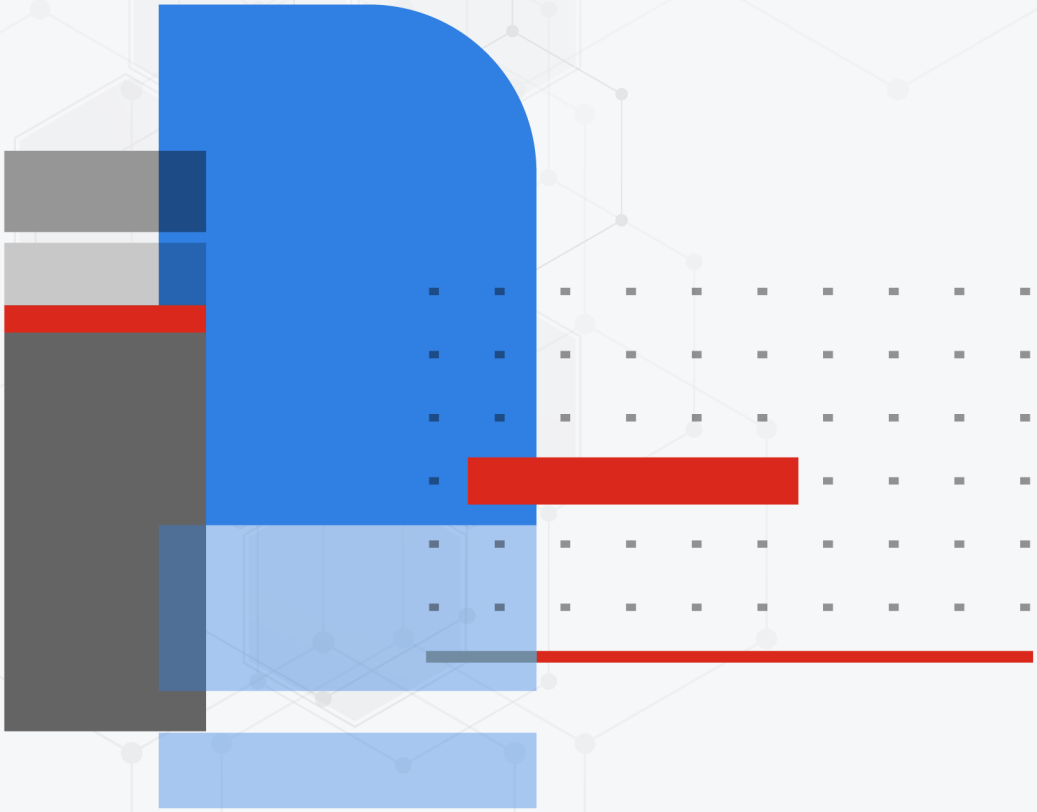
Deployment Guide

FortiSOAR Cloud 7.4.3



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, 2023
FortiSOAR Cloud 7.4.3 Deployment Guide
00-400-000000-20210416

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-12-01	Initial release of 7.4.3

Introduction

FortiSOAR Cloud is a cloud-hosted Security Orchestration & Automated Response (SOAR) platform. The FortiSOAR Cloud service subscription is available for purchase through an a la carte SKU. Having FortiSOAR run on the FortiSOAR Cloud provides for easier FortiSOAR VM deployment, management, and scaling.

FortiCloud creates a cloud-based FortiSOAR instance with an embedded FortiSOAR secure message exchange under the user account. You can launch the portal for the cloud-based FortiSOAR from FortiCloud, and its URL starts with the Account ID.

This section includes the following topics:

Requirements

The following items are required before you can initialize FortiSOAR Cloud:

- FortiCloud account: Create a FortiCloud account here if you do not have one. A primary FortiCloud account is required to launch FortiSOAR Cloud. A primary FortiCloud account can invite other users to launch FortiSOAR Cloud as secondary users.
- Internet access: You must have Internet access to create a FortiSOAR Cloud instance.
- Browser: A device with a browser to access FortiSOAR Cloud.

Only one FortiSOAR instance can be created per FortiCloud account.

FortiSOAR Cloud is supported for FortiSOAR v7.0.0 and later.

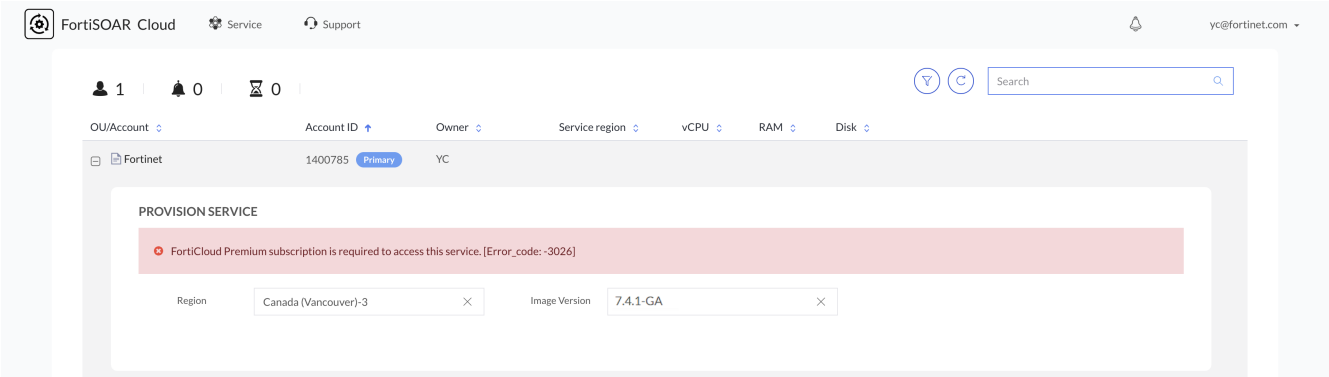
Licensing

License requirements are enforced when you log into the FortiSOAR Cloud portal.

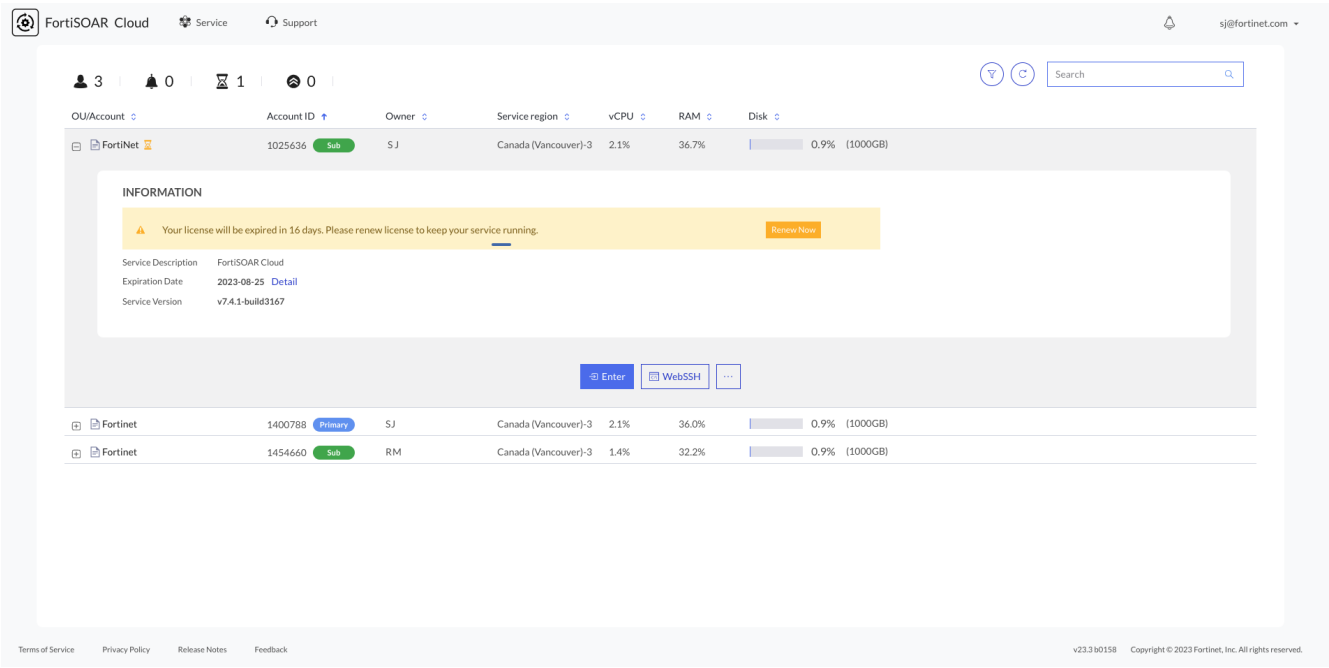
FortiSOAR Cloud requires the following licenses:

- FortiCloud Premium Subscription
- FortiSOAR Cloud Entitlement license. You can purchase FortiSOAR Cloud licenses from Fortinet.

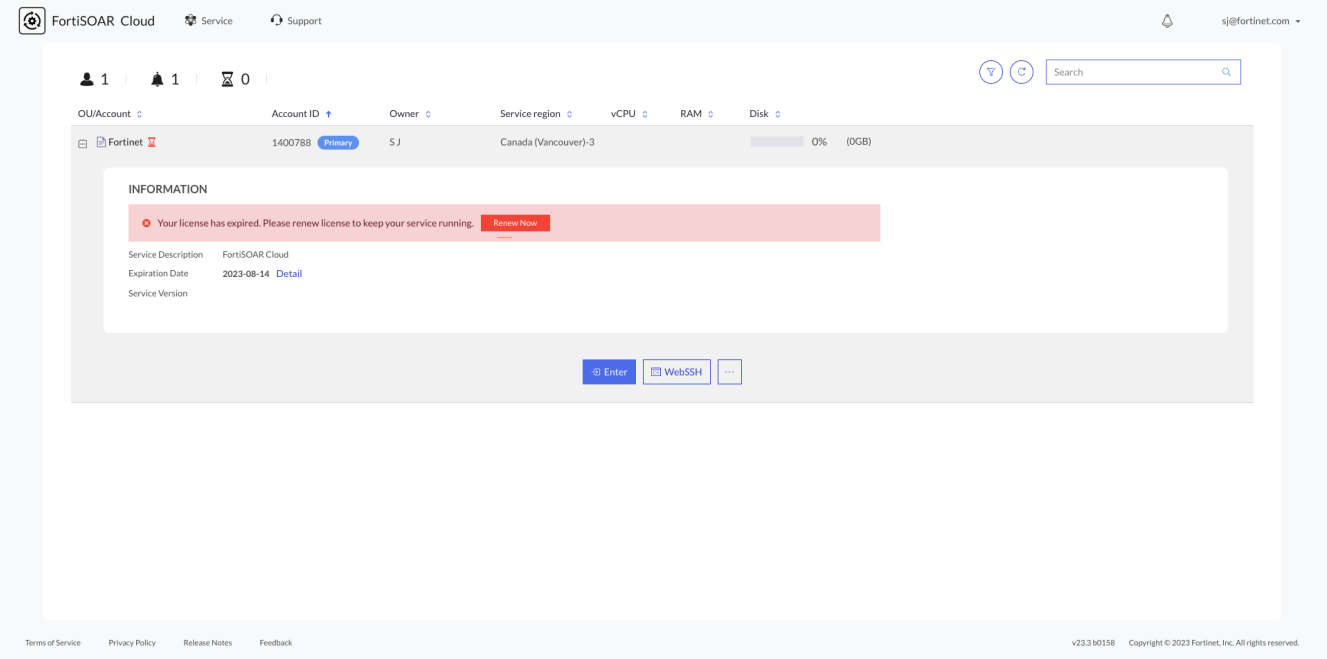
If either the FortiCloud Premium Subscription or the FortiSOAR Cloud entitlement expires, the cloud portal displays a notification to the customer.
The cloud portal displays the following notification when the FortiCloud Premium Subscription has expired:



The cloud portal displays the following notification when the FortiSOAR Cloud entitlement is due to expire:



Customers have a grace period, currently set at 30 days, which allows them to continue to use VM and renew the contract that has expired. After the grace period has expired, the cloud portal shuts down the VM, and customers will not be able to use the VM:



From FortiSOAR Cloud release 7.4.2 onwards, a new licensing option for FortiSOAR Cloud is introduced to support the subscription service for Threat Intelligence Management (TIM) Service, including FortiGuard Premium Threat Feeds. This service allows you to use the TIM service to its fullest extent and includes unrestricted consumption of FortiGuard feeds. To know more about unrestricted FortiGuard threat feeds and premium TIM features and TIM SKU, see the *Licensing* chapter in the FortiSOAR "Deployment Guide." For more information on TIM, see the Threat Intel Management Solution Pack documentation in the FortiSOAR Content Hub.

