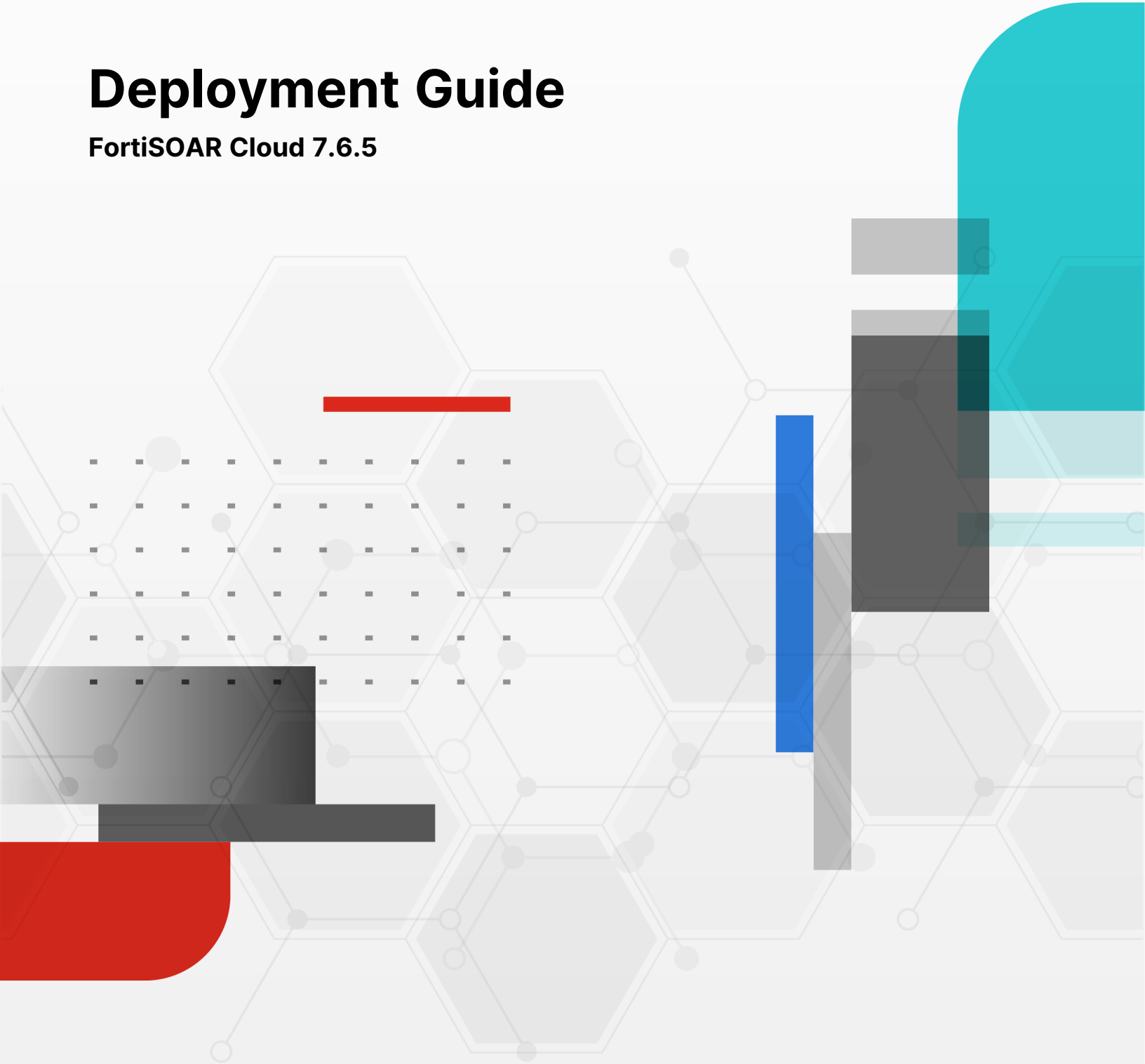


Deployment Guide

FortiSOAR Cloud 7.6.5



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



December, 2025

FortiSOAR Cloud 7.6.5 Deployment Guide

00-400-000000-20210416

TABLE OF CONTENTS

Change Log	5
Introduction	6
FortiSOAR Cloud Virtual Machine Specifications	6
Licensing	6
FortiSOAR Cloud license contract registration	7
Deploying FortiSOAR Cloud	9
Troubleshooting	13
Uniqueness error when adding a tenant in an MSSP setup using the Secure Message Exchange	13
Beginning with FortiSOAR Cloud	14
Accessing FortiSOAR Cloud	14
Accessing FortiSOAR Cloud console	18
Accessing FortiSOAR Cloud UI	19
Switching between Accounts	19
Secure Message Exchange	21
Cloud App Menu	21
Settings	22
User Preferences	22
List of logs that can be used for debugging FortiSOAR Cloud	24
Adding an organization	25
Adding a secondary account	26
Adding a secondary account using IAM	26
Adding a secondary account using FortiCare	32
Setting up External IdP roles	34
Identifying the public IP address	36
High Availability Capability for FortiSOAR Cloud	37
Creating a cluster on the FortiSOAR Cloud Portal	37
Managing a cluster on the FortiSOAR Cloud portal	38
Troubleshooting FortiSOAR Cloud HA instances	41
Default Secure Message Exchange Fails to Connect After HA Takeover	41
Backing up and Restoring FortiSOAR Cloud	42
Prerequisites	42
Backup Process	42
Data that is backed up during the backup process	43
Prerequisites for running the backup process	43
Performing a backup	43
Restoring data	44
Troubleshooting	45
Migration of FortiSOAR Cloud MSSP setup fails with the Secure Message Exchange Invalid credentials or certificate error	45

Upgrading FortiSOAR Cloud	46
Upgrading your FortiSOAR Cloud instance	46
Upgrading your FortiSOAR Cloud instance using the FortiSOAR Cloud portal	47
Upgrading your FortiSOAR Cloud instance by opening a Support ticket	48
Expanding resources for your FortiSOAR Cloud instance	48
Appendix A - Supported Regions	49

Change Log

Date	Change Description
2026-01-19	Enhanced the documentation related to disabling root shell access for csadmin users in the Deploying FortiSOAR Cloud chapter.
2025-12-22	Initial release of 7.6.5

Introduction

FortiSOAR Cloud is a cloud-hosted Security Orchestration & Automated Response (SOAR) platform, available via subscription through an a la carte SKU. FortiSOAR Cloud simplifies deployment, management, and scaling by eliminating the need for users to provision a virtual machine (VM) in their environment.

FortiCloud automatically sets up a cloud-based FortiSOAR instance with an integrated secure message exchange under your user account. Starting from release 7.6.0, FortiSOAR Cloud supports provisioning multiple FortiSOAR instances per account, enabling active-active clustering for horizontal scaling. For more details, see the [High Availability Capability for FortiSOAR Cloud](#) chapter.

Starting with release 7.6.1, Fortinet offers a managed upgrade service for FortiSOAR Cloud customers, simplifying the upgrade process. For more information, see the [Upgrading FortiSOAR Cloud](#) chapter.

This section includes the following topics:

- [Specifications](#)
- [Licensing](#)

FortiSOAR Cloud Virtual Machine Specifications

The FortiSOAR Cloud VM has the following default specifications:

- 8 available vCPUs
- 32 GB available RAM
- 1 TB available disk space: Recommended to have high-performance storage, preferably SSDs.
- 1 vNIC

High-volume systems (e.g., those with large alert ingestion or playbook execution) may require additional resources. Scale your FortiSOAR Cloud deployment by purchasing additional CPU, RAM, and Storage SKU, or by deploying a multi-node cluster. Contact your sales team for scalability and sizing details. For more information on expanding resources for your FortiSOAR Cloud instance, see the [Upgrading FortiSOAR Cloud](#) chapter.

A FortiCloud account is required to provision FortiSOAR Cloud. If you do not have one, create a FortiCloud account [[here](#)]. Access to FortiSOAR Cloud requires a primary FortiCloud account, which can invite secondary users to access FortiSOAR Cloud.

Licensing

You can purchase various FortiSOAR Cloud subscription licenses, including:

- FortiSOAR Cloud Enterprise License
- FortiSOAR Cloud MultiTenant Edition - Manager

- FortiSOAR Cloud Dedicated Tenant
- FortiSOAR Cloud Regional SOC

Each FortiSOAR Cloud instance license grants one VM instance for the duration of the license. Multiple instance licenses must be purchased to create a multi-node cluster, where clustering is supported by the license type.

Additional subscription feature licenses are available, including:

- FortiSOAR Cloud Threat Intel Management
This licensing option for the Threat Intelligence Management (TIM) Service includes FortiGuard Premium Threat Feeds, granting full access to TIM features, including unrestricted consumption of FortiGuard feeds. For details on unrestricted FortiGuard threat feeds, premium TIM features, and TIM SKUs, see the [Licensing](#) chapter in the FortiSOAR "Deployment Guide." For more information on TIM, see the [Threat Intel Management Solution Pack](#) documentation.
- FortiSOAR Cloud User Seat License
- FortiSOAR Cloud per-VM storage, CPU, and RAM Add-On, see the [Upgrading FortiSOAR Cloud](#) chapter for details

Contact your sales team to discuss licensing in detail.

A license expiration warning is displayed 30 days in FortiSOAR before the expiration date. Customers have a 3-day grace period to renew their contract and maintain access to the VM. After the grace period, the cloud portal will be inaccessible:

The screenshot displays the FortiSOAR Cloud management interface. The top navigation bar includes 'FortiSOAR Cloud', 'Service', and 'Support'. The user is logged in as 'admin.fsr@mailinator.com'.

The main content area is divided into three sections:

- Account Information:** Shows Account ID (1691118), Owner (FSR ADMIN), Account Email (admin.fsr@mailinator.com), Company (FortiSOAR), and Service Regions (Canada (Vancouver)-3).
- Assets:** Lists three assets with their IDs and status:

Asset ID	Status
FSRCLDTM23090082	Active
FSRCLDTM24090055	Expired
FSRCLDTM24090056	Active
- Instances / Clusters:** Shows a table of clusters:

Cluster	Region	Status	Health
Master Cluster	CA-WEST-3	Active	Available
Master Cluster_7_6_4	CA-WEST-3	Active	
Test	CA-WEST-3	Active	

FortiSOAR Cloud license contract registration

1. Ensure you have a FortiCare account.
2. Contact FortiSOAR Support for the FortiSOAR Cloud product SKU.
Note: By default, the FortiSOAR Cloud product SKUs comes with two users included. Additional users can be added by purchasing the 'Additional Users Entitlement' SKU.
3. Once you complete purchasing the FortiSOAR Cloud product SKU and/or the 'Additional Users' SKU, you will receive a service contract registration code at your registered email address.
4. Login to your FortiCare account and click **Asset > Register/Activate** to register your FortiSOAR Cloud product. Register your FortiSOAR Cloud product by following the instructions provided in the FortiCare

registration wizard.

Copy and paste the service contract registration code from the email to register FortiSOAR Cloud. After verification, click **Complete** to finalize the registration.

Deploying FortiSOAR Cloud

This section provides instructions on deploying FortiSOAR Cloud.



Starting with release 7.6.5, the `csadmin` user's `sudo` privileges are restricted to only the commands required to work with FortiSOAR Cloud, instead of providing full `'root'` access. This enhancement aligns with the principle of least privilege and reduces exposure to sensitive system files. Therefore, commands such as `yum`, `systemctl`, `csadm`, etc, must be prefixed with `sudo`, for example, `sudo csadm --help`.

To open or edit a file, prefix the command with `'sudo'` and specify the file's full path (`sudo vi <full path of file>`).

For example, `sudo vi /opt/cyops-auth/utilities/das.ini`.

Additionally note that for security reasons, `'root'` access is provided via the system console and is not available over SSH.

To deploy FortiSOAR Cloud:

1. Ensure that you have a product entitlement for FortiSOAR Cloud and note your account ID number in the FortiCloud portal:

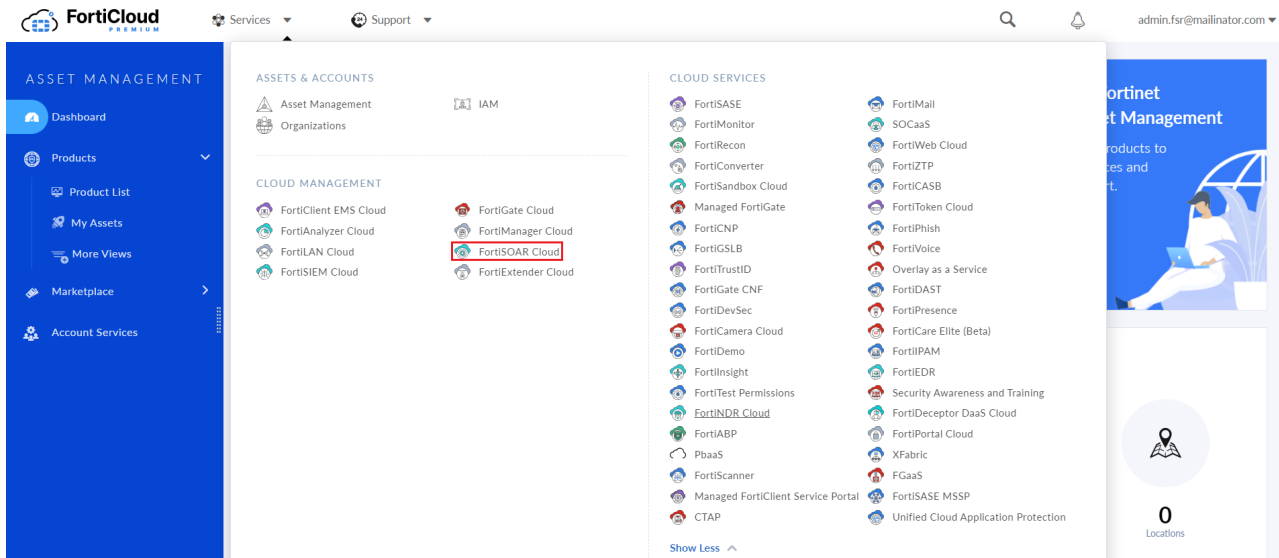
The screenshot shows the FortiCloud Premium portal interface. The top navigation bar includes 'Services', 'Support', and the user's email 'admin.fsr@mailinator.com'. The main content area is titled 'View Products: 18 Units' and contains a table of products. A red box highlights the account ID '1691118/FortiSOAR' in the top right corner of the product list. The table below shows various products, including FortiSOAR Cloud and HA Perpetual licenses.

SERIAL NUMBER	PRODUCT MODEL	DESCRIPTION	START DATE	END DATE
FCTEMS0000124139	FortiClient EMS	FortiClient EMS Cloud	2024-06-25	2024-06-26
FSRCLDTM23090042	FortiSOAR Cloud	FortiSOAR TENANT	22 days	2023-08-16
FSRCLDTM24090068	FortiSOAR Cloud	FortiSOAR Cloud For HA	2025-06-03	2024-06-03
FSRCLDTM24090069	FortiSOAR Cloud	FortiSOAR CLOUD	2025-06-03	2024-06-03
FSRCLDTM24090161	FortiSOAR Cloud	Tenant License	2025-07-11	2024-07-11
FSRVMPMTM24090056	FortiSOAR	HA Perpetual 1	No coverage	2024-07-10
FSRVMPMTM24090057	FortiSOAR	HA Perpetual 2	No coverage	2024-07-10

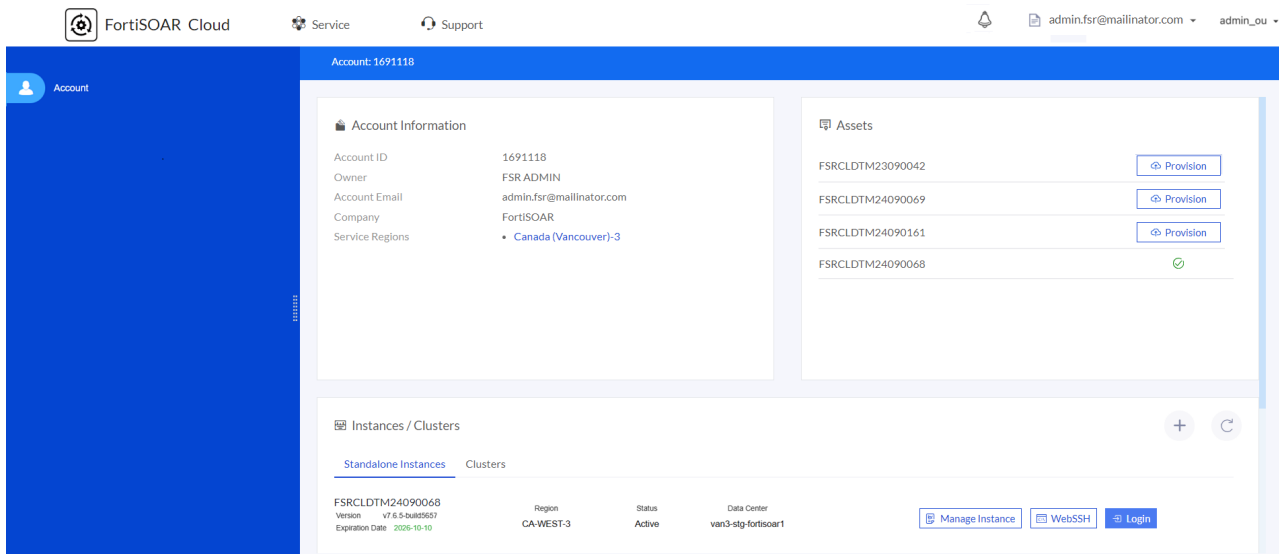


Wait for 30 minutes after creating a FortiCloud account before proceeding to the next step.

