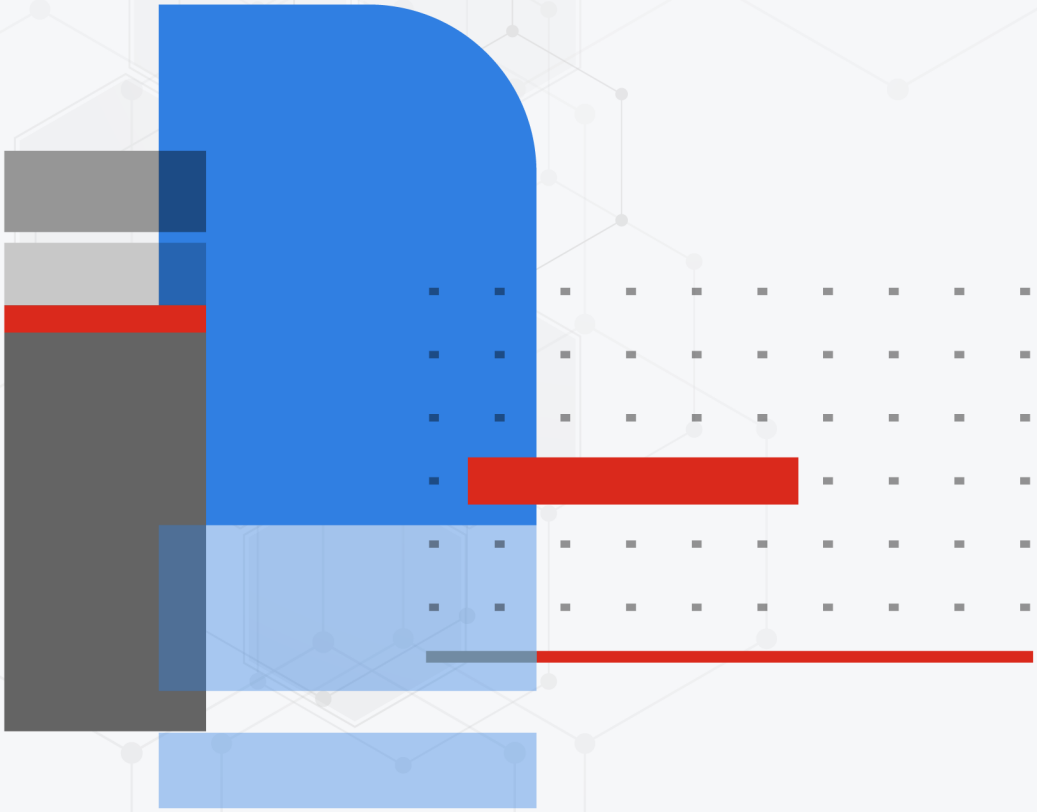
Admin Guide

FortiCASB 24.2.a



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

May 30th, 2024
FortiCASB 24.2.a Admin Guide
00-400-000000-20181031

TABLE OF CONTENTS

Change Log

Date	Change Description
07/01/2020	FortiCASB 20.2 Handbook release. Cloud Account **Activity and Alert Reports** are now available for export from Reports.
04/03/2020	FortiCASB 20.1 Handbook release. FortiCASB REST API reference added and Compliance Report feature upgraded in this revision.
09/07/2019	FortiCASB 4.2 Handbook release. IAAS applications and features migrated to FortiCWP.
04/05/2019	FortiCASB 4.1 Handbook release. Revised **Getting Started** documentation for Basic Setup and Install IAAS applications. Added documentations for **Topology**, **Resource**, **Resource Profile**, and **Traffic**. **Configuration** merged into **Risk Assessment .**
01/08/2019	FortiCASB 2.1 Handbook. First edition. Changing EU Users IP address from 52.59.74.73 or 18.195.109.67 to 34.254.217.50 or 52.18.7.98, in the section "Show IT discovery".
06/20/2023	FortiCASB 22.2.b release
08/11/2023	FortiCASB 23.3.a release

What's New

FortiCASB 24.2.a Release Highlights

Data Security Policy Update

- **Quarantine Files** – Any File matching the Data Security policy can now be quarantined. This functionality adds on top of preexisting quarantine feature that was available for malware file detection only. This feature is available for Office 365, Google Workspace, Box, and Dropbox Only.
- **File Activity Triggers** - File Activity threshold triggers can be customized under the file activity data security policy configurations. This feature allows to define how often the activity should occur before an action is triggered.

