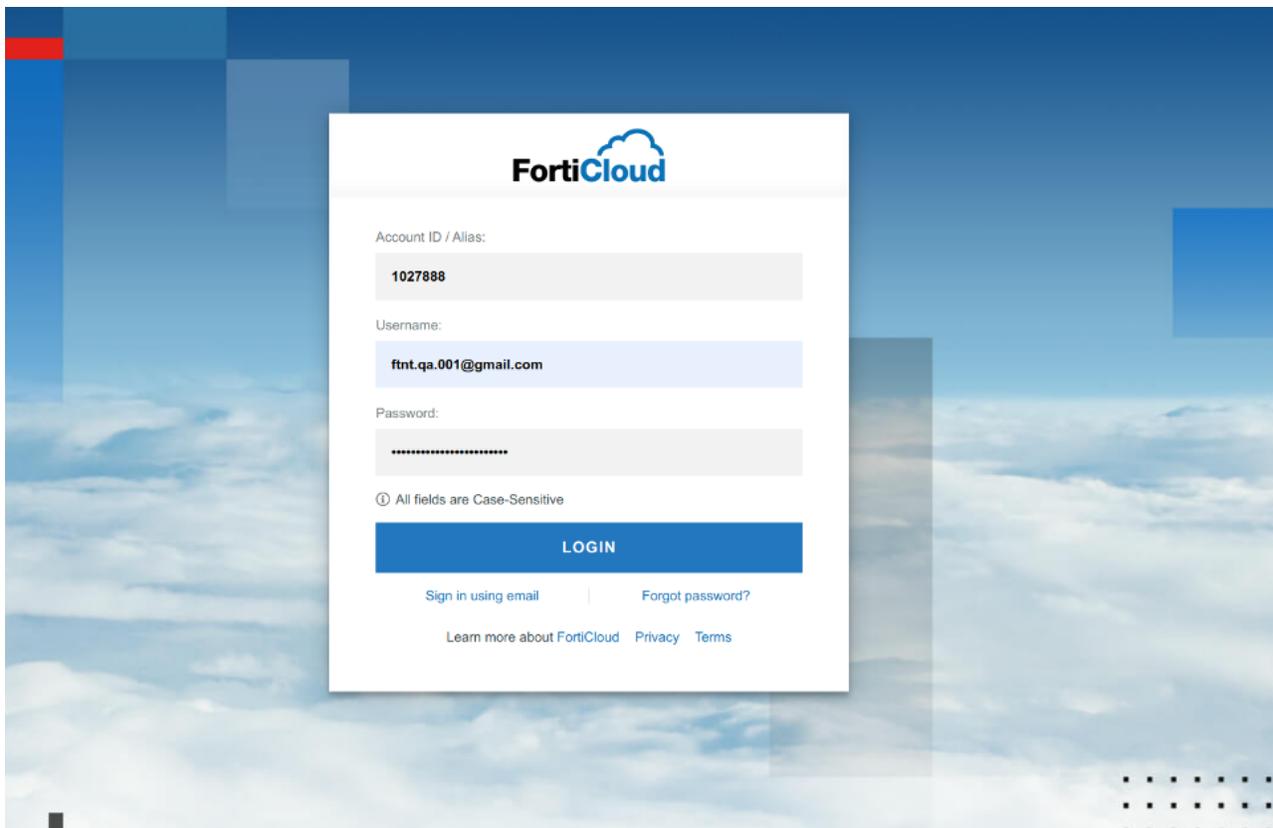
After logging in to FortiCloud, the IAM user has access to *FortiManager Cloud & Service* portal.

7. Enter the FortiManager Cloud instance, and go to *System Settings > Administrators* to view the IAM user.

Adding API users

API users can access FortiCloud services, including FortiManager Cloud, through the API.

In order to send API requests to FortiManager Cloud, you must first obtain an access token from FortiCloud using OAuth 2.0. You can use the access token to generate a session ID which is required to send an JSON API request to FortiManager.

To use the FortiManager Cloud API:

1. Create an API user in FortiCloud and download your API credentials. See Adding an API user in the FortiCloud Account Services documentation for instructions on how to add API users.

2. Obtain an access token from FortiCloud using your credentials. See Accessing FortiAPIs - Authentication and authorization for information on authentication and authorization for FortiAPIs.

3. Use the access token to get a FortiManager Cloud API session ID using the `https://<FortiManager_cloud_url>/p/forticloud_jsonrpc_login/` endpoint.

HTTP Method	POST
Endpoint	`https://<FortiManager_cloud_url>/p/forticloud_jsonrpc_login/`

| Request Body | ```
{
        "access_token": "<access token obtained in step 2>"
}
``` |
|---|---|
| Response example | ```
{
        "session": "ykF3W6G8CfZv+xecsZBC00n6P0TEbsO*****"
}
``` |

4. Send API requests to the `https://<FortiManager_cloud_url>/jsonrpc` endpoint with the session included in the body.

    For example:

HTTP Method	POST
Endpoint	`https://<FortiManager_cloud_url>/jsonrpc`
| Request Body | ```
{
        "method": "get",
        "params": [
            {
                "url": "/sys/status"
            }
        ],
        "id": 1,
        "verbose": 1,
        "session": "ykF3W6G8CfZv+xecsZBC00n6P0TEbsO*****",
}
``` |

The FortiManager Cloud API uses session-based authentication. The number of simultaneous API sessions allowed for an API user is controlled by the user's max login setting. By default, this setting is set to 20.

```
config system admin user
        edit <user>
        set login-max 20
```

Supporting external IdP users

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

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

FORTINET