2. Access your FortiSOAR Cloud instance by clicking **Services** on the FortiCloud portal, and then selecting **FortiSOAR Cloud** from the Cloud Management section:

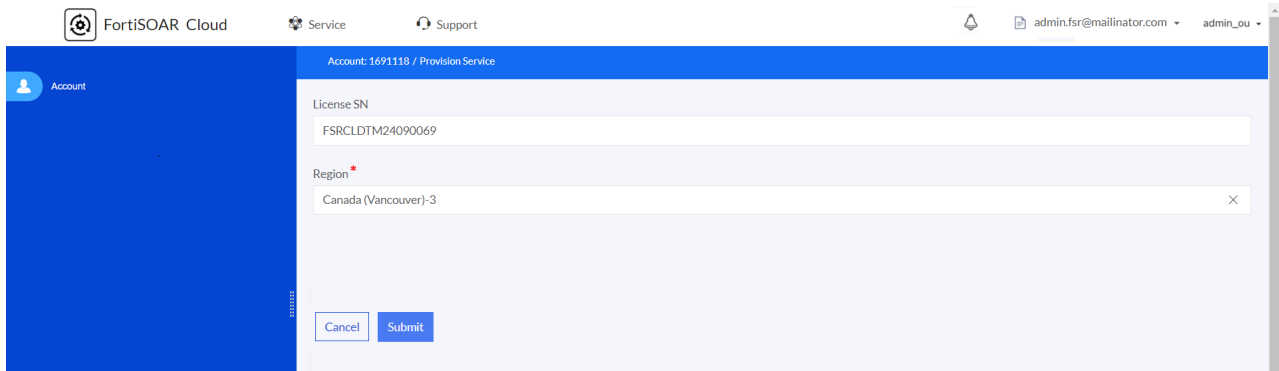


3. Once you log onto FortiSOAR Cloud, from the left menu select the 'Master' FortiSOAR account. This displays all the information associated with this account including the dedicated instance's Account ID:

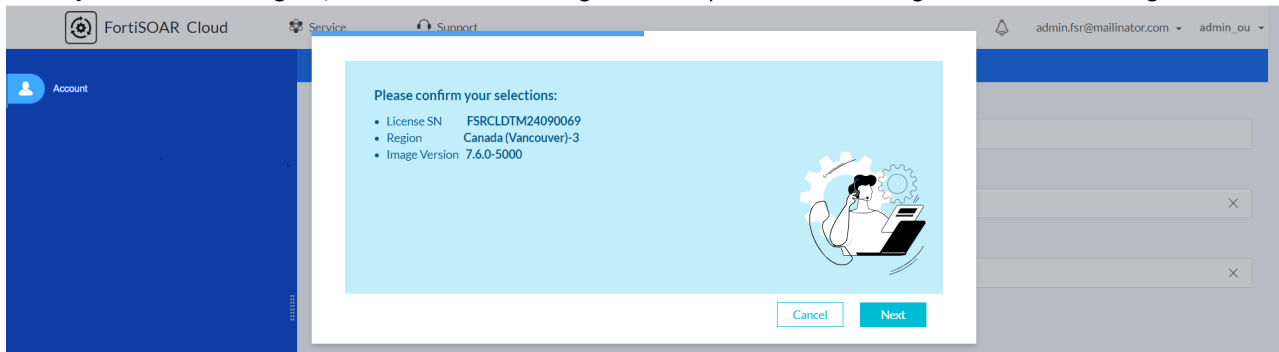


4. In the Asset section, click **Provision** next to the license serial number of the FortiSOAR instance you wish to provision. This opens the Provision Service page, where you can choose the **Region** for provisioning the

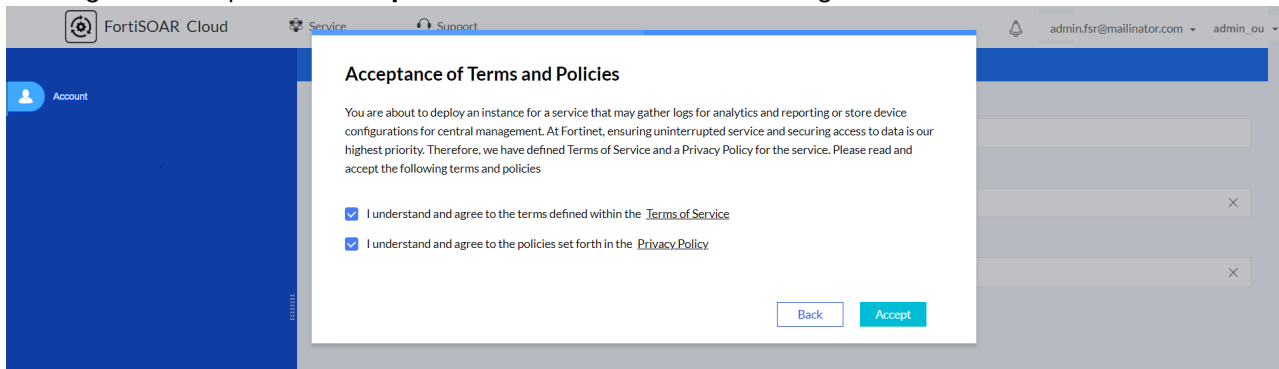
instance:



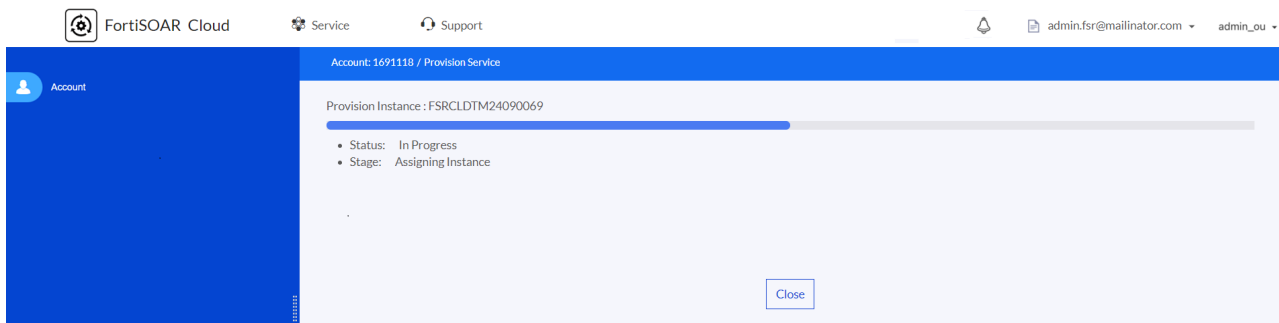
5. Once you select the region, click **Submit**. Clicking **Submit** opens the following confirmation dialog:



6. Clicking **Confirm** opens an **Acceptance of Terms and Policies** dialog:



Select the Terms and Policies and click **Accept** to initiate the provisioning of the FortiSOAR instance. The provisioning process takes a few minutes:



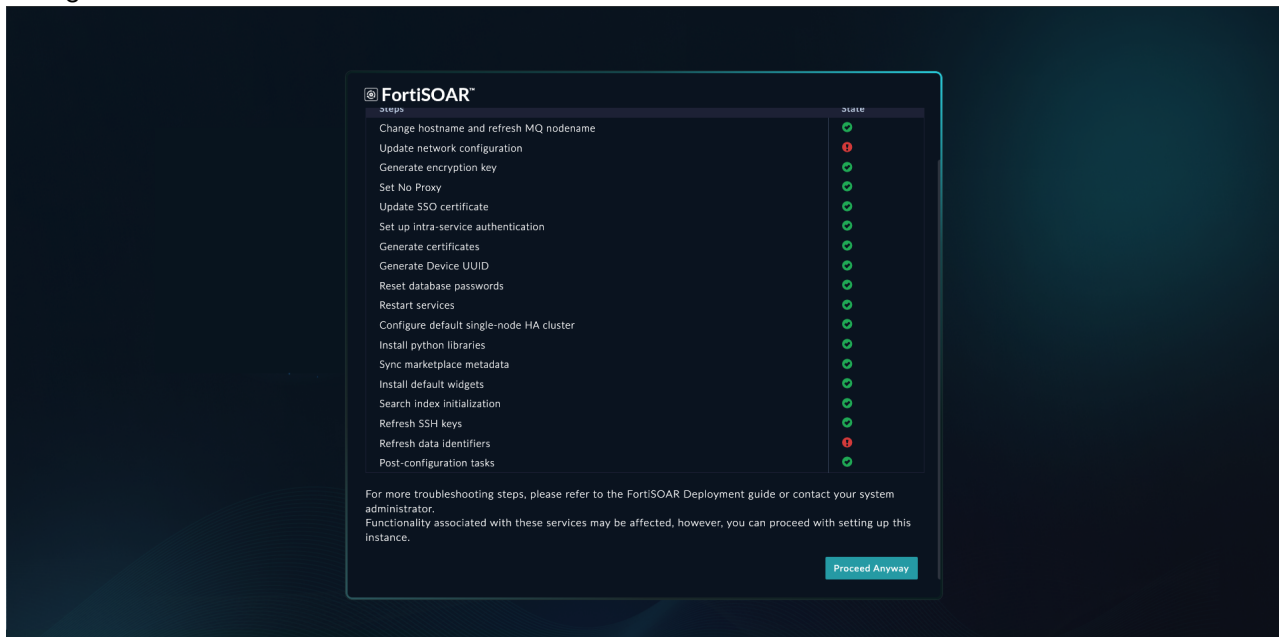
During provisioning, initial configuration steps for FortiSOAR are performed. These steps include running the automated, non-interactive FortiSOAR configuration wizard, enabling the embedded Secure Message

Exchange, triggering the heartbeat between FortiCloud and FortiSOAR, and installing the selected license.



FortiSOAR VM provisioning is considered successful only after FortiCloud receives the first heartbeat from FortiSOAR.

If there are any provisioning failures, such as failures during the initial configuration phase using the automated non-interactive FortiSOAR configuration wizard, including failures while configuring the embedded Secure Message Exchange, then a failure screen detailing the status of each configuration step is displayed, making it simpler to identify the issue. Before using FortiSOAR Cloud, you must use WebSSH to fix any issues with the failed steps as their functioning might be hampered. However, if you choose to access FortiSOAR Cloud without rectifying the failed steps, which can cause FortiSOAR functionality to deteriorate, a **Proceed Anyway** button is provided that lets you to use the product while acknowledging the configuration failure:



If your instance is not accessible even after clicking **Proceed Anyway**, you can try the following steps to fix the issues:

- Restart all the services using the `sudo csadm services --restart` command.
- Manually install ansible in the case of an ansible installation error using the following command:
`sudo -u nginx /opt/cyops-workflow/.env/bin/pip install ansible==7.4.0 --extra-index-url https://repo.fortisoar.fortinet.com/prod/connectors/deps/simple/`
- If the failure screen keeps getting displayed on the FortiSOAR Cloud UI, even after you have attempted to resolve all the backend issues, then you can update the `fsr-boot.json` to update its state from 'failed' to 'config_vm_failure_acknowledged'.

Contact support if failures persist even after troubleshooting.

Once provisioned successfully access the FortiSOAR web GUI by clicking **Login** or click **WebSSH** to access the FortiSOAR console to begin using FortiSOAR Cloud. For more information, see the [Beginning with FortiSOAR](#)

Cloud chapter.

Important notes to be considered before starting to use FortiSOAR Cloud instance:

- After provisioning the FortiSOAR Cloud instance, it is highly recommended that you log in to the WebSSH interface and immediately change the default 'csadmin' user's password. This step enhances the security of your FortiSOAR Cloud instances.
- Only the primary account holder can create secondary account holders in FortiCloud. Secondary account holders can log in as restricted users to the same instance. The primary account holder can modify the admin profile for the secondary user. For more information, see the [Adding a secondary account](#) chapter.
- To restrict access to your FortiSOAR instance, contact the FortiCloud team to add IP addresses to the allowlist. Once added, only those IP addresses can access your FortiSOAR instance.
- Starting with release 7.6.5, the 'Data Center ID' is displayed on the Manage Instance page, allowing users to identify which instance is deployed in which data center.

Troubleshooting

Uniqueness error when adding a tenant in an MSSP setup using the Secure Message Exchange

The embedded Secure Message Exchange (SME) that is enabled by default in the case of FortiSOAR Cloud throws the uniqueness error only when the tenant and master nodes are located in the same Cloud region.

Resolution

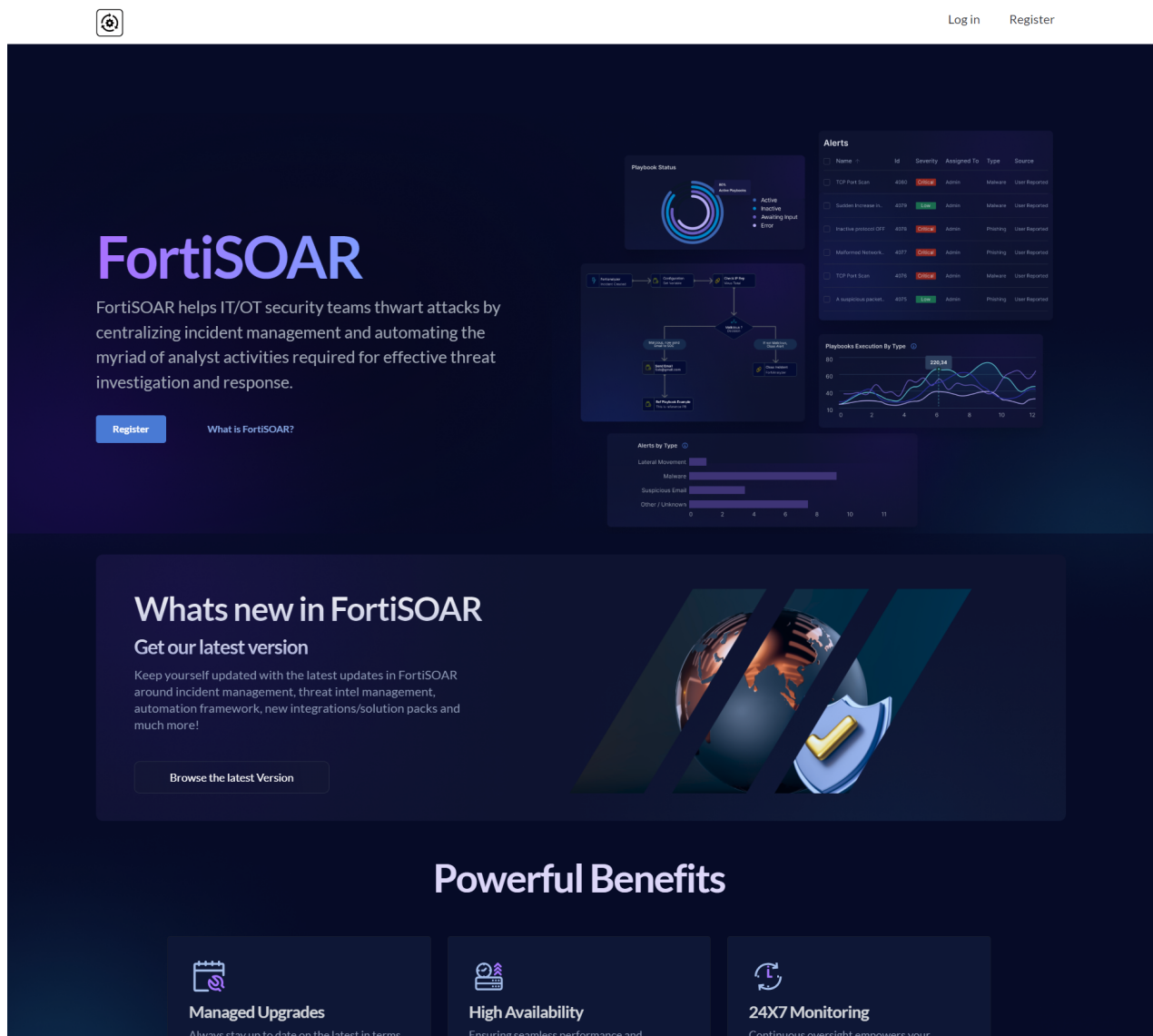
To resolve this issue, make sure to update the name of the SME on either the master node or the tenant node before configuring your MSSP setup.

