

Deployment Guide

FortiSOAR Cloud 7.3.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



November, 2022

FortiSOAR Cloud 7.3.0 Deployment Guide

00-400-000000-20210416

TABLE OF CONTENTS

Change Log	4
Introduction	5
Requirements	5
Licensing	5
FortiSOAR Cloud license contract registration	6
Deploying FortiSOAR Cloud	7
Beginning with FortiSOAR Cloud	10
Logging into FortiSOAR Cloud for the first time	10
Secure Message Exchange	10
Cloud App Menu	10
List of logs that can be used debugging FortiSOAR Cloud	12
Adding a secondary account	13
Adding a secondary account using IAM	13
Adding a secondary account using FortiCare	18
Identifying the public IP address	20
Backing up and Restoring FortiSOAR Cloud	21
Prerequisites	21
Backup Process	21
Data that is backed up during the backup process	21
Prerequisites to running the backup process	22
Performing a backup	22
Restoring data	23

Change Log

Date	Change Description
2022-11-30	Initial release of 7.3.0

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 running 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](#)
- [Licensing](#)

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 on 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 will display a notice to the customer. Customers have a grace period, currently set as 30 days, which allows the customers 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.

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 2 users included. If you want to get more users, you require to 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 codes 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 require 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.

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:



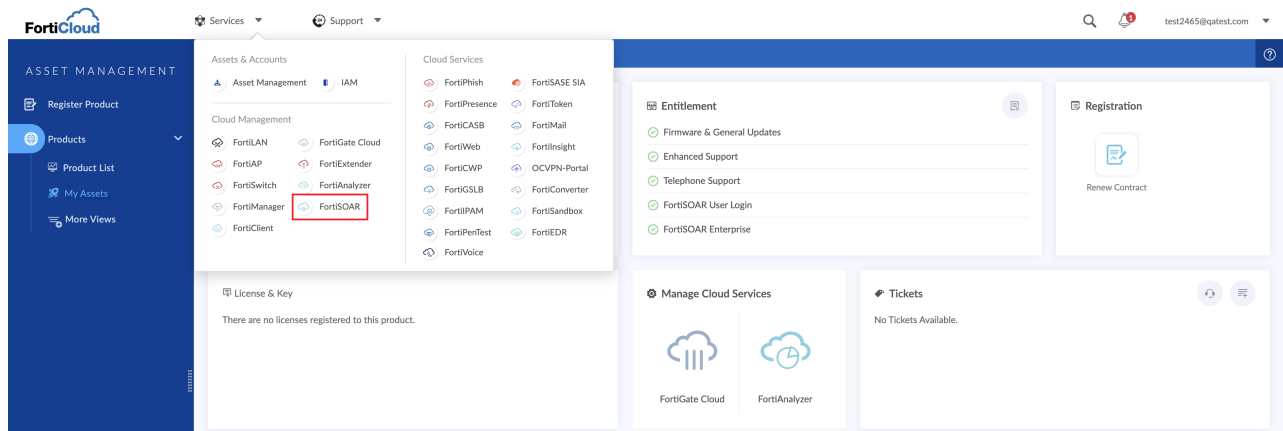
The screenshot shows the FortiCloud portal interface. The 'Products' menu is expanded, and the 'FortiSOAR Cloud' product is highlighted in the list. The account ID '1007046/Fortinet' is visible in the top right corner.

SERIAL NUMBER	PRODUCT MODEL	DESCRIPTION	DAYS TO EXPIRATION	REGISTER
FSRCLDTM21090039	FortiSOAR Cloud	Cloud Instance	2022-02-14	2021-0
FSRVMPTM20000061	FortiSOAR	dev_setup_E_Ent	No coverage	2020-0
FSRVMPTM20000065	FortiSOAR	51.41_E_Ent	No coverage	2020-0
FSRVMPTM20000072	FortiSOAR	FSR_Test_60_146	No coverage	2020-05-22
FSRVMPTM20000073	FortiSOAR	51.42_p_ent	No coverage	2020-05-22



