Deployment and Admin Guide

FortiSIEM Cloud 25.4.0

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

10/27/2025
FortiSIEM Cloud 25.4.0 Deployment and Admin Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
08/30/2022	FortiSIEM Cloud 22.3 Document Release.
12/14/2022	FortiSIEM Cloud 22.4 Document Release.
02/15/2023	FortiSIEM Cloud 23.1 Document Release.
04/05/2023	FortiSIEM Cloud 23.1.b changes added to document.
04/20/2023	Differences between FortiSIEM Cloud and FortiSIEM table updated.
06/26/2023	Differences between FortiSIEM Cloud and FortiSIEM table updated.
06/28/2023	Updated Registering FortiSIEM Cloud section.
09/08/2023	FortiSIEM Cloud 23.3 Document Release.
09/13/2023	Added Analytics Queries section.
10/16/2023	Updated License Types section. Second Steps section renamed to Next Steps. Archive Storage Setup expanded with FortiSIEM Cloud Event Retention section. Troubleshooting is now its own separate section.
11/21/2023	FortiSIEM Cloud 23.4 Document Release.
12/15/2023	FortiSIEM Cloud 23.4.a Document Release.
01/11/2024	Updated Differences between FortiSIEM Cloud and FortiSIEM table.
05/20/2024	Added External Storage.
07/30/2024	FortiSIEM Cloud 24.3.0 Document Release.
08/13/2024	FortiSIEM Cloud 24.3.a Document Release.
08/22/2024	Added Analytic Query Concurrency section.
08/29/2024	FortiSIEM Cloud 24.3.b Document Release.
10/29/2024	FortiSIEM Cloud 24.4.0 Document Release.
11/19/2024	FortiSIEM Cloud 24.4.a Document Release.
12/19/2024	FortiSIEM Cloud 24.4.b Document Release.
02/27/2025	FortiSIEM Cloud 25.1.0 Document Release.
03/31/2025	FortiSIEM Cloud 25.1.a Document Release.
04/24/2025	FortiSIEM Cloud 25.2.0 Document Release. Supported Regions section added.
05/09/2025	FortiSIEM Cloud 25.2.a Document Release. Region B SKU section added.

Date	Change Description
05/14/2025	FortiSIEM Cloud 25.2.a Document Release - Minor restructuring to improve ease of use.
06/25/2025	FortiSIEM Cloud 25.2.b Document Release.
07/01/2025	FortiSIEM Cloud 25.3.0 Document Release.
07/22/2025	Minor restructuring to improve ease of use.
10/27/2025	FortiSIEM Cloud 25.4.0 Document Release.

Getting Started

- A license is required before initializing FortiSIEM Cloud. See Licensing for detailed information.
- After licensing is completed, follow the steps in Provisioning and Deploying FortiSIEM Cloud.
- Information on next steps is provided here.

Beginning with FortiSIEM Cloud

The following introductory topic is available:

- Logging into FortiSIEM Cloud for the First Time

Logging into FortiSIEM Cloud for the First Time

From the FortiCloud portal, you can access the FortiSIEM web UI once an instance is at STATUS "Complete". To do this, select the serial number, which will open a new tab. When initially logging in, use `admin` for the USER ID. For the password, enter the administration password you provisioned your FortiSIEM Cloud instance with.

For information on FortiSIEM features and how to use and configure them, see the FortiSIEM Documentation Library.

Licensing

Requirements

The following items are required before you can initialize FortiSIEM Cloud.

- FortiCloud account: Create a FortiCloud account here if you do not have one. A primary FortiCloud account is required to launch FortiSIEM Cloud.
- Internet access: You must have Internet access to create a FortiSIEM Cloud instance.
- Browser: A device with a browser to access FortiSIEM Cloud.

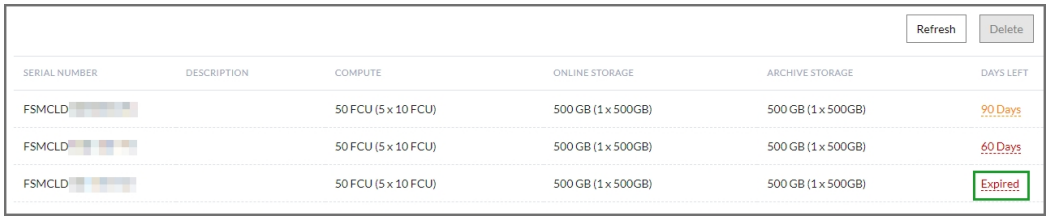
FortiSIEM Cloud is supported on FortiSIEM v6.6.0 and later.

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

FortiSIEM Cloud requires the following licenses:

- FortiSIEM Cloud Entitlement license. You can purchase FortiSIEM Cloud licenses from Fortinet. See License Types for more information.

If the FortiSIEM Cloud entitlement expires, the cloud portal will display a notice to the customer.



On contract expiry, FortiSIEM Cloud instances are automatically shut down, no grace period is provided. Customers will not be able to use the FortiSIEM Cloud instances after contract expiry. All data that the FortiSIEM Cloud has generated, such as event logs and incidents, will be automatically removed from the platform within 14 days of contract expiry.

License Types

FortiSIEM Cloud offers the following SKUs.

Description	SKU
FC-10-SMCLD-543-02-*DD*	FortiCloud entitlement (instance) with allocated FortiSIEM Compute Units (FCU). Annual Subscription. Includes FortiCloud Premium Support.
FC-10-SMCLD-541-02-*DD*	500GB additional online storage. Annual Subscription. Minimum quantity of 1 is required for FortiSIEM Cloud service.
FC-10-SMCLD-542-02-*DD*	500GB Archive storage space. Annual Subscription.

FortiSIEM Cloud licensed using FC-10-SMCLD-543-02-DD, FC-10-SMCLD-541-02-DD, FC-10-SMCLD-542-02-DD does not require additional device, agent, UEBA or FortiGuard IoC licenses to use these capabilities.

FortiSIEM Cloud License Contract Registration

- You must have an account in FortiCare.
- Contact FortiSIEM Support to obtain the FortiSIEM Cloud product SKU.
- Once you complete purchasing of the FortiSIEM Cloud product SKU(s), you will be sent service contract registration codes to your registered email address.

You can register your FortiSIEM Cloud entitlement, or upgrade/renew an existing FortiSIEM Cloud.

- Registering Base FortiSIEM Cloud
- License Upgrade/Renewal

Registering FortiSIEM Cloud

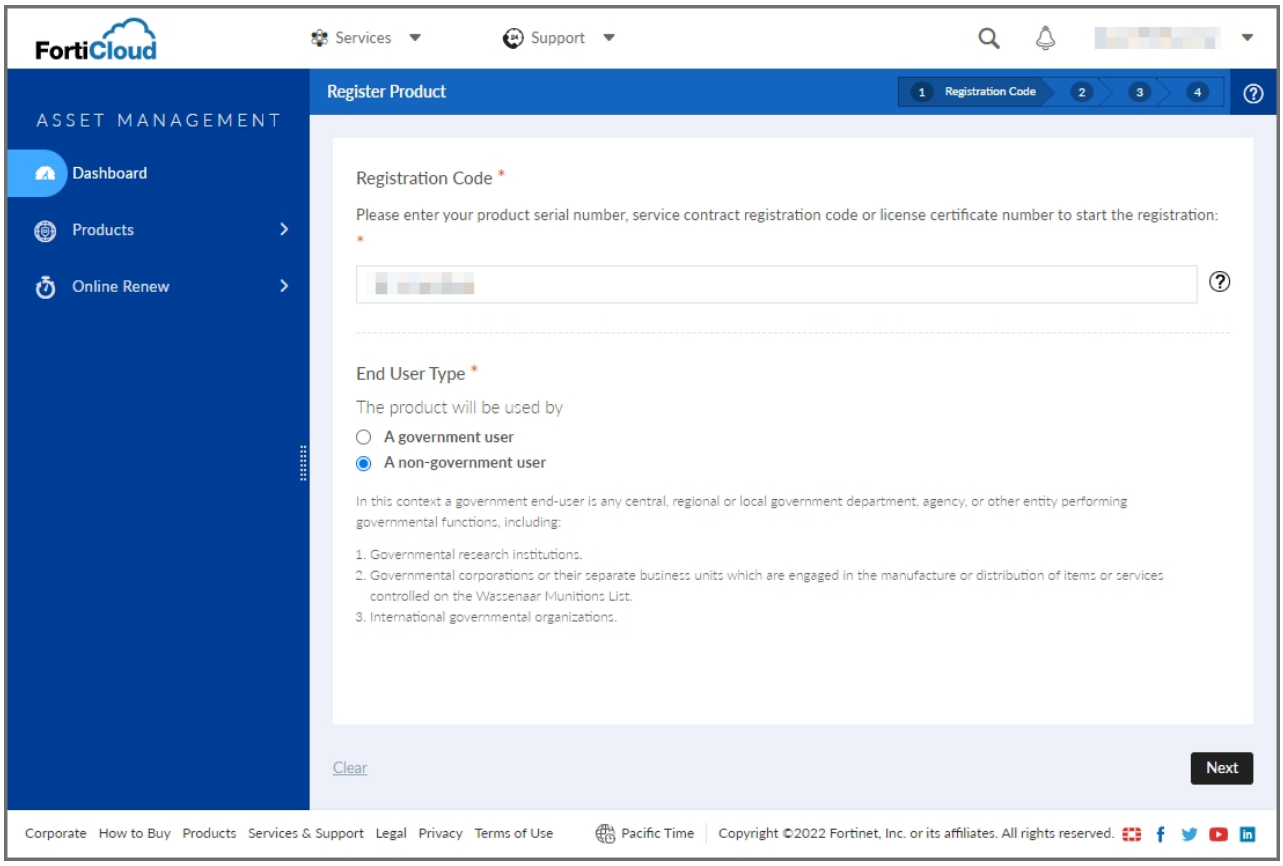
To register a new FortiSIEM Cloud entitlement (FC-10-SMCLD-543-02-*DD*) and FortiSIEM Cloud Online Storage entitlement (FC-10-SMCLD-541-02-*DD*), see Registering assets in the FortiCloud Account Services Guide. For licensing information, see Licensing Types.

License Upgrade/Renewal

To upgrade or renew an existing FortiSIEM Cloud entitlement, from the FortiCare site, take the following steps.

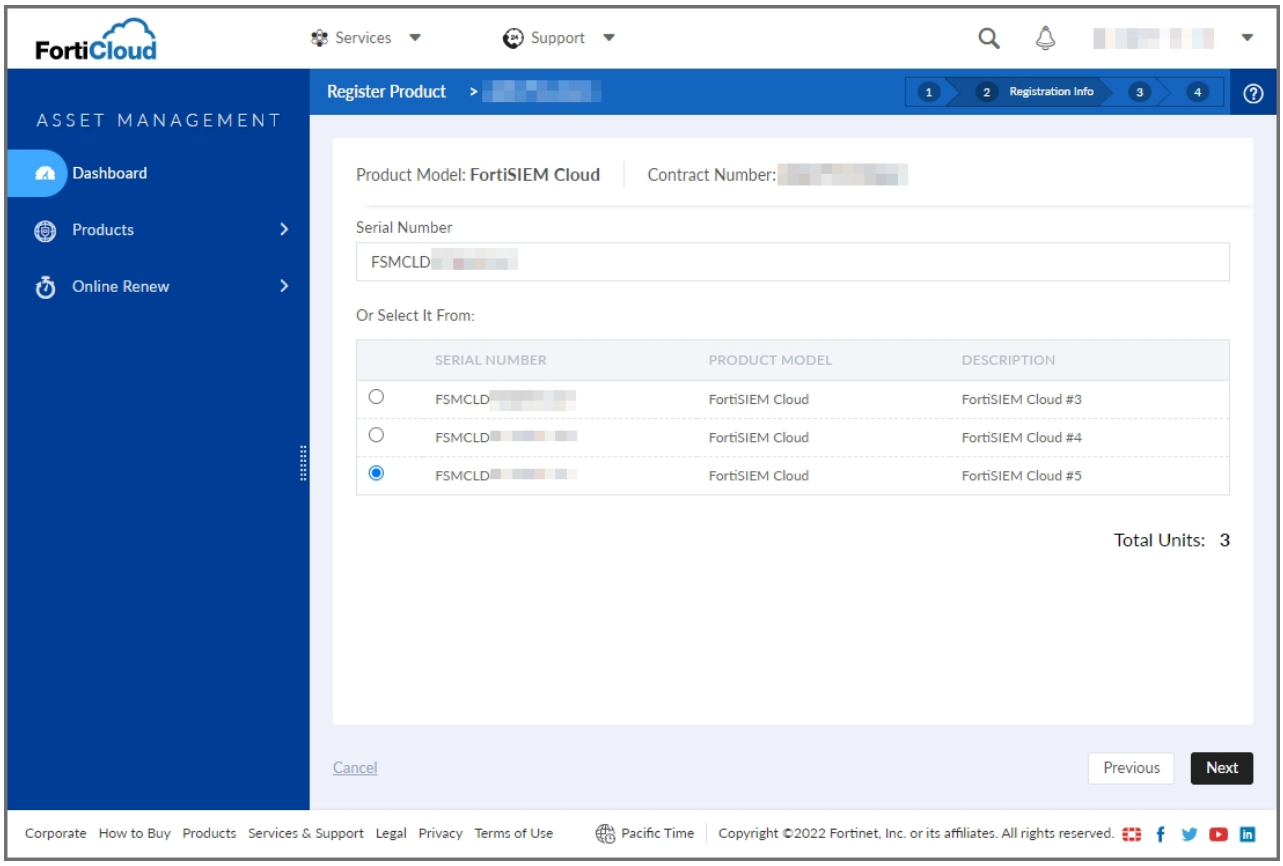
1. Click the **Register Now** or **Register More** button.

2. On the **Register Product > (1) Register Code** page, in the **Registration Code** field, enter the **Registration Code** of the FortiSIEM Cloud SKU.



3. Select the **End User Type** and click **Next**.

4. From the list of registered products, select the product (or enter its serial number in the Serial Number field), and click **Next**.



5. On the **Verification** page, read and agree to the terms, and click **Confirm**.
6. Verify the information displayed under **Product Info**.
7. Click **Done**.