FortiSOAR Cloud license contract registration

1. You must have an account in FortiCare.
2. Contact FortiSOAR Support to obtain the FortiSOAR Cloud product SKU.
   Note: By default, the FortiSOAR Cloud product SKUs come with two users included. If you need more users, you must purchase the SKU for 'Additional Users Entitlement'.
3. Once you complete purchasing the FortiSOAR Cloud product SKU and/or the 'Additional Users' SKU, you will be sent a service contract registration code to your registered email address.
4. Login to your FortiCare account and click **Asset** > **Register/Activate** to register your FortiSOAR Cloud product. You can register your FortiSOAR Cloud product using the instructions provided in the FortiCare registration wizard. You will need to copy-paste the service contract registration code from your email to register FortiSOAR Cloud. Once you have verified the registration, click **Complete** to complete the registration.

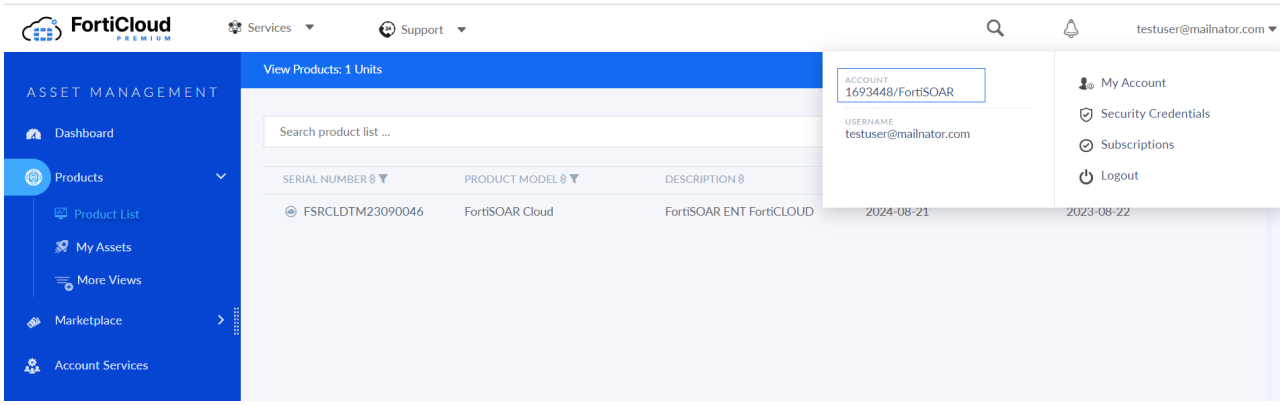
Deploying FortiSOAR Cloud

This section explains how to deploy FortiSOAR Cloud.

Release 7.4.3 addresses a critical issue of connectors not working after backup and restore due to missing 'Python' dependencies, which affects fresh installations of FortiSOAR Cloud 7.4.2. Therefore, it is highly recommended to upgrade fresh installations of 7.4.2 instances to 7.4.3.

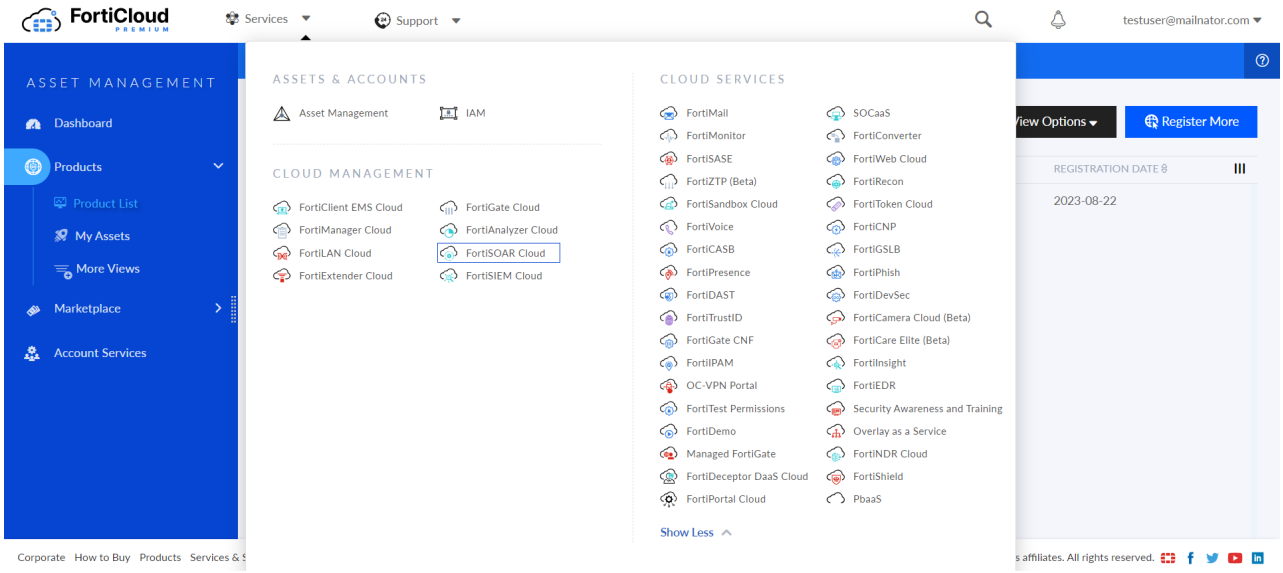
To deploy FortiSOAR Cloud:

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

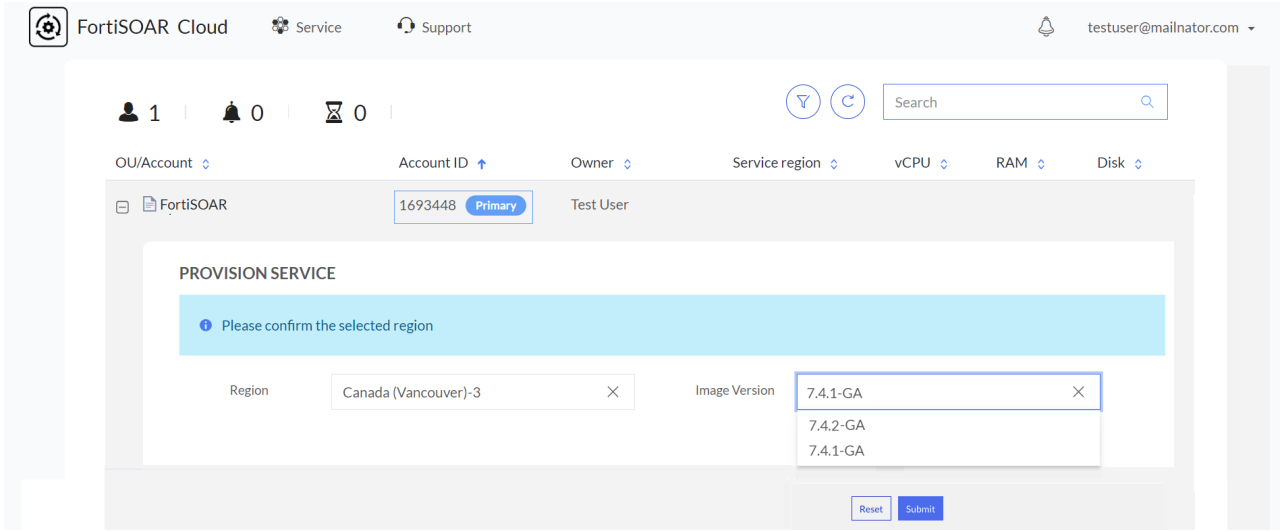


After creating a FortiCloud account, wait for 30 minutes before moving on to the next step.

2. On the FortiCare portal, click the FortiSOAR Cloud icon in the upper-left corner to access your FortiSOAR Cloud instance.

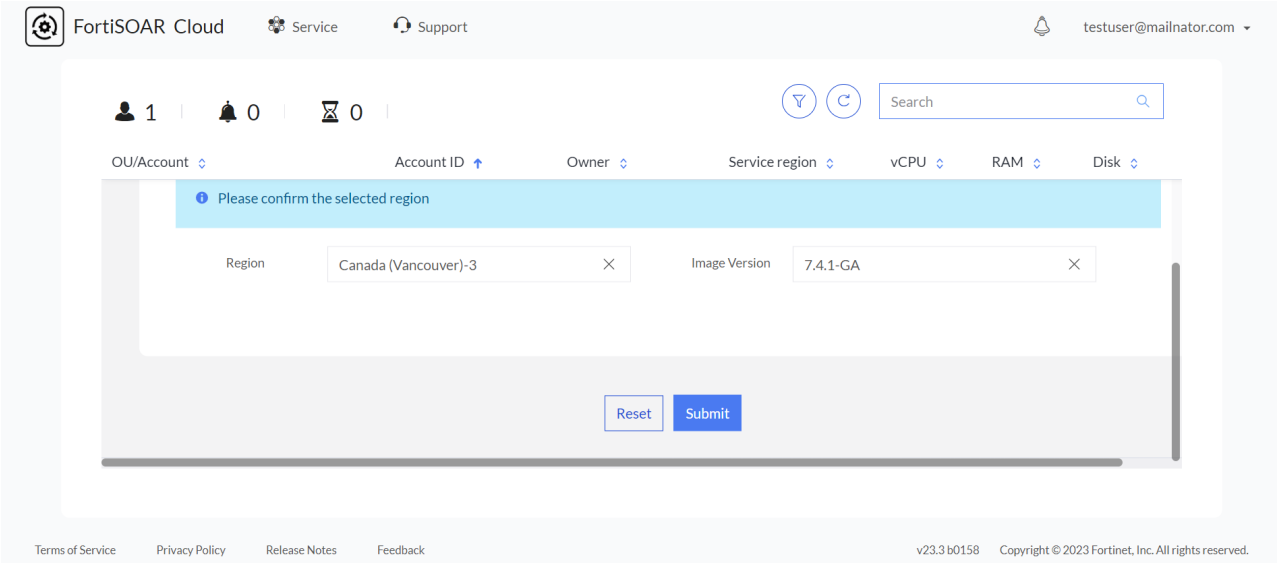


3. Once you log onto FortiSOAR Cloud, you need to select the region and version of the FortiSOAR Cloud image you want to provision:

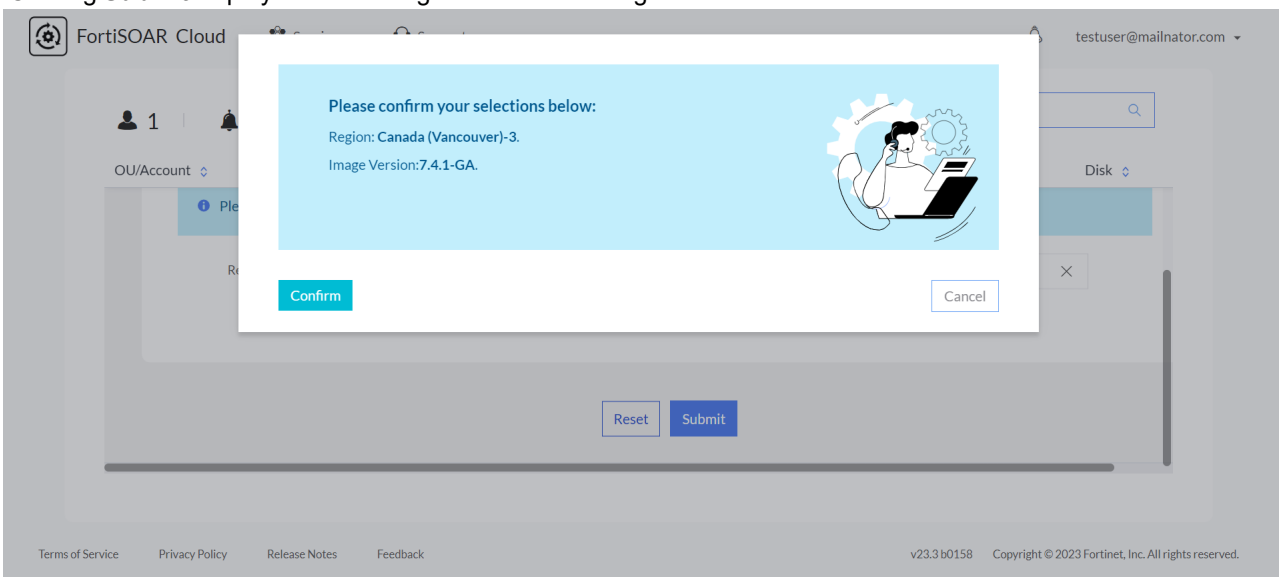


The Account ID on the FortiSOAR Cloud portal represents the dedicated instance.