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

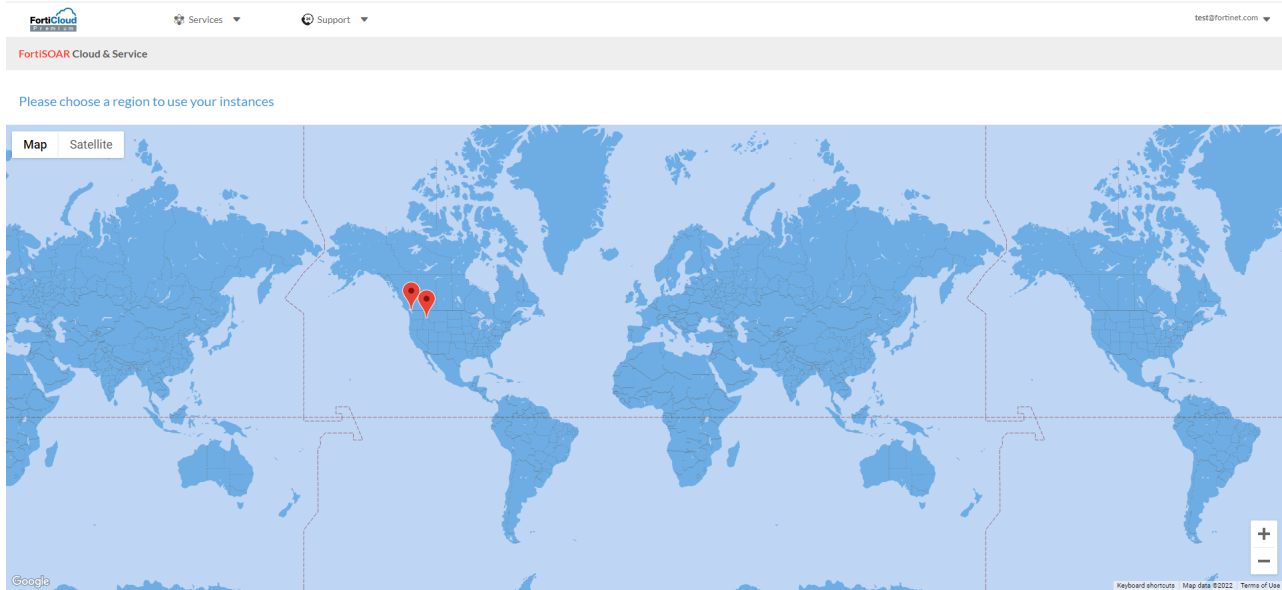
2. On FortiCare portal, click the FortiSOAR icon in the upper-left corner to access the FortiSOAR Cloud instance.



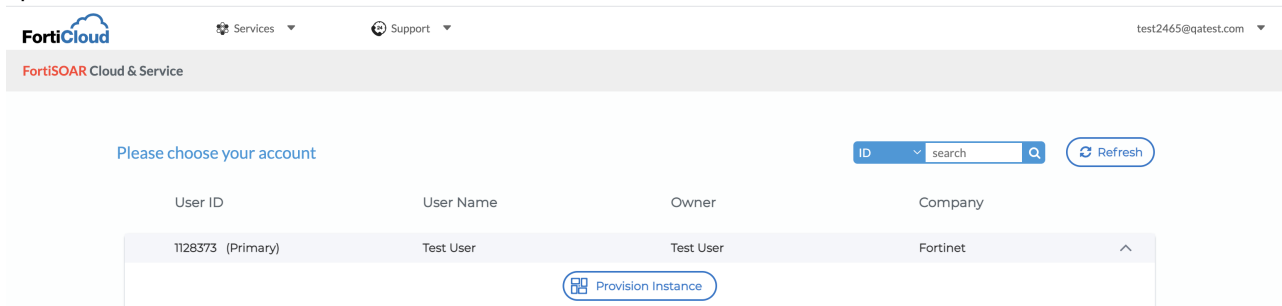
The screenshot shows the FortiCloud portal interface. The 'Cloud Services' section is expanded, and the 'FortiSOAR' icon is highlighted. The 'Entitlement' page shows various services and their status.

Service	Status
FortiSOAR	Active
FortiGate Cloud	Active
FortiAnalyzer	Active

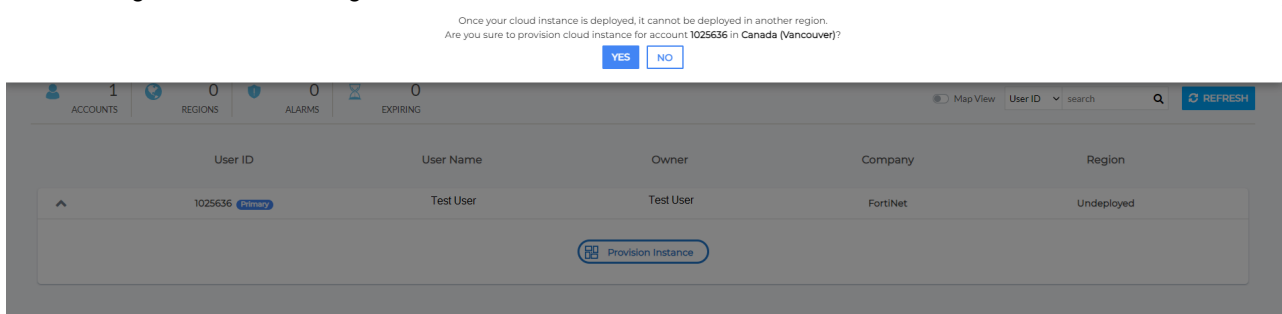
- Once you log onto FortiSOAR Cloud, you require to select your region for FortiSOAR Cloud:



- Once you select the region and expand the option, select the account which includes the FortiSOAR entitlement to open the menu drawer, then click **Provision Instance**.