Provisioning and Deploying FortiSIEM Cloud

Supported Regions

Region A SKU

FortiSIEM Cloud is available in the following regions with Region A SKU purchase:

North America	Europe	Middle East	Asia Pacific
Canada Central	Ireland	United Arab Emirates	India - Mumbai
USA West - Oregon	UK - London		Singapore
USA East - Ohio	France - Paris		Australia - Sydney
USA East - Northern Virginia	Sweden - Stockholm		
	Germany - Frankfurt		
	Italy - Milan		

Region B SKU

FortiSIEM Cloud is available in the following regions with Region B SKU purchase:

South America	Europe	Middle East	Asia Pacific	Africa
Brazil	Switzerland	Bahrain	Hong Kong	South Africa

How to Provision

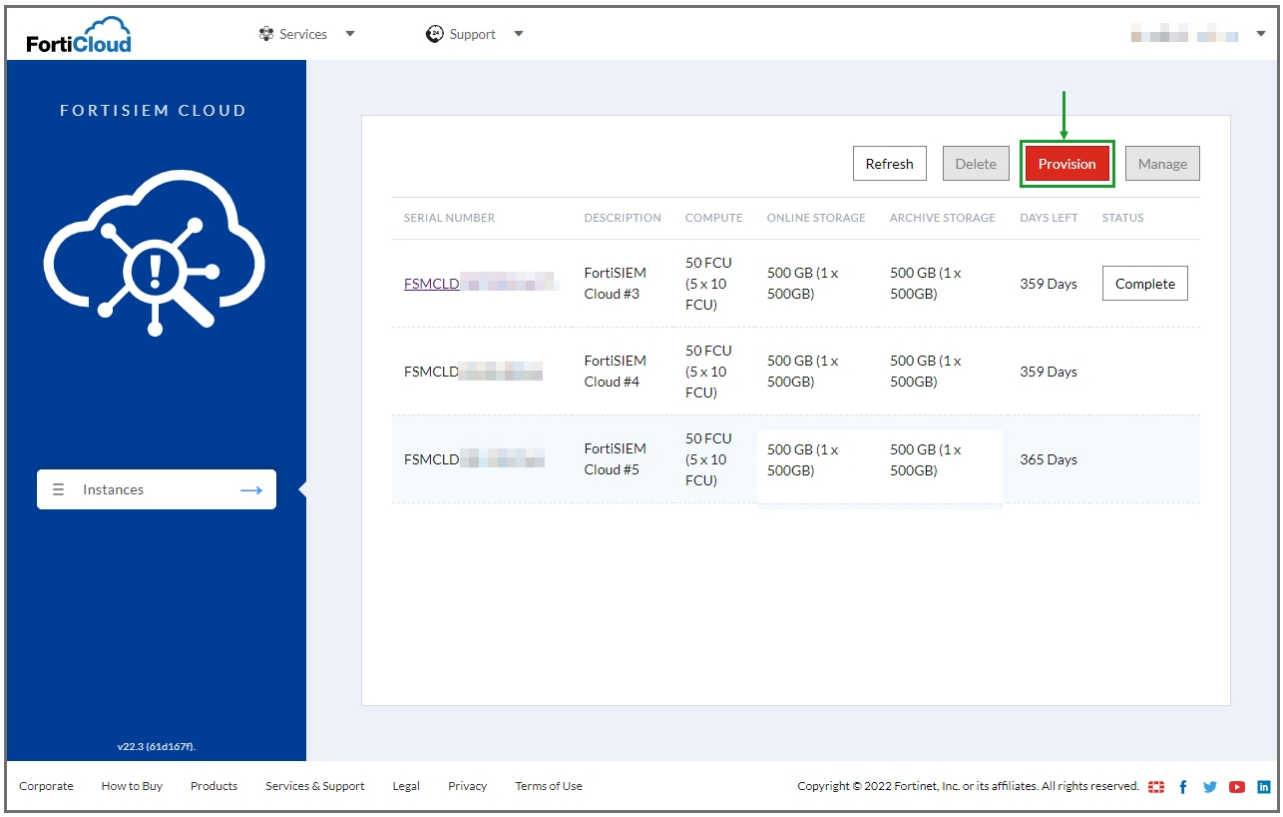
This section explains how to provision and deploy FortiSIEM Cloud.

To provision and deploy FortiSIEM Cloud, take the following steps.

1. In the FortiCloud portal, ensure that you have a product entitlement for FortiSIEM Cloud.

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

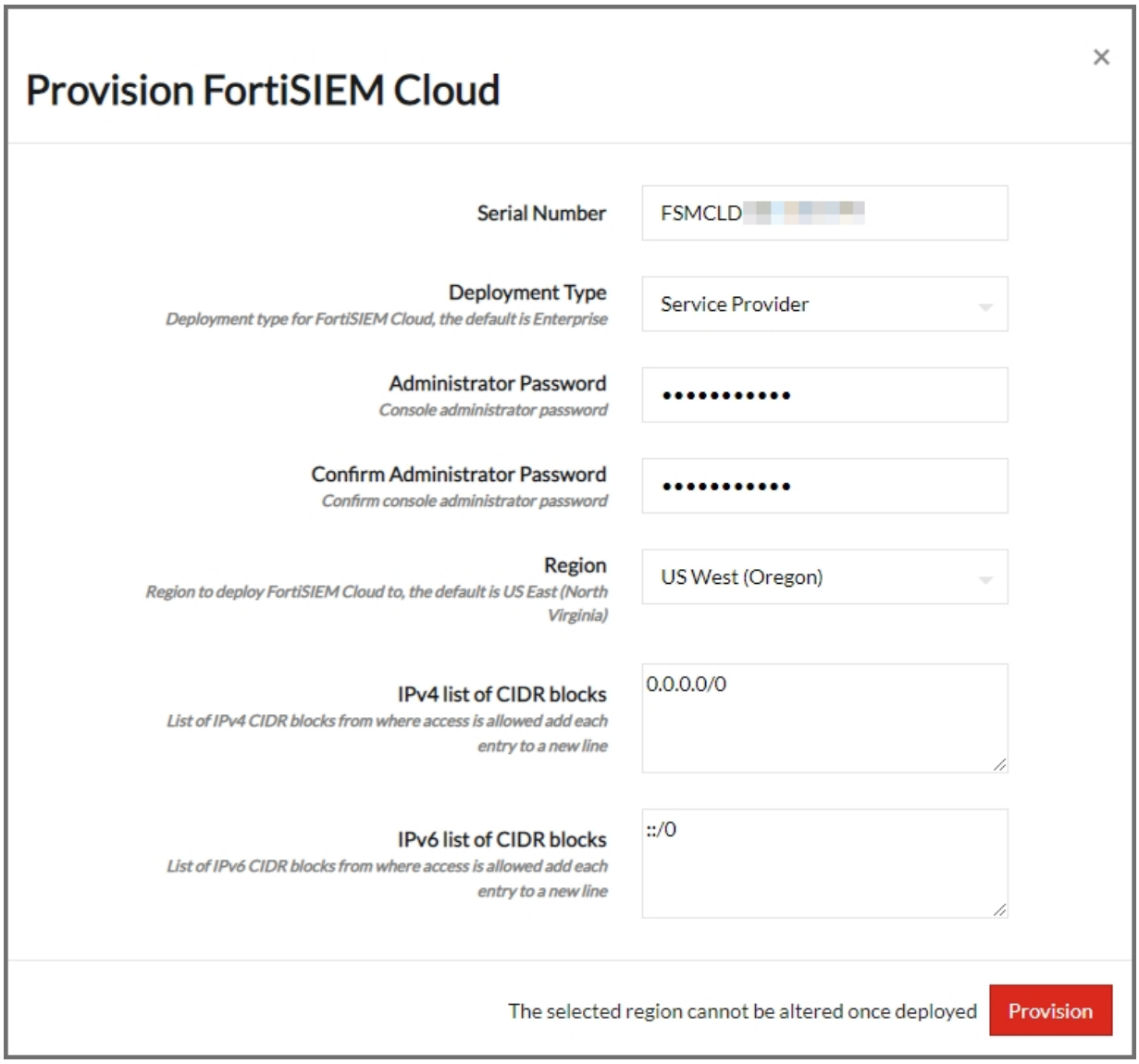
2. On FortiCare portal, click on the **Services** drop-down icon, and click **FortiSIEM Cloud** to access the FortiSIEM Cloud portal.
3. Select the FortiSIEM Cloud instance and click **Provision**.



From the **Provision FortiSIEM Cloud** window, take the following steps.

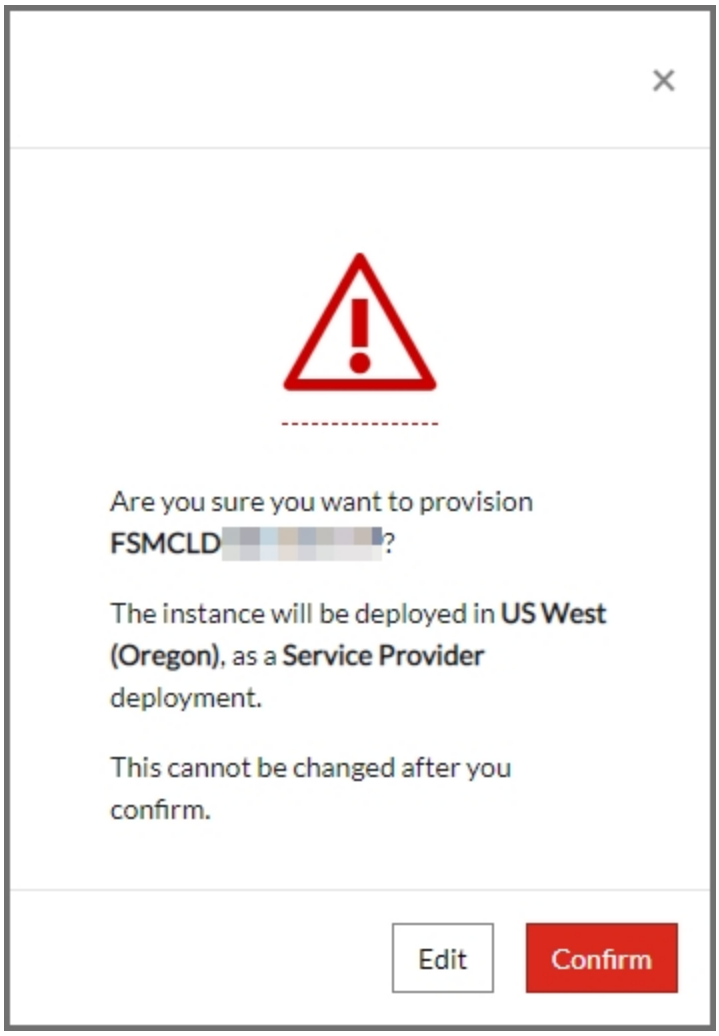
a. Select the **Deployment Type** drop-down list, and select your deployment type, either **Enterprise** or **Service Provider**.
b. Select **Administrator Password**, and enter the Administrator Password you plan to use.
c. Select **Confirm Administrator Password**, and re-enter the Administrator Password you plan to use.
d. Select the **Region** drop-down list, and select the region closest to the personnel who will be using the product for optimal performance.

   Note: Region cannot be changed after initial Provision.
e. In the **IPv4 list of CIDR blocks** and/or **IPv6 list of CIDR blocks**, select and input any addition IPv4 or IPv6 addresses for access in the respective section. This setting locks down your FortiSIEM Cloud instance to the specified CIDR blocks.