Beginning with FortiSOAR Cloud

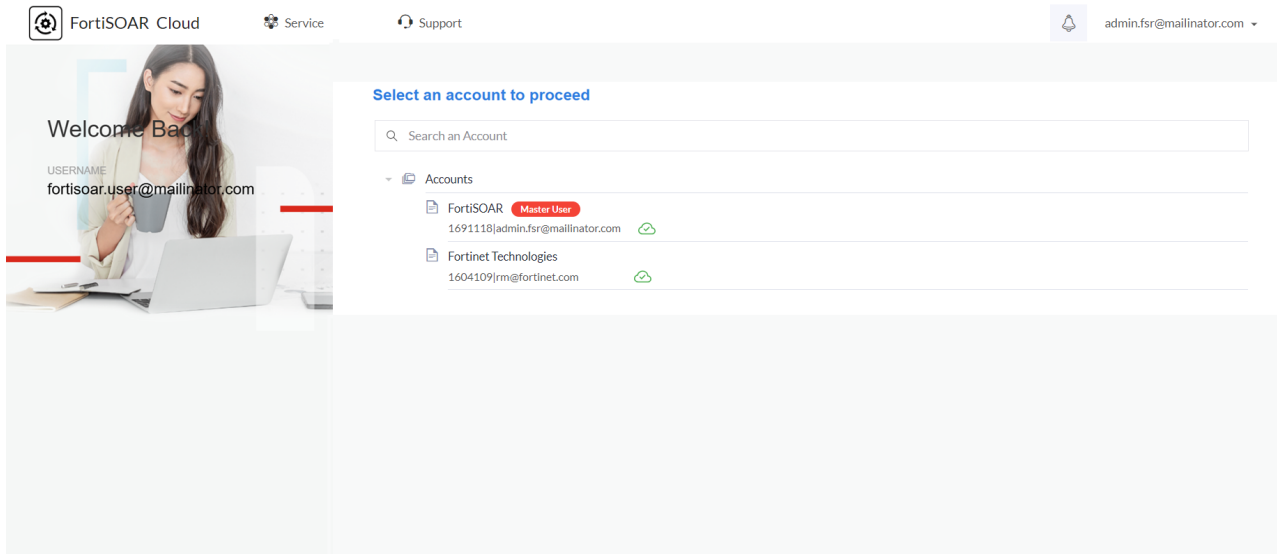
Accessing FortiSOAR Cloud

You can access FortiSOAR Cloud in the following ways:

- Using fortisoar.fortinet.com - This displays the FortiSOAR Cloud portal's landing page:



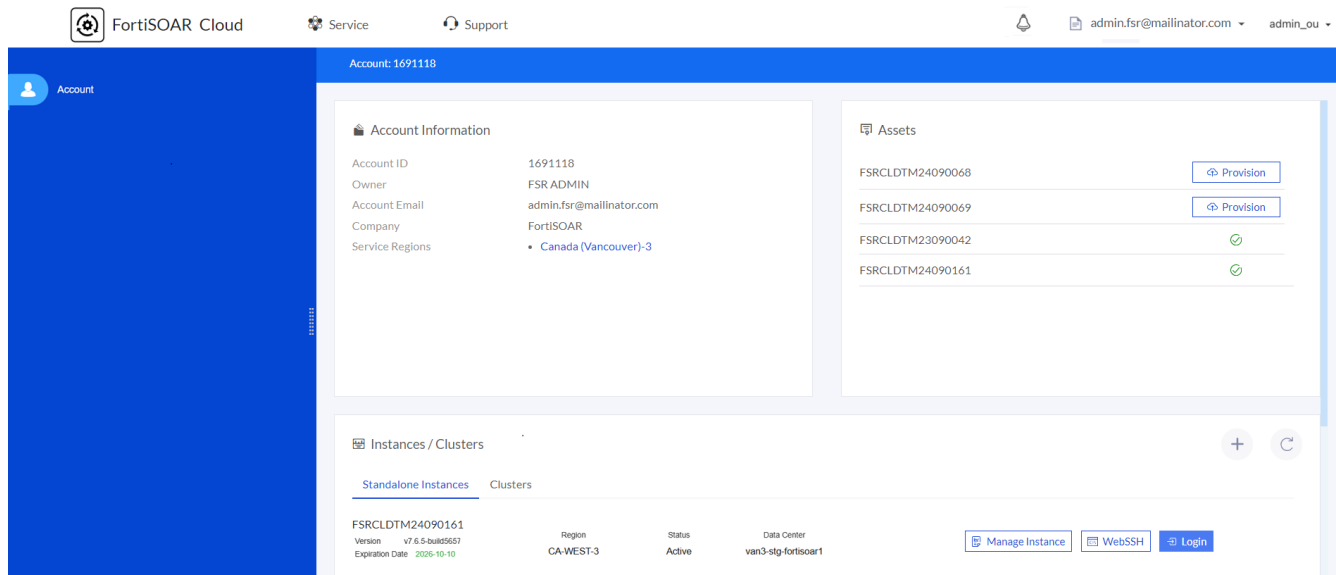
Clicking **Log in** displays the Organization Unit (OU) or Accounts page, which lists the master account and all the sub-user accounts:



Select the account whose details you want to view.

- Using support.fortinet.com - This directly displays the Organization Unit (OU) or Accounts page if the FortiSOAR Cloud instance is provisioned with a valid license.

Selecting an account Organization Unit (OU) or Accounts page displays a page containing the details of that account, as well as any assets, instances, and clusters associated with it:



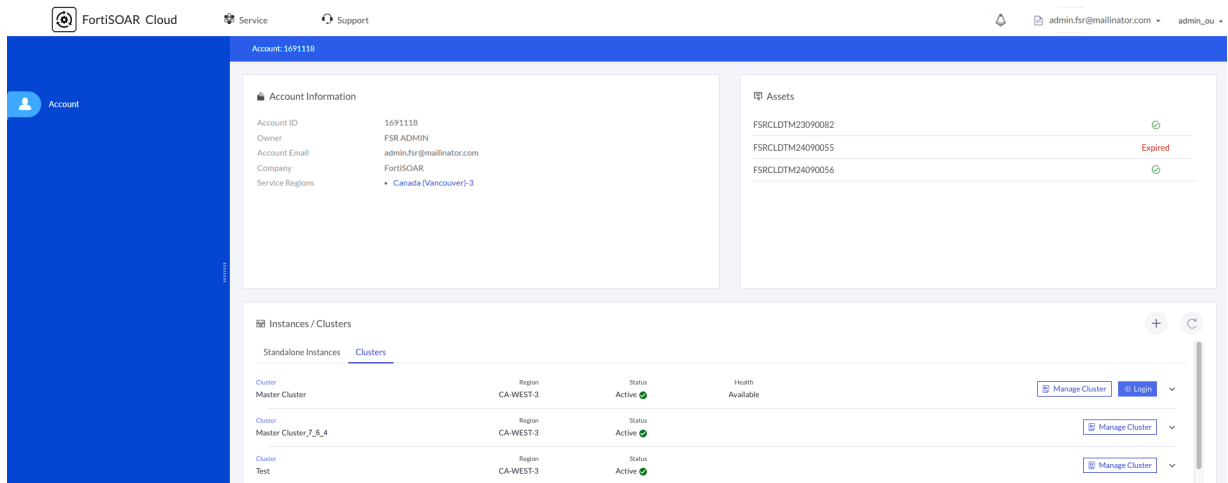
The **Master** tag is used to indicate the master account while the rest are sub-user accounts.

NOTE: Provisioning can only be done by the 'Master' account.

The account page also displays the following details:

- **Account Information:** Displays general information about the account including its ID, owner, email address, company, and service region.
- **Assets:** This section displays a list of assets (active licensed instances) associated with account, categorized as follows based on the icons/buttons next to each asset:

- **Green Check** icon: Successfully provisioned instance.
- **Blue Provision** button: Instance yet to be provisioned.
- **Red Provision** button: Provisioning failure for the instance.
NOTE: If provisioning fails for an instance, you can view the details of the failure by clicking on the **Red Provision** button.
- **Expired** text in red: License for the instance has expired:



- **Instances/ Clusters:** This section includes the following tabs:
 - **Standalone Instances:** Displays a list of provisioned standalone instances that are not part of any cluster. Each row provides brief details of the instance including its version, expiration date, region and status. You can also use the following buttons:
 - **Login:** To access the FortiSOAR UI. For more information, see the [Accessing FortiSOAR Cloud UI](#) topic.
 - **WebSSH:** To access the FortiSOAR Cloud console. For more information, see the [Accessing FortiSOAR Cloud console](#) topic.
 - **Manage Instance:** To view the Instance page that contains details about that instance and is used to manage the instance. For more information, see the [Instance page details](#) topic.
 - **Clusters:** Displays a list of clusters. Each row provides brief details of the cluster including its name, region, status, and health. Click the arrow to expand the cluster row and view information about instances in the cluster. You can also use the following buttons:
 - **Login:** To access the FortiSOAR UI. For more information, see the [Accessing FortiSOAR Cloud UI](#) topic.
 - **Manage Cluster:** To view the Cluster Info page that contains details about that cluster and is used to manage the cluster. For information about cluster instances, see the [High Availability capability for FortiSOAR Cloud](#) chapter.

Instance page details

The Manage Instance page provides details such as the instance ID, license information, disk usage etc.

The screenshot displays the FortiSOAR Cloud interface for managing an instance. The top navigation bar includes 'FortiSOAR Cloud', 'Service', and 'Support'. The user is logged in as 'admin.fsr@mailinator.com'.

The main content area is divided into several sections:

- Instance Information:** Contains two tabs: 'General' and 'Cluster Node Info'. The 'General' tab shows:
 - Instance ID: ad3a5012-9cbc-4fe3-ad14-07de675c18a
 - Expiration Date: 2028-10-07
 - License SN: FSRLDTM24090338
 - Service Version: v7.6.5-build5657
 - Region: CA-WEST-3
 - Status: Active
 A 'Reboot' button is located at the bottom of this section.
- License Details:** A table showing license information:

Support Type Desc	Type	Level	Start Date	End Date	Status
FortiSOAR Multi Tenant - Regional S...	143	6	Oct 7, 2025	Oct 7, 2026	Active
FortiSOAR User Login	144	6	Oct 7, 2025	Oct 7, 2026	Active
- Disk Usage:** A donut chart showing 0.84% usage. Below the chart, it states: 'Disk: 1000.00 GB Used: 8.40 GB'.
- Resource Usage:** Two progress bars:
 - vCPU (8): 1.5%
 - RAM (32 GB): 32.2%
- Upgrade:** A section with the text: 'You can raise an upgrade request for your FortiSOAR instance by clicking on "Initiate Upgrade Request" button'. A blue 'Initiate Upgrade Request' button is present.

At the bottom of the page, there are links for 'Terms of Service', 'Privacy Policy', 'Release Notes', and 'Feedback'. The footer includes 'v24.4 b5029 Copyright © 2024 Fortinet, Inc. All rights reserved.'

It includes the following sections:

- **Instance Information:** This section has two tabs, General and Cluster Node Info. You can reboot the instance by clicking the **Reboot** button.
 - **General:** Displays details such as the instance ID, its expiration date, FortiSOAR release on which the instance is provisioned, such as release 7.5.0-4015, its status, etc.
 - **Cluster Node Info:** If the instance is part of a cluster, then this tab shows information about the node's role, health, and status, etc.
- **License Details:** Displays details such as the type of license deployed on the instance, the start and end date for the license, etc.
- **Disk Usage:** Displays disk usage details in percentage and numbers.
- **Resource Usage:** Displays the vCPU and RAM usage.

NOTE: If you need to expand the resources for your FortiSOAR Cloud instance, follow the Expanding resources for your FortiSOAR Cloud instance process mentioned in the [Upgrading FortiSOAR Cloud](#) chapter.
- **Upgrade:** Fortinet offers a managed upgrade service for FortiSOAR Cloud customers, simplifying the upgrade process. To initiate an upgrade, click the **Initiate Upgrade Request** button. For more information on the upgrade process, see the [Upgrading FortiSOAR Cloud](#) chapter.

Accessing FortiSOAR Cloud console

To access the FortiSOAR Cloud console, click **WebSSH** on the FortiCloud portal. If you are logging into the console for the first time, then you must enter the default SSH credentials, which are `csadmin/<your_account_id>`. You will be asked to change the default SSH passwords after successfully logging into the console:

```
You are required to change your password immediately (administrator enforced)
-----
Built on: 2023-06-24
Rocky Linux Version: 8.8
FortiSOAR Version: 7.4.1-3167
-----
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user csadmin.
Current password:
```

Once you update the default password, you will be logged out and again asked to log in using the updated credentials. Once you log in, you will be presented with the EULA acceptance pages (2 pages):

```
| EULA - Page 2 of 2 |
GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by
the copyright holder saying it may be distributed under the terms of this General
Public License. The "Program", below, refers to any such program or work, and a "work
based on the Program" means either the Program or any derivative work under copyright
law: that is to say, a work containing the Program or a portion of it, either verbatim
or with modifications and/or translated into another language. (Hereinafter,
translation is included without limitation in the term "modification".) Each licensee
is addressed as "you".

Activities other than copying, distribution and modification are not covered by this
License; they are outside its scope. The act of running the Program is not restricted,
and the output from the Program is covered only if its contents constitute a work
based on the Program (independent of having been made by running the Program). Whether
that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you
receive it, in any medium, provided that you conspicuously and appropriately publish
on each copy an appropriate copyright notice and disclaimer of warranty; keep intact
all the notices that refer to this License and to the absence of any warranty; and
5%
```

Click **Accept** to accept the EULA. Once the EULA is accepted, you can start to use the FortiSOAR Cloud console. You can use the FortiSOAR Cloud console and perform various administrative tasks using the 'csadm' commands

on the console:

```
Rocky Linux Version: 9.4
FortiSOAR Version: 7.6.0-5012
Upgraded on: 2025-12-12
-----
Last login: Fri Dec 12 10:56:51 2025 from 10.96.131.138
[csadmin@idnea5135o76t2o2zbf ~]$ sudo csadm
usage: csadm [-subcommand] [-options]
          [-subcommand] [-options] Run subcommand
          [-subcommand] [-help] Show detailed help of subcommand
          [-help] Show this message

csadm subcommands are:
certs          - Generate and deploy certificates
db             - Manage database
hostname      - Change hostname
license       - Manage license
user          - Manage users
log           - Manage log
mq            - Manage message queue
secure-message-exchange - Manage Default (Embedded) Secure Message Exchange
network       - Manage network
services      - Manage services
ha            - Manage HA cluster
system        - Manage system settings
package       - Manage package
upgrade       - Manage upgrade
[csadmin@idnea5135o76t2o2zbf ~]$
```

Accessing FortiSOAR Cloud UI

To access the FortiSOAR UI, click **Login** on the FortiCloud portal. On the FortiSOAR UI, you will be asked to accept the EULA if it is not already accepted. Once you accept the EULA, you will be logged into the FortiSOAR UI. The role that you have been assigned, i.e., a 'Full Access' user or a 'Limited Access' user, determines the actions you can perform in FortiSOAR. For information on FortiSOAR features and how to use and configure them, see the [FortiSOAR Documentation Library](#).

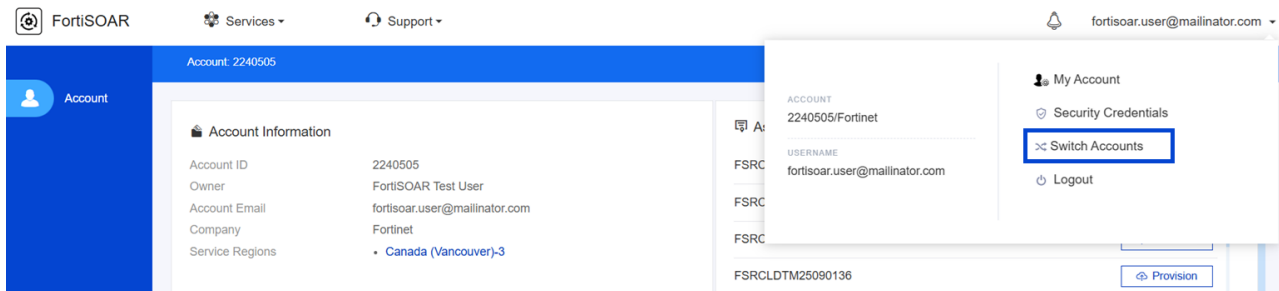
By default, the SOAR Framework Solution Pack is installed on FortiSOAR Cloud. The SOAR Framework Solution Pack (SP) is the **Foundational** Solution Pack that creates the framework, including modules, dashboards, roles, widgets, etc., required for effective day-to-day operations of any SOC. Also, the Incident Response modules, i.e., Alerts, Incidents, Indicators, and War Rooms, are not part of the FortiSOAR Cloud platform, making it essential to optimally use and experience FortiSOAR Cloud's incident response. For detailed information about the SOAR Framework SP, see the [SOAR Framework SP](#) documentation.

Switching between Accounts

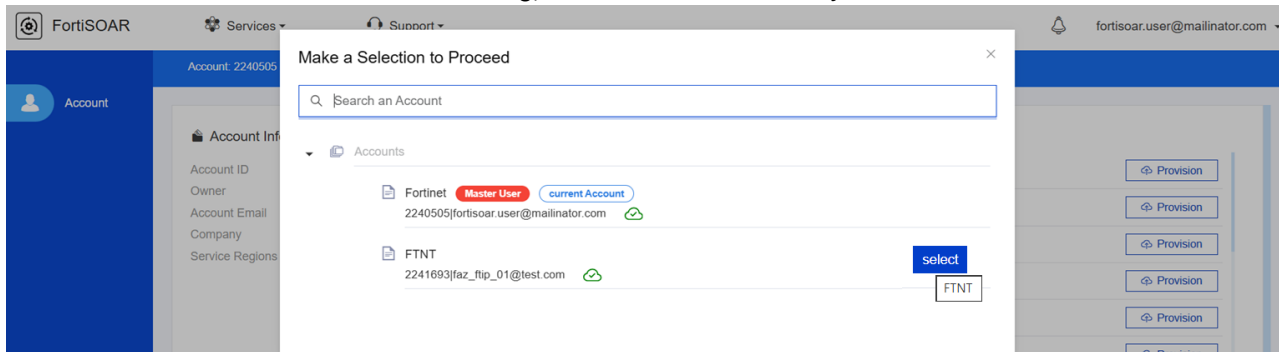
You can switch between your available accounts using the **Profile** menu. If you are signed in with your email credentials, you can switch to any linked user accounts. Note that available options may vary depending on your account permissions and linked accounts.