The Account ID on the FortiSOAR portal represents the dedicated instance. Clicking **Provision Instance** displays the following confirmation dialog:



Clicking **Yes** 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.

- Once provisioned, click **Enter** to access the FortiSOAR web GUI or select SSH 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.

Beginning with FortiSOAR Cloud

Logging into FortiSOAR Cloud for the first time

From the FortiCloud portal, you can access the FortiSOAR web UI. On the FortiSOAR UI, you will be asked to accept the EULA, if it is not already accepted, and then get logged into the FortiSOAR UI and you will be able to perform actions in FortiSOAR based on the roles you have been assigned, i.e., a 'Full Access' user or a 'Limited Access' user.

You can also access the FortiSOAR Cloud console from 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 will be again asked to log in using the updated credentials and then you will be presented with the EULA acceptance page. Once the EULA is accepted, you can start to use the FortiSOAR console.

For information on FortiSOAR features and how to use and configure them, see the [FortiSOAR Documentation Library](#).

Also, by default, the SOAR Framework Solution Pack (SP) is installed. The SOAR Framework Solution Pack (SP) is the **Foundational** Solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. From release 7.2.0 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.



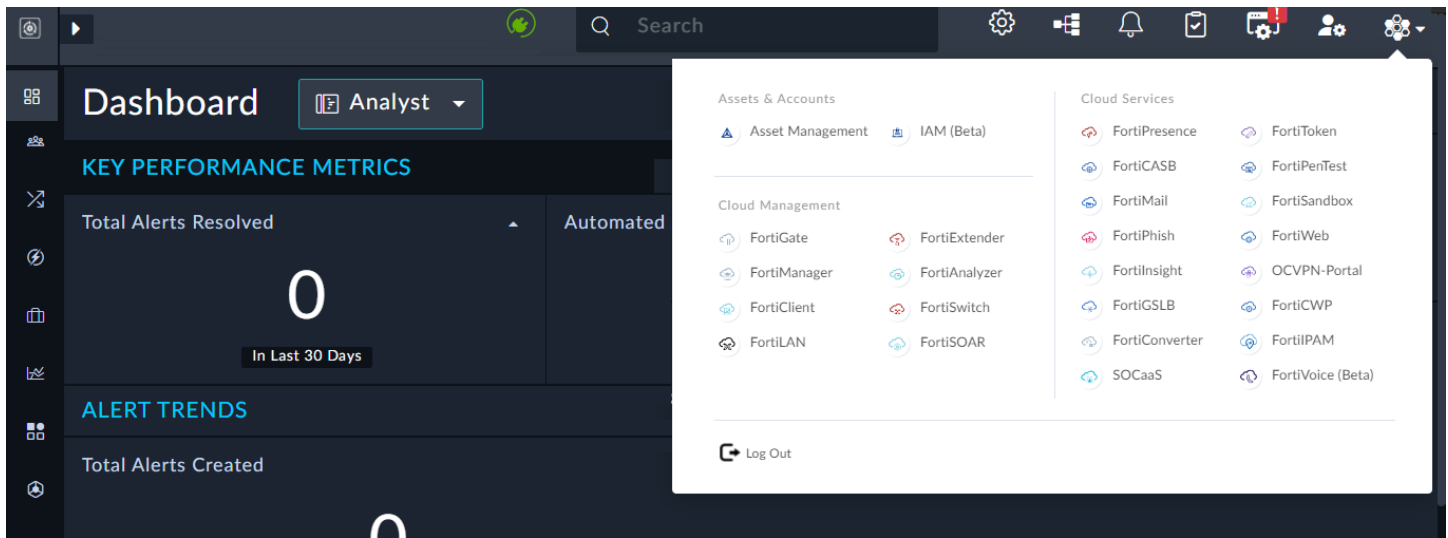
From release 7.2.0 onwards, the SOAR Framework Solution Pack is installed by default with the fresh installations of FortiSOAR Cloud .