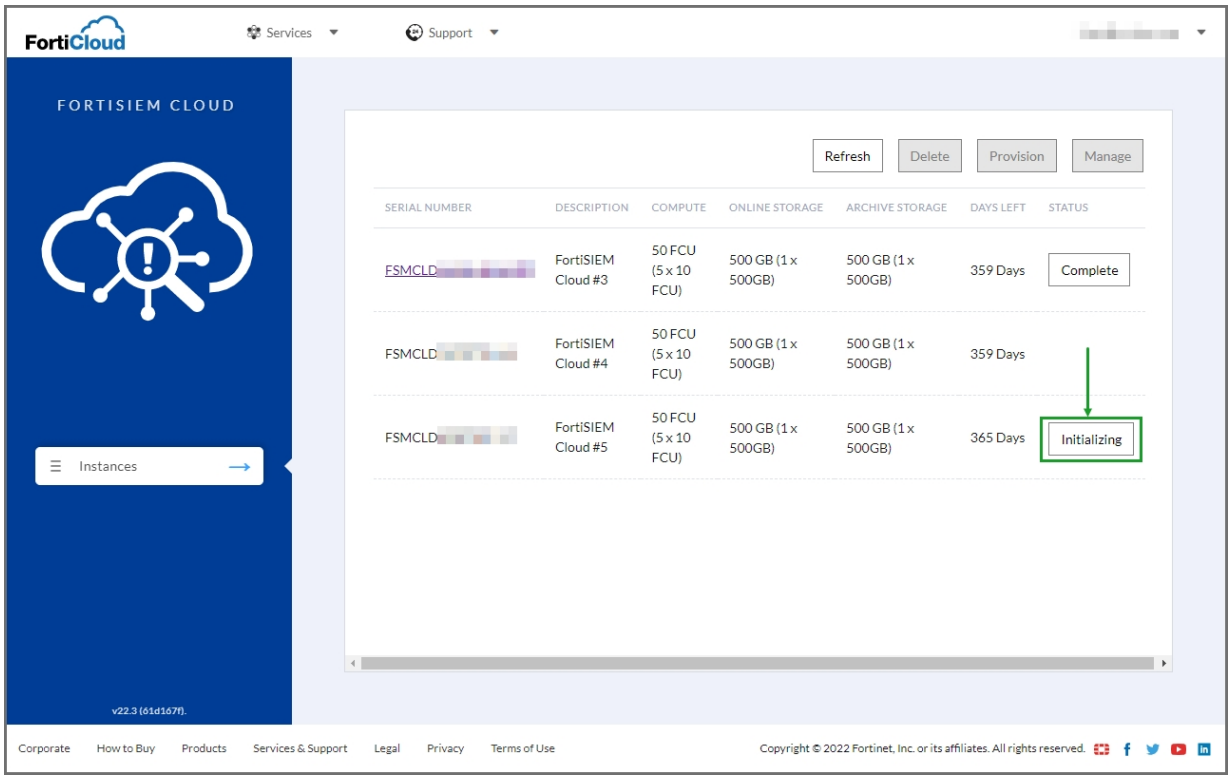


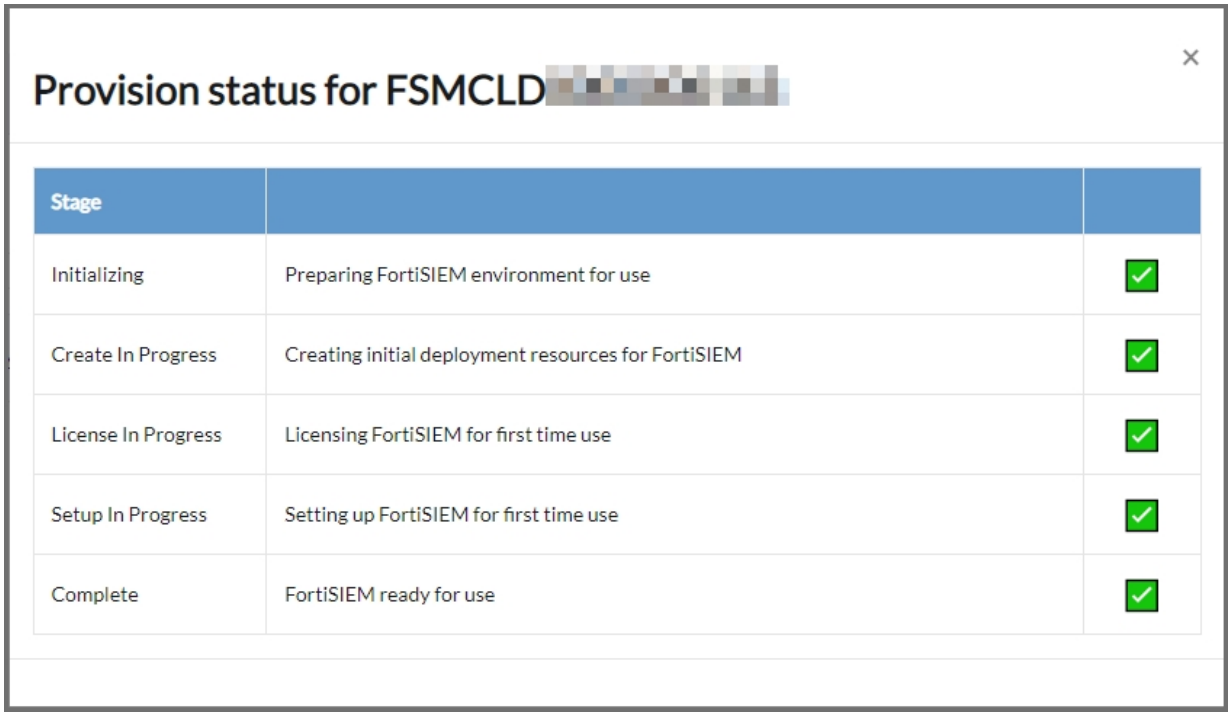
f. Click **Provision**.

g. Click **Confirm** when shown the summary of your instance, and provision.



The status can be seen under the **STATUS** column or by clicking the **Refresh** button. When provisioning is done, the STATUS will be shown as **Complete**. To get real time updates, click on the **STATUS** button and it will provide you with live information.





4. Once provisioned, select the instance to access the FortiSIEM web GUI to begin using FortiSIEM Cloud. For more information, see Beginning with FortiSIEM Cloud.

Next Steps

Integrations

FortiSIEM Cloud does not allow any insecure communication inbound. Only HTTPS TCP/443 is available inbound.

It is recommended that integrating and monitoring of devices or applications by FortiSIEM is performed by a FortiSIEM Collector. FortiSIEM Cloud can directly monitor device API integrations such as Office 365 and AWS CloudTrail, however this is not recommended as it can increase the load on the FortiSIEM Cloud and require the purchase of additional FortiSIEM Compute Units to compensate for this overhead.

Collector Deployment from FortiSIEM Cloud

When configuring your collectors for deployment from FortiSIEM Cloud, you will need to provide the FortiSIEM Cloud FQDN, for example `fsmcld0000000000111.fortisiem.cloud`, as the FortiSIEM Supervisor IP address. To get the FortiSIEM FQDN, take the following steps:

1. Navigate to the FortiCloud portal.
2. Click on your FortiCloud instance.
3. Click **Manage**.
4. Copy the FQDN.

For more information on Collector deployment, see the **Register Collectors** section from the appropriate hardware configuration guide or VM installation guide from the FortiSIEM Document Library.

Agent Deployment from FortiSIEM Cloud

When configuring your agents for deployment from FortiSIEM Cloud, you will need additional information from the FortiCloud Portal. Take the following steps:

1. Navigate to the FortiCloud portal.
2. Click on your FortiCloud instance.
3. Click **Manage**.
4. Use the information from this page to complete your agent deployment.

For more information on Agent deployment, see the appropriate agent installation guide (FortiSIEM Windows Agent Installation Guide, FortiSIEM Linux Agent Installation Guide) from the FortiSIEM Document Library.

Archive Storage Setup

If you have purchased any “FC-10-SMCLD-542-02-DD" entitlements with your FortiSIEM Cloud Instance, a separate Archive storage module will be deployed alongside your instance. This provides you with the infrastructure to move data to Archive, using your own defined retention policies.

The FortiSIEM Cloud platform will automatically deploy your Archive storage, the FortiSIEM Cloud instance will then automatically move data from Online to Archive based on your retention policy needs.

To setup your custom retention policies, see the following topics:

- FortiSIEM Cloud Event Retention
  - How FortiSIEM Cloud Event Retention Works
  - Explanation of Retention Policies in Detail
  - Creating FortiSIEM Cloud Event Retention Policy

FortiSIEM Cloud Fundamentals

The following FortiSIEM Cloud fundamental topics are available.

- Differences between FortiSIEM Cloud and FortiSIEM
- Analytics Queries
- Analytic Query Concurrency

Differences between FortiSIEM Cloud and FortiSIEM

Please note the following differences between FortiSIEM Cloud and FortiSIEM.

- FortiSIEM Cloud does not offer a Licensing page from the FortiSIEM GUI. Licensing is handled automatically by the FortiCloud platform.
- FortiSIEM Cloud does not offer a Cloud Health page from the FortiSIEM GUI. The FortiSIEM Cloud Portal provides you with high level utilization information such as how much storage is currently being used, and how much is available.
- FortiSIEM Cloud storage is setup via provisioning, and not available via the FortiSIEM GUI.

The following table provides additional details on differences between FortiSIEM Cloud vs. customer Virtual and Hardware Appliance deployments:

Feature	FortiSIEM Cloud Support
FortiSIEM Manager	FortiSIEM Cloud does not support FortiSIEM Manager integration.
Console and SSH access to FortiSIEM	Not available. For any configuration that requires SSH access, customers should contact customer support.
Event Forwarding from FortiSIEM Super or Workers	Event Forwarding via FortiSIEM Cloud using Syslog forwarding or as a Kafka Producer is not supported. Event Forwarding via Syslog or as a Kafka Producer is supported from FortiSIEM Collectors used in conjuction with FortiSIEM Cloud.
FortiSIEM Cloud Health	Not available.
FortiSIEM License Screen	Not available.
Configure Storage	Not available.
Configure Query and Event Workers	Not available.
Configure "Event Worker" on Collectors	Not available.
Remediate Incidents	Remediation actions are supported where Remediation is performed via Collectors only.
"Connect To" remote device via Collector	Not available. See here for more information on this feature.
API Access	API associated with FortiSIEM management are not supported. For example: "Performance and Health API", “Event/Query Worker Configuration API”, “Rest API to Return Worker Queue State”.
Connectivity to FortiSIEM Cloud	HTTPS/TCP/443 is the only permitted protocol to FortiSIEM Cloud. Customers should deploy Collectors to collect events from devices, which in turn upload to FortiSIEM Cloud.

Feature	FortiSIEM Cloud Support
External Authentication using RADIUS, LDAP (S)	As defined here, external authentication requires access from FortiSIEM directly to the authentication provider. To support RADIUS or LDAP(S) external authentication, this would require access from FortiSIEM Cloud to the RADIUS or LDAP(S) server over the Internet.
Custom Java or Python based Malware Feed Integration. See here for more details.	Adding a custom Java module or custom Python script for Malware Feed Integration is not supported on FortiSIEM Cloud.
Admin > Settings > Database	FortiSIEM Cloud differences: • **Online Data** and **Archive Data** are not available on FortiSIEM Cloud. Total Online and Archive storage usage can be monitored in the FortiSIEM Cloud portal. See Managing Your FortiSIEM Cloud Instance -Overview. • **Online Retention Policy** has been renamed to **Retention Policy**. On FortiSIEM Cloud, the retention policy spans the data independent of the Online Storage or Archive Storage location. • **ClickHouse Config** is not available. This is managed by FortiSIEM Cloud and is not applicable.
Analytics behavior for searches involving event source	Selecting the event source (**Online** or **Archive**) is not applicable in FortiSIEM Cloud. In FortiSIEM Cloud, queries are performed across Online and Archive storage automatically. There is no need to define if the query should be performed on Archived data separately. See Analytics Queries for more details.

Analytics Queries

FortiSIEM Cloud analytics unifies the search across the Online event data and the Archive event data. There is no need to restore data from Archive to Online to perform an analytic search; however, queries of data that is stored in the Archive will be significantly slower than Online data.

Analytic Query Concurrency

An Analytics query to the Event Database runs under the following conditions:

- User executes a Search from **Analytics > Search** and **Analytics > Machine Learning > Train**.
- User executed Search performed when user visits a Widget Dashboard
- Scheduled report runs
- Scheduled rule runs
- Machine learning inference job executes
- User looks up Triggered events for an Incident in **Incidents > List View**

More FortiSIEM Compute Units (FCU) enables more Analytics queries to run in parallel. If the concurrent query limit is hit, then submitted queries wait for one or more currently running queries to finish.

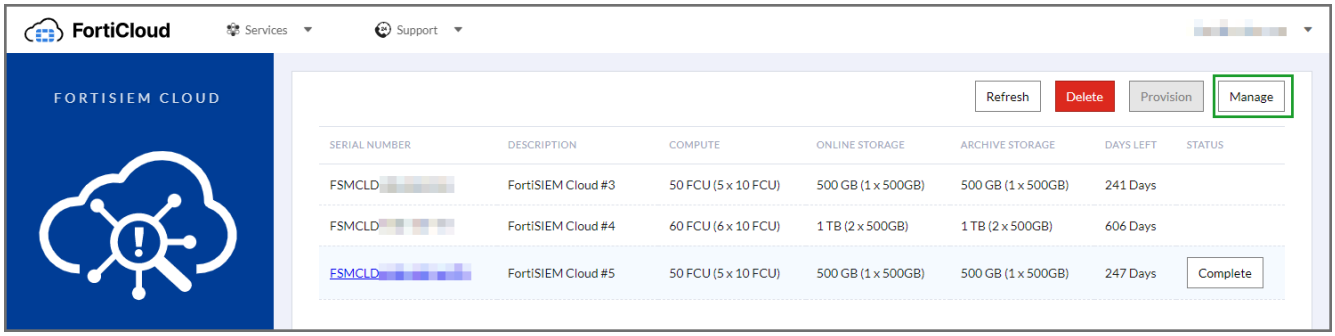
The following table shows the concurrent queries for several FCU combinations.

FortiSIEM Compute Units (FCU)	Concurrent Queries
10	2
20 - 30	4
40 - 100	8
110 - 200	16
210 - 290	32
300 - 600	64

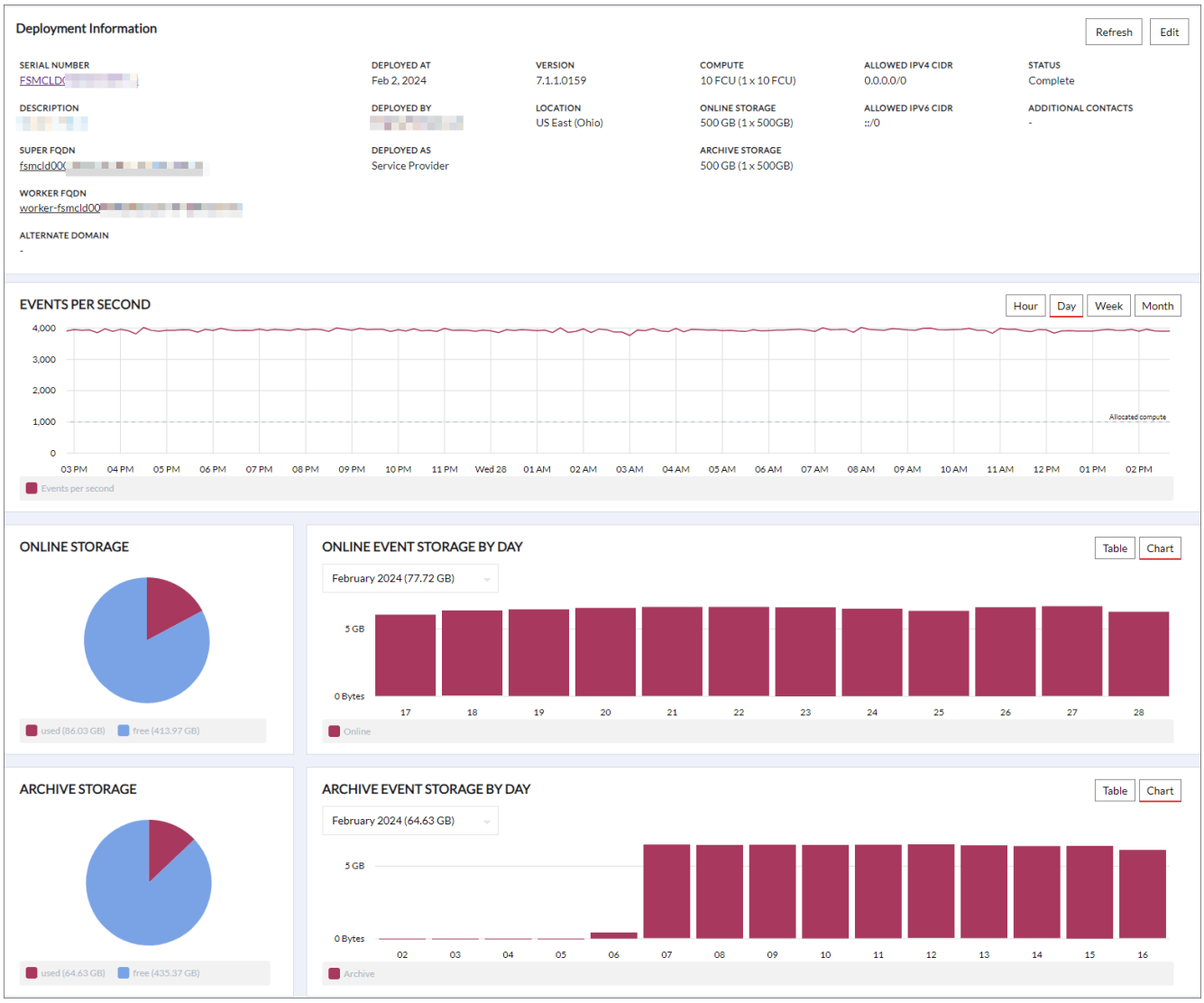
Managing Your FortiSIEM Cloud Instance

Overview

To manage your FortiSIEM Cloud Instance settings, such as whitelisting Network Classless Inter-Domain Routing (CIDR), managing notification settings, and adding alternate domains, select your instance from the Instances Table, and select **Manage** to go to the Manage page.