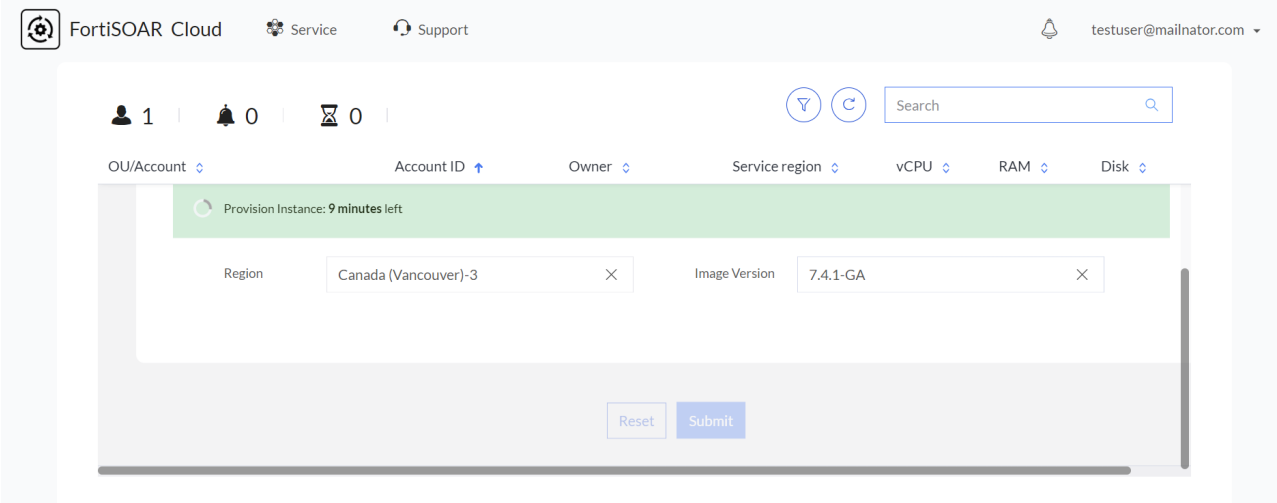
4. Once you select the region and image version, click **Submit**.



Clicking **Submit** displays the following confirmation dialog:



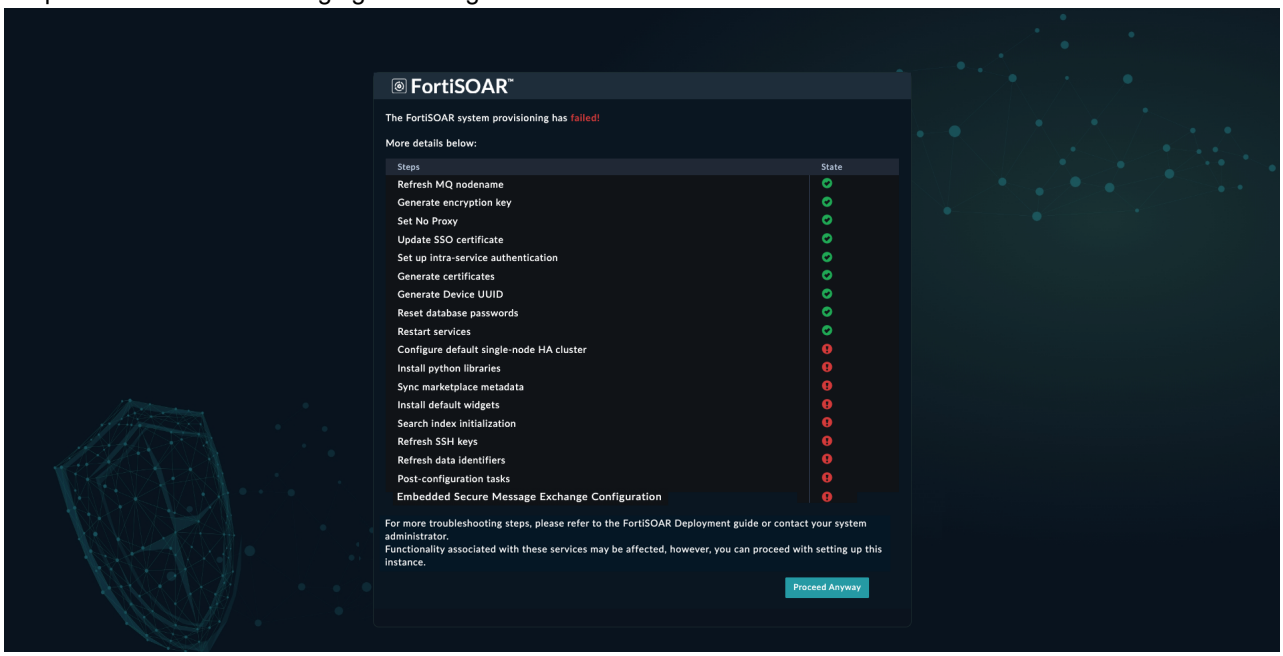
Clicking **Confirm** starts the provisioning of the FortiSOAR Cloud instance, which gets provisioned in a few minutes:



During provisioning, FortiSOAR Cloud performs certain initial configuration steps that are required for FortiSOAR. Initial configuration steps include running the automated, non-interactive FortiSOAR configuration wizard, enabling the embedded Secure Message Exchange, triggering the heartbeat between FortiCloud and FortiSOAR etc.

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

If there are any provisioning failures, such as failures while FortiSOAR Cloud is performing 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 the CLI to fix any issues with the failed steps as their functioning might be hampered. However, if you decide to access FortiSOAR Cloud without rectifying the failed steps, a **Proceed Anyway** button is provided that enables you to continue using the product while acknowledging the configuration failure:

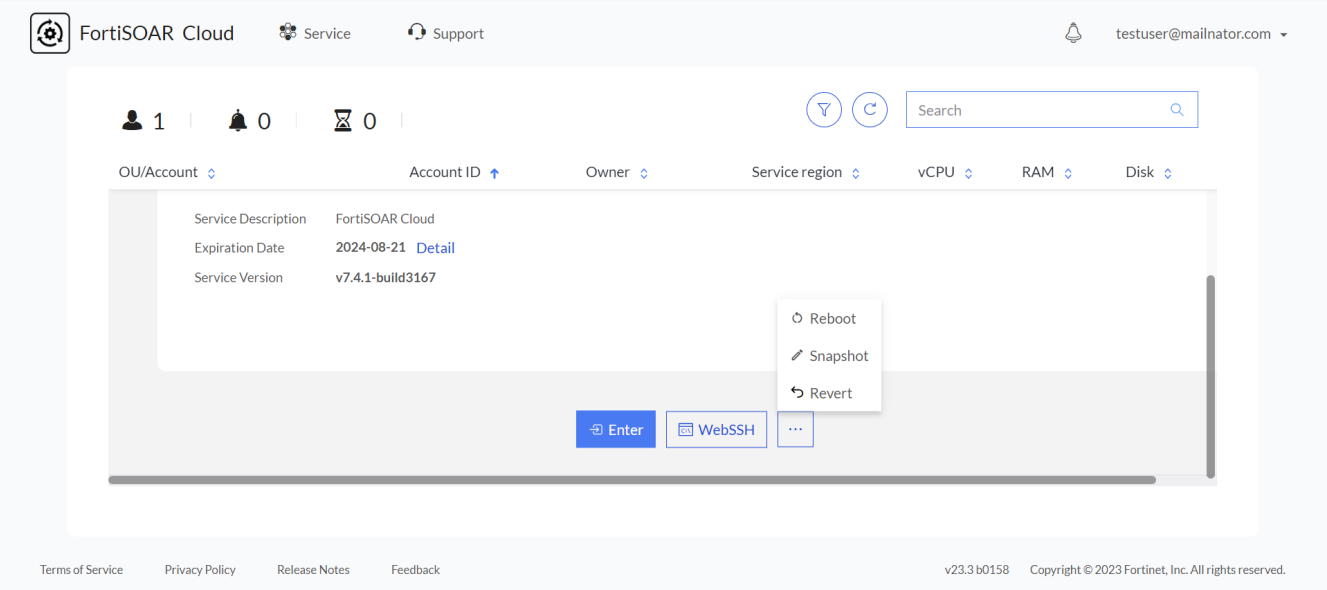


If your instance does not come up even after clicking **Proceed Anyway**, you can try the following steps to fix the issues:

- Restart all the services using the `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, click **Enter** to access the FortiSOAR web GUI or click **WebSSH** to access the FortiSOAR console to begin using FortiSOAR Cloud. For more information, see the Beginning with FortiSOAR Cloud chapter.



Important: Once the VM is provisioned successfully, you must update the correct hostname value in the "`Server_fqhn`" global variable. You can update `Server_fqhn` using by opening the playbook designer and clicking **Tools** > **Global Variables**. In the 'Global Variables' list, click the edit icon beside `Server_fqhn` and in the **Field Value** field, replace the current hostname value with `fortisoar.localhost`. The hostname will be `<forticare_accountId>.fortisoar.forticloud.com`.

Only the primary account holder can create secondary account holders in FortiCloud. The secondary account holder can log in to the same instance as a restricted user. The primary account holder can modify the admin profile for the secondary user. For more information, see the Adding a secondary account chapter.

It is highly recommended that you set up a backup user for the FortiSOAR appliance so that, in the event you forget the '`csadmin`' CLI password for CLI access and your `csadmin` user gets locked, you can still access the CLI using the backup user's account. For the steps to create a backup user, see the `Creating a backup user for the FortiSOAR appliance to allow access to the CLI` topic in the *Deploying FortiSOAR* chapter of the "Deployment Guide" that is part of the FortiSOAR Documentation.

To restrict access to your FortiSOAR instance, contact the FortiCloud team to add the IP addresses to the allowlist. Once the IP addresses are added to the allowlist, only those IP addresses can access your FortiSOAR instance.

Troubleshooting

Uniqueness error while 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 are in the same Cloud region.

Resolution

Before you configure your MSSP setup, ensure that you update the name of the SME on either the master node or the tenant node.