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 the external agents or dedicated tenant nodes. The address of the embedded SME is set as the Cloud portal address and SME runs on port 5671.

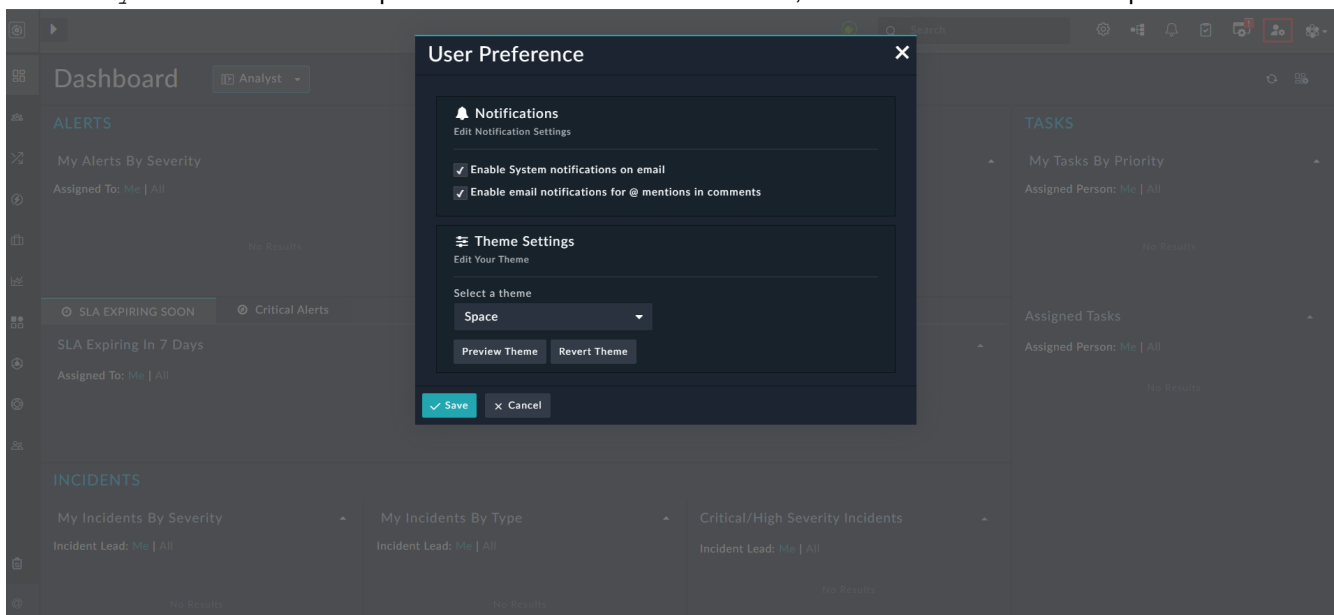
Cloud App Menu

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, FortiCare, etc:



Whenever you click on another cloud app, such as FortiAnalyzer, 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.

From release 7.2.1 onwards, a user profile icon is added to the top bar so that users who do not have access to the 'Security' module can edit their profile to set the theme for FortiSOAR, as well as email notification options.



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 debugging FortiSOAR Cloud

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.