After clicking **Manage**, the Manage page will appear. Also from here, you can view Events per Second rate for your FortiSIEM Cloud instance, either by last Hour, Day, Week or Month.



Viewing Online and Archive Storage Usage

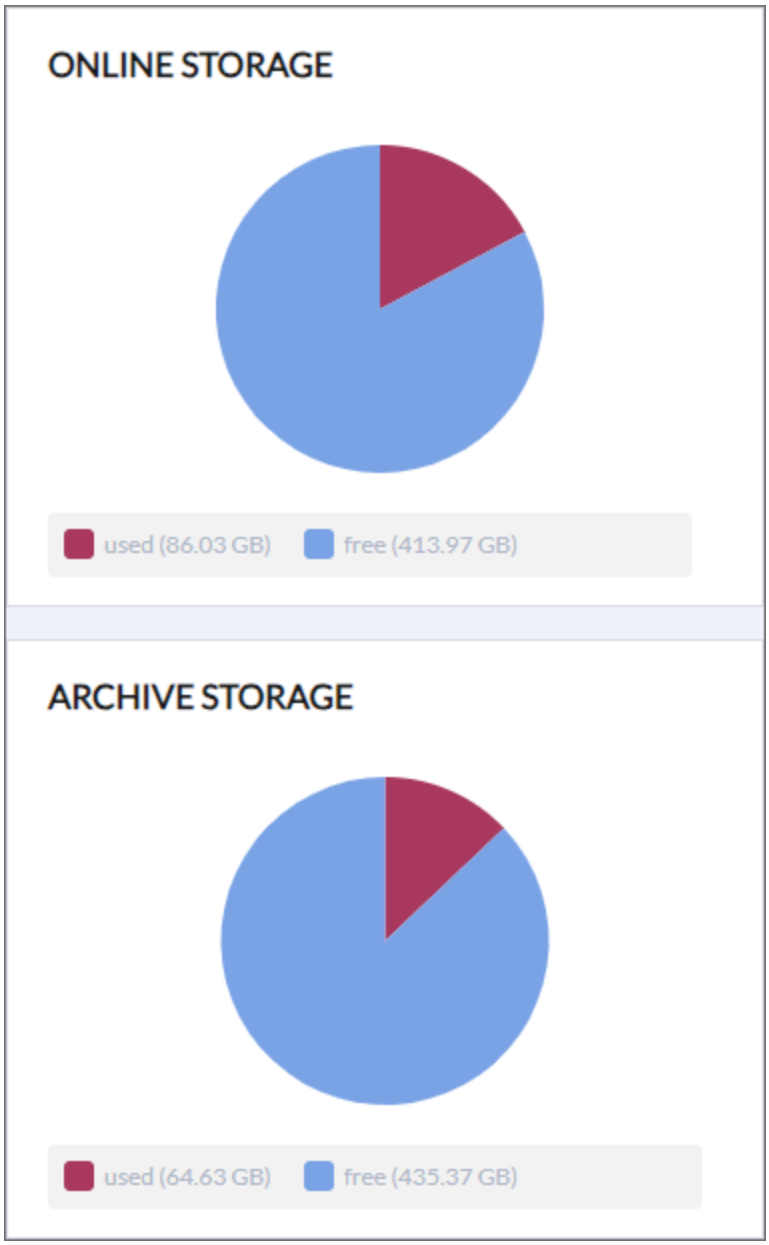
FortiSIEM Cloud instances will track your Online and Archive storage usage in two ways:

1. Total usage, which includes both events and any system data, such as daily summary statistics.
2. By stored events per day.

The total Online and Archive Storage charts are displayed using the **free** and **used** space statistics. Also, provided is EVENT STORAGE BY DAY, either as a chart or a table.

Total Usage for ONLINE STORAGE and ARCHIVE STORAGE

An example of total usage for Online Storage and Archive Storage is shown here:



Used: Relates to the total amount of disk usage used. It can include events and any summary data.

Free: Relates to the amount of storage purchased, minus the USED calculation.

These statistics are updated on an hourly basis within the FortiSIEM Cloud platform.

Storage Usage by Day for Online or Archive Storage

An example of daily usage event storage (Online Event Storage by Day and Archive Event Storage by Day) is shown here:

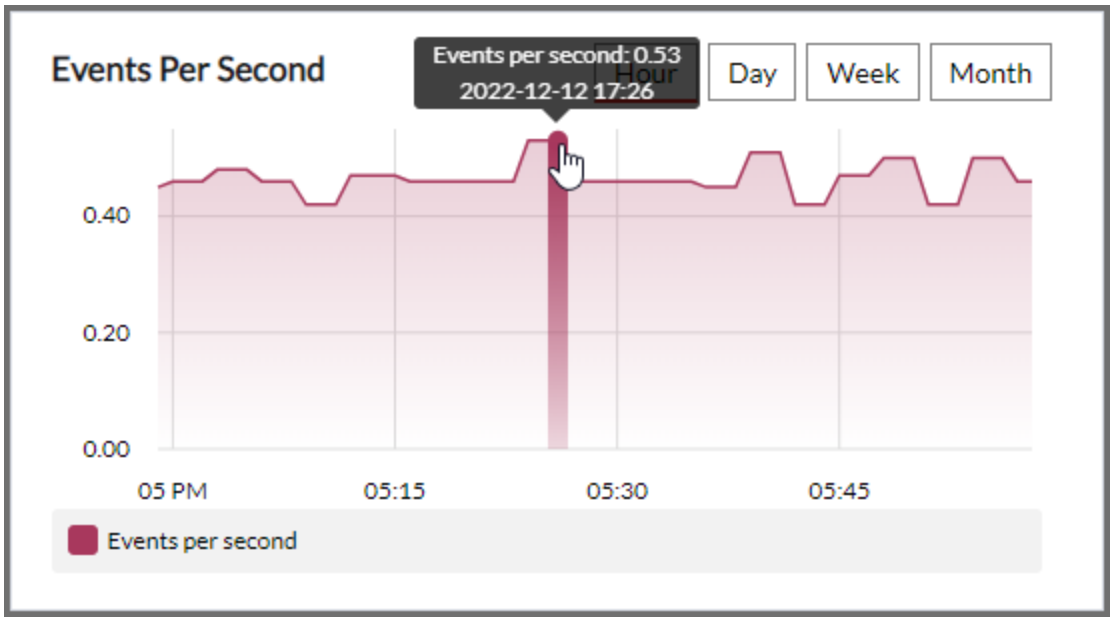
Internally, all event data is stored in daily (UTC) data portions. Here, the data shown relates to these buckets and the total storage they currently take on disk. Note that only event data is summarized in this view, as it will take the majority of space available in Online or Archive storage.

In Chart mode, each bar represents the total amount of storage taken by that particular bucket.

Note: Data across the FortiSIEM Cloud platform can occasionally show storage being used by both Online and Archive for a short period on the same day; this typically occurs when data is moved from Online storage to Archive storage. Data must first move to Archive storage before being removed from Online storage. This data is refreshed hourly.

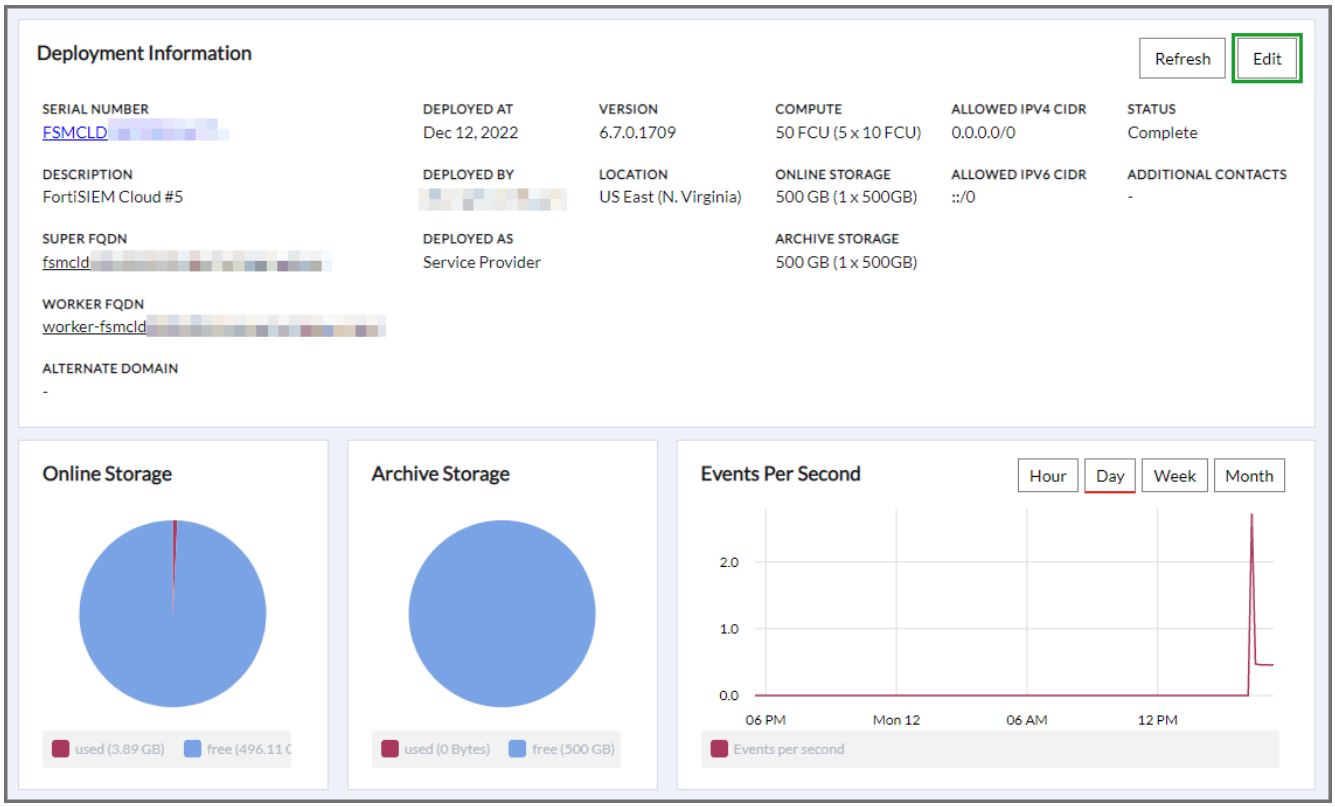
Viewing Events per Second Rate

FortiSIEM Cloud instances will monitor your Events per Second rate after provisioning. You can view this rate by either last Hour, Day, Week or Month. Simply navigate to the Manage page, and on the **Events per Second** widget, select the required time interval. Hovering over any points will show their underlying value for that time span.



If you wish to update your settings, click **Edit**. The following settings can be updated.

- **Network** - Updating Network CIDR
- **Notifications** - Updating Notification Settings with Additional Contacts
- **Alternate Domain** - Updating Alternate Domain Settings



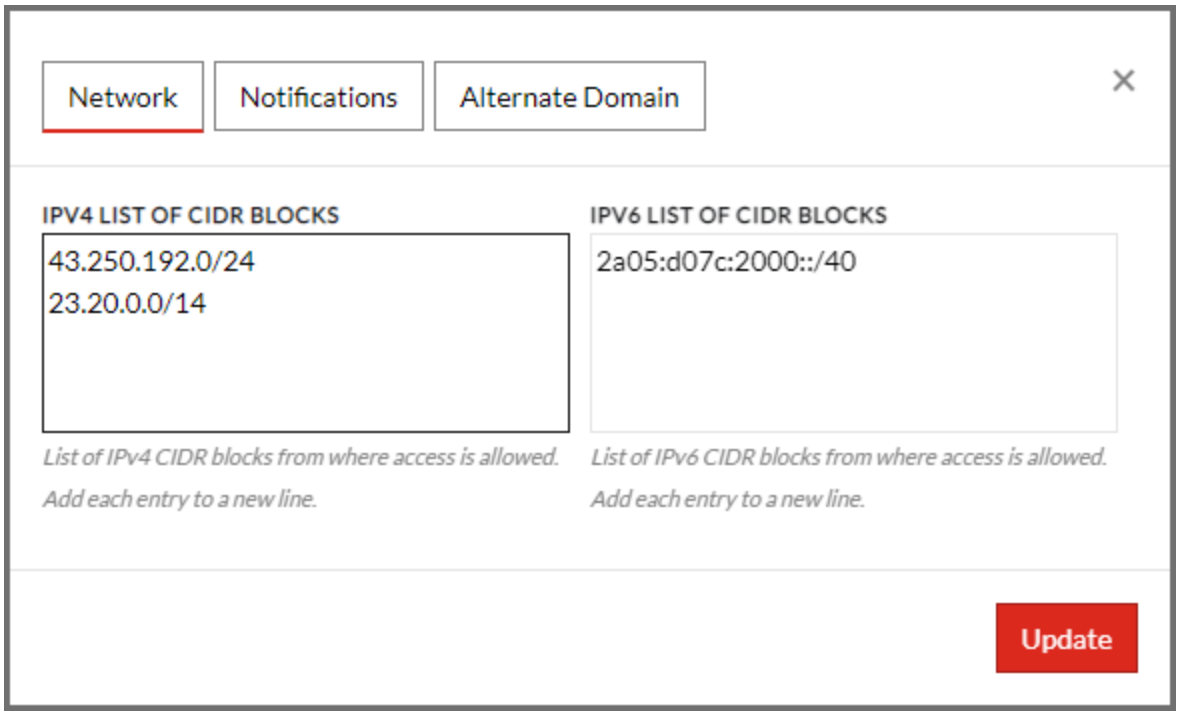
Updating Network CIDR

Each FortiSIEM Cloud deployment is segmented from others, and you can provide individual network Classless Inter-Domain Routing (CIDR) that can be whitelisted to allow access to the Console, and Ingestion routes. You can provide both IPV4 and IPV6 CIDR blocks.