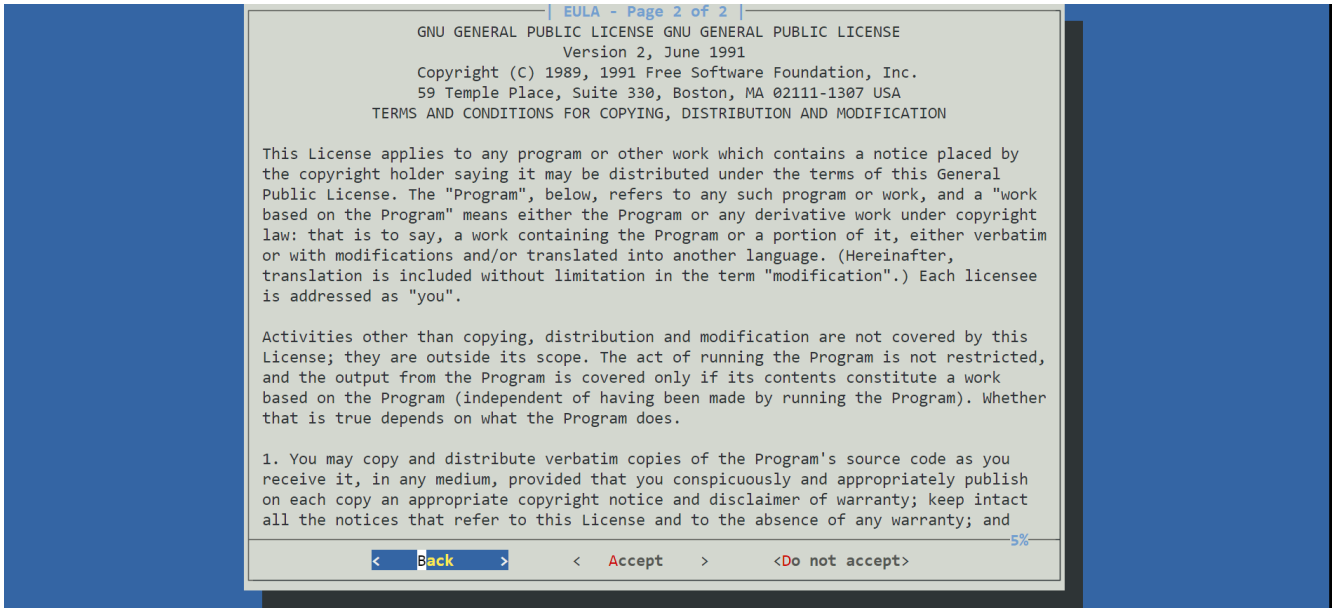
Beginning with FortiSOAR Cloud

Logging into FortiSOAR Cloud for the first time

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):



Click **Accept** to accept the EULA. Once the EULA is accepted, you can start to use the FortiSOAR Cloud console:

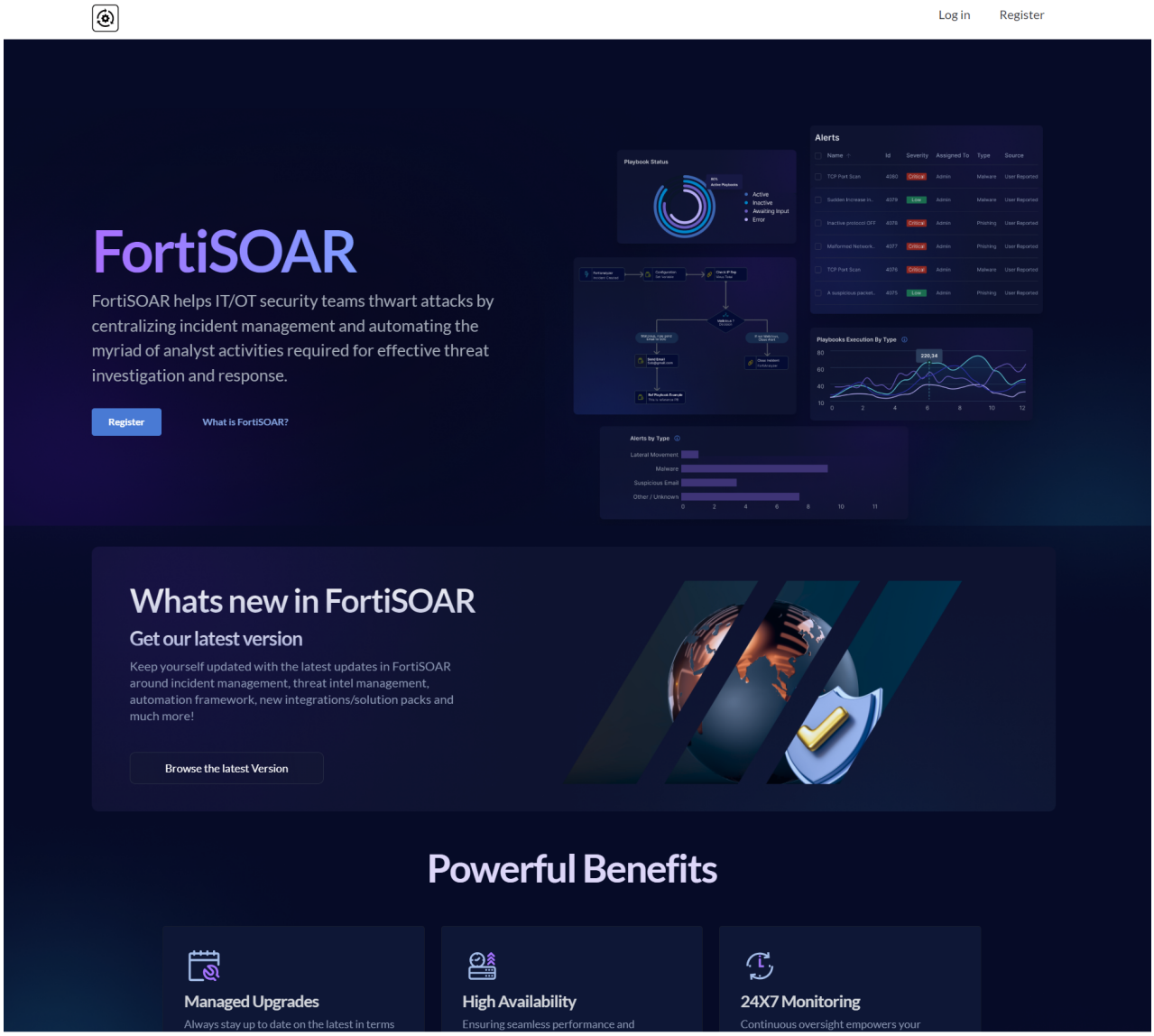
```
---------------------------------------------------------------
Built on: 2023-06-24
Rocky Linux Version: 8.8
FortiSOAR Version: 7.4.1-3167
---------------------------------------------------------------
Last login: Thu Aug 24 08:46:57 2023 from 10.96.131.138

[csadmin@1693448 ~]$ sudo su
[root@1693448 csadmin]# csadm
usage: csadm [<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
    source-control                - Source control allows import / export FSR configurations, for CICD
    network                       - Manage network
    services                      - Manage services
    ha                            - Manage HA cluster
    system                        - Manage system settings
    package                       - Manage package
[root@1693448 csadmin]#
```

To access the ForiSOAR UI, click **Enter** 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.

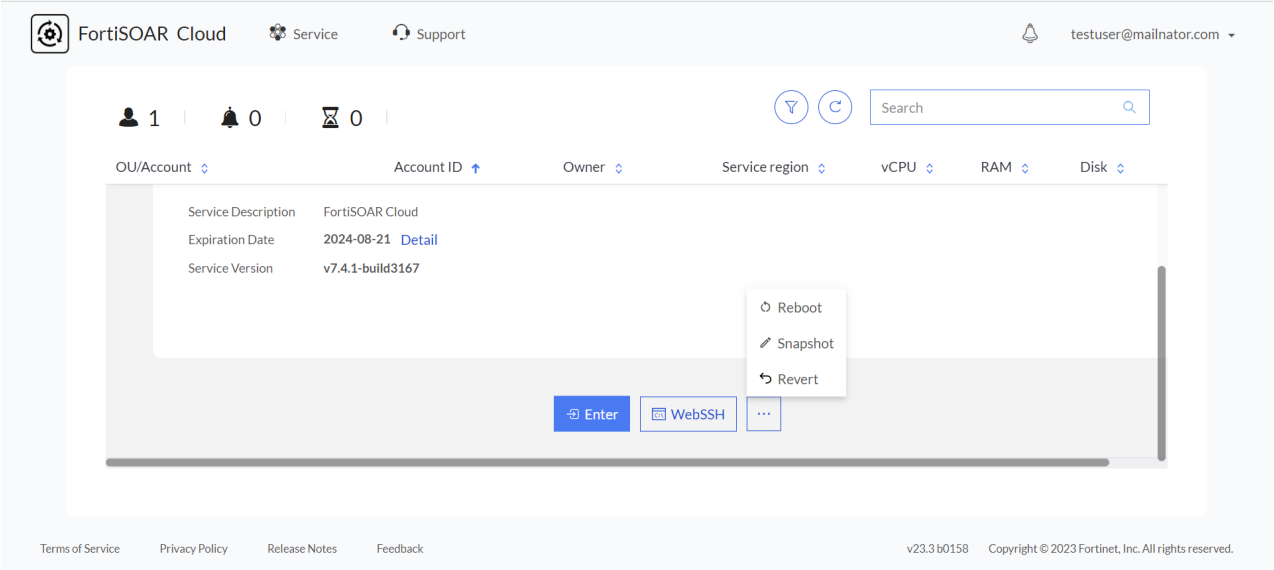
By default, the SOAR Framework Solution Pack is installed with fresh installations of FortiSOAR Cloud .The SOAR Framework Solution Pack (SP) is the **Foundational** Solution Pack that creates the framework, including modules, dashboards, roles, widgets, etc., required for effective day-to-day operations 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 for users to install the SOAR Framework SP to optimally use and experience FortiSOAR Cloud's incident response. For detailed information about the SOAR Framework SP, see the SOAR Framework SP documentation.

You can access FortiSOAR Cloud in the following ways:

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



Click **Log in** to display your FortiSOAR Cloud account page:



Click **Enter** to access the FortiSOAR Cloud UI.

- Using support.fortinet.com - This directly displays the FortiSOAR Cloud UI if the FortiSOAR Cloud instance is provisioned with a valid license.

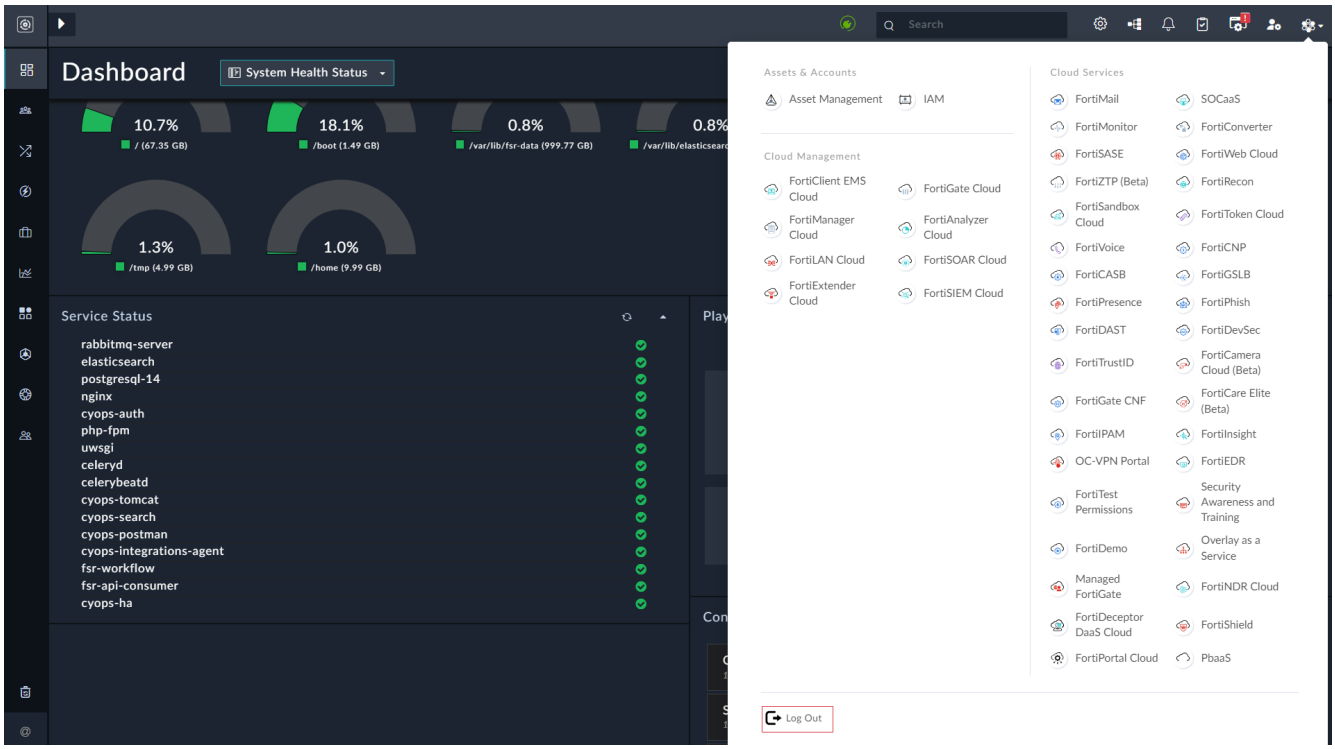
Secure Message Exchange

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 the SME runs on port 5671.