To switch to a new account:

1. Click your **Profile** icon in the top-right corner.
2. Select **Switch Accounts**:



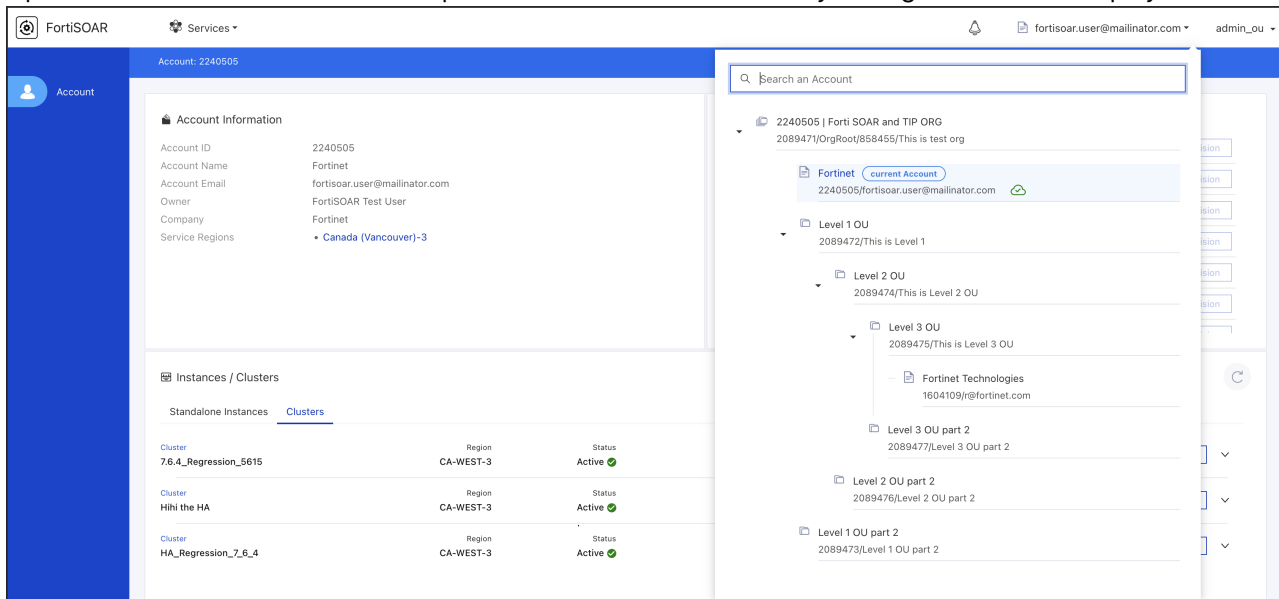
3. In the **Make a Selection to Proceed** dialog, select the user account you want to switch:



To switch to a different Organizational Unit (OU) account:

Note: This process applies to **IAM and IdP users** only.

1. Open the **OU Account Selection** drop-down menu. Accounts within your organization are displayed:



2. Select an account within your available scope (OU) by hovering over the appropriate member account and clicking **Select**.

Secure Message Exchange

The FortiSOAR Cloud instance contains an embedded FortiSOAR Secure Message Exchange (SME). A secure message exchange establishes a secure channel that is used to relay information to external agents or dedicated tenant nodes. The address of the embedded SME is set as the Cloud portal address, and Server Name Indication to the instance URL. The embedded SME runs on port 5671.

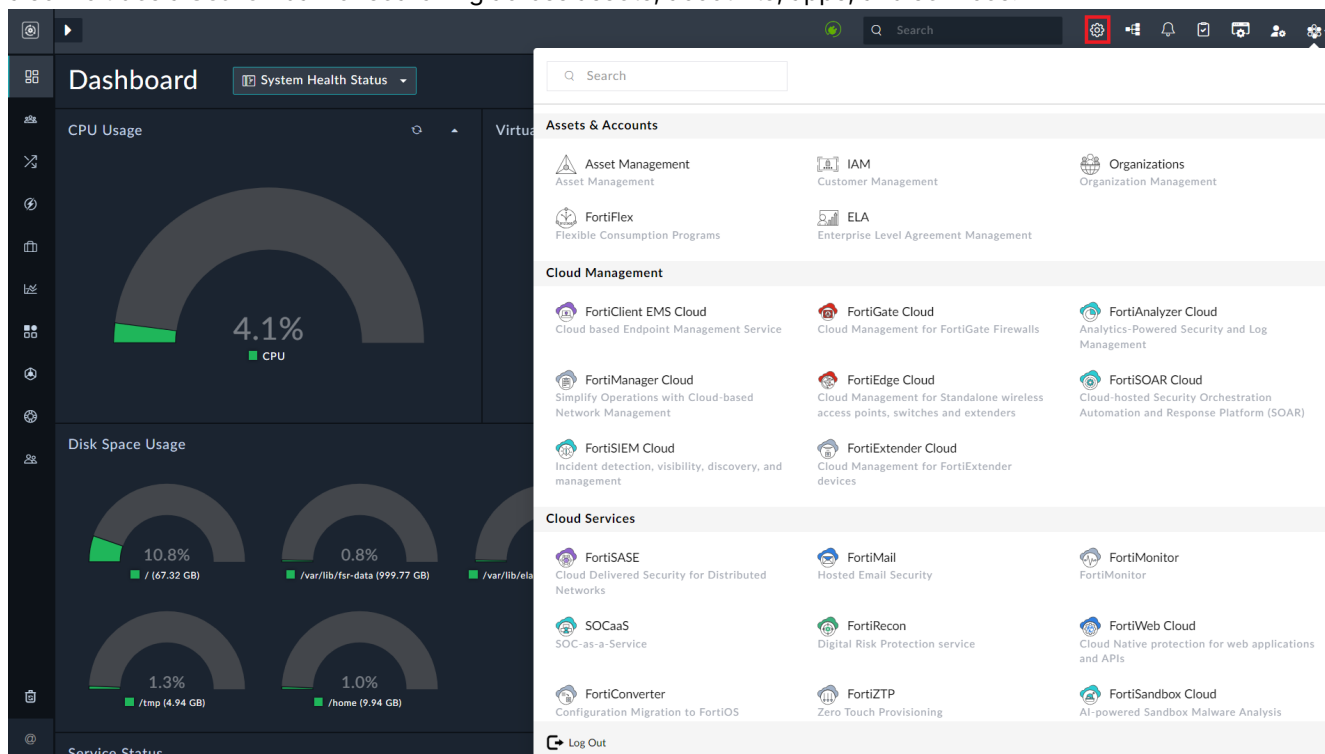


If a FortiCloud account is migrated, you must update the Server Name Indication to the URL of the new instance.

In case of a cluster, the Server Name Indication of the SME must be updated to the URL of the cluster. This ensures that requests are load balanced between instances.

Cloud App Menu

FortiSOAR displays an **App Menu** for users logging in through the Cloud portal. The App Menu appears in the FortiSOAR top bar and provides access to other cloud applications, such as FortiEDR and FortiAnalyzer Cloud. It also includes a **Search** bar for searching across assets, accounts, apps, and services:



When you click on another cloud app, such as FortiAnalyzer Cloud, you will be redirected to that app's cloud portal and logged out of both FortiSOAR and the FortiSOAR Cloud Portal. Clicking the **Log Out** button will also log you out of both FortiSOAR and the FortiSOAR Cloud Portal.

Settings

The 'Settings' icon in the top bar allows administrators to customize FortiSOAR Cloud and configure default options used throughout the system. For more information, see the "Administration Guide" that is part of the [FortiSOAR Documentation](#).

FortiSOAR supports internationalization via a system widget named "Language Pack" that includes the supported languages. This widget is automatically installed during the installation or upgrade of FortiSOAR Cloud to release 7.5.0 or later.



The "Language Pack" widget is a system widget that cannot be uninstalled, and you should not modify it. Making changes to it can result in translation issues, causing the FortiSOAR Cloud UI to appear in English. English serves as the fallback language for FortiSOAR Cloud. Any content that is not translated will be shown in English.

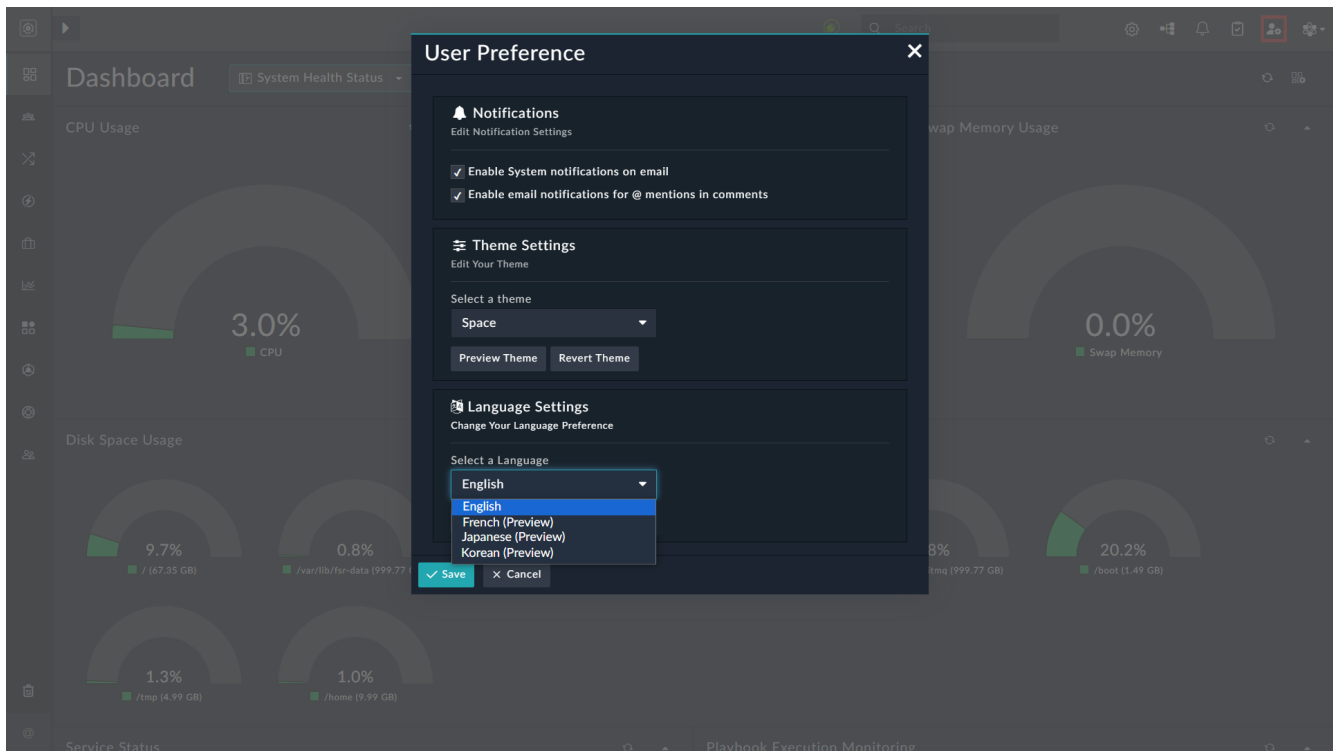
Administrators must be assigned the 'Read' or 'Usage' permission on 'Widgets' (in addition to other necessary permissions) to modify the global language settings. Without this permission, the FortiSOAR UI remains in English, regardless of the language you set. Administrators can set the language for FortiSOAR from the supported options:

- English (Default)
- Japanese (Preview)
- Korean (Preview)
- Simplified Chinese (Preview)
- French (Preview) [added in FortiSOAR release 7.6.4]
- Traditional Chinese (Preview) [added in FortiSOAR release 7.6.4]

This language setting will apply to all users; however, users can set their language preference in their user profile, and the user's preference will take precedence over the administrator's setting.

User Preferences

The 'user profile' icon in the top bar allows users without access to the 'Security' module to edit their profile. You can customize your profile to set the email notification options, theme, and language for your FortiSOAR instance:



To edit your user preferences, click the **User Profile** icon to display the User Profile dialog. On the User Profile dialog, you can set the following preferences:

- In the Notifications section, set your notifications preference:
 - Select **Enable System notifications on email** to receive system notifications on your email account.
 - Select **Enable email notifications for @mentions in comments** to receive notifications for @ mentions in comments.
- In the Themes Settings section, select the FortiSOAR theme you want to use; you can choose between **Dark**, **Light**, and **Space**, with **Space** being the default. Click **Preview Theme** to see the UI in the selected theme. To go back to the original theme, after previewing the theme, click **Revert Theme**.
- In the Language Settings section, set your language preference from the supported options: English, Japanese (Preview), Korean (Preview), Simplified Chinese (Preview), French (Preview) [added in FortiSOAR release 7.6.4], and Traditional Chinese (Preview) [added in FortiSOAR release 7.6.4]. Starting with release 7.5.0, FortiSOAR supports internationalization via a system widget named "Language Pack" that includes the supported languages.

NOTE: To customize the language for your FortiSOAR instance, you must be assigned the 'Read' or 'Usage' permission on 'Widgets'. Without this permission, the UI of your FortiSOAR instance will remain in English, regardless of the language you set in your profile.

Your preferred language will take precedence over the administrator's setting. For example, if the administrator has set the language to 'Korean', but you prefer 'Japanese', you can select Japanese in your profile, and the UI of your instance will be displayed in Japanese.

To set your language preference, from the **Select a Language** drop-down list select your preferred language.

Once you have completed updating your profile, click **Save** on the User Profile dialog.

List of logs that can be used for debugging FortiSOAR Cloud



If you face any issues with your FortiSOAR Cloud instance, contact Fortinet Support for assistance.

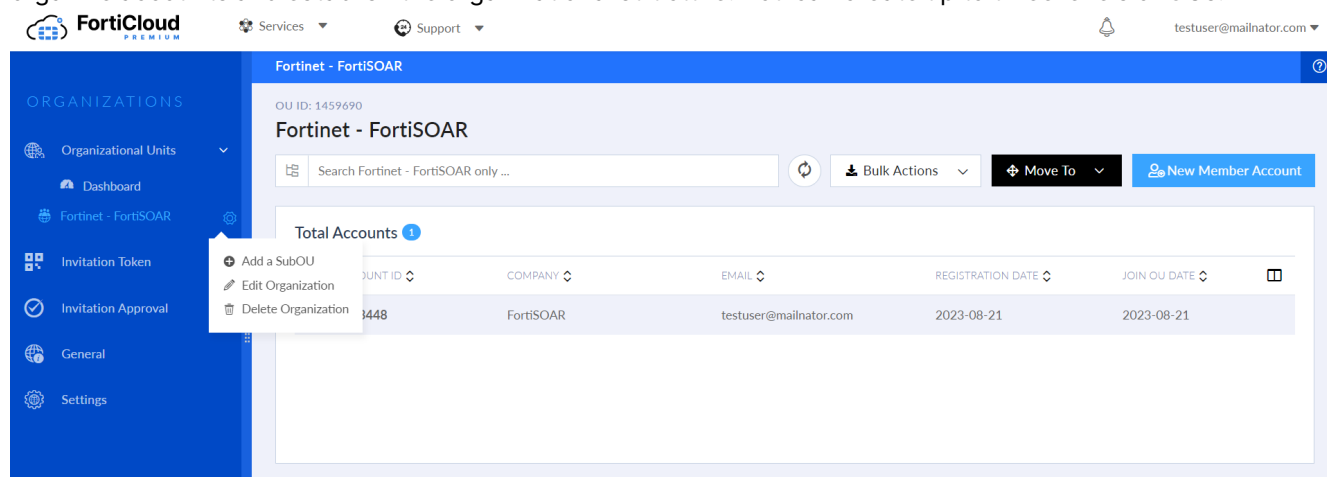
Additionally, administrators can use various logs that FortiSOAR generates to troubleshoot FortiSOAR Cloud issues:

Log Name	Purpose
<code>/var/log/cyops/install/config-vm-<time-stamp-here>.log</code>	Used for troubleshooting issues that occur while configuring the VM.
<code>/var/log/cyops/fcloud/</code>	Used for troubleshooting issues related to other cloud-related apps.
<code>/var/log/cyops/csadm/secure-message-exchange.log</code>	Used for troubleshooting issues related to the secure message exchange.

Adding an organization

You can create an organization for FortiSOAR Cloud. An organization is a centralized account management service that consolidates multiple FortiSOAR Cloud accounts into Organization/Organizational Units (OUs). The service offers a unified management interface across FortiCloud accounts to manage assets and cloud services, inviting accounts, hierarchical account grouping (OUs), and access roles for user permissions. For more information, see the [FortiCloud Account Services Organization Portal](#) documentation.

Create your organization, for example, 'Fortinet FortiSOAR', using the steps mentioned in the [FortiCloud Account Services Organization Portal](#) documentation. The account used to set up the organization serves as the 'root' account. Authorized users can add OUs and invite members to join the organization. OUs act as folders to organize accounts and establish the organizational structure. You can create up to three levels of OUs:



After creating the Organization and OUs, you can invite Member Accounts to join the OUs using invitation tokens as described in the [FortiCloud Account Services Organization Portal](#) documentation. Additionally, you can add an administrative IAM user for the organization to create and manage IAM users within the OUs. For more information see the [Adding a secondary account](#) chapter.