To edit Network CIDR, take the following steps.

1. From the **Manage** page, click **Edit**.
2. Click **Network**.
3. Select the field below **IPV4 LIST OF CIDR BLOCKS** or **IPV6 LIST OF CIDR BLOCKS**, depending on whether you wish to modify IPV4 or IPV6 respectively, and enter a new CIDR block on a new line, or edit an existing one.
4. When done, click **Update** to apply the new network settings.

   An example of editing **IPV4 LIST OF CIDR BLOCKS** is provided below.



Note: This update can take some time to propagate fully.

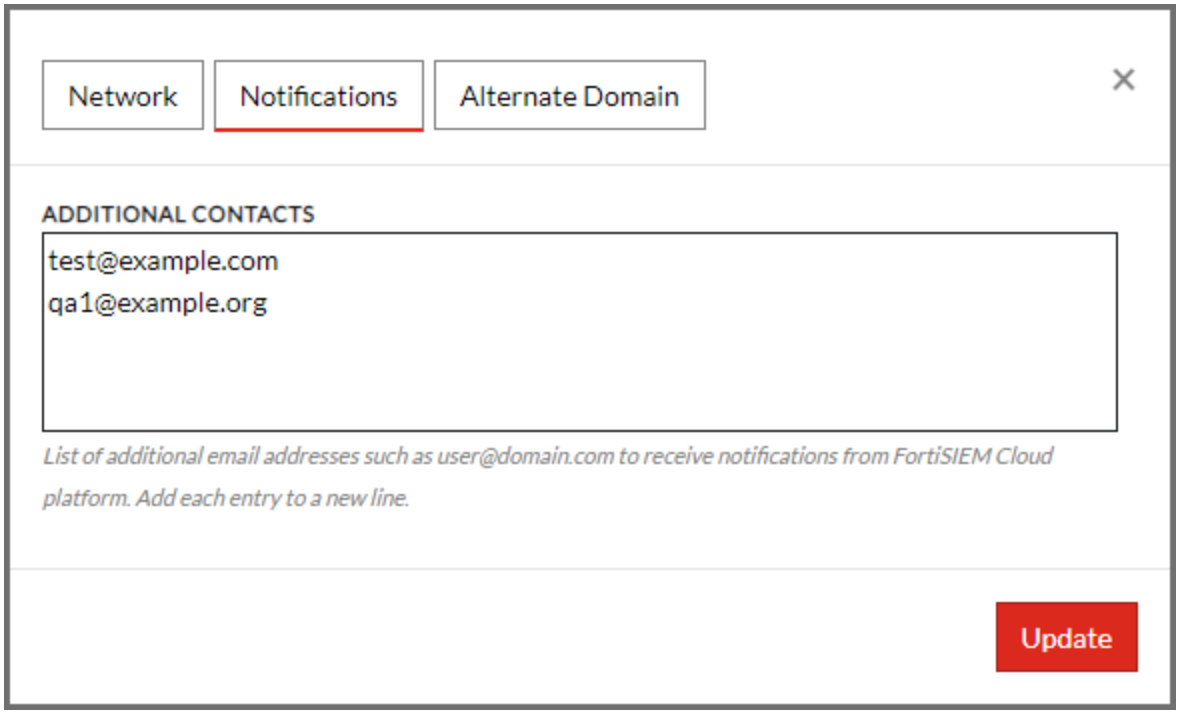
Updating Notification Settings with Additional Contacts

Notification settings allow you to specify email addresses for others to receive notifications for your FortiSIEM Cloud instance. These will include early warnings for any FortiSIEM Cloud instances that are near expiration.

To edit Additional Contacts, take the following steps.

1. From the **Manage** page, click **Edit**.
2. Click **Notifications**.
3. Select the field below **Additional Contacts**.
4. Enter each email address on a new line.
5. When done, click **Update**.

   An example of editing **ADDITIONAL CONTACTS** is provided below.



Note: This update can take some time to propagate fully.

Updating Alternate Domain Settings

FortiSIEM Cloud instances, by default, come with a secure TLS certificate which provides HTTPS access to your console and event ingestion. These fall under the fortisiem.cloud domain. However, you can optionally provide a secondary domain to use with your FortiSIEM Cloud instance.

To update this setting, you must:

1. Have control of the domain in order to create a CNAME record, which will point to the FortiSIEM Cloud default route.
2. Have a TLS certificate, extracting the public, private keys and any certificate authority chains, and provide these to the FortiSIEM Cloud portal to attach to your deployment.

To update the alternate domain for your FortiSIEM Cloud instance, you must provide the private key, the certificate and optionally, any certificate authority chain. The certificate must specify one of the following cryptographic algorithm and key sizes:

- RSA 1024 bit
- RSA 2048 bit
- RSA 3072 bit
- RSA 4096 bit
- ECDSA 256 bit
- ECDSA 384 bit (API name: EC_prime256v1)
- ECDSA 521 bit (API name: EC_secp384r1)

Also note the following:

- The certificate provided must be an SSL/TLS X.509 version 3 certificate. It must contain a public key, the fully qualified domain name (FQDN) for your alternate domain, and information about the issuer.
- The certificate can be self-signed by a private key that you own, or by the private key of an issuing certificate authority (CA).
  - If the certificate is self-signed, you must provide the private key. The private key must be no larger than 5 KB (5,120 bytes), and it must be unencrypted.
  - If the certificate is signed by a CA, you must provide the private key, and certificate chain, and the cryptographic algorithm of the certificate must match the algorithm of the CA. For example, if the CA key type is RSA, then the certificate key type must also be RSA.
- The certificate must be valid at the time of upload. You cannot upload a certificate before its validity period begins or after it expires. The **NotBefore** certificate field contains the validity start date, and the **NotAfter** field contains the end date.

Example commands to extract a certificate, private key and CA chain from P12 is provided in the following table.

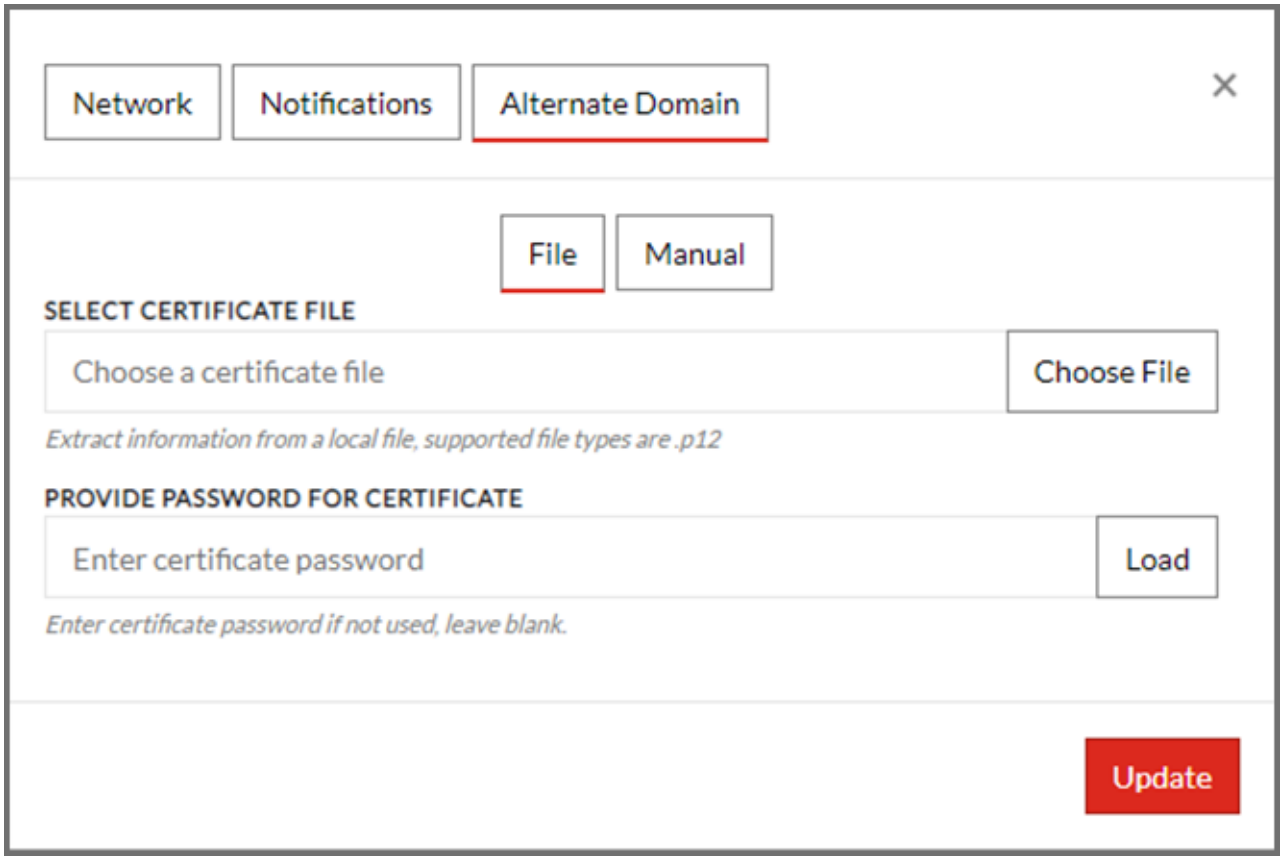
Extraction	Command
Private Key	`openssl pkcs12 -in "<FILE_PATH>" -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > 1_clientcert.key`
Certificate	`openssl pkcs12 -in "<FILE_PATH>" -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > 2_clientcert.cer`
CA Chain	`openssl pkcs12 -in "<FILE_PATH>" -cacerts -nokeys -chain | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > 3_cacerts.cer`

Once uploaded, the certificate is securely stored in the FortiSIEM Cloud platform.

To edit the Alternate Domain settings, take the following steps.

1. From the **Manage** page, click **Edit**.
2. Click **Alternate Domain**.
3. From here, you can select **File** if you have a file in PKCS#12 format, or select **Manual** to provide the information

manually.



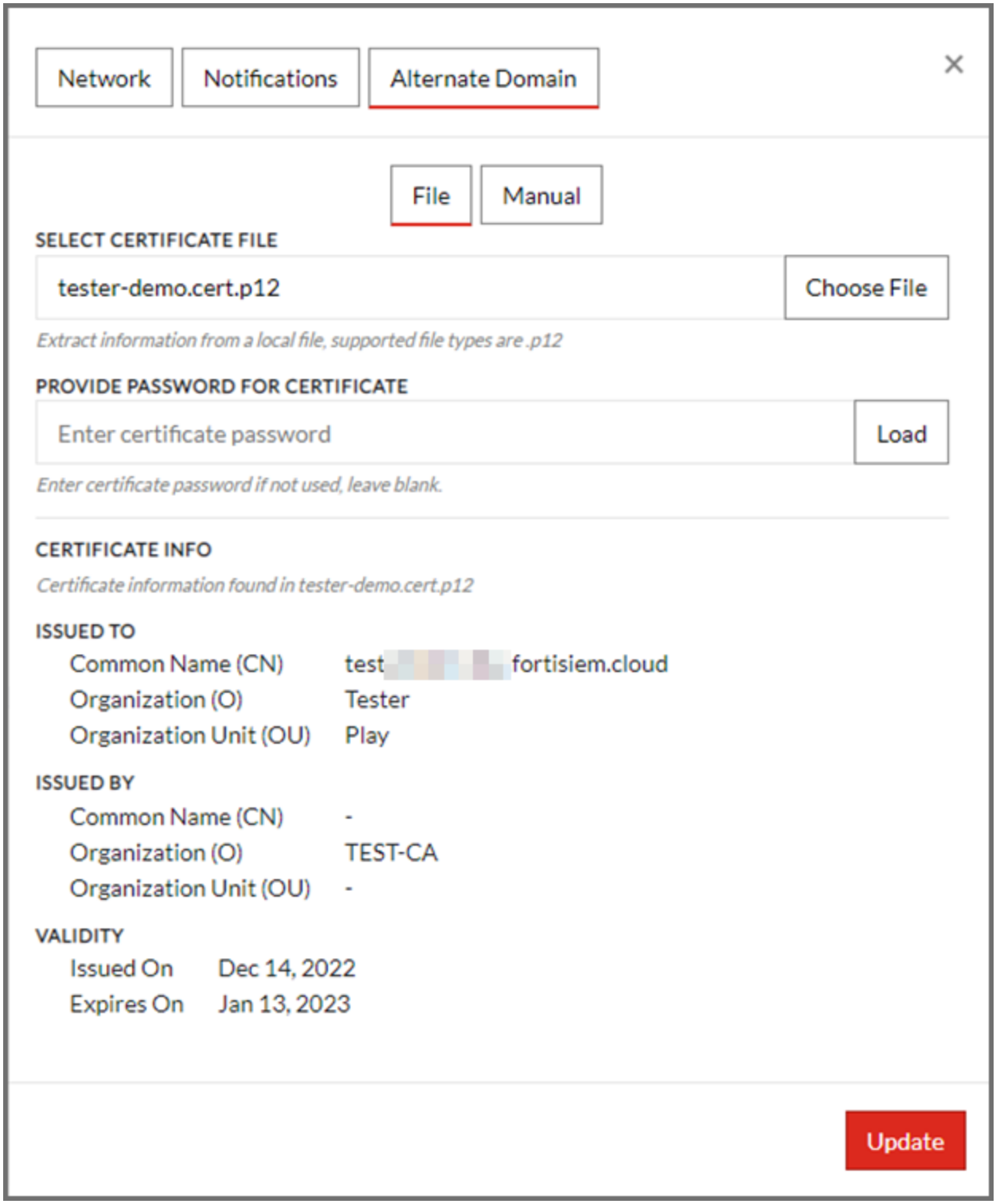
Steps for Importing PKCS#12 Format File

To import PKCS#12 file information, you will choose the certificate from your local computer, and the information will be extracted from it.

Take the following steps.

1. Select the **File** tab.
2. Select **choose file**.
3. Enter the certificate password, or leave it blank if no password is necessary.
4. Click **Load**.

Once the certificate is loaded, the information will be shown below.