Cloud App Menu

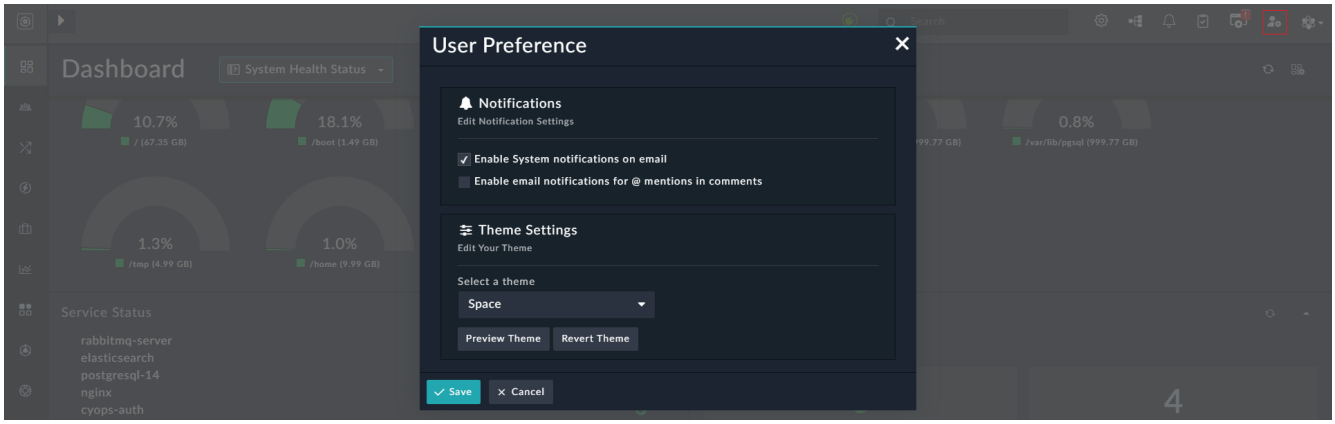
FortiSOAR displays a Cloud App Menu for users logging in through the Cloud portal. The Cloud App Menu is displayed in the FortiSOAR top bar and can be used to access other cloud applications such as FortiEDR, FortiAnalyzer Cloud,

etc.:



Whenever you click on another cloud app, such as FortiAnalyzer Cloud, you will be redirected to the cloud portal of that app, and you will be logged out of FortiSOAR and the FortiSOAR Cloud Portal. Clicking the **Logout** button also logs you out of both FortiSOAR and FortiSOAR Cloud Portal.

The 'user profile' icon in the top bar can be used by users who do not have access to the '`Security`' module to edit their profile to set the email notification options and the theme for their FortiSOAR instance:



To edit your user preferences, click the **User Profile** icon to display the `User Profile` dialog. On the `User Profile` dialog, in the `Notifications` section, select whether you want to get notified on your email account for system notifications and @mentions in the 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. 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

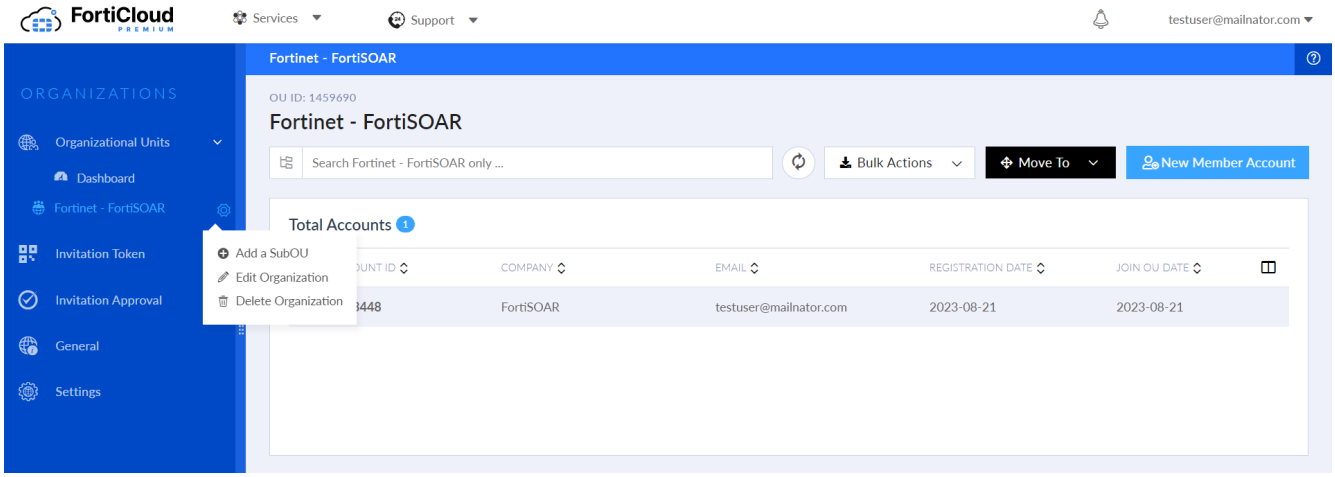
Administrators can use various logs that FortiSOAR generates to troubleshoot FortiSOAR Cloud issues:

Log Name	Purpose
`/var/log/cyops/install/config-vm-<time-stamp-here>.log`	Used for troubleshooting issues that occur while configuring the VM.
`/var/log/cyops/fcloud/`	Used for troubleshooting issues related to other cloud-related apps.
`/var/log/cyops/csadm/secure-message-exchange.log`	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 provides a single pane of visibility management 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 using the steps mentioned in the FortiCloud Account Services Organization Portal documentation, for example, 'Fortinet FortiSOAR'. The account used to create the organization becomes the 'root' account for the organization. Users with the proper permissions can add OUs and invite members to join the organization. OUs are folders for organizing your accounts and helps to build the structure of your organization. You can create a maximum of three levels of OUs:



Once you have created the Organization and OUs, you can invite Member Accounts to join the OUs using invitation tokens, using the steps mentioned in the FortiCloud Account Services Organization Portal documentation. You can also add an administrative IAM user for the Organization that can create and manage IAM users for the OUs. For more information see the Adding a secondary account chapter.

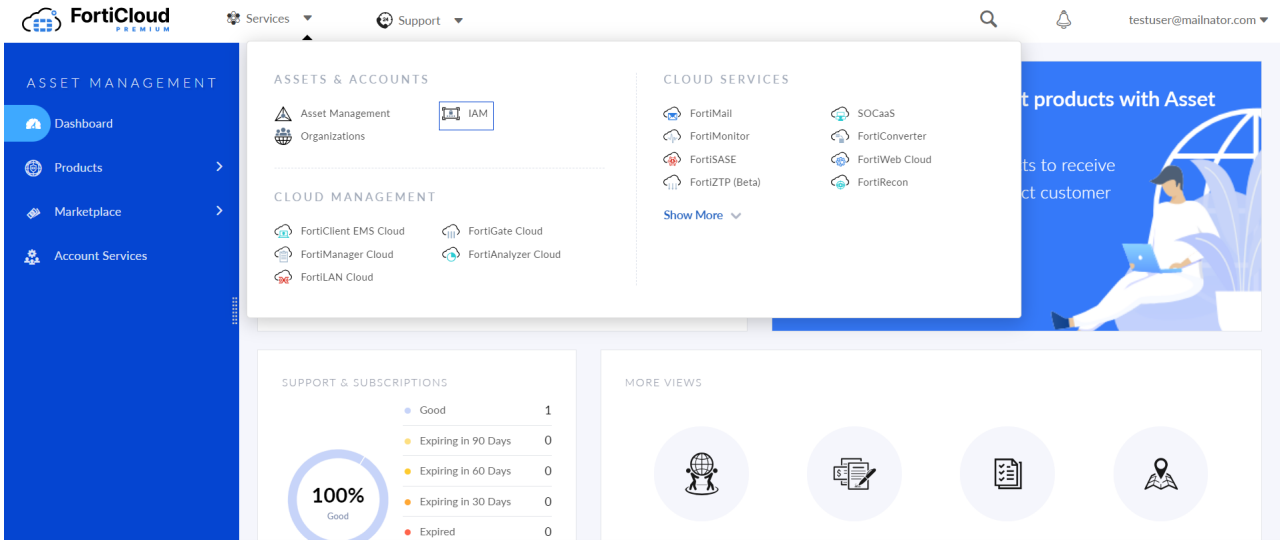
Adding a secondary account

You can create a secondary account for FortiSOAR Cloud. A secondary account allows the Fortinet support team to troubleshoot the FortiSOAR Cloud deployment. You can add a secondary account using Identity & Access Management (IAM) or FortiCare or by setting up External IdP roles. IAM is a service to help you control access to FortiSOAR Cloud portals and assets. You can use the portal to manage users, authentication credentials, and asset permissions.

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

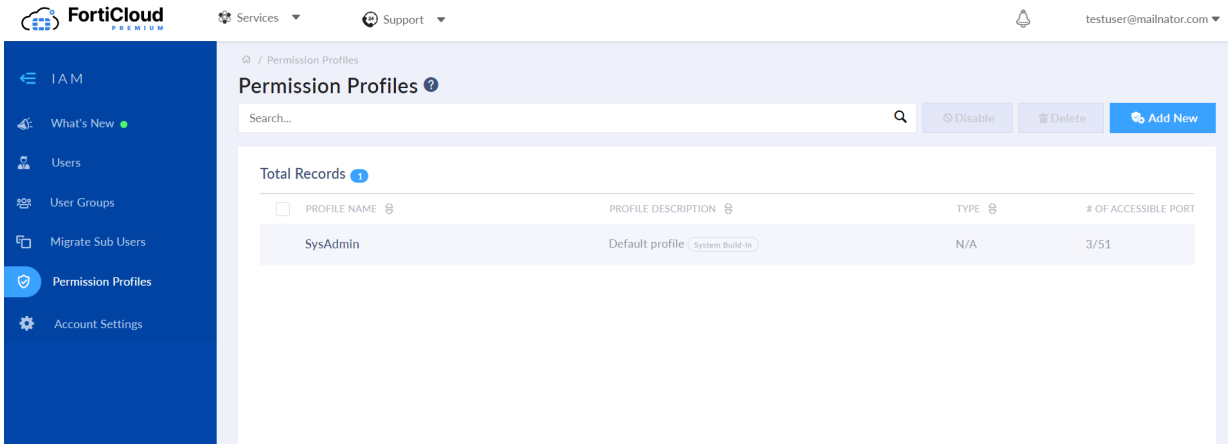
Adding a secondary account using IAM

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

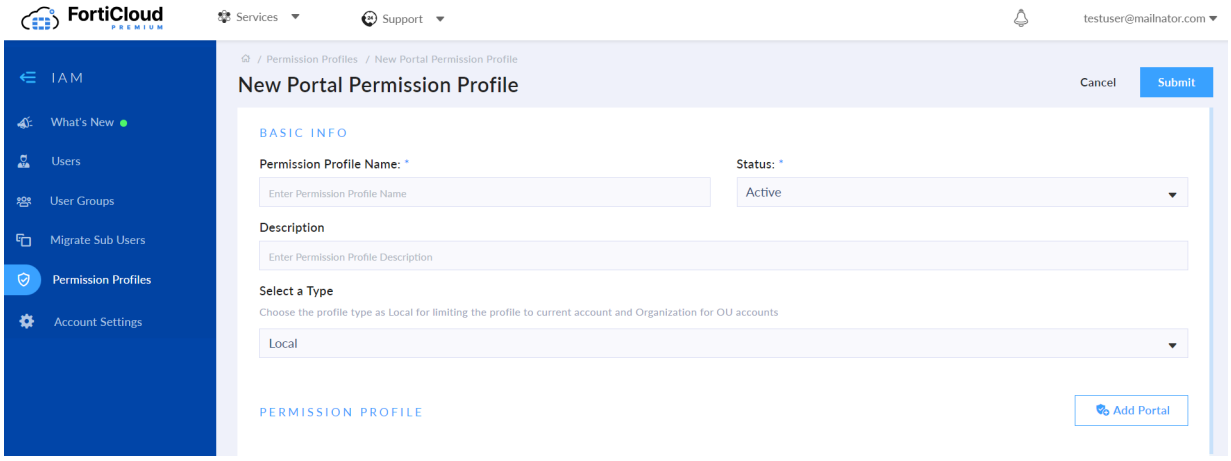


3. Before you can create IAM users, you must create permission profiles. Permission profiles define the level of portal access and permissions a user has. Permission profiles allow you to explicitly enable or disable access to FortiSOAR Cloudportals and grant portal-specific permissions for the enabled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