Office 365 Features Update

- **Office 365 File Status** – When Office 365 files cannot be scanned, they will receive granular status that reflects the source of error on the File menu item tooltips.
- **Office 365 Onboarding** – Office 365 onboarding has been improved and now supports higher rates of file scanning by using a dedicated service account instead of a user account that was previously used. For this functionality A client application needs to be registered in Microsoft Entra ID on Azure to onboard Office 365 in FortiCASB.

Introduction

Welcome, and thank you for selecting FortiCASB for your cloud security and monitoring needs.

FortiCASB is Fortinet's cloud-native Cloud Access Security Broker (CASB) service, which provides visibility, compliance, data security, and threat protection for cloud-based services.

Using direct API access, FortiCASB enables deep inspection and policy management for data stored in cloud application platforms. It also provides detailed user analytics and management tools to ensure that policies are enforced and that your organization's data is secure.

FortiCASB works by focusing on Gartner's four pillars of security: visibility, compliance, data security, and threat protection.

- **Visibility**—Visibility is one of the most important aspects of cloud security. FortiCASB uses a series of methods such as data scans and analytics to answer the questions: who accessed information, what was accessed, when it was accessed, and from where did the access originate.
- **Compliance**—FortiCASB provides file content monitoring to find and report on regulated data in the cloud.
- **Data security**—FortiCASB runs scans to check for sensitive data, such as social security numbers or credit card numbers. It then classifies this data under different levels of sensitivity and sends different alerts depending on the sensitivity level of the data accessed.
- **Threat protection**—FortiCASB uses User Entity Behavior Analytics to watch for suspicious or irregular user behavior. It also sends out alerts for malicious behavior.

Cloud Security Features

FortiCASB comes with a series of features that give you visibility of data access and usage, control over data security and threat protection, and peace of mind over compliance with standards and federal regulations.

Visibility

- **Automatic on-demand data scan**—FortiCASB examines existing content in all folders to identify sensitive data subjects or security policies.
- **Cloud usage analytics**— FortiCASB visually summarizes key usage statistics, including trends over different time periods as well as drilldown, access count, and usage over time.
- **User entitlements review**— FortiCASB gives visibility of privileged users, dormant users, and external users.
- **File exposure**— FortiCASB highlights the most shared files overall, as well as each user's most shared files.

Data security and threat protection

- **Cloud data loss prevention**— FortiCASB enforces DLP policies based on data identifiers, keywords, and regular expressions for data at rest.
- **Threat detection**—FortiCASB offers an abundant number of out-of-the-box policies to immediately detect account-centric threats.
- **Malware detection**— FortiCASB features a malware detection policy to detect malicious files before they compromise sensitive data.
- **Geo-location analytics**—FortiCASB visualizes global access patterns and analyzes activity to identify unlikely cross-region access attempts indicative of compromised accounts.
- **Shadow IT discovery** — FortiCASB offers an overview of unsanctioned cloud applications used in the organization and gives users the ability to control application usage.
- **Configuration assessment** —FortiCASB offers an large number of out-of-the-box policies for automated validation of best security practices against the your cloud storage account.

Compliance

- **Predefined compliance policies**—FortiCASB provides predefined compliance policies designed to help maintain compliance with ISO 270001, NIST 800-53 V4, and NIST 800-171 regulations.
- **Compliance report**—FortiCASB can produce compliance reports for audit purposes. These reports show compliance with ISO 270001, NIST 800-53 V4, and NIST 800-171 regulations.

FortiCASB License Subscription

There are two types of FortiCASB license subscription: **FortiCASB SaaS Protection License** and **FortiCASB Data Protection License**.

FortiCASB license usage is based on the number of protected users as well as volume of DLP data scanning performed by FortiCASB.