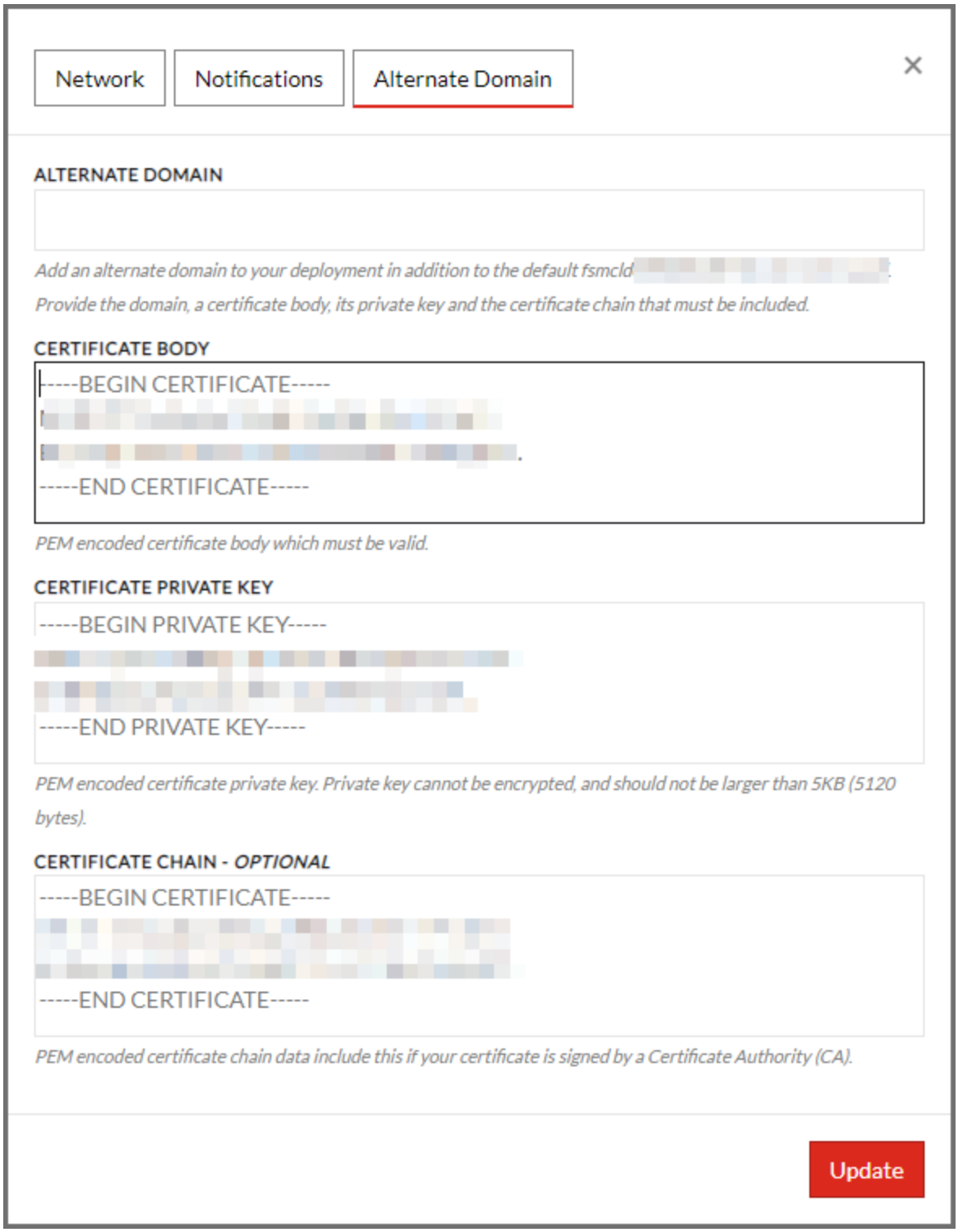


Steps to Manually Provide Alternate Domain Information

To manually provide the information, take the following steps.

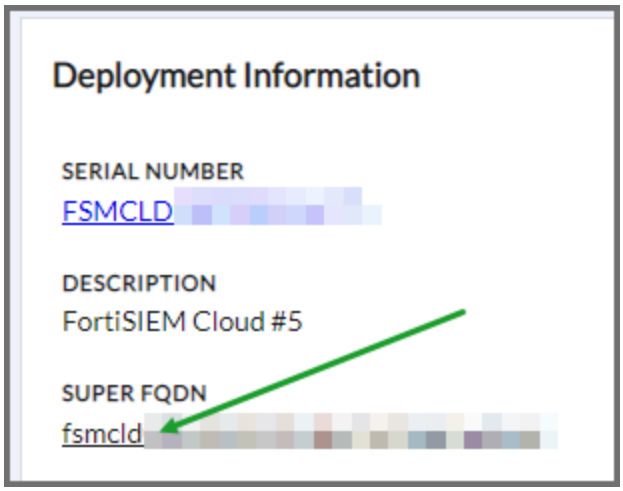
1. Select the **Manual** tab.
2. Click on the field below **CERTIFICATE BODY** and provide the base64 encoded certificate (PEM encoding).
3. Click on the field below **CERTIFICATE PRIVATE KEY** and provide the base64 encoded Private Key (PEM encoding).
4. (Optional) Click on the field below **CERTIFICATE CHAIN - OPTIONAL** and provide the base64 encoded CA Chain (PEM encoding).
5. When done, click **Update**.

   An example of editing **Alternate Domain** is provided below.



Note: This update can take some time to propagate fully.

6. Once complete, you must then add a new CNAME onto your domain, this CNAME record should point to your FortiSIEM Cloud instance FQDN. This FQDN is provided in the Manage page, under **Super FQDN**. To copy this value, simply click the **Super FQDN** link, and the content will be copied to clipboard.



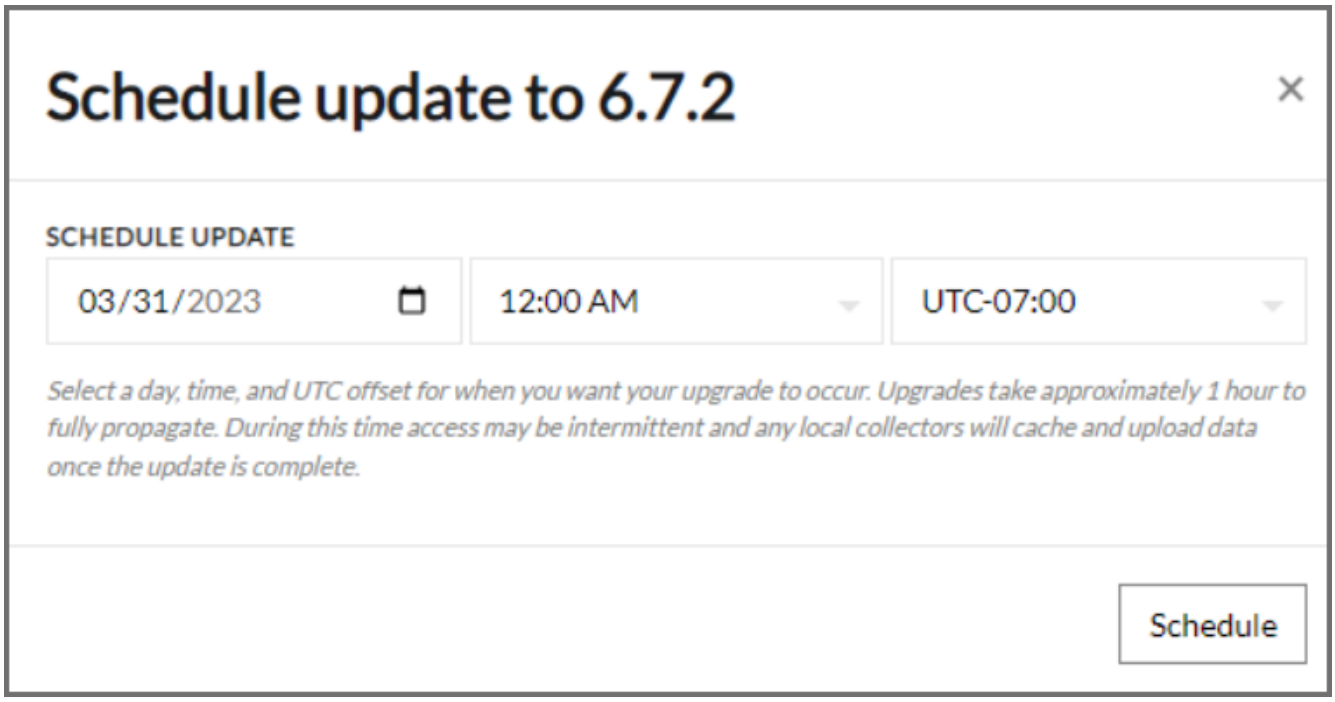
This can then be used when creating a new CNAME record for your domain, and will allow the newly added alternate domain to be served correctly during resolution.

Scheduling Upgrades to Instances

FortiSIEM Cloud regularly releases upgrades to the underlying FortiSIEM version. These provide improved availability, performance and security to your deployment.

When an update is available, you will be notified on the **Manage** screen, and will be able to schedule a convenient time to upgrade.

To do this, click on the **Schedule/Reschedule** button on the “New Version” information panel, then enter a convenient day for the upgrade to take place.

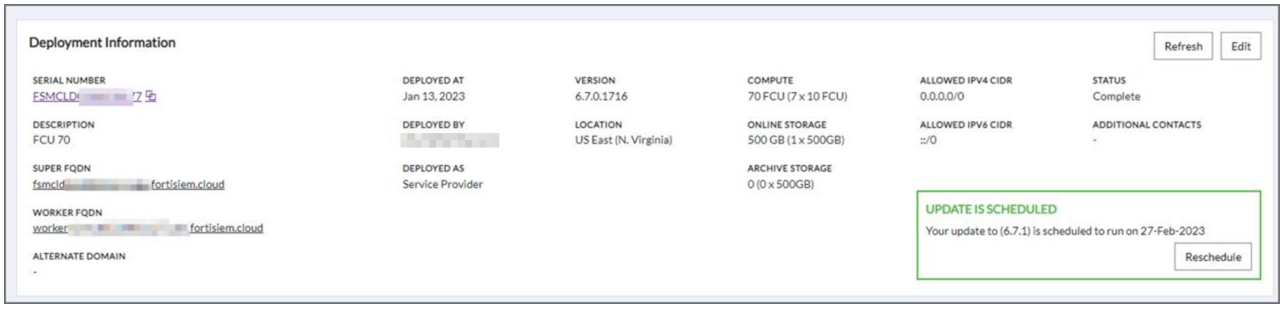


Note: Upgrades are scheduled to run at the time you specify. During this time, your instances may have intermittent access,

and any collectors connected to your FortiSIEM Cloud instance will cache locally and upload once the upgrade is completed.

To upgrade, follow these steps:

1. Click on **Schedule/Reschedule** button.
2. Click on the calendar icon and select a day when you want to update. A new date must be at least 1 day from the current day.
3. Select a time. You can select between an hour and half an hour time frame.
4. Select a UTC offset. By default, your current local offset will be selected.
5. Click **Schedule**.
   The upgrade will run on your scheduled date.



External Storage

External storage provides you with the ability to seamlessly transfer data from your FortiSIEM Cloud instance to an external Amazon S3 Bucket. Once you specify a new location and apply the provided policy to your bucket, data will automatically be transferred prior to being removed from Archive storage.

If you have not purchased Archive storage, this data will be transferred once your Online storage exceeds your purchased capacity.

Data transferred is formatted in gzipped parquet to provide convenient and optimal storage once transferred. This data can then be loaded into other tools which support the compressed Parquet format.

Transfer will only occur when space based usage is applied. Transfer of data will not occur for data that is subject to Retention policies. For example, if you have enough space in either Archive or Online storage, and have a 90 retention policy applied to data, this will be automatically removed during normal operation.

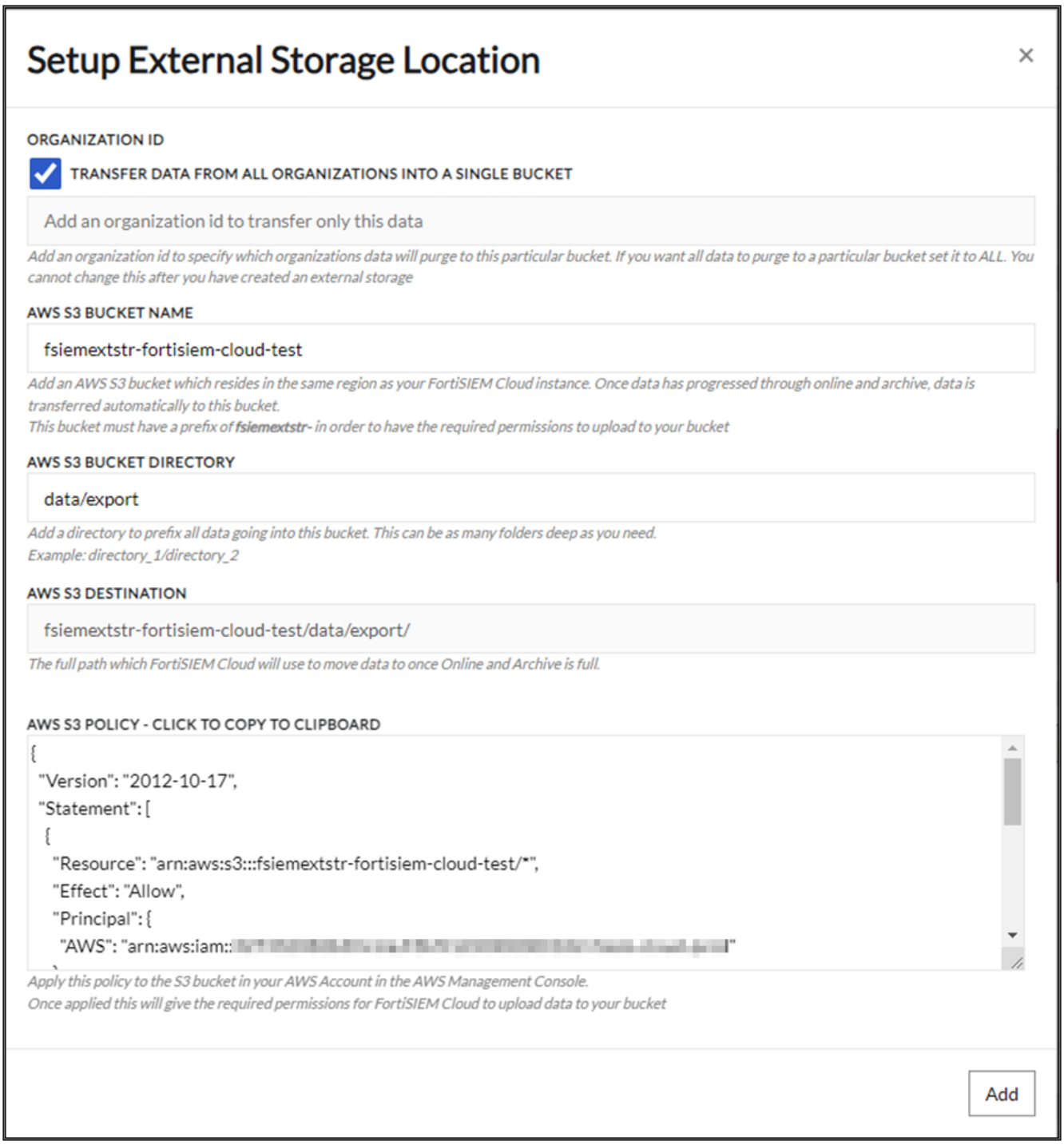
Setting up External Storage

To setup external storage locations using Amazon S3 buckets, click **New**, and then provide the following information:

Parameter	Description
ORGANIZATION ID	Provide the Organization ID, or select the **TRANSFER DATA FROM ALL ORGANIZATIONS INTO A SINGLE BUCKET** checkbox. Multiple bucket locations can be provided. For Service Providers, copy selected data to multiple customer owned buckets.
AWS S3 BUCKET NAME	Provide a bucket name with the prefix: `fsiemextstr-` Example: `fsiemextstr-fortisiem-cloud-data` **Note**: If the bucket does not start with `fsiemextstr-`, then the applied policy will be unable to transfer any data.
AWS S3 BUCKET DIRECTORY	Provide any additional prefixes to include for your bucket. Amazon S3 prefixes act similar to directories. If, for example, you have multiple prefixes for different organizations, you can include these.
AWS S3 DESTINATION	Provide the full path where FortiSIEM Cloud will move data to, when Archive or Online storage reaches capacity.
AWS S3 POLICY	Copy the AWS S3 Policy to your Amazon S3 bucket to apply. Adding this policy to your bucket will allow FortiSIEM Cloud to upload data to your bucket.