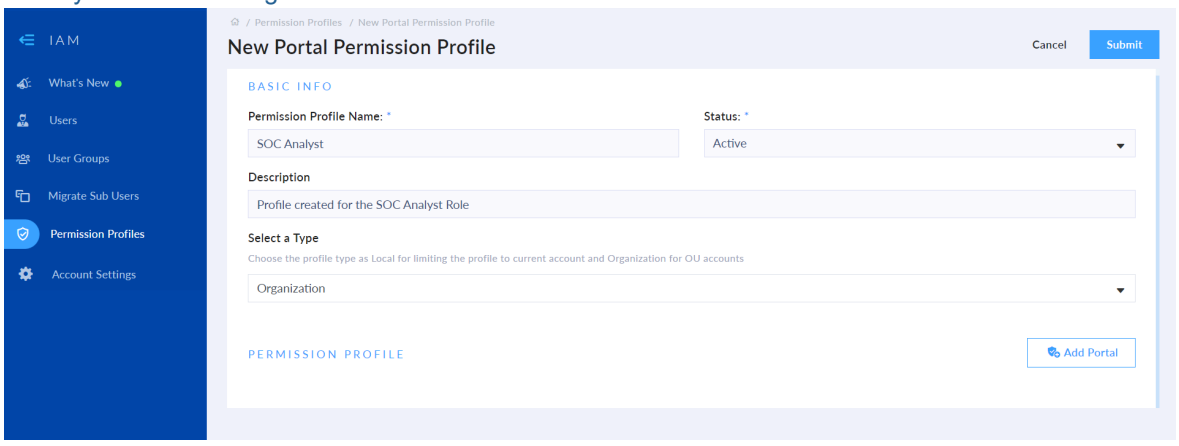
a. Click the **Permission Profiles** menu item on the IAM portal:



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

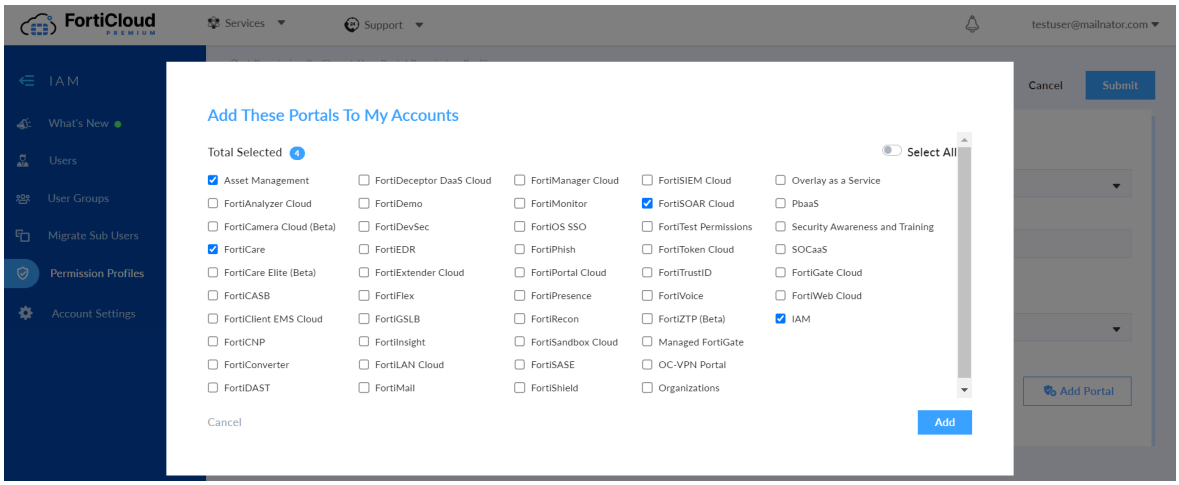


i. In the `Basic Info` section, add the required information to create the permission profile as per your requirements. For information on creating permission profiles, see the FortiCloud Account Services Identity & Access Management documentation:

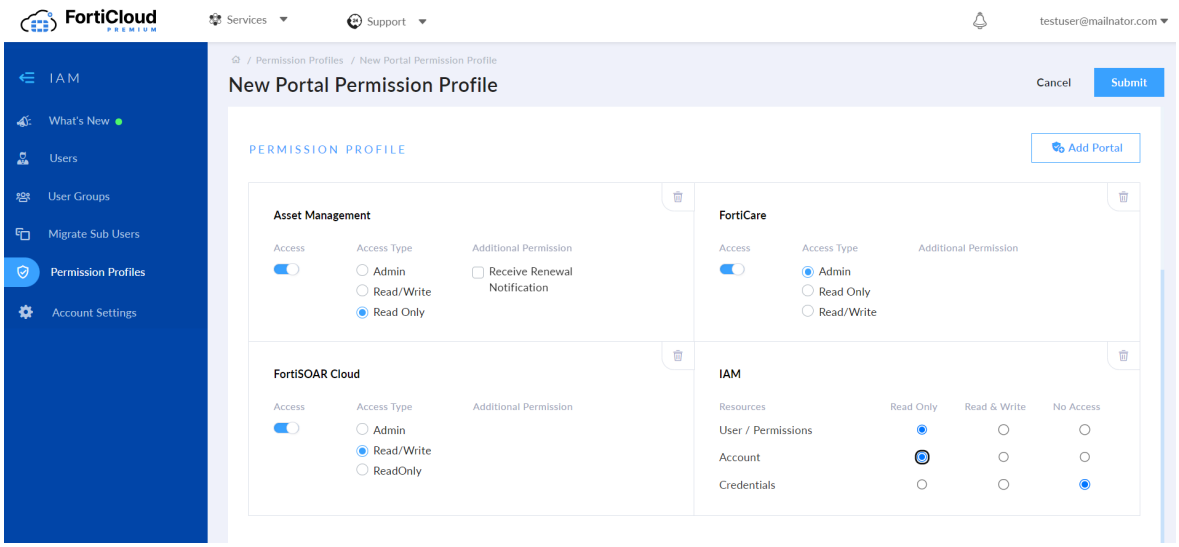


ii. Click **Add Portal** to display the `Add These Portals To My Account` pop-up. Use this pop-up to assign portal permissions to the user. You can assign the following permissions: Asset Management,

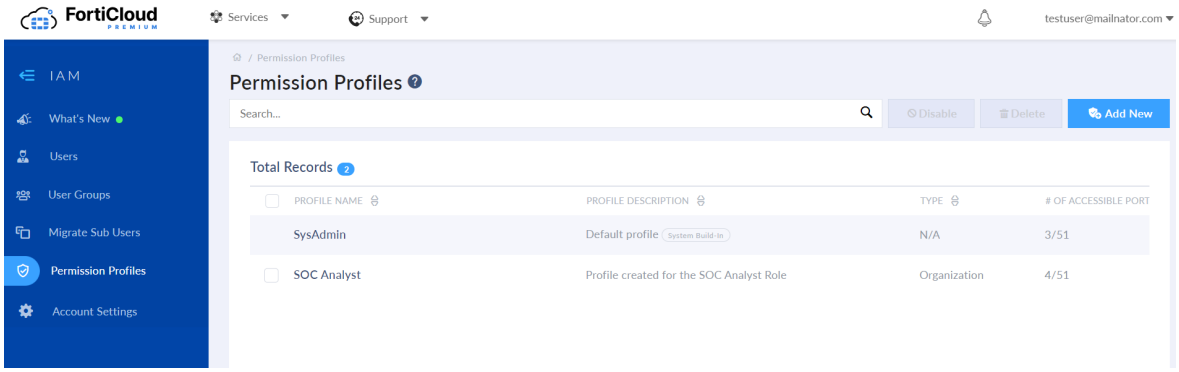
FortiCare, FortiSOAR Cloud, IAM, etc and click **Add**:



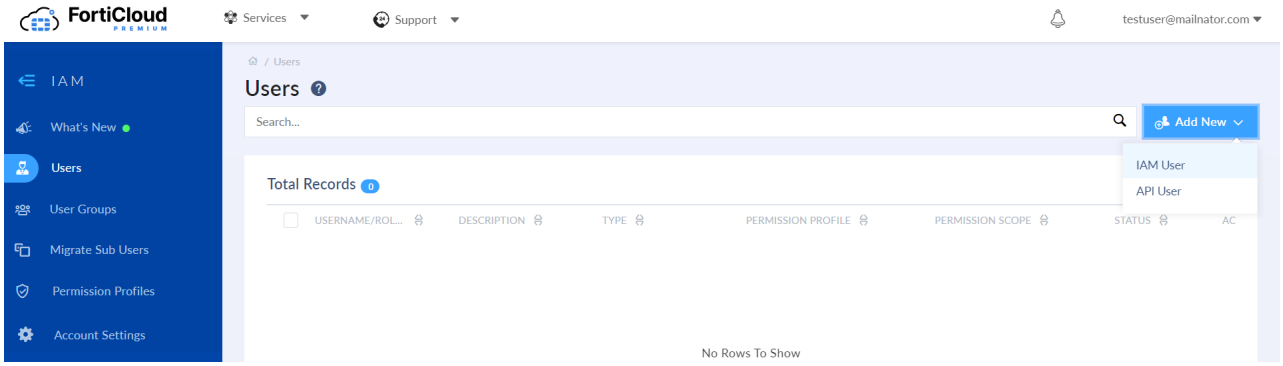
iii. In the `Permissions Profile` section, select the access type you want to assign to the user for the selected permission profiles, and click **Submit**:



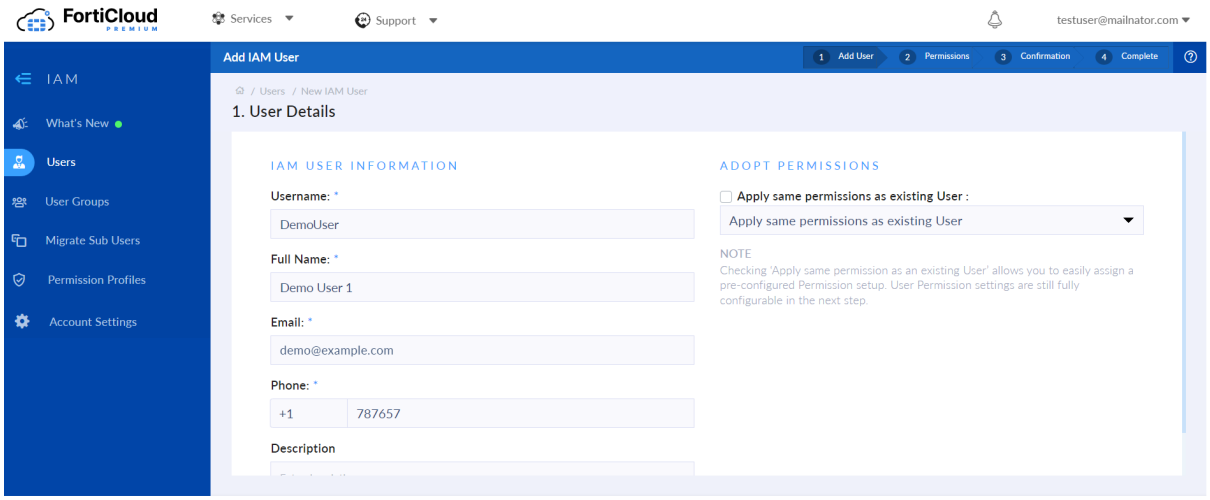
This adds the permission profile that can be assigned to users:



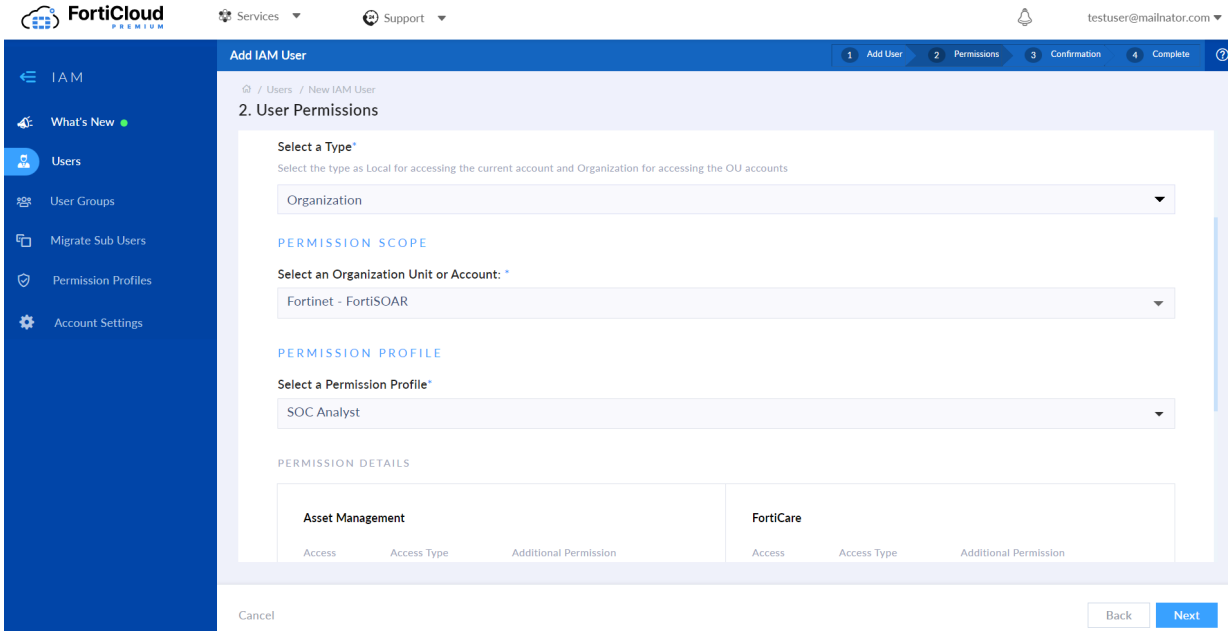
4. Click the **Users** menu item on the IAM portal, and then select **Add New** > **IAM User**:



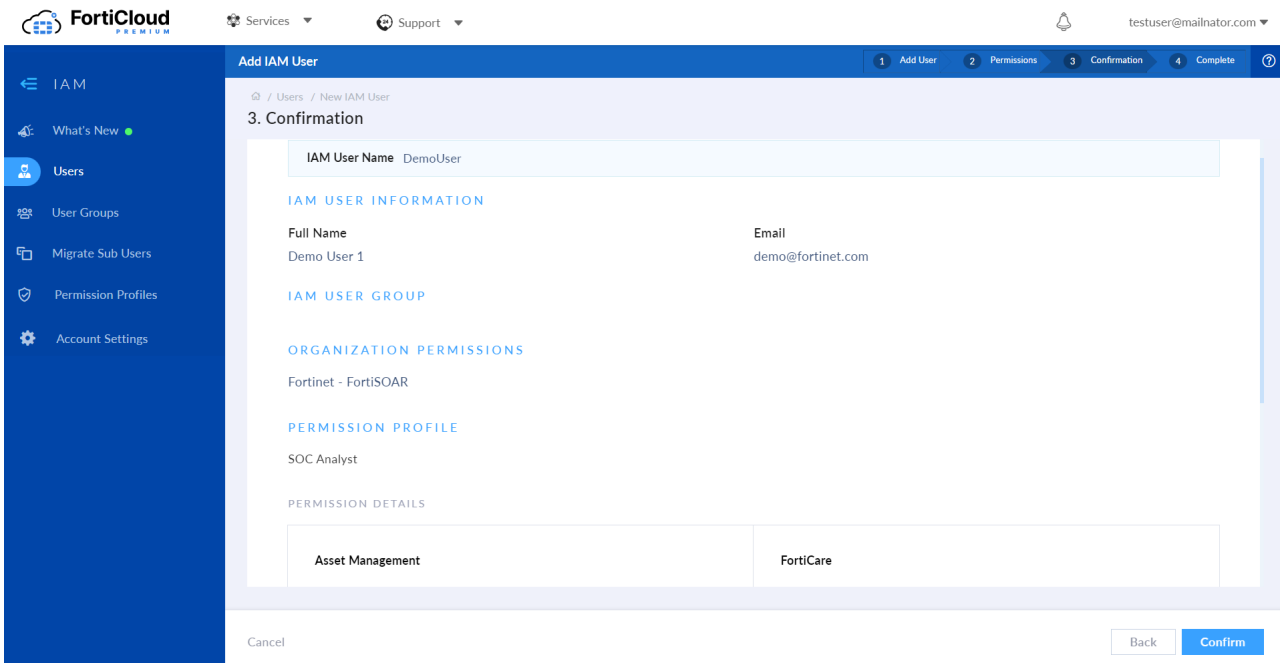
   a. On the `IAM User` page, add the details of the user to create a new IAM user, and then click **Next**.



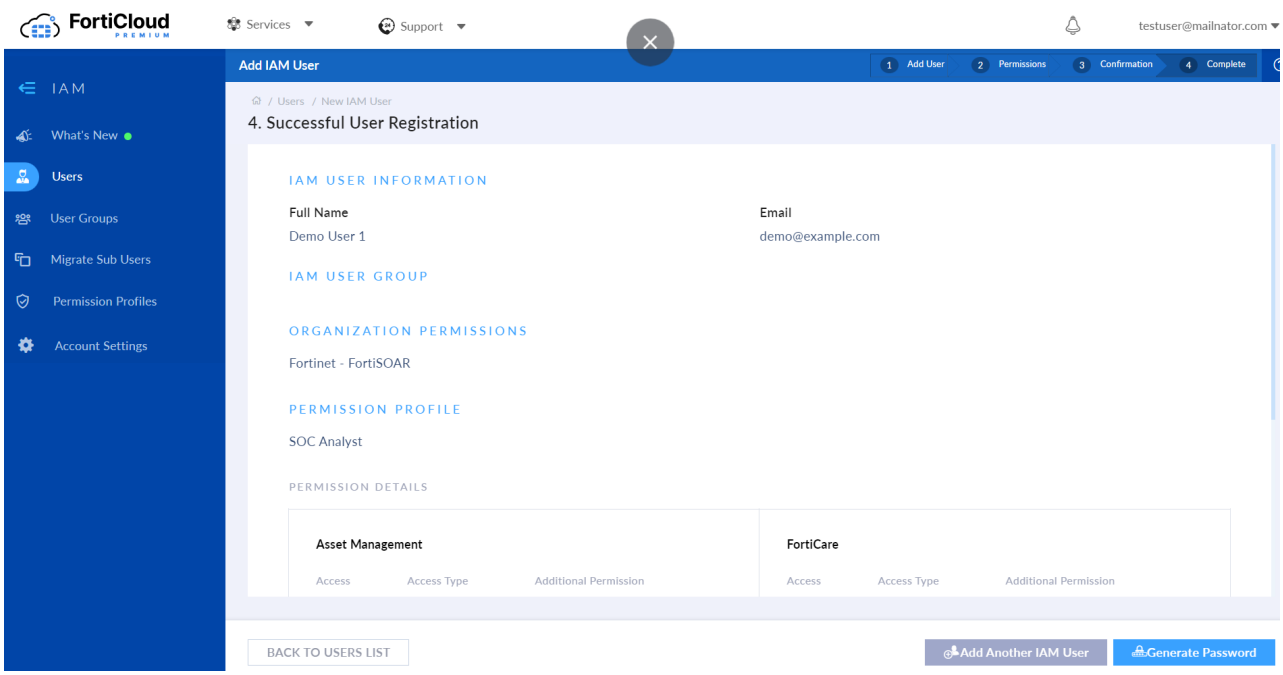
b. On the `User Permissions` page, assign the IAM user the appropriate permission type, scope, profile, etc., and then click **Next**:



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

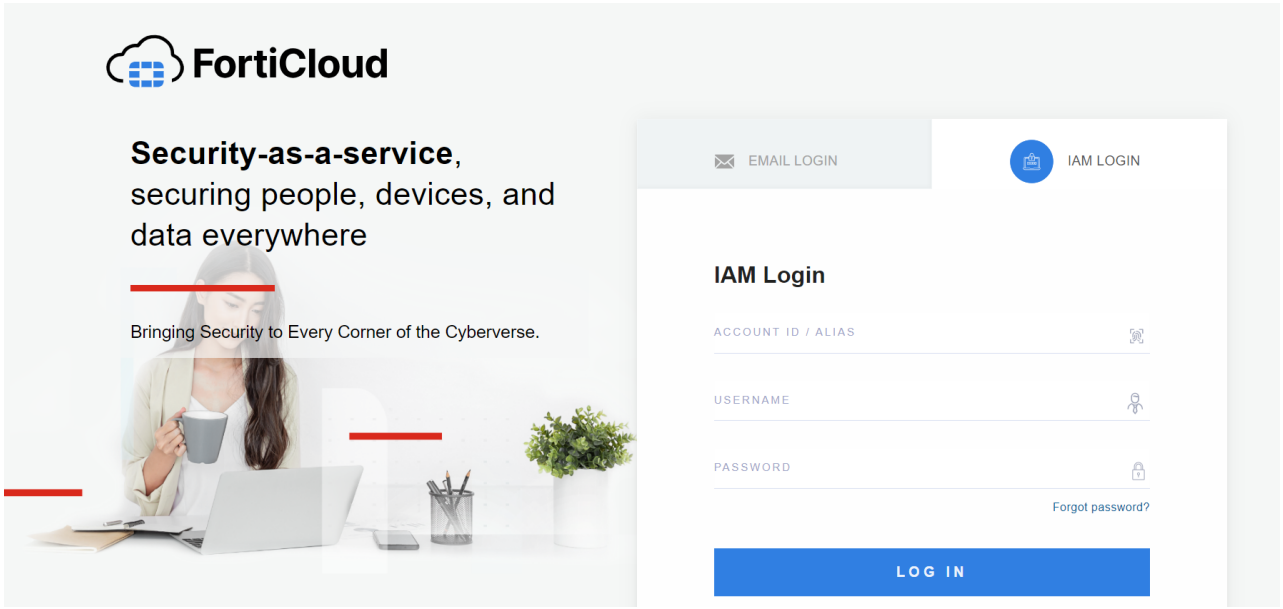


6. On the `Successful User Registration` page, click **Generate Password** to generate a reset password link for the user to login.