Data scans are triggered by the Data Security Policy applied to the protected SaaS applications.

FortiCASB SaaS Protection License

FortiCASB SaaS Protection license provides license seats to monitor SaaS application user activities and detect suspicious behavior. Additionally the SaaS protection license provides Data protection scanning capacity to perform DLP and malware/AV scanning.

After the DLP scan capacity is depleted, only more DLP scan capacity is required through purchase of FortiCASB Data Protection License.

Serial Number	Description
FC1-10-FCASB-145-02-DD	Protection and monitoring of 100 SaaS users including Data Scanning of 1TB
FC2-10-FCASB-145-02-DD	Protection and monitoring of 500 SaaS users including Data Scanning of 5TB

If the number of users in onboarded cloud applications exceeds the total user capacity allowed by the FortiCASB SaaS Protection license, the ability to onboard new cloud applications will be temporarily suspended until an additional license is purchased. This behavior is expected during the cloud application onboarding process. However, existing cloud applications that are already onboarded will remain unaffected.

FortiCASB Data Protection License

During day-to-day operation, Data scans triggered by FortiCASB Data Security Policies consume scan capacity based on the volume of scanned files. Once the initial scan capacity which is included with the FortiCASB SaaS Protection license is depleted, customers will need to add FortiCASB Data Protection license to continue scanning data.

FortiCASB Data Protection License is an add-on license for the existing FortiCASB SaaS Protection License users and/or FortiClient ZTNA users when the Data scan capacity is depleted.

Serial Number	Description
FC1-10-FCASB-307-02-DD	100GB Data scan add-on for FortiCASB SaaS Protection users or FortiClient ZTNA users
FC5-10-FCASB-307-02-DD	1TB Data scan add-on for FortiCASB SaaS Protection users or FortiClient ZTNA users

FortiCASB License For FortiClient ZTNA Users

Customers that have purchased the FortiClient ZTNA license are entitled to the equivalent number of FortiCASB SaaS protection seats (500 FortiClient ZTNA seats will entitle customers to 500 Protected SaaS users in FortiCASB). As part of the ZTNA license customers will be entitled to the equivalent of 1GB of data scanning per user seat.

As an example, a FortiClient ZTNA customer with 500 user seats, will also be entitled to 500GB of Data Protection. For further Data scanning capacity customers will need to purchase the FortiCASB Data Protection license.

When there is insufficient DLP data scan capacity, only FortiCASB Data Protection License is required for additional DLP data scan capacity. It is not necessary to purchase FortiCASB SaaS Protection License for FortiClient ZTNA users.

AWS S3, **Google Workspace**, and **Azure Storage** only requires FortiCASB Data Protection License to perform DLP scan. All other SaaS applications require both user license seat and DLP scan capacity licenses.

Purchase Option

Contact your local sales representative and ask for a quote for the FortiCASB SaaS Protection license or FortiCASB Data Protection license.

If you don't have a sales contact, please kindly visit the link below to find your nearest sales contact.

https://www.fortinet.com/partners/partner-program/find-a-partner

Cloud Application Native Apps Support

In enterprise scale applications, like Google Workspace, Office 365, AWS S3, etc. they offer cloud application subscriptions in a package where they also support other native apps. **For example**, Google Workspace supports drive, gmail, meet, etc.

FortiCASB does not support monitoring for all cloud application native apps, but only provides monitoring in areas that are close to the core of FortiCASB's fundamental. Every cloud application's native apps support varies, here are details on what is being supported specifically to each cloud application.

What Cloud Data Are Scanned?

Generally, for all cloud applications supported by FortiCASB data scan and monitoring only starts after the cloud application is onboarded in FortiCASB. All data resides on the cloud application prior to onboarding is not supported for data scan.

However, all user activities including but not limited to file access are supported in FortiCASB data scan through Data Security, Threat Protection, and Compliance policies.

Google Workspace Native Apps Support

There are two Google Workspace native apps that FortiCASB supports:

- **Google Drive**
- **Google Workspace Marketplace**

FortiCASB monitors file activities and file access conducted on these two Google Workspace native apps through the method of API polling every 15 minutes.