After you have provided the necessary information, click the **Add** button to complete the setup.

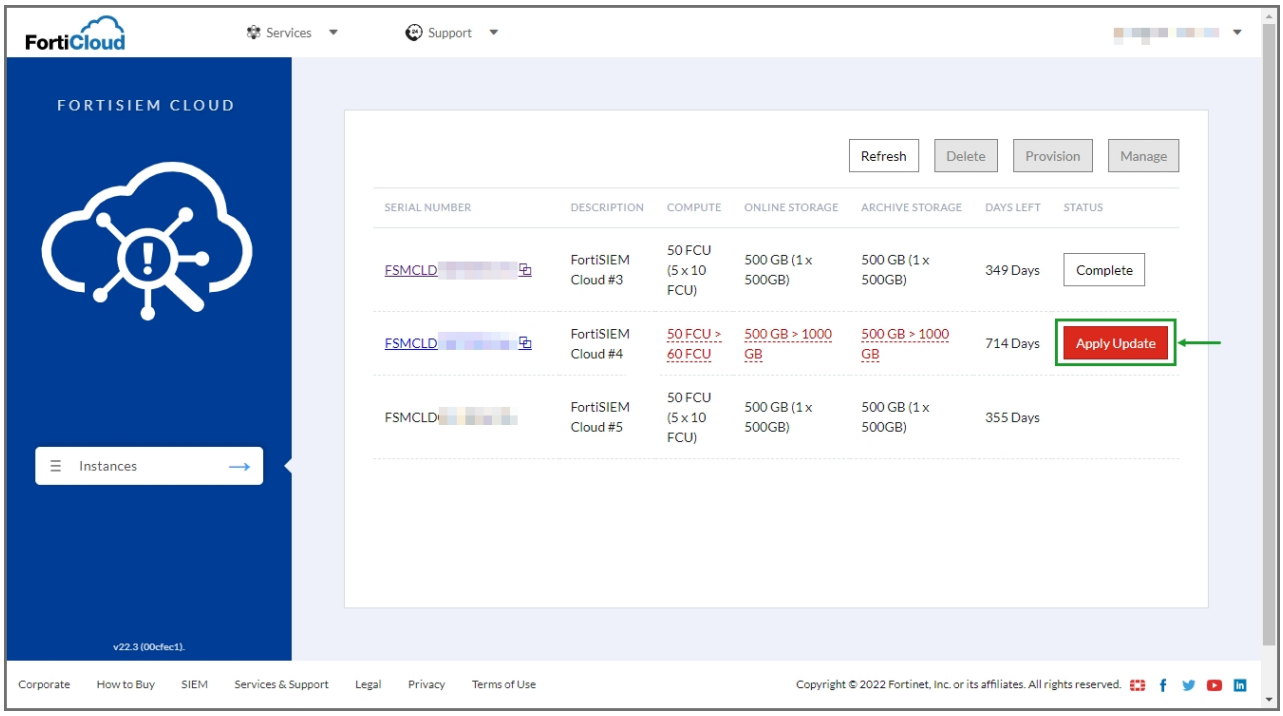
Once **Archive** or **Online** storage reaches its capacity, data will be automatically transferred to your external storage. Each location is evaluated and transferred in order. Once complete, you will see a notification for the data transferred amount and when the action was last completed or an error message.


Setup External Storage Location
ORGANIZATION ID
TRANSFER DATA FROM ALL ORGANIZATIONS INTO A SINGLE BUCKET
Add an organization id to transfer only this data
Add an organization id to specify which organizations data will purge to this particular bucket. If you want all data to purge to a particular bucket set it to ALL. You cannot change this after you have created an external storage
AWS S3 BUCKET NAME
fsiemextstr-fortisiem-cloud-test
Add an AWS S3 bucket which resides in the same region as your FortiSIEM Cloud instance. Once data has progressed through online and archive, data is transferred automatically to this bucket.
This bucket must have a prefix of fsiemextstr- in order to have the required permissions to upload to your bucket
AWS S3 BUCKET DIRECTORY
data/export
Add a directory to prefix all data going into this bucket. This can be as many folders deep as you need.
Example: directory_1/directory_2
AWS S3 DESTINATION
fsiemextstr-fortisiem-cloud-test/data/export/
The full path which FortiSIEM Cloud will use to move data to once Online and Archive is full.
AWS S3 POLICY - CLICK TO COPY TO CLIPBOARD
{
"Version": "2012-10-17",
"Statement": [
{
"Resource": "arn:aws:s3:::fsiemextstr-fortisiem-cloud-test/*",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::
Apply this policy to the S3 bucket in your AWS Account in the AWS Management Console.
Once applied this will give the required permissions for FortiSIEM Cloud to upload data to your bucket
Add

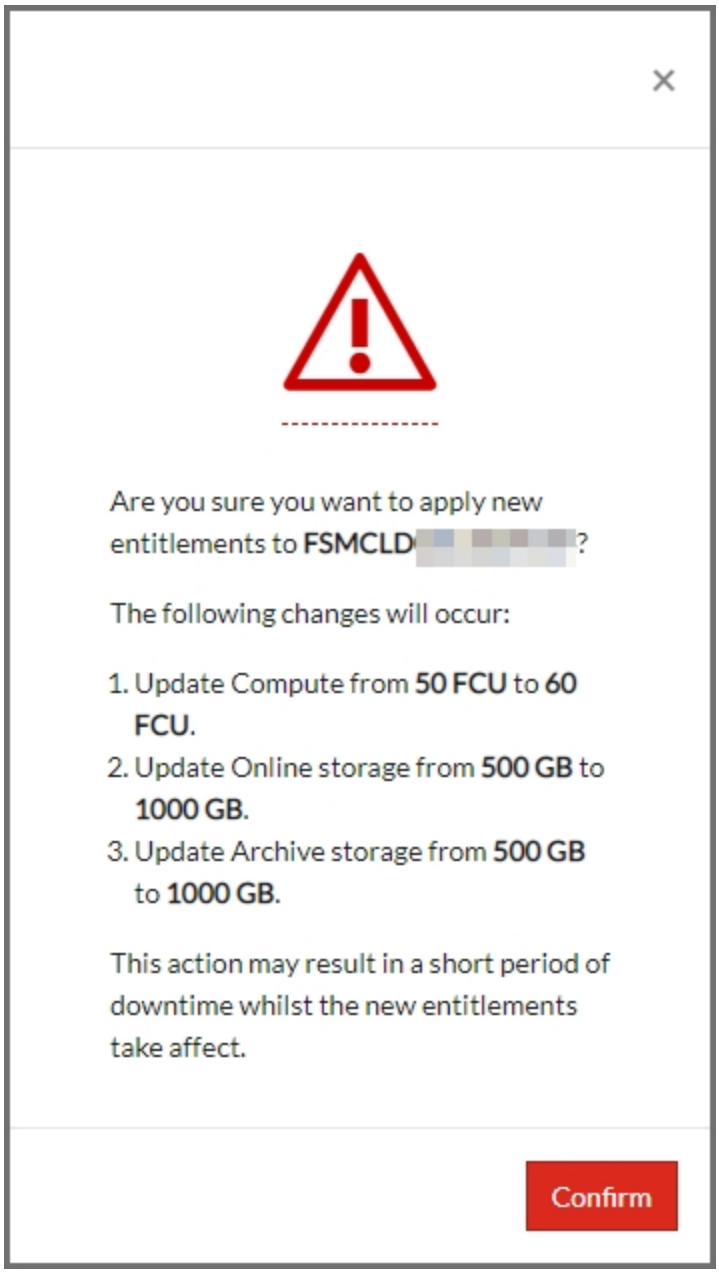
Applying Updates to your Entitlements

To apply update(s) to your entitlements, take the following steps.

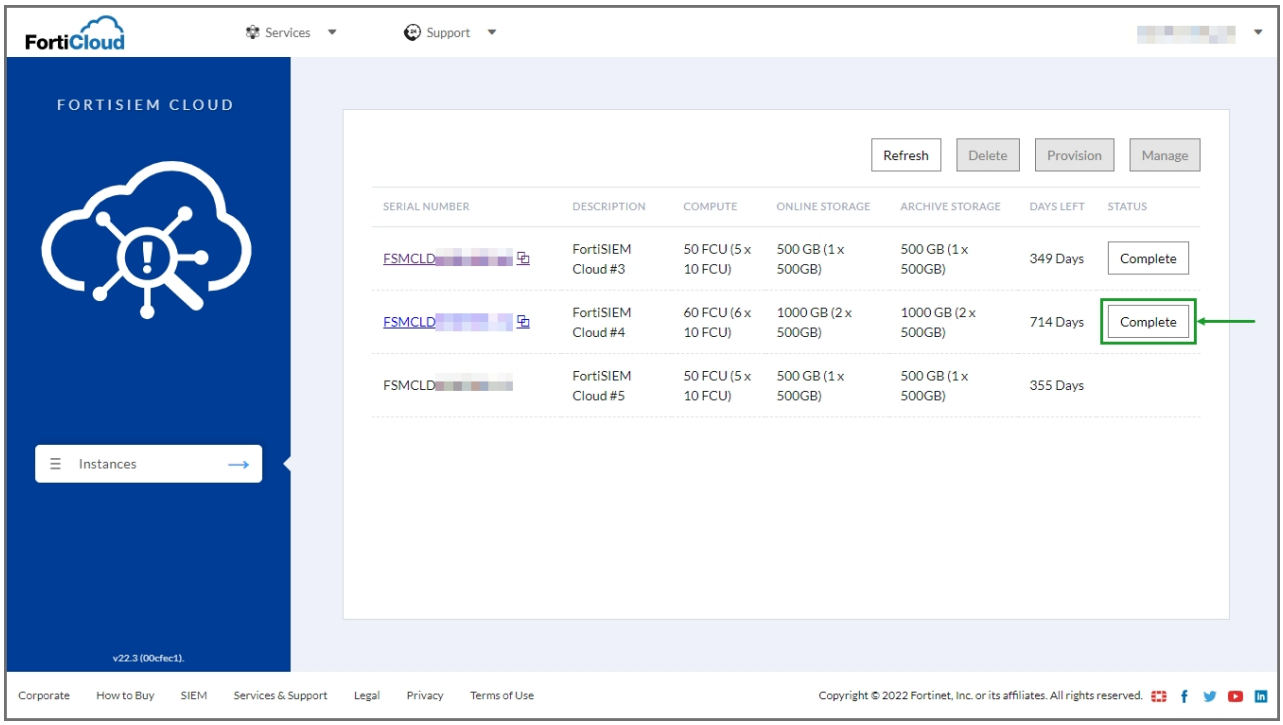
1. Select the FortiSIEM Cloud instance with the new entitlements and click **Apply Update**.



2. Click **Confirm** when shown the entitlement updates.



3. The status can be seen under the **STATUS** column or by clicking the **Refresh** button. To get real time updates, click on the **STATUS** button and it will provide you with live information.



When the entitlement update is done, the STATUS will be shown as **Complete**, and you can click on the FortiSIEM Cloud instance hyperlink to go directly to the FortiSIEM Cloud GUI.

FortiSIEM Cloud Event Retention

How FortiSIEM Cloud Event Retention Works

For FortiSIEM Cloud, the Online and Archive storage is managed together.

- **Space based retention**: If free Online storage utilization is less than 10%, then oldest events are moved to the Archive until free Online storage utilization is more than 20%. When FortiSIEM Cloud removes event data, FortiSIEM goes through each retention policy (90 days, 180 days, ...) and within each policy, FortiSIEM removes the oldest data.
- **Time based retention**: You can use Online event retention policies to specify the duration for which certain events need to be retained. The policies can take event attributes such as Organization, reporting Device and Event Type as input. See Creating FortiSIEM Cloud Event Retention Policy. During the retention period, the events can be in Online or Archive storage depending on the space based retention, e.g. if Online storage becomes full then the event may move to Archive storage. After retention period expires, events that meet the policy will be purged from Online and Archive storage.

For further information about Retention Policies, see Explanation of Retention Policies in Detail.

Explanation of Retention Policies in Detail

Retention policies are set to denote data lifetime, regardless of whether the data is in Online or Archive storage at the time of evaluation; these policies are not used to maintain a balance between Online storage and Archive storage.