Adding a secondary account

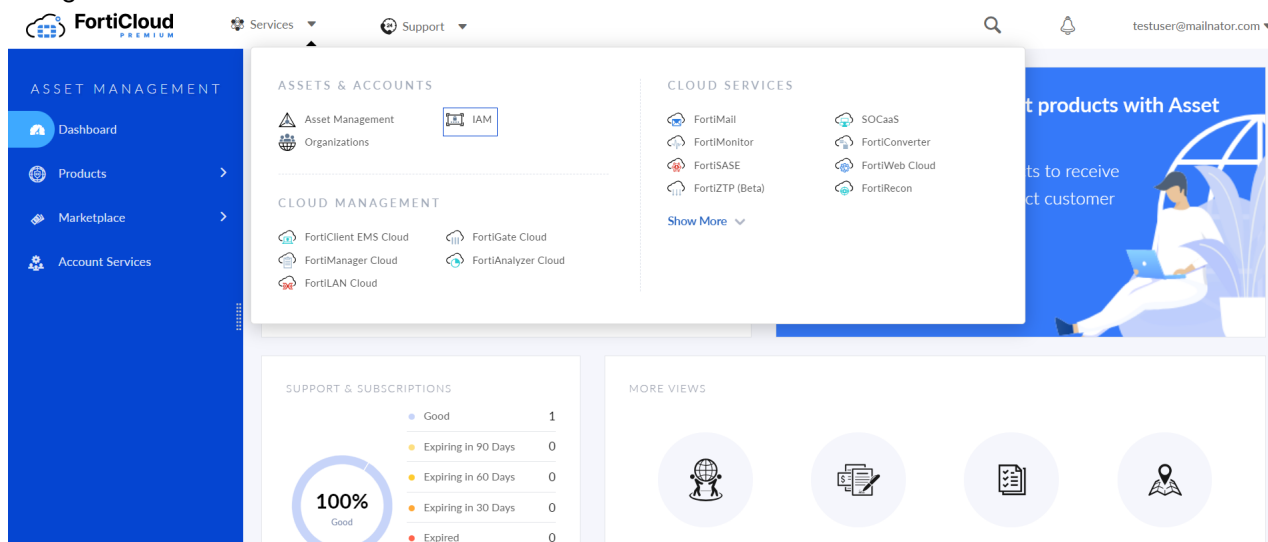
You can create a secondary account for FortiSOAR Cloud to allow the Fortinet support team to troubleshoot FortiSOAR Cloud deployment. A secondary account can be added using Identity & Access Management (IAM), or FortiCare, or by setting up External IdP roles. IAM helps manage access to FortiSOAR Cloud portals and assets, allowing control over users, authentication credentials, and asset permissions.



Organizational Units (OUs) are only visible to IAM users, not to secondary users added using FortiCare.

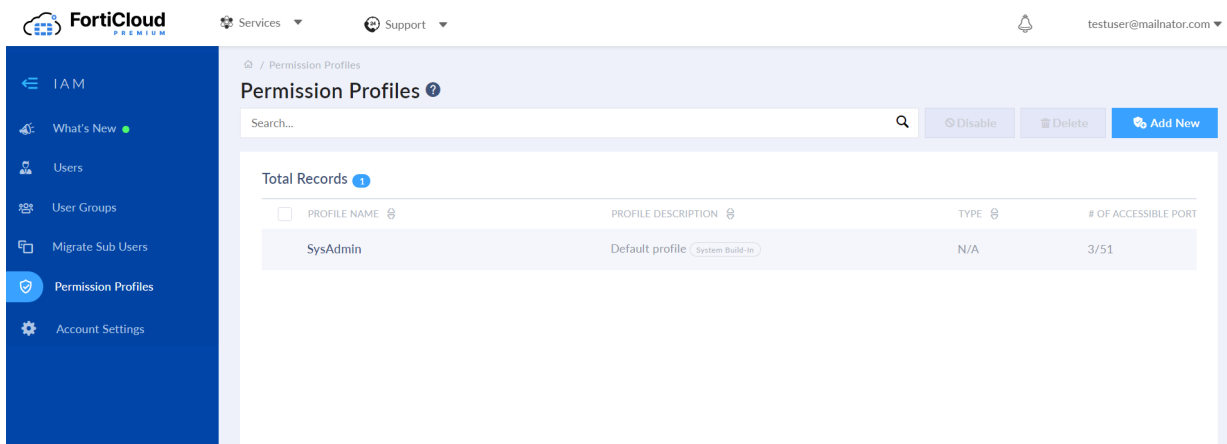
Adding a secondary account using IAM

1. Login to <https://support.fortinet.com/>.
2. Navigate to **Services > IAM**.

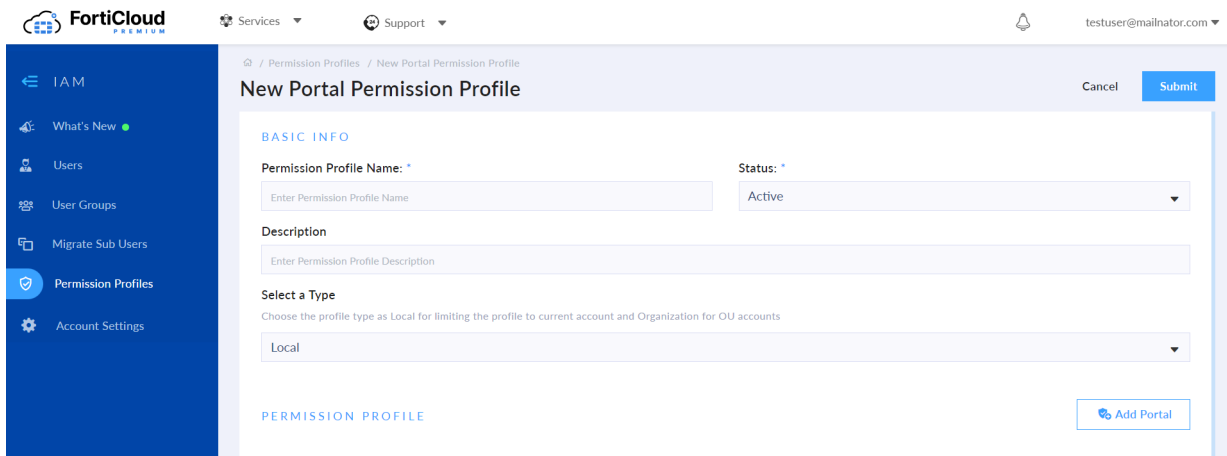


3. Before you can create IAM users, you must create permission profiles. Permission profiles define the level of portal access and permissions a user has. Permission profiles allow you to explicitly enable or disable access to FortiSOAR Cloud portals and grant portal-specific permissions for the enabled portals. To create permission profiles, do the following:

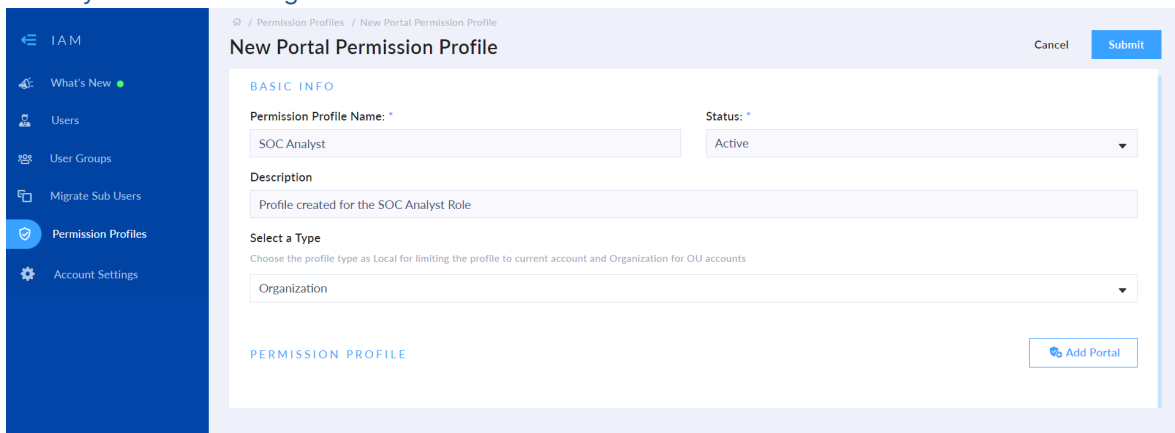
- a. Click the **Permission Profiles** menu item on the IAM portal:



- b. Click **Add New** to display the New Portal Permission Profile page:

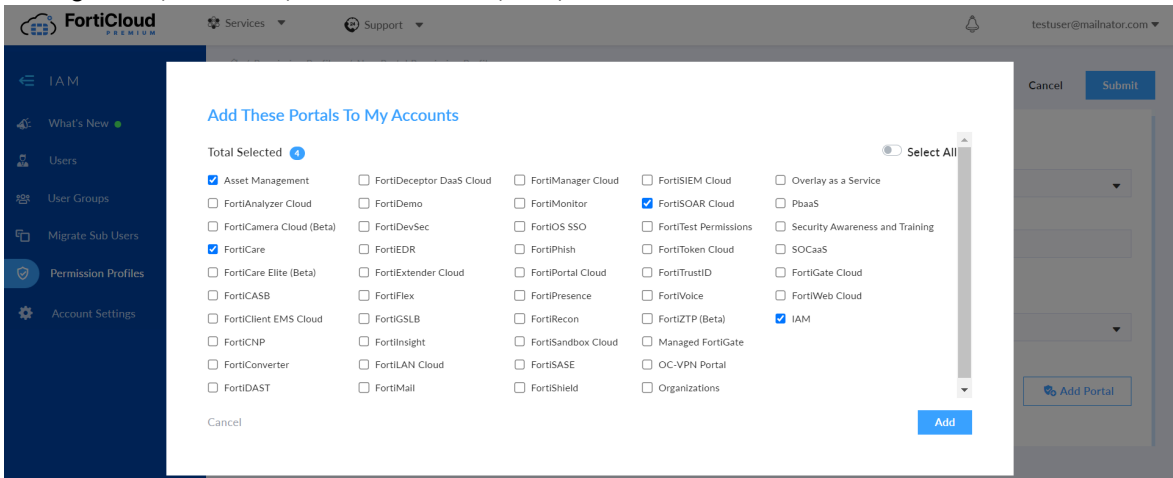


- i. In the **Basic Info** section, add the required information to create the permission profile as per your requirements. For information on creating permission profiles, see the [FortiCloud Account Services Identity & Access Management](#) documentation:

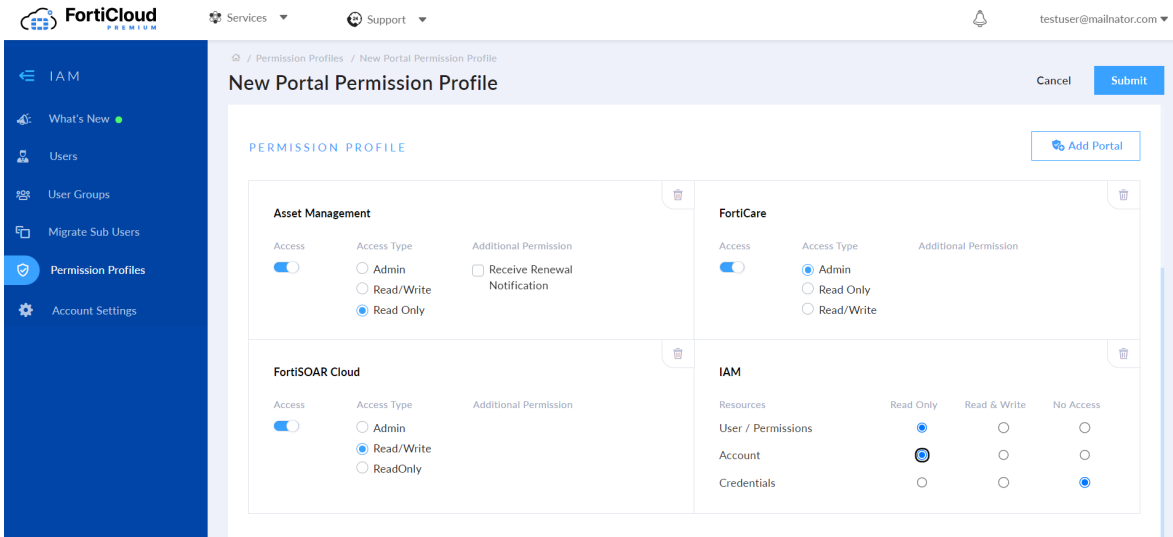


- ii. Click **Add Portal** to display the **Add These Portals To My Account** pop-up. Use this pop-up to assign portal permissions to the user. You can assign the following permissions: Asset

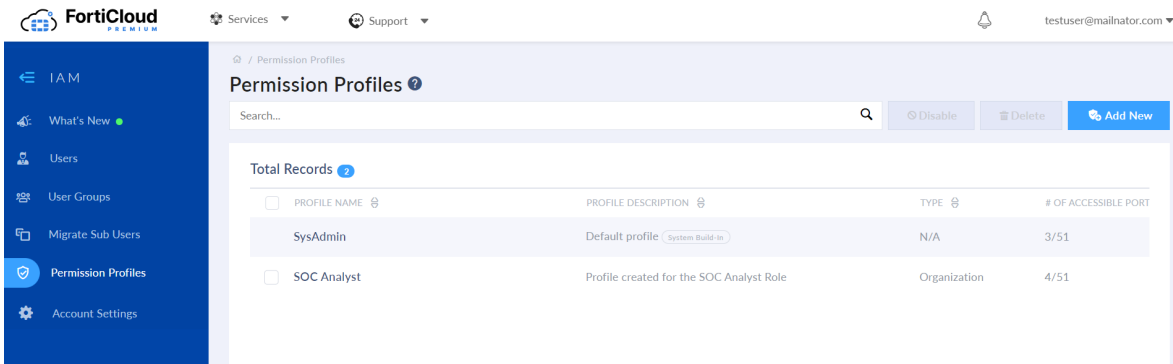
Management, FortiCare, FortiSOAR Cloud, IAM, etc and click **Add**:



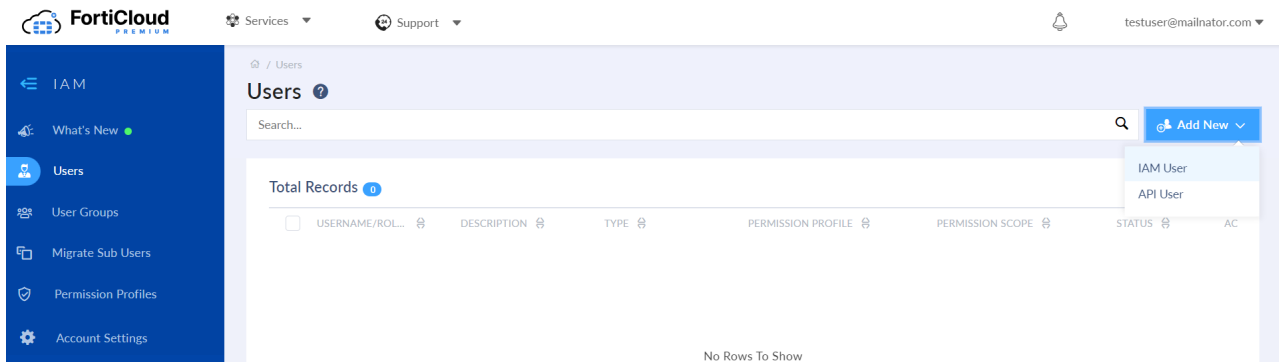
iii. In the Permissions Profile section, select the access type you want to assign to the user for the selected permission profiles, and click **Submit**:



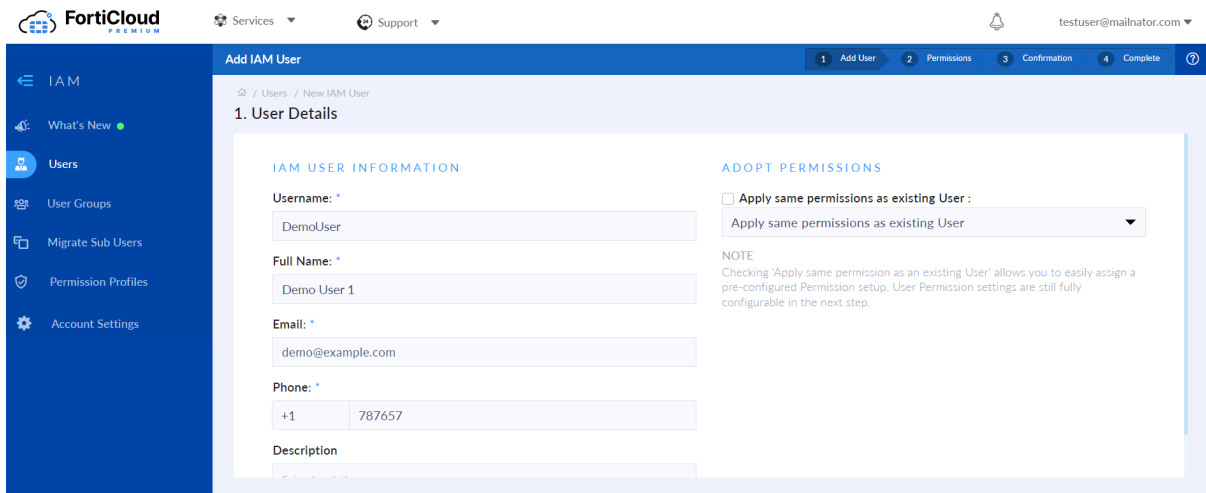
This adds the permission profile that can be assigned to users:



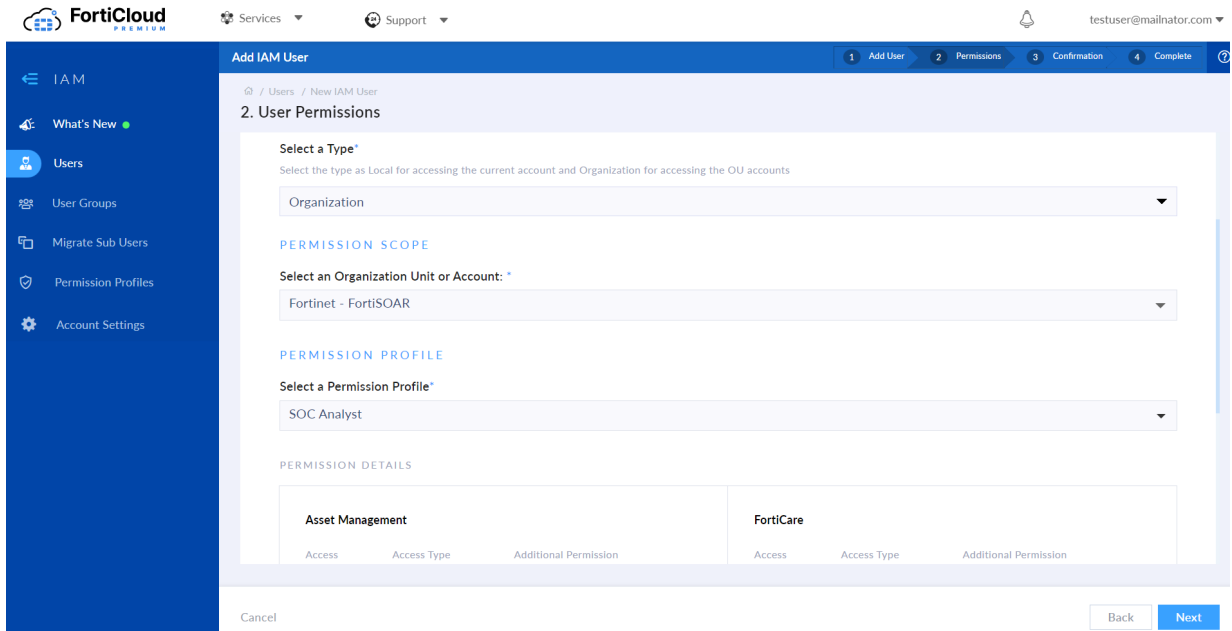
4. Click the **Users** menu item on the IAM portal, and then select **Add New > IAM User**:



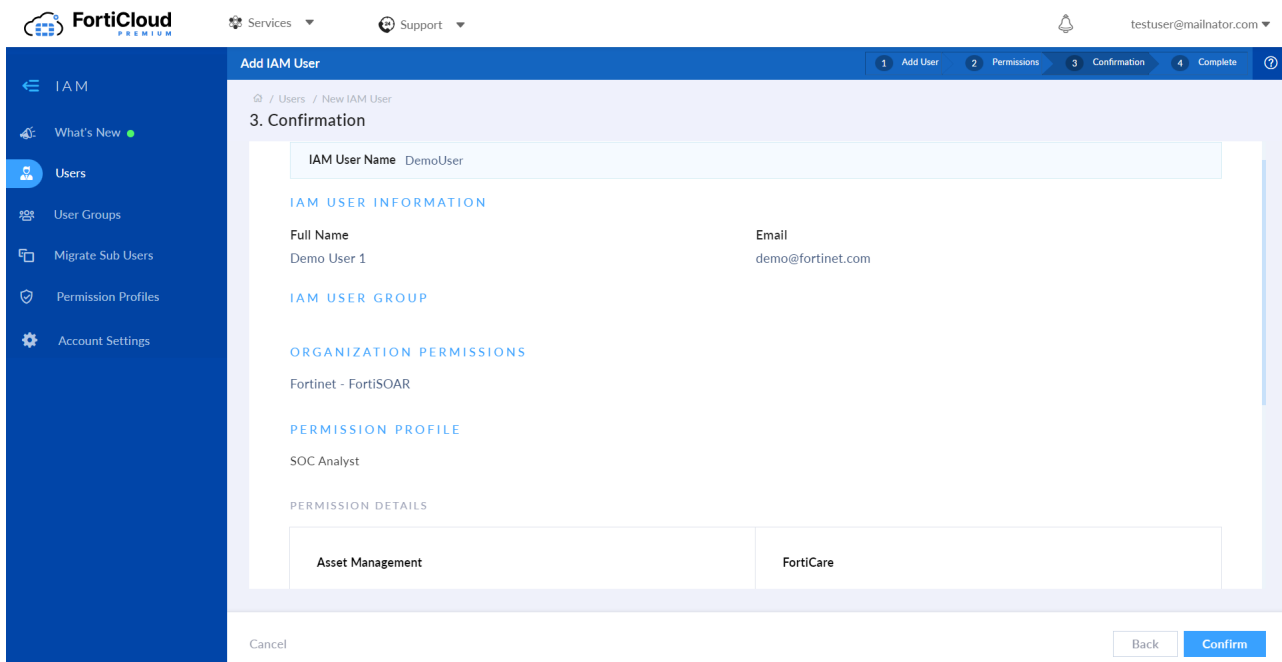
a. On the IAM User page, add the details of the user to create a new IAM user, and then click **Next**.



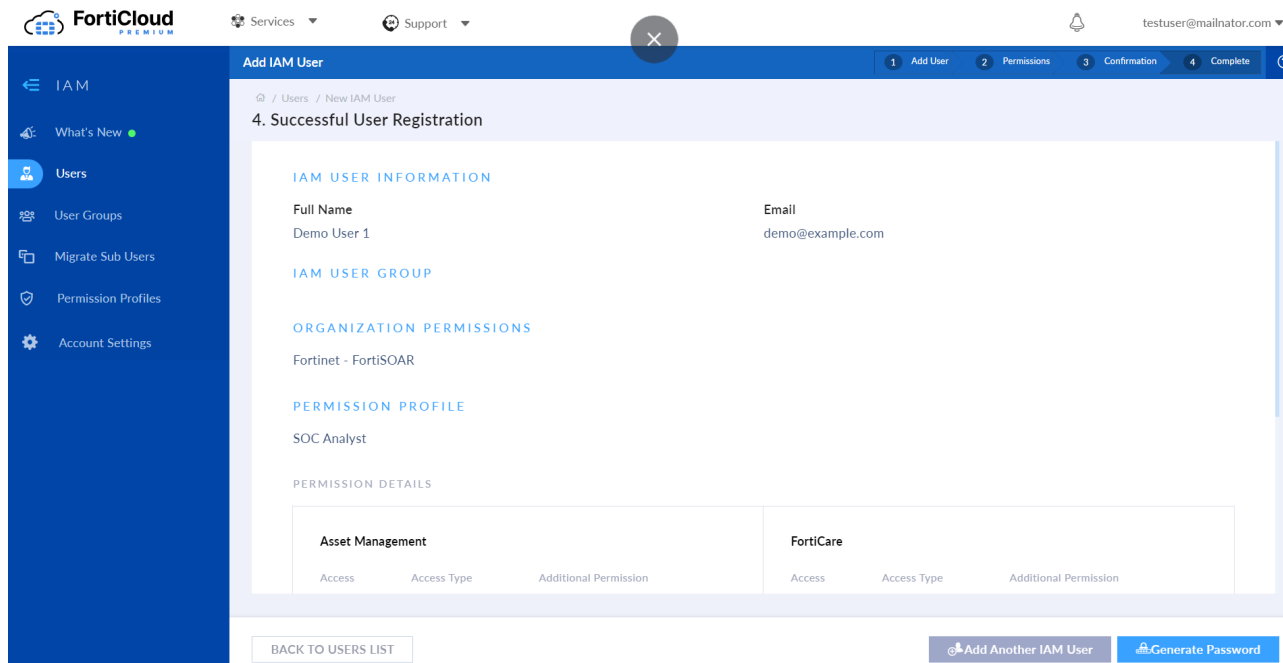
- b. On the User Permissions page, assign the IAM user the appropriate permission type, scope, profile, etc., and then click **Next**:



5. Click **Confirm** to complete the user creation process:

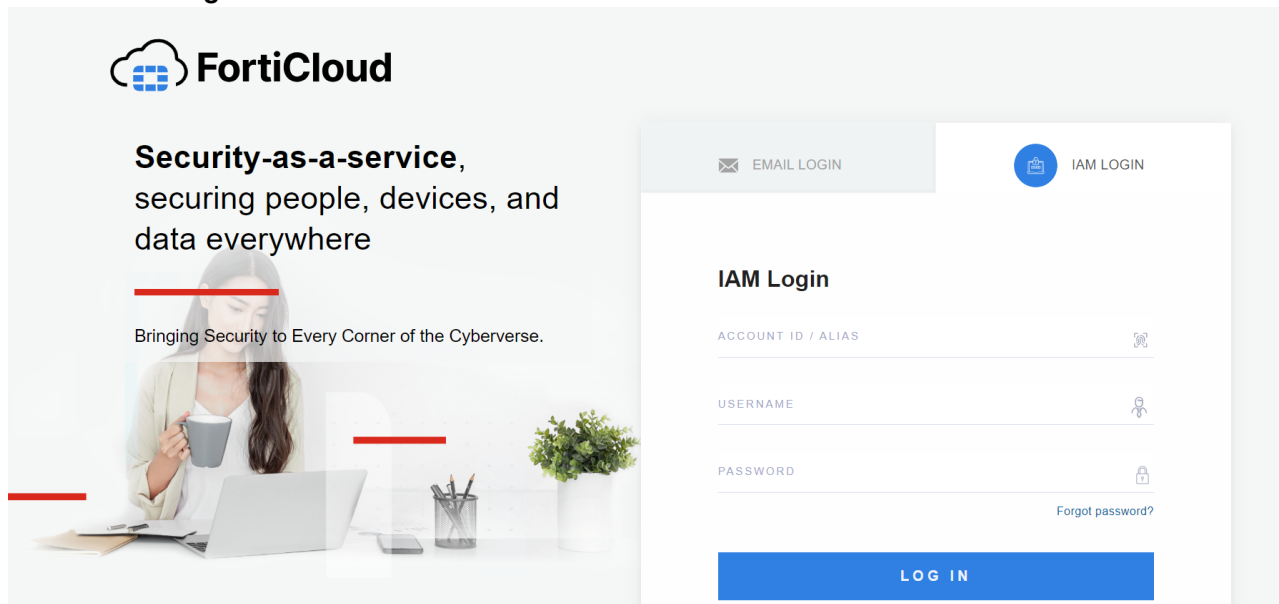


6. On the Successful User Registration page, click **Generate Password** to generate a reset password link for the user to login.



Regenerating the password renders the previous password invalid and expires in 5 days.

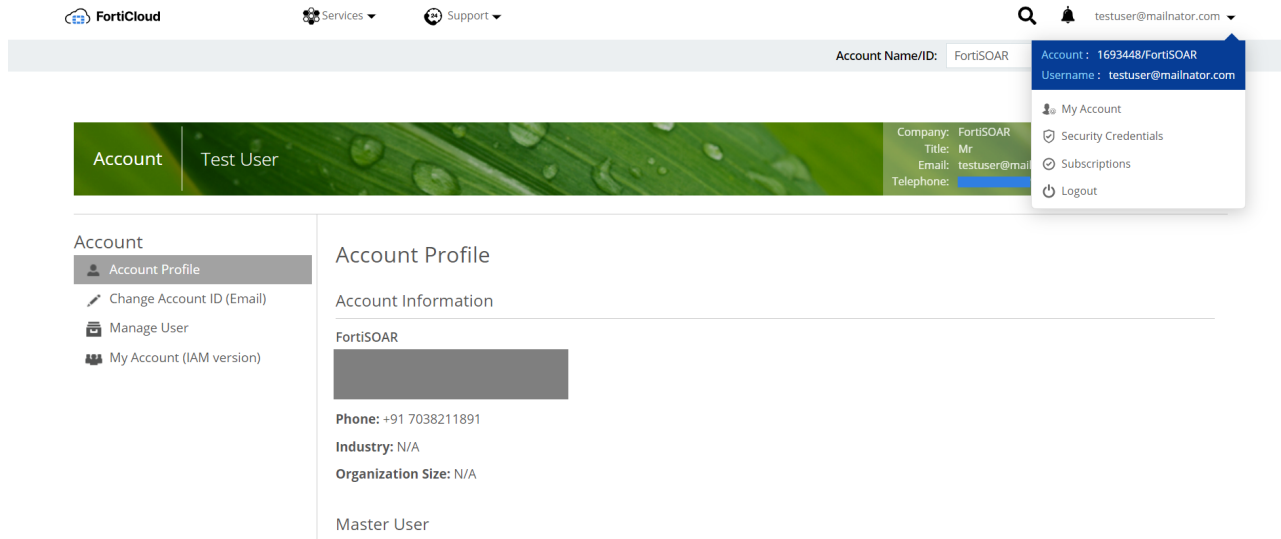
7. Navigate to <https://support.fortinet.com/>.
8. Click the **IAM Login** tab:



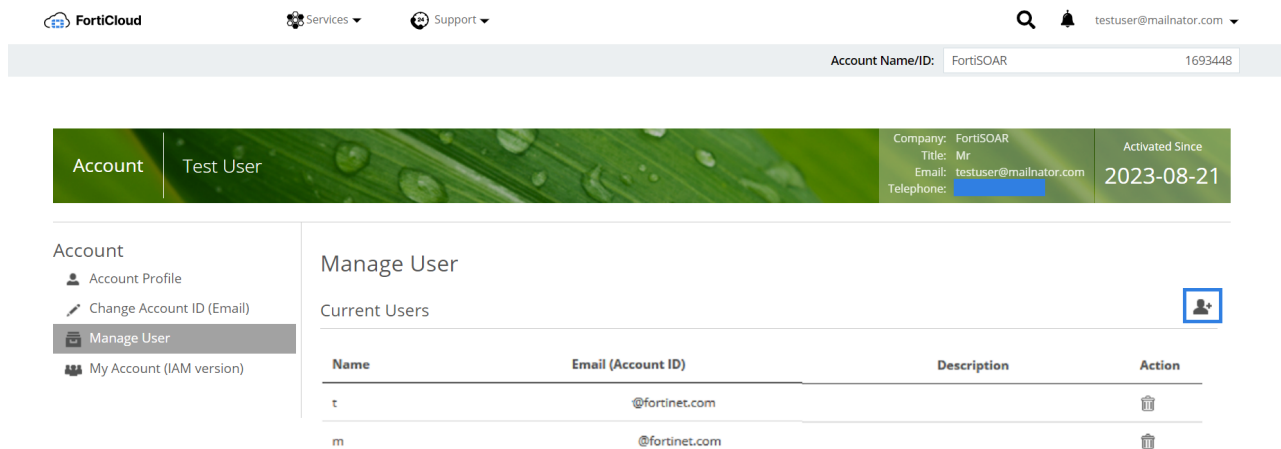
9. Enter your account ID, username, and new (regenerated) password, and click **Log in**.
10. Once you have successfully logged in, select **Services > FortiSOAR Cloud** to start working in FortiSOAR Cloud.

Adding a secondary account using FortiCare

1. Login to <https://support.fortinet.com/>.
2. Click the user profile in the top-left corner and click **My Account** to display the Account Profile page:



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.

Account

- [Account Profile](#)
- [Change Account ID \(Email\)](#)
- [Manage User](#)

Add User

User Information

User Name:*

Telephone:*

Email (Account ID):*

Confirm Email (Account ID):*

Description:

Permissions

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

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

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

Save
Cancel

6. Login to <https://support.fortinet.com/>. In the FortiSOAR Cloud section, you will see an account listed as a secondary member.
7. Click the entry to expand the view.



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

To modify a secondary account:

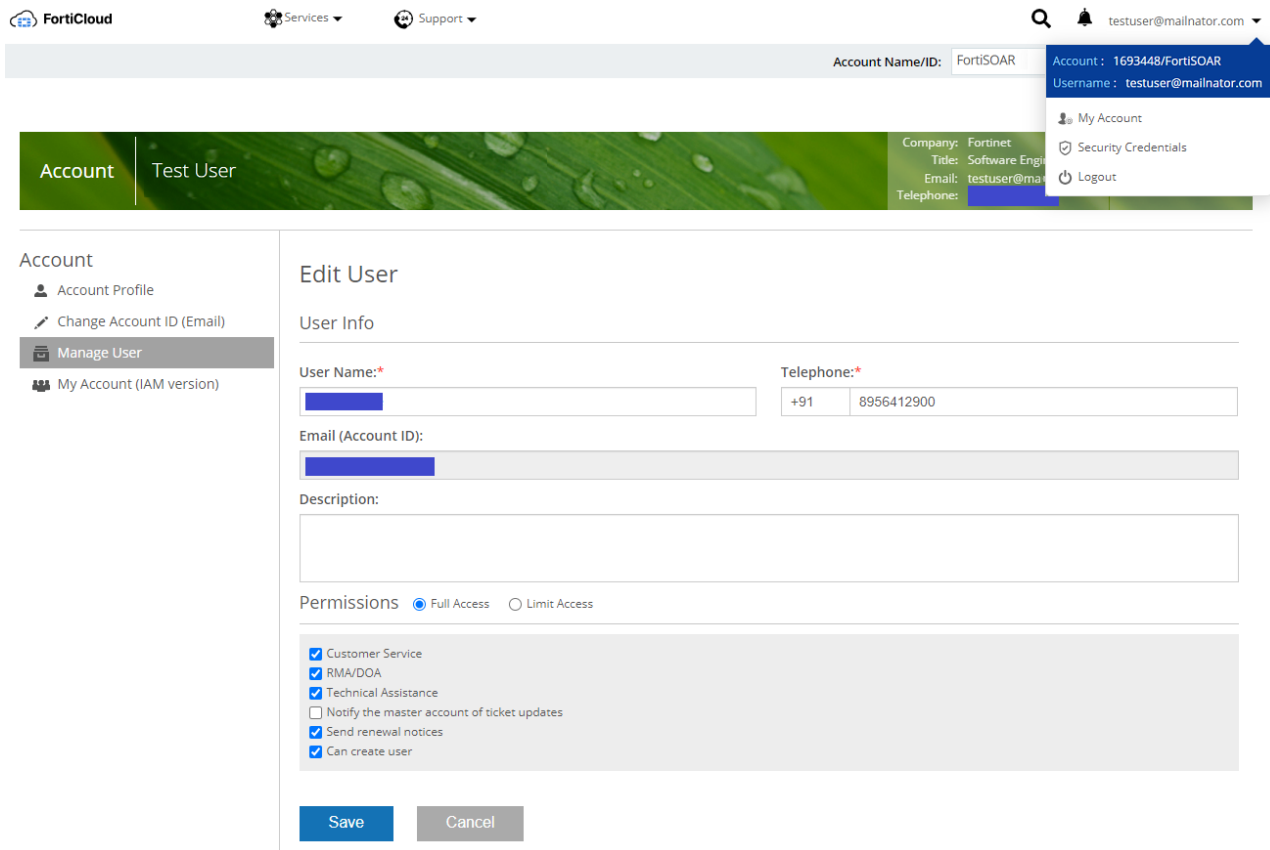


The new user must log in to FortiSOAR Cloud for the account to be displayed in the FortiSOAR instance. When a new user logs in to their account, they are automatically assigned *Admin* roles on FortiSOAR, if they are added as 'Full Access' users in FortiCare, and the *SOC Analyst* role on FortiSOAR if they are added as 'Limit Access' users in FortiCare.