Cloud Application Polling Intervals

Introduction

Polling Interval is the frequency in which FortiCASB communicates with the cloud application host onboarded to retrieve real time data. This process ensures that the data that FortiCASB monitors is in synchronization with the cloud application data.

There are two types of polling:

1. **API Polling** - FortiCASB queries the cloud application host according to a fixed interval regardless an event occurs or not. The shorter the polling interval, the closer it is to real-time update.
2. **Webhook Polling** - Query requests automatically made by the source or the cloud application server when an event occurs thus there is no delay in synchronization between the cloud application host and data monitored by FortiCASB.

Cloud Applications with API Polling and the Polling Intervals

Cloud Application	Polling Interval (min)
AWS S3	10
Azure Storage	20
Box	10
Dropbox	2
Egnyte	10
GCP Storage	5

Cloud Application	Polling Interval (min)
Google Workspace	1
Office 365	1
Salesforce	4
SAP IAS	10
SAP Success Factors	4
ServiceNow	2
Zendesk	10

Cloud Applications with Webhook Integration

- **Citrix**
- **Confluence**
- **Facebook Workplace**
- **Github**
- **Jira**
- **Webex**
- **Zoom**

Company Management

Company system configuration, business unit and user management of FortiCASB.

In Company, these are the key functionality of Company management:

- **View License Purchased**
- **Data Protection Usage**
- **Company and Business Unit Configuration**
- **User Management**
- **Microsoft Entra ID AU (Administrative Unit) Management**
- **Generate and Manage API Credentials**

When you first log into FortiCASB, you are prompted to create a company, business unit(s), and users.

FortiCASB account permissions can have one of the following:

- **Administrator**— can have full permissions, including the ability to create, access, assign companies and organizations.
- **Business users with full access**— business users from FortiCloud who have been granted full access also have full permissions, including the ability to create, access, assign companies and organizations.
- **Business users with limited access**— business users from FortiCloud who have been granted limited access can only view companies they are a part of.

If you are an administrator, continue to First Time Setup on page 23.

If you are a business user with limited access, not an administrator in charge of setup or a user with full access, skip to Switch between business units on page 29.

FortiCASB requires different setup procedures, depending on your organization's hierarchy and needs. A company with a branched hierarchy, such as a company with multiple branch offices or a compartmentalized organizational structure, will have different requirements than a company with only one unified office.

First Time Setup

To set up your FortiCASB for the first time, you or your organization must have the following in place:

- A valid FortiCASB license. Contact your primary Fortinet Service Provider to obtain a license if you do not already have one.