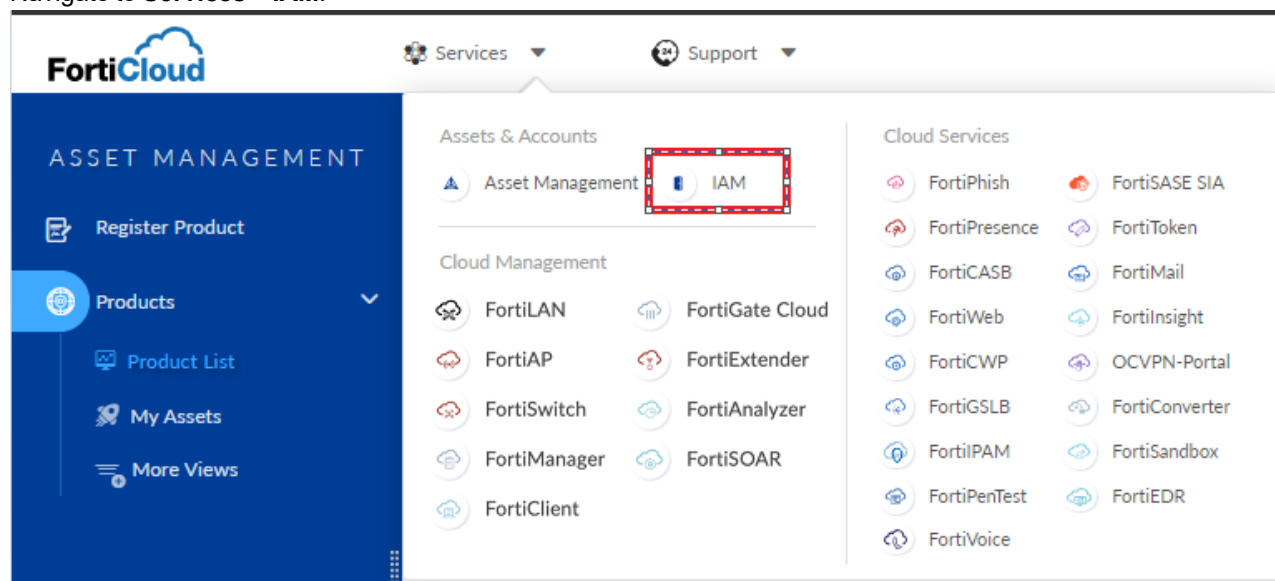
Adding a secondary account

You can create a secondary account for FortiSOAR Cloud. A secondary account allows the Fortinet support team to troubleshoot the FortiSOAR Cloud deployment.

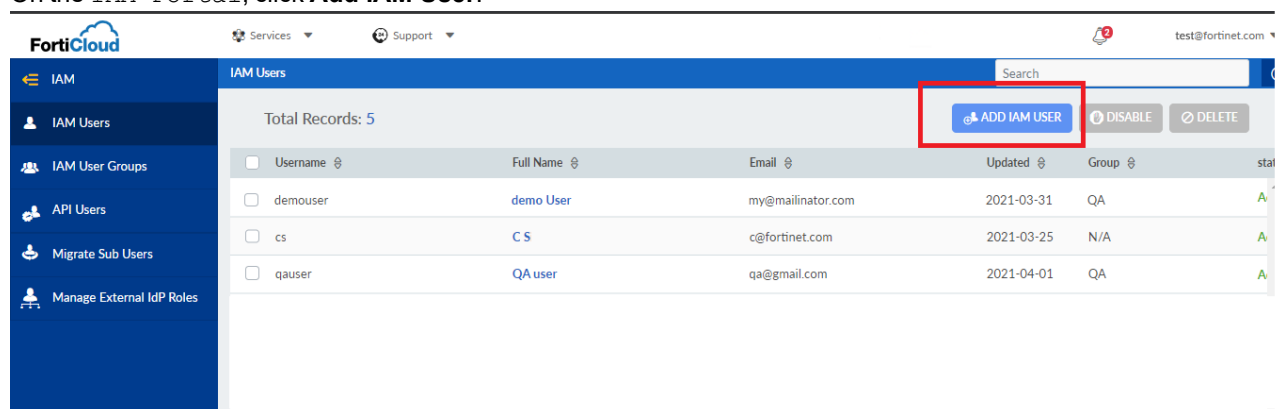
You can add a secondary account using IAM or FortiCare.