The move of data from Online to Archive storage is performed on a per-retention day "fair usage" configuration. When Online storage has 10% or less storage available, FortiSIEM will begin to archive or purge the data if no Archive storage is available. The fair usage policy will move 1 day of data in Online storage from each retention policy to Archive storage if available. This process continues to iterate through each retention policy until the pre-defined safety threshold is met (20% free Online storage) and ALL policies are evaluated in a particular round.

This means that each retention policy (Forever, 3 months (90 days), 6 months, etc.) is considered and given equal priority when moving data to Archive storage.

As an example, lets examine a scenario of 2 policies being set up, one Forever, and the other 3 Months. When the Online storage thresholds are met, the archival process is triggered. The process will take the oldest data, residing in each policy in a balanced fashion and move this to Archive storage.

If FortiSIEM was deployed in January and then subsequently a 3 Months retention policy was defined on the 1st of August, and your online threshold is met on the 1st of September, FortiSIEM will move the oldest data from the Forever policy (prior to August 1) as well as data from the 3 Months retention policy which may be newer data. This process

continues to iterate through each retention policy until the pre-defined safety threshold is met (20% free Online storage), and all policies are evaluated in each round.

FortiSIEM Cloud performs daily checks on your Archive storage usage, and once usage is 100%, then the oldest events, regardless of retention policy, will be purged from Archive storage.

FortiSIEM Cloud, when used without Archive storage, will purge the oldest events based on the retention policy definition. When multiple retention policies are configured, FortiSIEM will use the "fair usage" approach and move a 1 day of events at a time from all retention policies until Online storage has 20% free disk space.

Creating FortiSIEM Cloud Event Retention Policy

Online event retention policies specify which events are retained, and for how long, in the online event database. Take the following steps to create an Online Event retention policy for FortiSIEM Cloud.

1. Navigate to **ADMIN > Settings > Database > Retention Policy**.
2. Under Online Retention Policy, click **New**.
3. Check the **Enabled** checkbox if the policy has to be enforced immediately.
4. From the **Organizations** drop-down list, choose the organizations that the policy must be applied to (for service provider installations). Check the **All** checkbox if the policy should apply to all organizations.
5. For **Reporting Device**, click the edit icon to choose the reporting devices to apply this policy to, and click **Save** when done.
6. For **Event Type**, click the edit icon to choose the event type or event type groups to apply this policy to, and click **Save** when done.
7. Select the **Retention Period** from the drop-down list (3 Months, 6 Months, 1 Year, 3 Years, 5 Years, 10 Years, Forever (50 Years). Each month is 30 days.
8. Enter any **Description** related to the policy.
9. Click **Save**.
10. When done, confirm that the policy is selected, and click **Apply**.

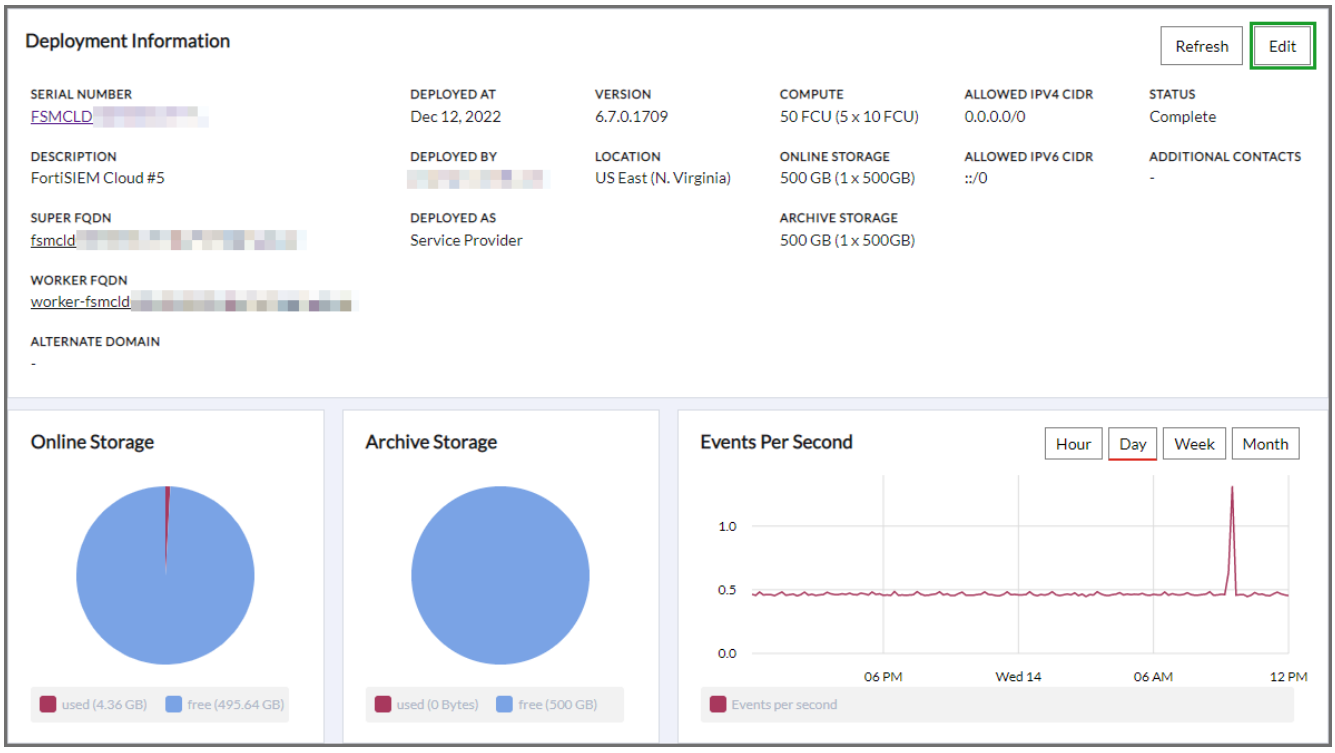
Troubleshooting

My FortiSIEM Cloud instance is not receiving events via deployed collectors. How do I resolve this?

First, ensure that the network CIDR blocks are your expected values. FortiSIEM Cloud inbound network is locked down by specific CIDR blocks that you decide.

To obtain the current list of CIDR blocks associated with your FortiSIEM Cloud instance, select the instance on the Instances view, click **Manage**, and then check the following headings: **ALLOWED IPV4 CIDR** and **ALLOWED IPV6 CIDR**.

To update the CIDR blocks, from the Manage page, follow the instructions in Updating Network CIDR. The platform will take a few minutes to update your network settings. If correct, the collector will automatically start to send in any cached data.

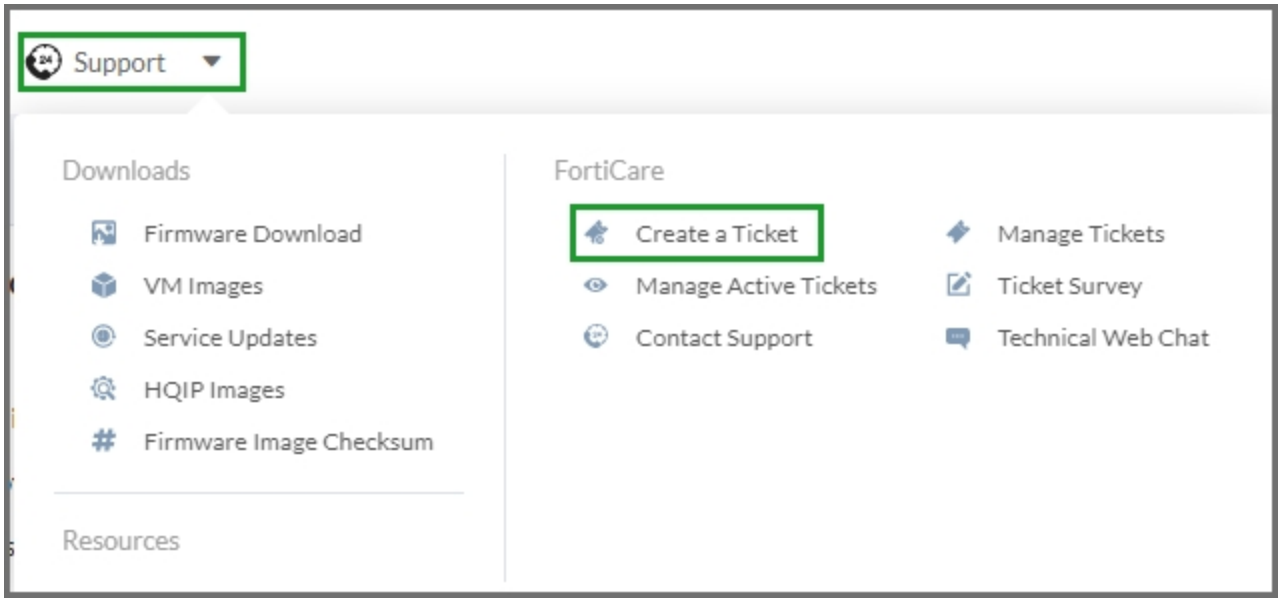


I'm unable to login into my newly provisioned instance. What do I do?

If the error you are seeing is network related, i.e., you cannot access the FortiSIEM Cloud GUI, then you should follow the steps above to ensure that the CIDR blocks contain the expected routes that you would be accessing the FortiSIEM Cloud instance from.

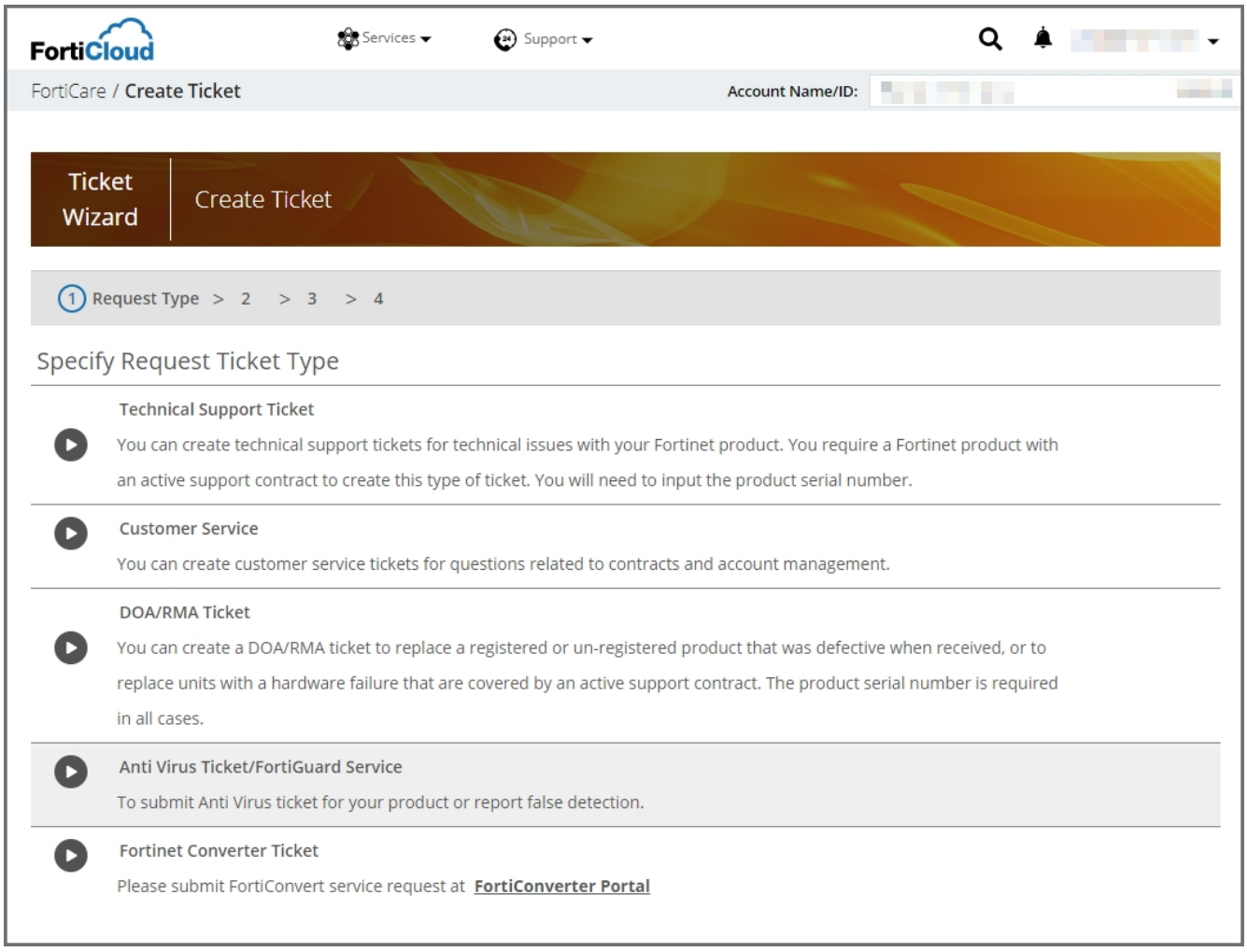
If you have forgotten the provisioned password, then you should follow the steps in I forgot my password for my FortiSIEM Cloud instance.

Failing these, you can raise a support ticket for the FortiSIEM Cloud support team to investigate any issues that you are having. Simply click on the Support menu in the FortiSIEM Cloud portal, click **Create a Ticket**, and follow the Fortinet support portal guide to complete your support ticket.



I forgot my password for my FortiSIEM Cloud Instance. How do I recover it?

If you have forgotten the password that you provisioned with your FortiSIEM Cloud instance, you must raise a support ticket. To do this on the FortiSIEM Cloud portal, select the Support menu, and then click **Create a Ticket**. A new tab will open for the Fortinet Customer Care portal, and you can then raise a Customer Service Ticket. To ensure quick resolution, include the serial number associated with your entitlement.


FortiCloud
Services
Support
FortiCare / Create Ticket
Account Name/ID:
Ticket Wizard
Create Ticket
1 Request Type > 2 > 3 > 4
Specify Request Ticket Type
Technical Support Ticket
You can create technical support tickets for technical issues with your Fortinet product. You require a Fortinet product with an active support contract to create this type of ticket. You will need to input the product serial number.
Customer Service
You can create customer service tickets for questions related to contracts and account management.
DOA/RMA Ticket
You can create a DOA/RMA ticket to replace a registered or un-registered product that was defective when received, or to replace units with a hardware failure that are covered by an active support contract. The product serial number is required in all cases.
Anti Virus Ticket/FortiGuard Service
To submit Anti Virus ticket for your product or report false detection.
Fortinet Converter Ticket
Please submit FortiConvert service request at FortiConverter Portal

www.fortinet.com