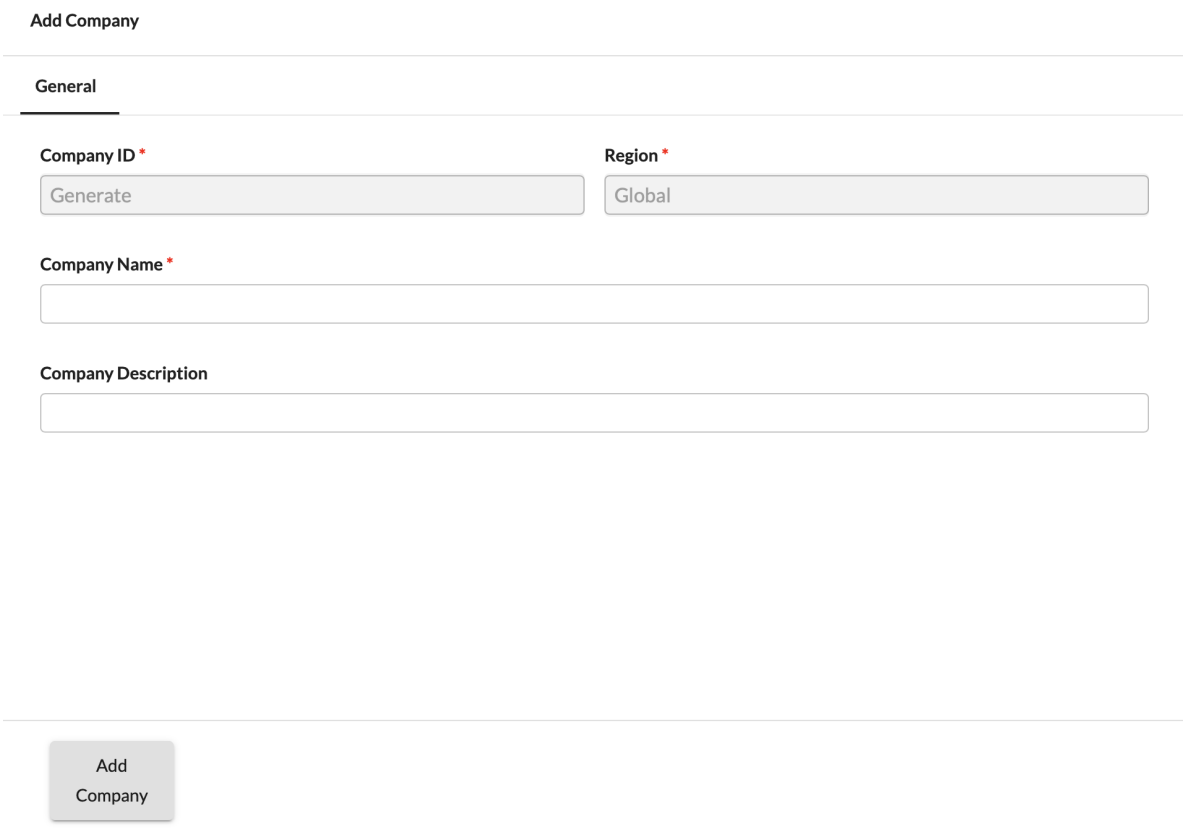
- An administrator with a **Primary FortiCloud account** to add your company, business units, and users in FortiCASB.

In accordance with European Union laws and regulations, all data that FortiCASB collected for European Union (EU) companies must be located in the EU region. To accommodate for this, you can choose to host your CASB cloud service either on the Global site or the EU site.

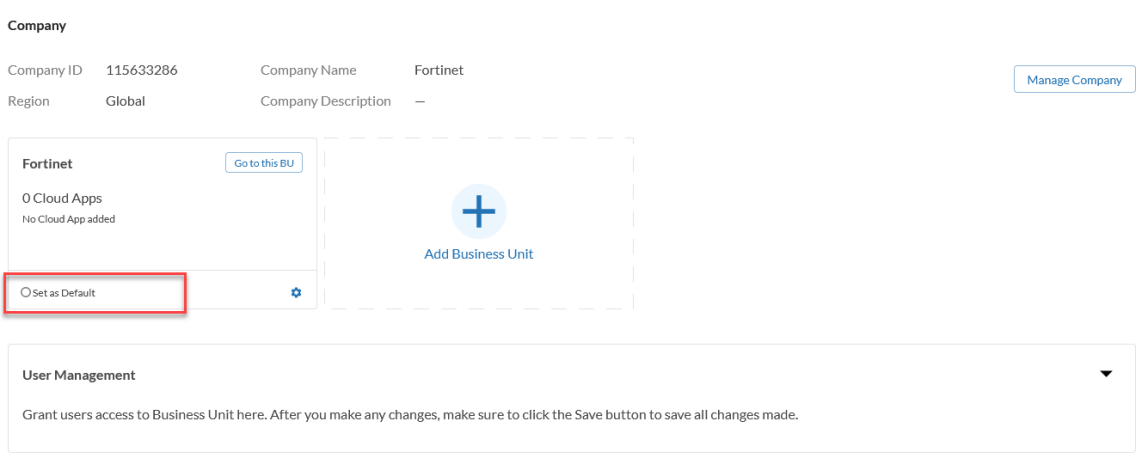
First Time Setup Steps

In the first time setup, a default company and business unit will be created using your admin account.