The primary user or a super user can update user accounts, to, for example, change the user permissions, phone numbers, etc. as follows:

1. Use the primary or super user credentials and login to <https://support.fortinet.com/>
2. Click **My Account > Manage Users**.
The Manage User page displays a list of users.
3. Click the user whose account you want to modify to display the User Details page.
4. On the User Details page, click **Edit**.

- On the Edit User page, modify the user account as required and click **Save**. For example, change the Permissions from 'Full Access' to 'Limit Access':



Setting up External IdP roles

External IdP roles enable external users to log in to the Cloud portal using their company's credentials through a third-party ID provider. The company's ID provider verifies the identity of external IdP users. Following authentication, users can access the cloud application according to their role.

Brief process to set up External IdP roles is as follows:

- Send an enrollment request to forticloud-enroll-extidp@fortinet.com.
- The FortiCloud team will review and approve the request.
- Once the enrollment request is approved, the External IdP will be configured and linked to the appropriate FortiCloud accounts by the FortiCloud FAC and Customer Ops teams.

For more information on External IdP, see the External IdP roles topic in the *Identity & Access Management (IAM)* guide of the [FortiCloud Account Services](#) documentation.

Adding a secondary account

Once the External IdP integration is complete, log into FortiCloud, and ensure that the defined External IDP role has access permissions in the FortiSOAR Cloud's Permissions Profile section of the IAM portal:

PERMISSION PROFILE Add Portal

PERMISSION DETAILS

FortiSOAR Cloud			Asset Management				IAM			
Access	Access Type	Additional Permission	Resources	Read Only	Read & Write	No Access	Resources	Read Only	Read & Write	No Access
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Admin		Entitlement Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	User / Permissions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	<input type="radio"/> Read/Write		Asset Maintenance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Account	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	<input type="radio"/> ReadOnly		Renewal Notice	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Credentials	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
			Vulnerability List	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>				
			Account Services	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>				

Additionally, note that after logging into FortiCloud, you are directed to the Asset Management portal, from which you can access the FortiSOAR Cloud portal using the same External IdP user access.

Identifying the public IP address

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

To determine the public IP address:

1. Login to <https://support.fortinet.com/>.
2. Click **Services > FortiSOAR Cloud**.
If FortiSOAR Cloud is not visible, click on the **Show More** link to reveal all the services.
3. On the FortiSOAR Cloud portal, click **WebSSH** to access the FortiSOAR Cloud console.
4. On the SSH Login page, enter the credentials to access the FortiSOAR Cloud.
5. Run the following command to get the public IP:

```
[csadmin@<primary-user-id-here> ~] $ sudo curl ifconfig.me
```

You can use the public IP address to set up connections with third-party services, such as LDAP or the AWS Management Portal for vCenter.

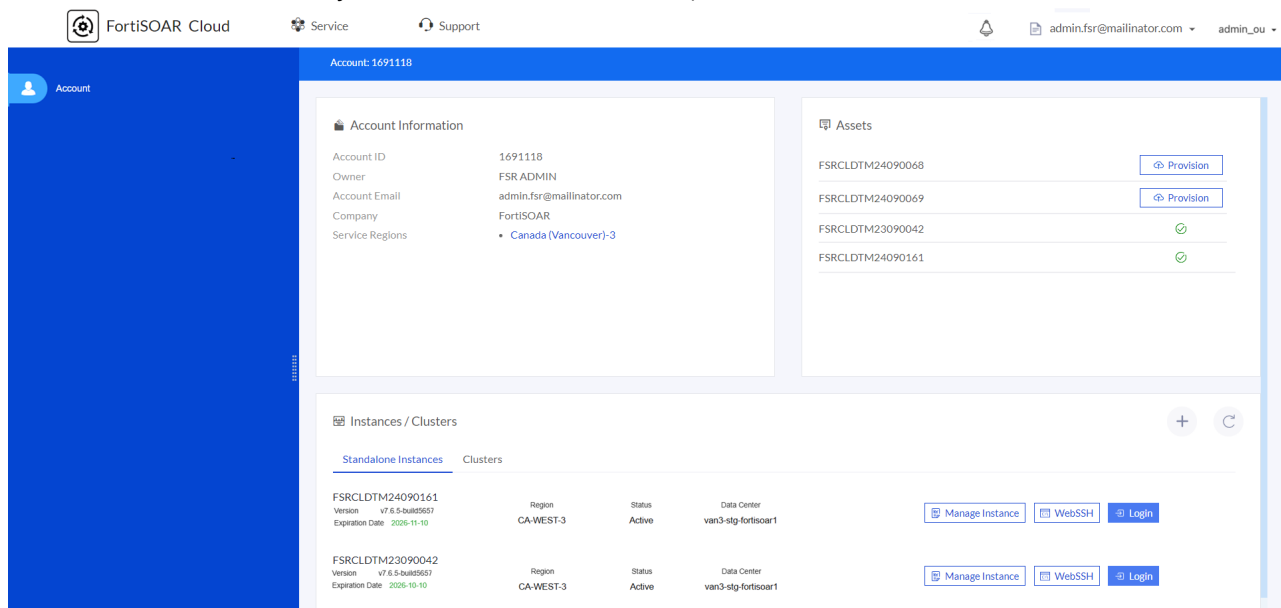
High Availability Capability for FortiSOAR Cloud

FortiSOAR Cloud supports provisioning multiple FortiSOAR instances per account, allowing the creation of an active-active cluster to enable horizontal scaling.

Creating a cluster on the FortiSOAR Cloud Portal

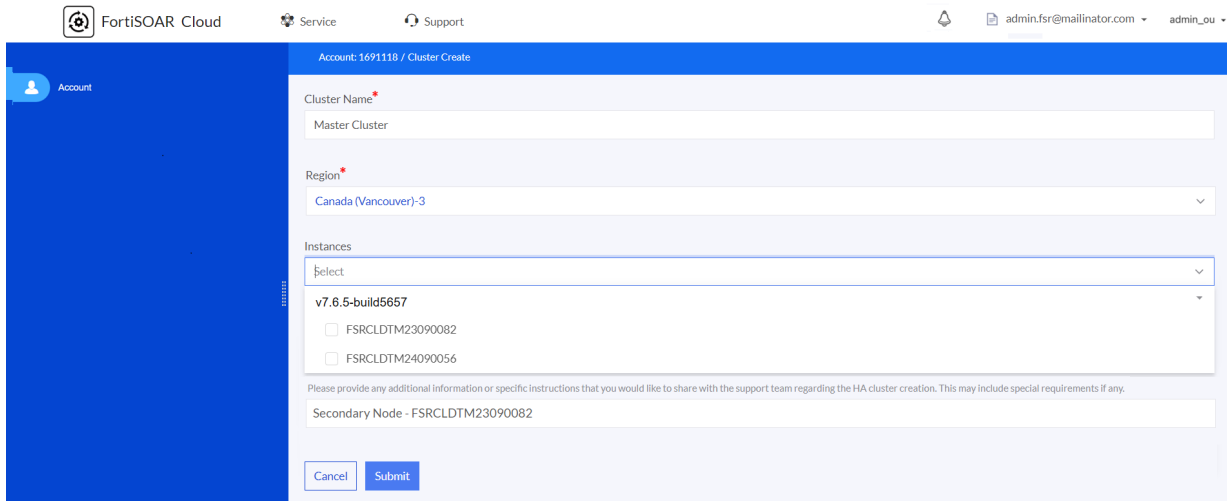
Access your FortiSOAR Cloud account as described in the [Beginning with FortiSOAR Cloud](#) chapter.

1. Click on the account where you want to create the cluster, then select the **Clusters** tab:



NOTE: Only the 'Master' account can create a cluster, and a cluster can only be created using provisioned instances.

2. Click the **+** button to open the **Cluster Create** page.
3. Enter the following details on the **Cluster Create** page, then click **Submit** to create an cluster on FortiSOAR Cloud:
 - a. **Cluster Name:** Enter the name of the HA cluster.
 - b. **Region:** Select the FortiCloud service region where you want to create the cluster.
 - c. **Instances:** Select the instances to include in the cluster.
NOTE: The FortiSOAR version and license type of the instances must match for cluster creation.
 - d. **Notes:** (Optional) Provide the support team with additional details about the HA cluster to be created. Designating a specific instance as Active/Secondary or Active/Primary in the cluster is an example of what could be added in the Notes field.

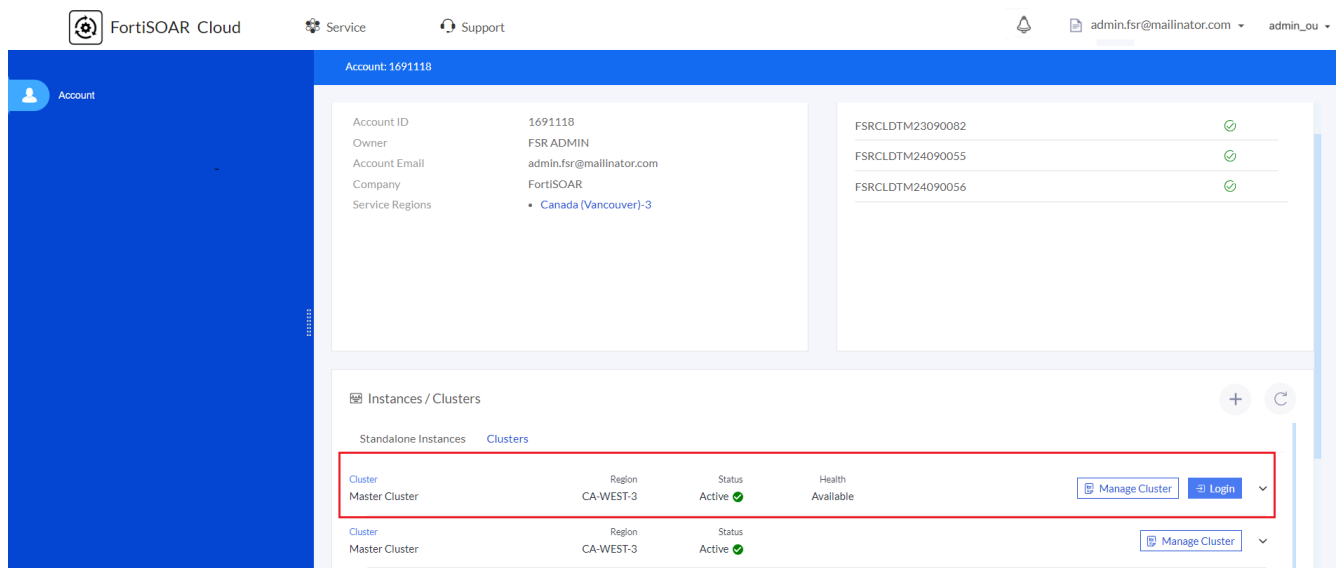


Once instances are selected, click **Submit** to create the cluster:

After clicking **Submit**, a notification is sent to Fortinet Support to set up a cluster between the selected instances and configure a load balancer. They will create a support ticket on your behalf and contact you if needed to complete the process. After the support team completes the setup, you will receive a notification and can view your cluster in your account. For detailed information on high availability support in FortiSOAR, see the [High Availability Configuration and Maintenance](#) chapter in the "FortiSOAR Administration Guide".

Managing a cluster on the FortiSOAR Cloud portal

Access your FortiSOAR Cloud account as described in the [Beginning with FortiSOAR Cloud](#) chapter. On your account page, click the Clusters tab:



The cluster created in your account will display the following details:

- **Name:** Name of the cluster
- **Region:** Region where the cluster is provisioned
- **Status:** Indicates if the cluster is successfully provisioned and ready to use. It can be in the following states:
 - **Configuring:** Initial configuration and network setup for the selected instances.
 - **Active:** Cluster is successfully formed and ready to use.
- **Health:** Indicates the health of the cluster with values like Available, Requires Attention, or Error.
- You can also perform the following actions using the following available buttons:
 - **Login:** Access the FortiSOAR UI of an instance within the cluster.
NOTE: The load balancer determines which FortiSOAR instance's UI is displayed. For more information, see the [Accessing FortiSOAR Cloud UI](#) topic in the [Beginning with FortiSOAR Cloud](#) chapter.
 - **Manage Cluster:** View the Cluster Info page, which includes details about that cluster and is used to manage the cluster. For more information, see the [Cluster Info page details](#) topic.

Click the arrow to expand the cluster row and view information about instances in the cluster:

The screenshot shows the FortiSOAR Cloud management interface. At the top, there's a navigation bar with 'FortiSOAR Cloud', 'Service', and 'Support' links. The user is logged in as 'admin.fsr@mailinator.com'. The main content area is titled 'Instances / Clusters' and has two tabs: 'Standalone Instances' and 'Clusters'. The 'Clusters' tab is active, showing a table of clusters. One cluster, 'Master Cluster', is expanded to show its instances. The instances table has columns for Instance ID, Version, Expiration Date, Cluster Name, Status, Data Center, Health, and Node Role. Two instances are listed: a Primary node and a Secondary node, both with 'Active' status and 'Available' health.

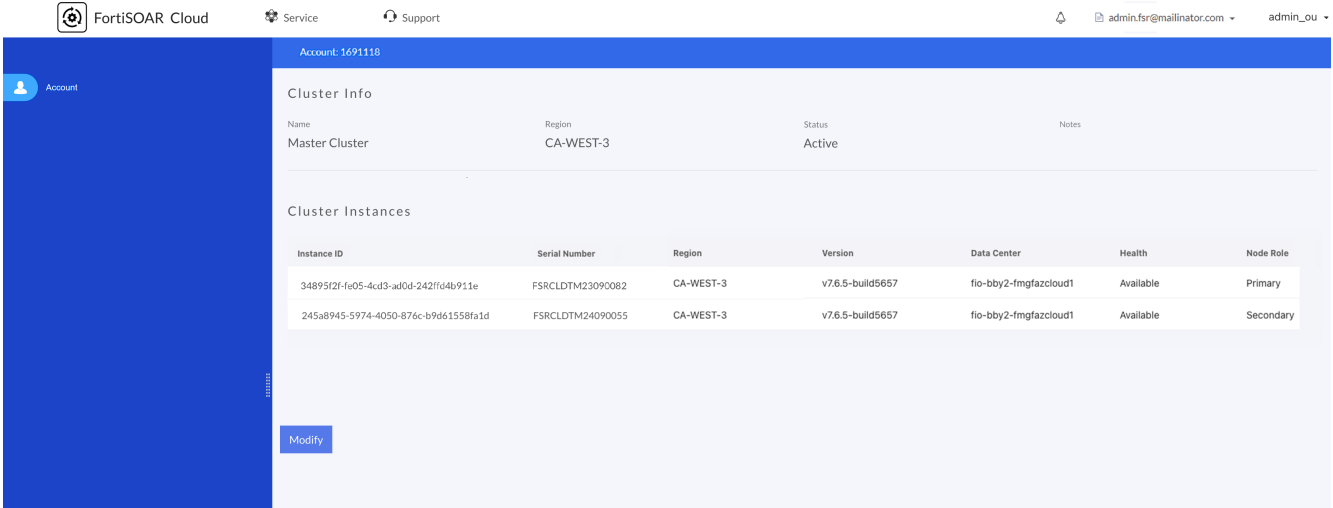
Cluster	Region	Status	Health	Buttons
Master Cluster	CA-WEST-3	Active	Available	Manage Cluster, Login
FSRCLDTM25090174	7.6.5 cluster	Active	Available	Manage Instance, WebSSH, Login
FSRCLDTM25090175	7.6.5 cluster	Active	Available	Manage Instance, WebSSH, Login

The expanded view shows the following details of the instances within the cluster:

- **Node Details**, including the instance's ID, its expiration date, and the FortiSOAR release on which the instance is provisioned.
- **Name** of the cluster associated with the instance.
- **Status** of the node, whether Active or Inactive.
- **Role** of the node, whether Primary or Secondary.
NOTE: Initially, all nodes are set as 'Primary' on FortiCloud. Roles are updated during HA cluster creation in FortiSOAR using the 'csadm ha' CLI. For information on the `csadm ha` command, see the [High Availability Configuration and Maintenance](#) chapter in the "FortiSOAR Administration Guide".
- You can also perform the following actions using the following available buttons:
 - **Login:** Access the FortiSOAR UI of an instance.
 - **WebSSH:** Access the FortiSOAR Cloud console of an instance.
 - **Manage Instance:** View the Instance page that includes details about that instance and is used to manage the instance.
 For more information, see the [Beginning with FortiSOAR Cloud](#) chapter.