Adding a secondary account using IAM

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



3. On the IAM Portal, click **Add IAM User**.

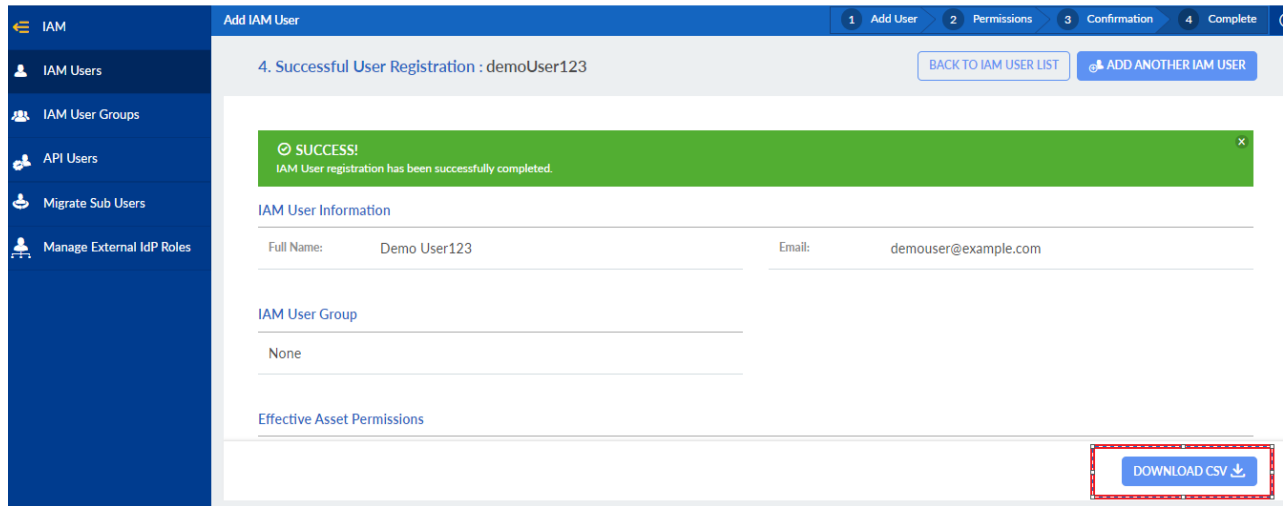


4. On the **IAM User** page, add details of the user to create a new IAM user, and then click **Next**.

5. On the **User Permissions** page, assign the IAM user appropriate permissions. You can assign the following permissions to a user:
- Portal Permission: IAM, Asset Management, Forticare – Admin
 - Cloud Management & Services:
 - Add FortiSOAR as Service
 - Specify Admin Permissions for a FortiSOAR Admin user access (Roles – Full App permissions, Security Admin, Application Admin)
 - Specify Readonly/ReadWrite permissions for a normal FortiSOAR user access (Role – SOC Analyst)

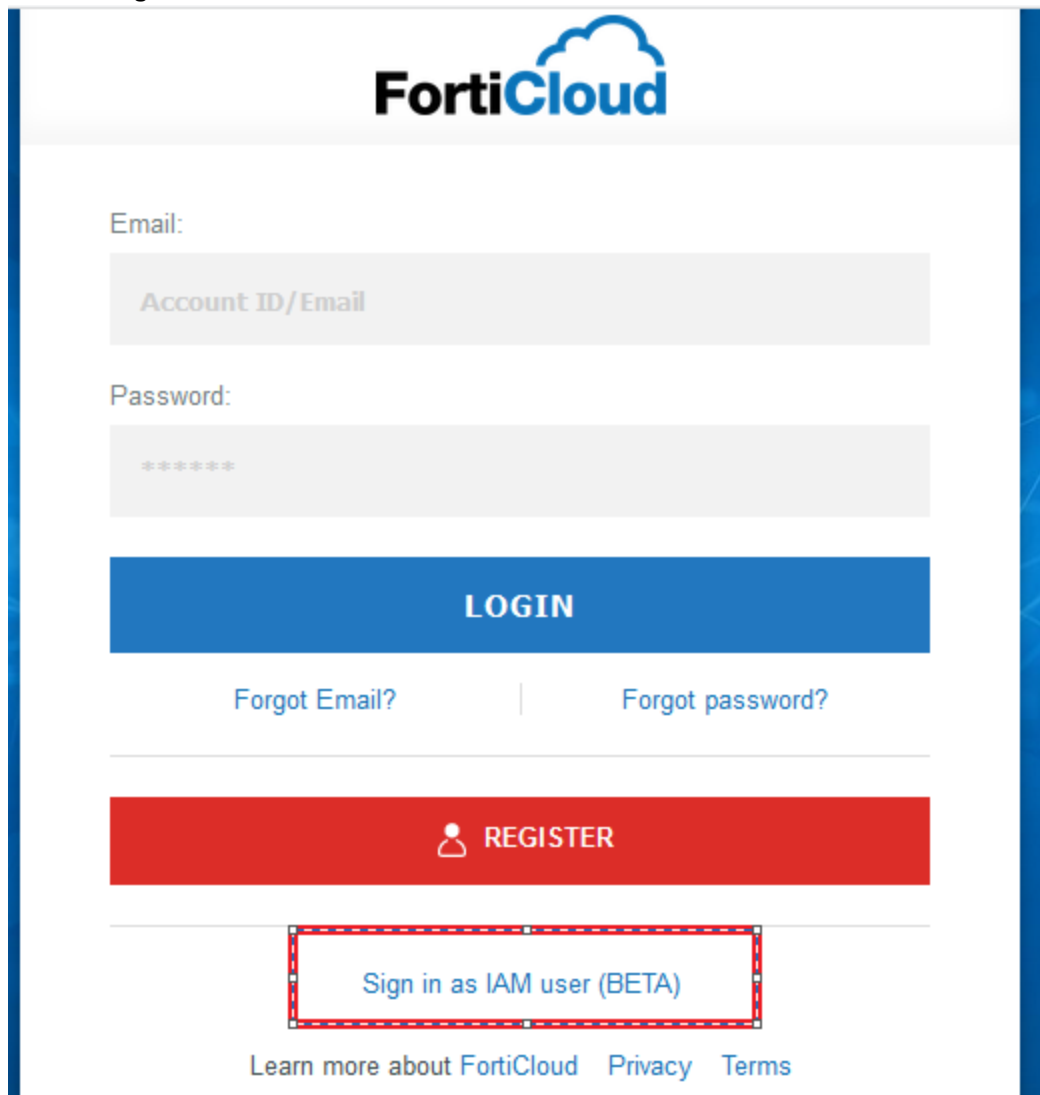
6. Click **Next** and then click **Confirm** to finish user creation process.