1. Go to https://www.forticasb.com/.
2. Click **Login**. You will be redirected to the Fortinet single sign-on webpage.
3. Log into FortiCASB with your admin account, or create a new admin account if you do not already have one.
4. If applicable, in FortiCASB account selection page, select an account.
5. A popup prompts you to create a company, enter a company name and description.
6. Click **Add Company** to finish creating a company.



7. After the default Company is created, a **default Business Unit** needs to be created. (Important)
   In the **Company** page, click **Set as Default** to make the first business unit as default.



8. Click **Go to this BU** to verify that the default Business Unit is created successfully.

   After the default company and business unit are created, proceed to Add a Business Units on page 25 to create additional business unit(s).

If you have a pop-up blocker, it will block the FortiCASB GUI.
Set an exception for the FortiCASB GUI, or open the GUI manually.

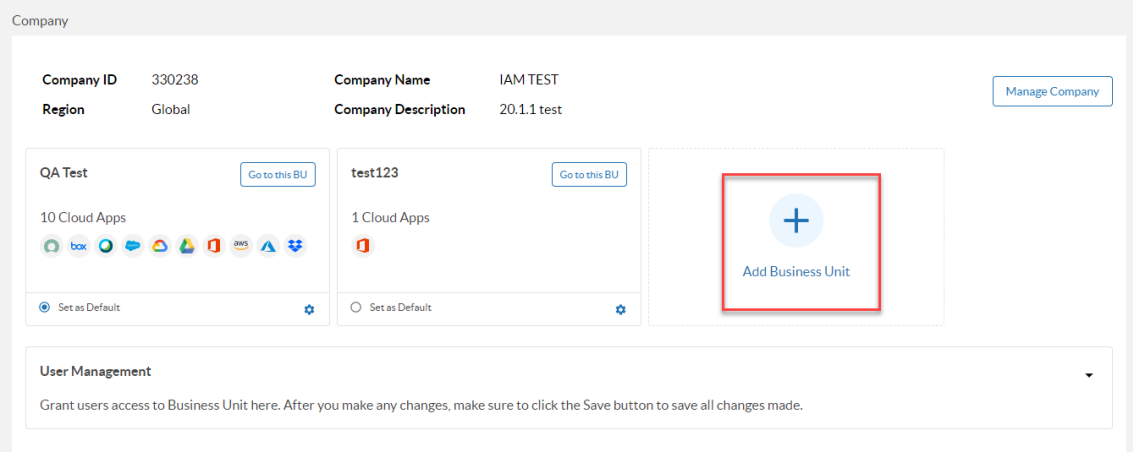
Add a Business Units

After a default company and business unit are created, log into FortiCASB to add additional business unit.

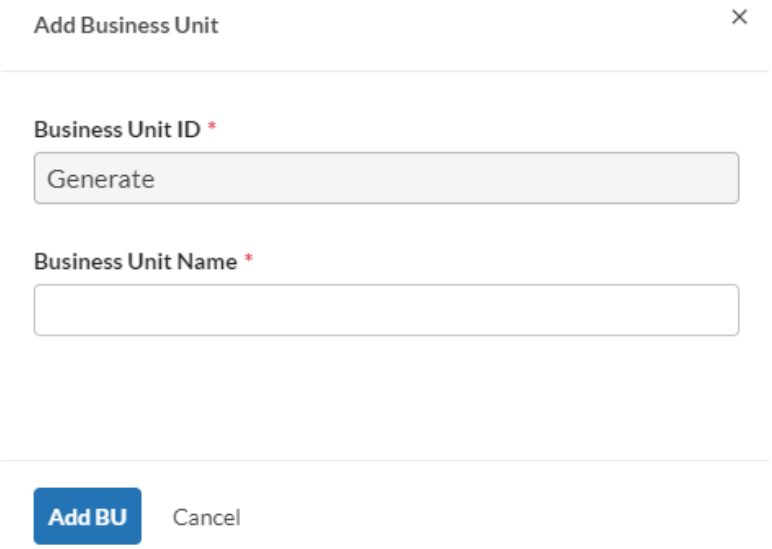
To add a business unit:

1. Log into FortiCASB with your primary FortiCloud account.
2. Click on **Company** from the top right hand side.

3. Click on **+Add Business Unit** under **Company** management.



4. Enter the Business Unit ID and a name, then click **Add BU** to complete adding the business unit.

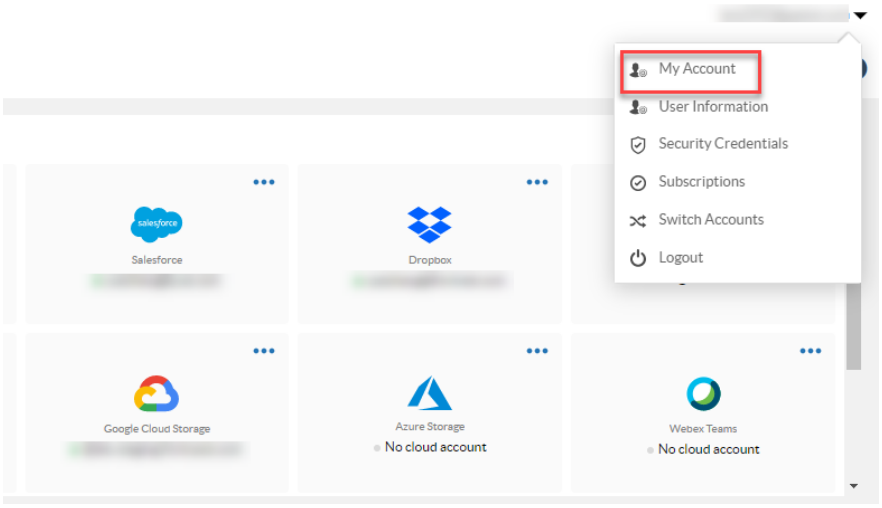


Repeat this process to add additional business units if applicable.

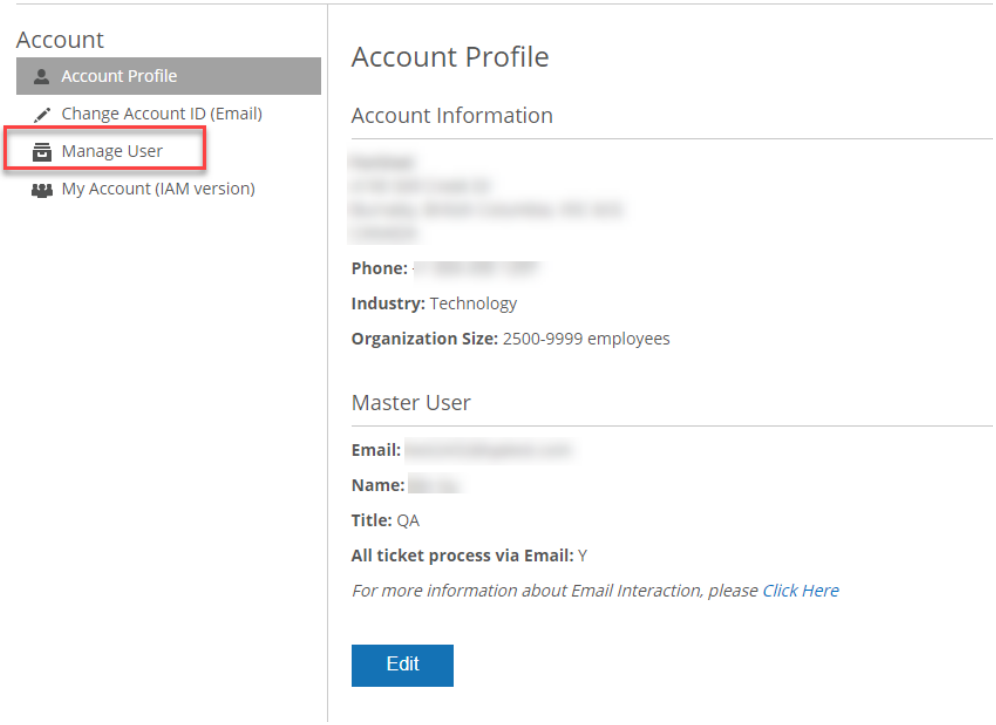
Create a Business User

You must create business users on FortiCloud. Only FortiCloud primary account user can create business user. After you create a business user, it will be appear in **User Management** on FortiCASB.