Cluster Info page details

The Cluster Info page that displays details about a cluster including its name, region, description, and status. It also lists the instances within the cluster, along with their IDs, regions, health statuses, etc.



Account: 1691118

FortiSOAR Cloud Service Support admin.fsr@mailinator.com admin_ou

Account

Cluster Info

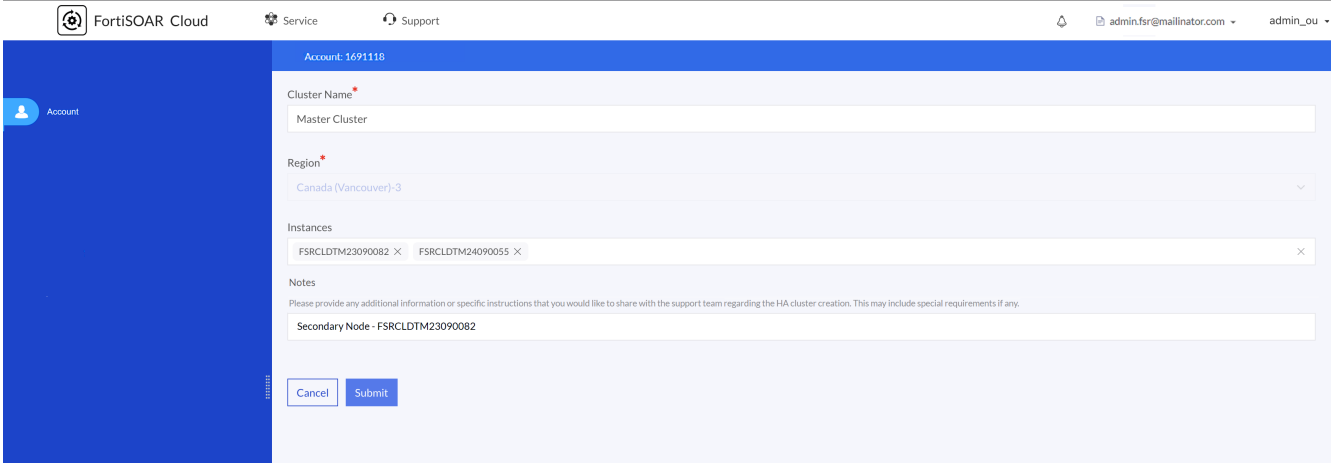
Name	Region	Status	Notes
Master Cluster	CA-WEST-3	Active	

Cluster Instances

Instance ID	Serial Number	Region	Version	Data Center	Health	Node Role
348952f-f005-4cd3-ad0d-242f04b911e	FSRCLDTM23090082	CA-WEST-3	v7.6.5-build5657	fio-bby2-fmgfazcloud1	Available	Primary
245a8945-5974-4050-876c-b9d61558fa1d	FSRCLDTM24090055	CA-WEST-3	v7.6.5-build5657	fio-bby2-fmgfazcloud1	Available	Secondary

Modify

To make changes to the cluster, click the **Modify** button to access the Modify Cluster page:



Account: 1691118

FortiSOAR Cloud Service Support admin.fsr@mailinator.com admin_ou

Account

Cluster Name*

Master Cluster

Region*

Canada (Vancouver)-3

Instances

FSRCLDTM23090082 X FSRCLDTM24090055 X

Notes

Please provide any additional information or specific instructions that you would like to share with the support team regarding the HA cluster creation. This may include special requirements if any.

Secondary Node - FSRCLDTM23090082

Cancel Submit

On the Modify Cluster page, where you can:

- Update the cluster's name or notes.
- Add or remove instances.
 - Add an instance: When you add an instance to the cluster, a notification is sent to Fortinet Support, who will update the cluster and load balancer. They will create a support ticket on your behalf and contact you if needed to complete the process. After the support team completes adding the instance to the existing FortiSOAR cluster, you will receive a notification and can view your cluster in your account.
 - Remove an instance: When you remove an instance from the cluster, the cluster on FortiSOAR will be automatically broken.

For detailed information on high availability support in FortiSOAR, see the [High Availability Configuration and Maintenance](#) chapter in the "FortiSOAR Administration Guide."

NOTE: The region of the cluster cannot be changed.

Troubleshooting FortiSOAR Cloud HA instances

Default Secure Message Exchange Fails to Connect After HA Takeover

After a takeover in a high-availability (HA) FortiSOAR Cloud deployment, the embedded (default) Secure Message Exchange (SME) may fail to connect. This issue occurs in HA instances where the embedded Secure Message Exchange (SME) is enabled.

Resolution

Reset the `mq admin` password on all nodes in the HA cluster by running the following command on each node:

```
rabbitmqctl change_password admin <old_primary_uuid>
```

Replace `<old_primary_uuid>` with the UUID of the former primary node.

Backing up and Restoring FortiSOAR Cloud

This chapter describes the process of backing up and restoring FortiSOAR Cloud.



Before release 7.5.0, FortiSOAR Cloud did not support static IP configuration for FortiSOAR Cloud, leading to issues with disaster recovery. Therefore, with release 7.5.0, support for static IP configuration in FortiSOAR Cloud deployment has been added. For the process of [Setting a static IP](#), see the [Deploying FortiSOAR](#) chapter of the "Deployment Guide."

Prerequisites

You must have sudo permissions to perform backups and restores.



Ensure that you have enough disk space available to perform backup and restore tasks. It is recommended that you have available disk space of around 3X the data size; for example, if your data size is 2GB, then you should have around 6GB of available disk space to ensure that the processes do not stop or fail.

Backup Process

Use the FortiSOAR Admin CLI (`sudo csadm db`) option to regularly perform backups and restores, which restores the data seamlessly to a new FortiSOAR Cloud environment.

The FortiSOAR Admin CLI performs a full database backup of your FortiSOAR Cloud server each time. There is no provision for incremental backups. Backups are performed for a particular version of FortiSOAR Cloud, and backups should be restored on the exact version of FortiSOAR Cloud.



The FortiSOAR Cloud Admin CLI backs up the latest three backups every time it creates a new backup. Any backups older than the latest three backups are deleted.

Data that is backed up during the backup process

The FortiSOAR Cloud Admin CLI backs up the following files, configurations, and data during the backup process:

- site-packages
- connectors
- application.conf
- db_config.yml
- pg_hba.conf
- Syslog forwarding configuration
- All major configuration files, such as das.ini, postgresql.conf
- PostgreSQL database backups as per requirements
- User-defined custom expressions



Backups of the configuration files are taken only in the case of localized databases.

Prerequisites for running the backup process

Verify that you have the local backup storage path or NFS.

Performing a backup

To perform a backup, run the `csadm` command on any FortiSOAR Cloud machine using any terminal. A user who has `sudo` permissions can run the `csadm` command.

1. SSH to your FortiSOAR Cloud VM.

2. To perform a backup, type the following command:

```
# sudo csadm db --backup [<backup_dir_path>]
```

[<backup_dir_path>] is the directory where backup files will be created. If you do not specify any path, then by default, the backup file is stored in the current working directory.

Optionally, you can specify the `--exclude-workflow` option to exclude all the "Executed Playbook Logs" and the `--exclude-audit` option to exclude all the "Executed Audit Logs" from the backup. Executed playbook and audit logs are primarily meant for debugging, so they are not a very critical component to be backed up. However, they constitute a major part of the database size, so excluding them from the backup reduces the time and space needed for the backup. For example, to exclude all the "Executed Playbook Logs" from the backup, type the command as follows:

```
# sudo csadm db --backup [<backup_dir_path>] --exclude-workflow
```

Important: FortiSOAR Cloud backs up the latest three backup files every time it creates a new backup. Any backups older than the latest three backups are deleted.

3. (Optional) If you only want to back up your configuration files only, then type the following command:

```
# sudo csadm db --backup-config [<backup_dir_path>]
```

Once you run the above command, you will be asked to provide the path of the configuration backup file. If you do not specify any path, then by default, the backup file is stored in the current working directory.

Running a backup as a scheduled job

Following is an example of running a backup as a scheduled cron job on your FortiSOAR Cloud system or external Secure Message Exchange that will run at 12:30 am every day. You can schedule the backup process based on your requirements.

Add the cron job to run at 12:30 a.m. every day as follows:

```
$ sudo crontab -e
30 00 * * * sudo csadm db --backup <backup_dir_path>
```

Once the backup process is successfully completed, the final `DR_BACKUP_<FortiSOARCloud_version>_timestamp.tgz` file is located in the directory where the backup files are created. It would be the same directory that you have specified when you ran the `sudo csadm db --backup <backup_dir_path>` command. The `DR_BACKUP_<FortiSOARCloud_version>_timestamp.tgz` file includes the timestamp of when the backup was created.

The `DR_BACKUP_<FortiSOARCloud_version>_timestamp.tgz` file includes all the backup files. You can run the following command to check the contents of the `DR_BACKUP_<FortiSOARCloud_version>_timestamp.tgz` file:

```
# sudo tar -tvf <DR_BACKUP_<FortiSOARCloud_version>_timestamp.tgz>
```

Restoring data

1. Move the backup file to the new FortiSOAR Cloud VM.
2. SSH to the new FortiSOAR Cloud VM.
3. To restore the data, type the following command:

```
# sudo csadm db --restore <backup_file_path>
```

[<backup_file_path>] is the directory where you have saved the backed-up files. Note that the backup process, by default, stores the backup in a locally saved file: `/home/csadmin/db_backup/DR_BACKUP_<yyyymmdd_hhmmss>.tgz`

Important: Once you have restored FortiSOAR Cloud, you are required to reinstall the license for this FortiSOAR Cloud instance. To reinstall the license, click the **Retry Sync** button on the UI.

Troubleshooting

Migration of FortiSOAR Cloud MSSP setup fails with the Secure Message Exchange Invalid credentials or certificate error

A FortiSOAR Cloud MSSP setup that you want to migrate by backing up your FortiSOAR Cloud instance and then restoring it on a new instance fails with the Secure Message Exchange (SME) "Invalid credentials or certificate" error.

Resolution

This issue occurs as the hostname and certificate from the original backup overwrites the hostname and certificate of the new FortiSOAR Cloud instance/account.

1. Use the FortiSOAR Cloud UI to change the name of the embedded SME.
2. SSH to your new FortiSOAR Cloud instance and run the following command:
`sudo csadm secure-message-exchange update-exchange-event-listener-certs`

Upgrading FortiSOAR Cloud

Fortinet offers a managed upgrade service for FortiSOAR Cloud customers to simplify and streamline the upgrade process. You can request the following types of upgrades:

- [Upgrade the release of your FortiSOAR Cloud instance](#)
- [Expand resources for your FortiSOAR Cloud instance](#)

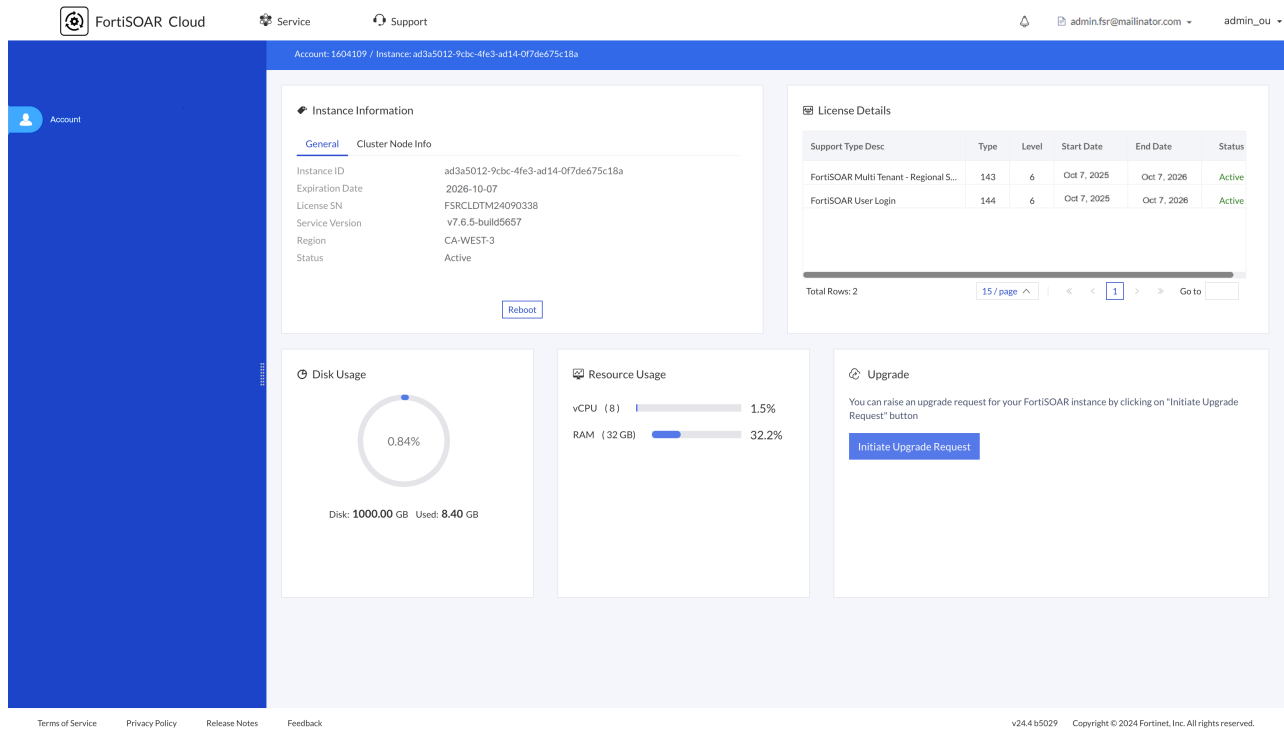
Upgrading your FortiSOAR Cloud instance

You can request a FortiSOAR Cloud instance upgrade using either of the following methods:

- [Using the FortiSOAR Cloud portal](#)
- [Opening a Support ticket](#)

Upgrading your FortiSOAR Cloud instance using the FortiSOAR Cloud portal

1. Log into the FortiSOAR Cloud Portal and navigate to your FortiSOAR Cloud instance page.
2. On the Manage Instance page, click the **Initiate Upgrade Request** button in the Upgrade section:



3. Clicking **Initiate Upgrade Request** opens the Create Upgrade Request form, where you will need to verify or provide the following details:
 - a. Account Name (Read Only): Pre-populated and read-only based on the logged-in account.
 - b. Account Email ID (Read Only): Pre-populated and read-only based on the logged-in account.
 - c. Primary Account ID (Read Only): Pre-populated and read-only based on the logged-in account.
 - d. Type of Deployment (Enterprise, Multitenant, Cluster): Select the appropriate deployment type based on your requirements:
 - **Enterprise:** Standalone instances with license type set to 'Enterprise'.
 - **Multitenant:** Instances with license type set to 'multitenant'.
 - **Cluster:** Instances that are part of a HA cluster.

NOTES:

 - For a high availability (HA) cluster contains instances whose license type is set to 'multitenant', select 'Multitenant.'
 - If your instance is part of a cluster, submit separate upgrade requests for each system in the cluster.
 - e. Upgrade Path: Specify the upgrade path from the supported options.
 - f. Instance ID (Read Only): Pre-populated and read-only based on the current instance.
4. After completing the form, click the **Submit Upgrade Request** button. This will display a pop-up with the upgrade details based on your inputs. Submitting the form will send an email to the Fortinet support team, who will create a support ticket on your

behalf and contact you to complete the upgrade. You can view your submitted requests in the 'Upgrade' section of your Manage Instance page.

Upgrading your FortiSOAR Cloud instance by opening a Support ticket

1. Create a support ticket for upgrade. The ticket must include the following information:
 - a. Account Name
 - b. Account Email ID
 - c. Primary Account ID
 - d. Type of Deployment: Specify the appropriate deployment type based on your requirements, from the following options:
 - **Enterprise:** Standalone instances with license type set to 'Enterprise'.
 - **Multitenant:** Instances with license type set to 'multitenant'.
 - **Cluster:** Instances that are part of a HA cluster.**NOTES:**
 - For a high availability (HA) cluster contains instances whose license type is set to 'multitenant', select 'Multitenant.'
 - If your instance is part of a cluster, submit separate upgrade requests for each system in the cluster.
 - e. Upgrade Path: Specify the upgrade path from the supported options
 - f. Instance ID
2. The Support team will contact you to complete the upgrade process. Once completed, you will receive a notification, and the ticket will be closed.

Expanding resources for your FortiSOAR Cloud instance

If you need to expand the resources for your FortiSOAR Cloud instance, you can purchase additional resources. The SKU provides 1000 GB storage, 8 GB RAM and 4 vCPUs. After purchasing the SKU for additional resources, follow these steps:

1. Register the contract for the extra resources on the Support portal.
2. Create a Support ticket for resource expansion. The ticket must include the following information:
 - a. Account ID
 - b. Service Region
 - c. Instance ID
 - d. Serial Number
3. The Support team will manage the resource expansion process. Once completed, you will receive a notification, and the ticket will be closed.

Appendix A - Supported Regions

The following provides a list of ingress and egress IP addresses for FortiSOAR Cloud. You can use this list in access control lists to allow access to internal applications from FortiSOAR Cloud only.

Region	Data Center	Security ingress	Security egress
North America	Burnaby, Canada	160.223.172.26	160.223.172.16/28
North America	Dallas, United States	154.52.5.160	154.52.9.20
Europe	Frankfurt, Germany	154.52.2.165	194.69.174.8



www.fortinet.com

Copyright © 2026 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.