7. On the Successful User Registration page, click **Download** to download the credentials of the created user in the CSV format.



8. Navigate to <https://support.fortinet.com/>.

9. Click the **Sign in as IAM User** link.



The image shows the FortiCloud login and registration interface. At the top is the FortiCloud logo. Below it are two input fields: 'Email:' with a placeholder 'Account ID/Email' and 'Password:' with a masked password '*****'. A blue 'LOGIN' button is positioned below the password field. Under the login button are two links: 'Forgot Email?' and 'Forgot password?'. Below these is a red 'REGISTER' button with a user icon. At the bottom, a link 'Sign in as IAM user (BETA)' is highlighted with a red dashed border. At the very bottom are links for 'Learn more about FortiCloud', 'Privacy', and 'Terms'.

FortiCloud

Email:

Account ID/Email

Password:

LOGIN

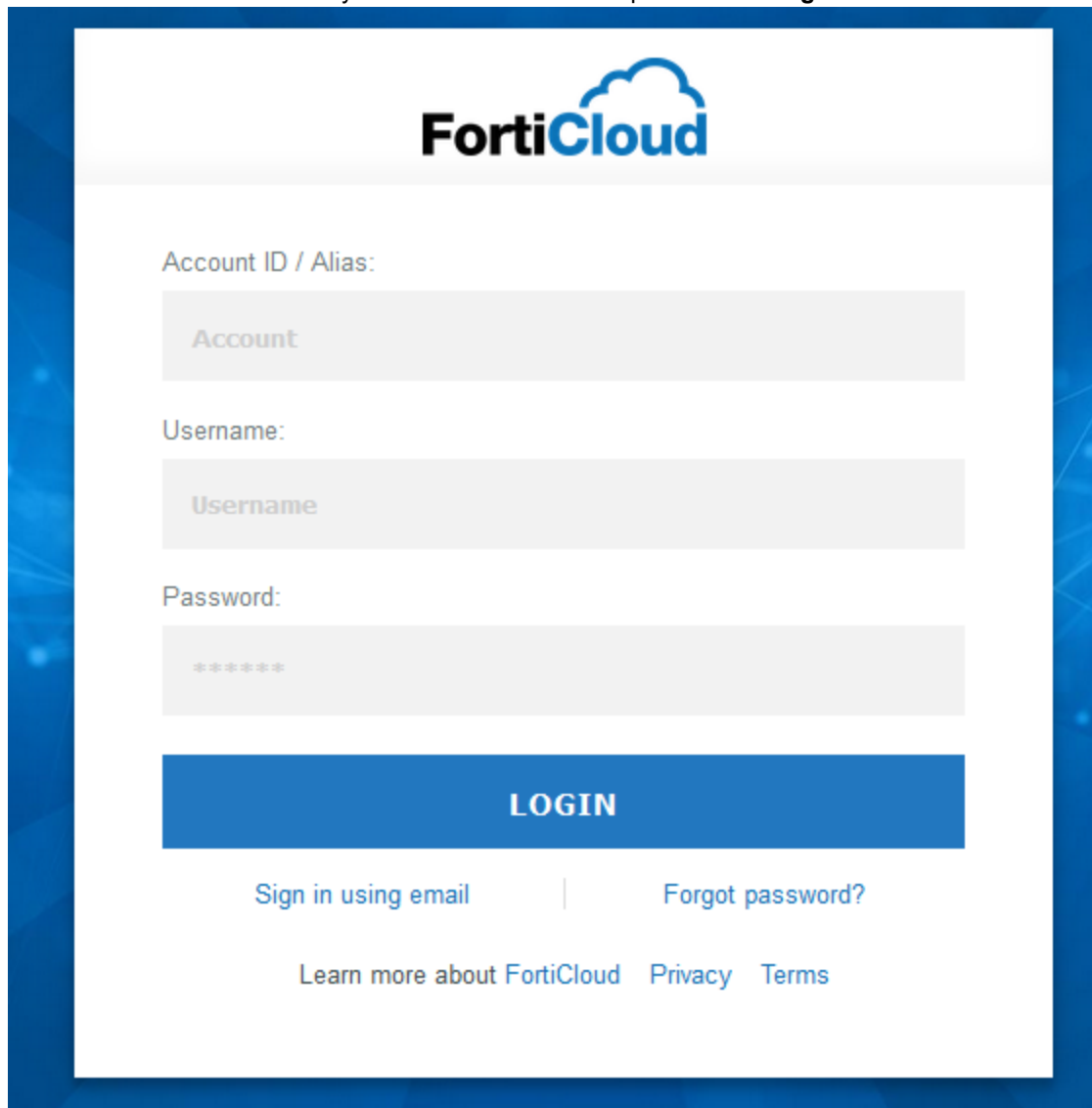
[Forgot Email?](#) | [Forgot password?](#)