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

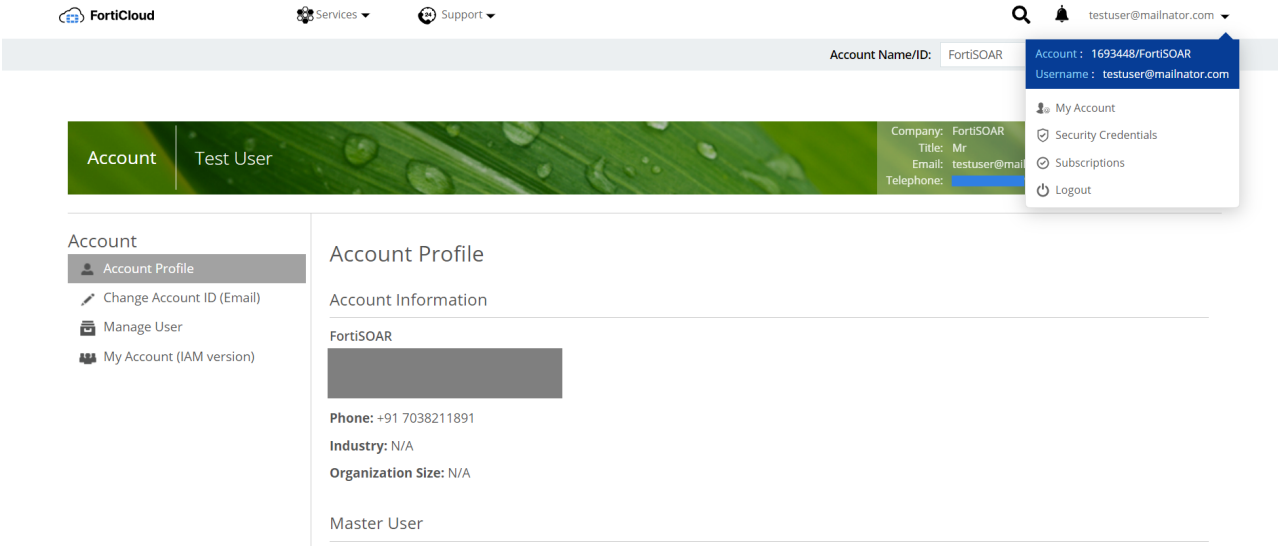
7. Navigate to https://support.fortinet.com/.
8. Click the **IAM Login** tab:



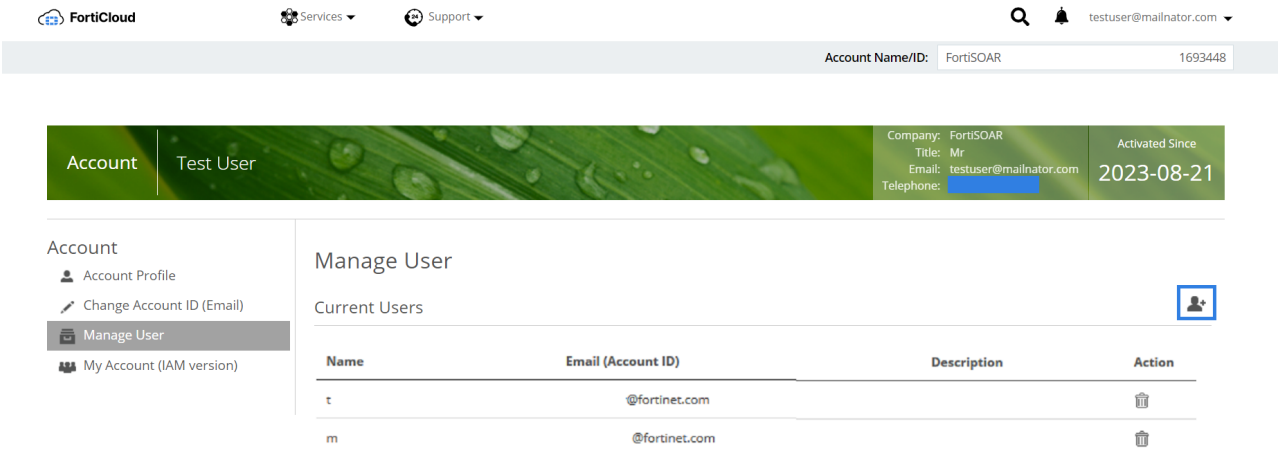
9. Enter your account ID, username, and new (regenerated) password, and click **Log in**.
10. Once you have successfully logged in, select **Services** > **FortiSOAR Cloud** to start working in FortiSOAR Cloud.

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:

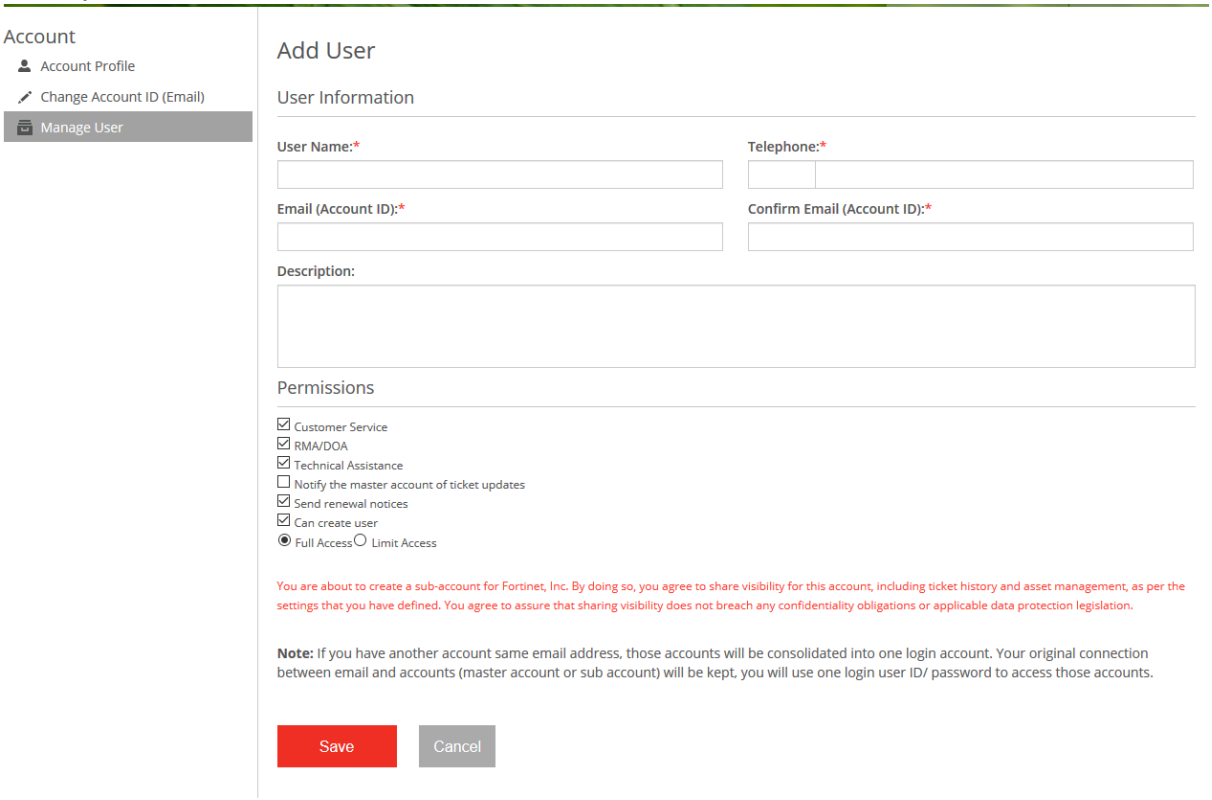


3. Click **Manage User**.
4. Click the new user icon to add a new user.



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.



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.

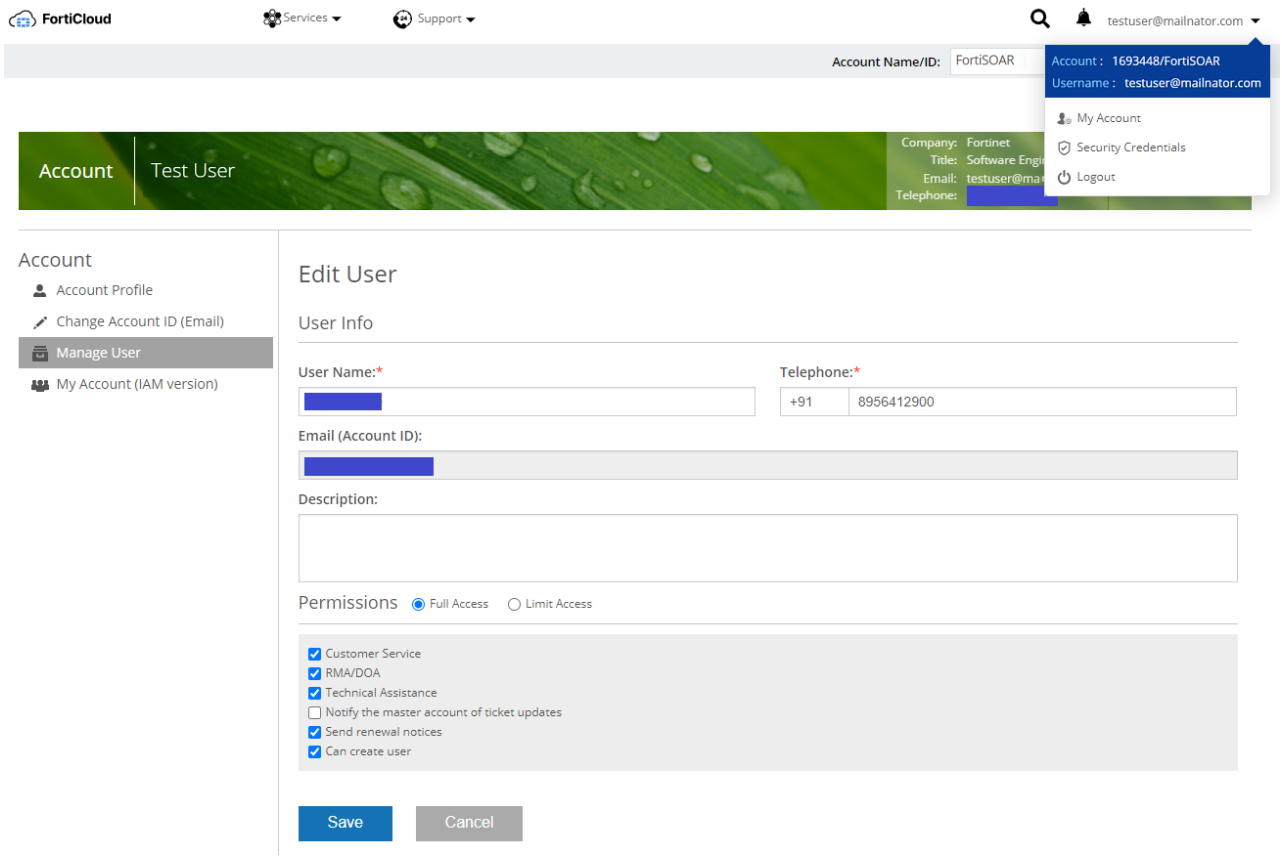
To modify a secondary account:

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**.

5. 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

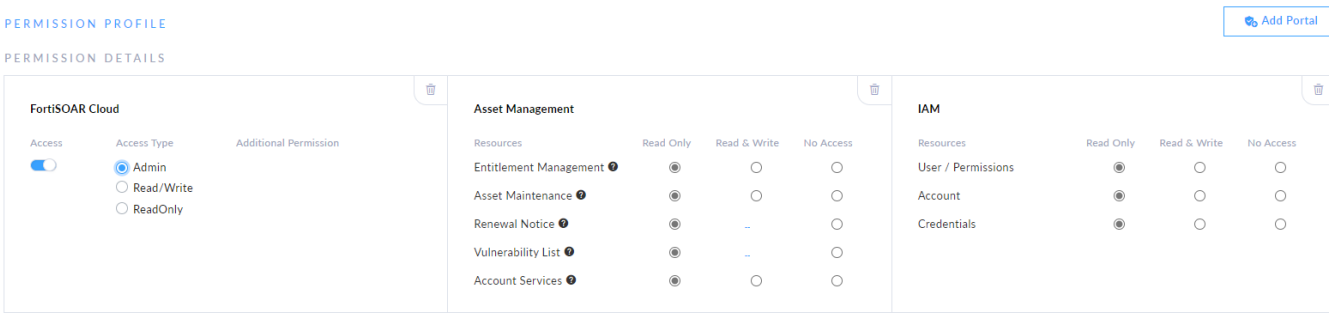
External IdP roles allow external users to log in to a cloud portal using their company's user credentials with a third-party ID provider. The company's ID provider verifies the identity of external IdP users. Following authentication, users can access the cloud application according to their role.

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

1. Send an enrollment request to forticloud-enroll-extidp@fortinet.com.
2. The enrollment request will be reviewed and approved by the FortiCloud team.
3. 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.

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:



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.
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> ~] $ 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.

Backing up and Restoring FortiSOAR Cloud

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

Prerequisites

You must have `root` or `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 (`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. If a newer version of FortiSOAR Cloud is available and you want to move to that newer version of FortiSOAR Cloud, you must restore the backed-up version only and then upgrade to the latest FortiSOAR Cloud version. This is to ensure that all the new changes will be present.

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.
- Make sure to disable the embedded SME before taking a backup from a self-hosted (enterprise) instance that has enabled its embedded SME.

Performing a backup

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

1. SSH to your FortiSOAR Cloud VM and login as a *root* user.
2. To perform a backup, type the following command:
   `# 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" from the backup. Executed playbook 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. To exclude all the "Executed Playbook Logs" from the backup, type the command as follows:
   `# 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 backup your configuration files only, then type the following command:
   `# 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 * * * 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 `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 :
`# 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 and login as a *root* user.
3. To restore the data, type the following command:
   `# 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:
   `csadm secure-message-exchange update-exchange-event-listener-certs`

www.fortinet.com