REGISTER

[Sign in as IAM user \(BETA\)](#)

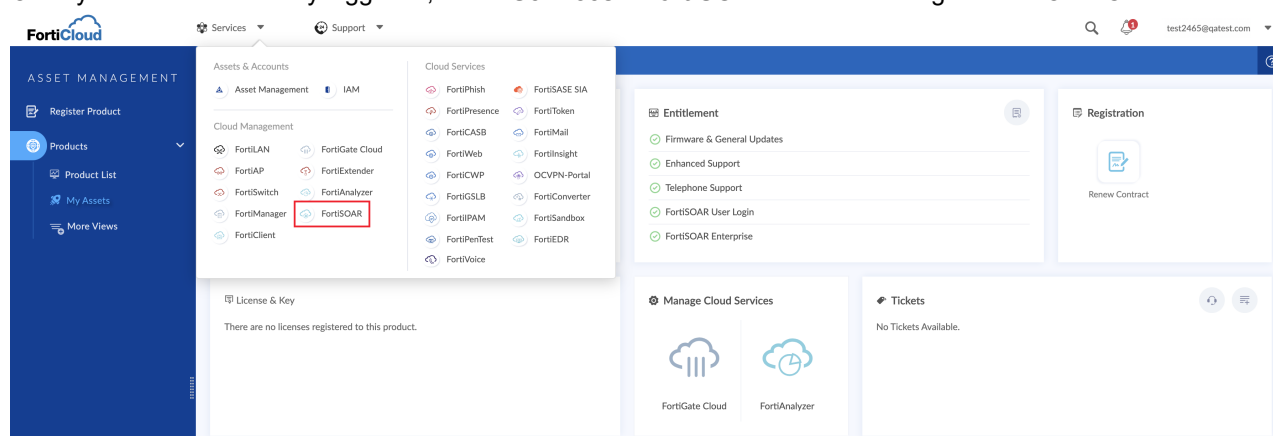
[Learn more about FortiCloud](#) [Privacy](#) [Terms](#)

10. Enter the CSV credentials that you had downloaded in step 7 and click **Login**.



The image shows the FortiCloud login interface. At the top is the FortiCloud logo. Below it are three input fields: 'Account ID / Alias:' with a placeholder 'Account', 'Username:' with a placeholder 'Username', and 'Password:' with a placeholder '*****'. A large blue 'LOGIN' button is centered below the fields. At the bottom, there are links for 'Sign in using email', 'Forgot password?', 'Learn more about FortiCloud', 'Privacy', and 'Terms'.

11. Once you have successfully logged in, select **Services > FortiSOAR** to start working in FortiSOAR Cloud.



Adding a secondary account using FortiCare

1. Login to FortiCare.
2. Click **Manage User**.
3. Click the new user icon to add a new user.

Customer Service & Support Home Asset Assistance Download Feedback 363363 Fortinet

Account

Account Profile
Change Account ID (Email)
Manage User

Manage User

Current Users

Add new user

Name	Email (Account ID)	Description	Action
t	@fortinet.com		
m	@fortinet.com		

4. 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

5. Log in to the personal FortiCare portal. In the FortiSOAR Cloud section, you will see an account listed as a secondary member.
6. 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' user in FortiCare and are assigned the *SOC Analyst* role on FortiSOAR, if they are added as 'Limit Access' user in FortiCare.

After the user has logged in to the account, the primary user or a super user can modify the account.

1. Log in to FortiCare.
2. Click **System Settings > Administrators**.
3. Edit the 'administrator', and assign a different profile.

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. Go to FortiSOAR Cloud and perform SSH to the FortiSOAR instance. 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 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 backup and restore.



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 of 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 restore, 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 of incremental backups. Backups are performed for a particular version of FortiSOAR Cloud, and backups should be restored on the exact versions 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



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

Prerequisites to running the backup process

You must have the NFS or local backup storage path.

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 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 only your configuration files, 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 am 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 on when the backup is 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.



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.