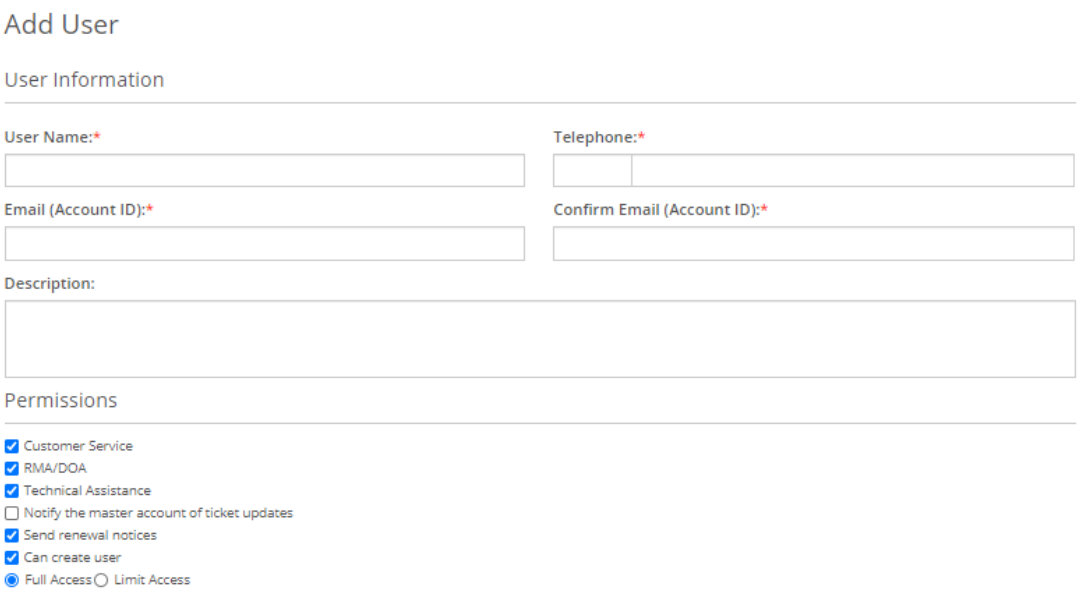
1. Log into FortiCloud. (https://support.fortinet.com)
   (Alternatively, you can access FortiCloud after you log into FortiCASB by clicking the account drop down menu button at the right hand side and select **My Account**.)



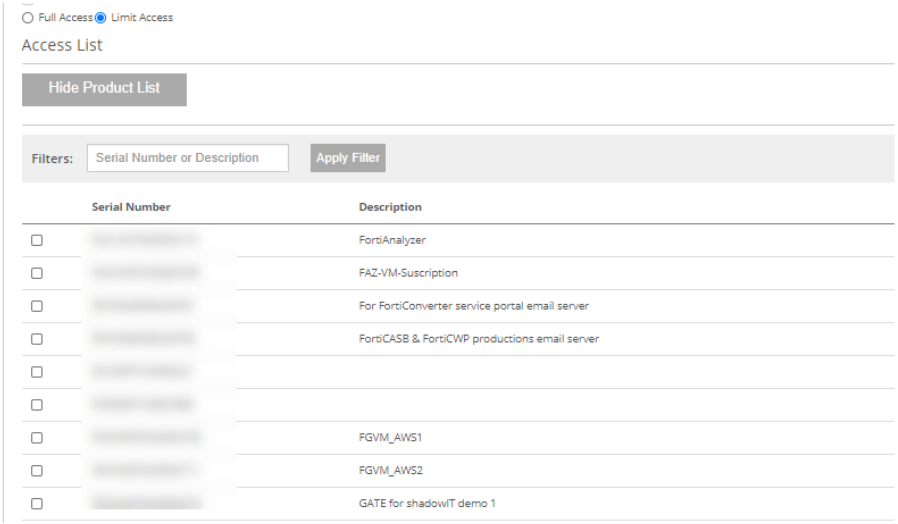
2. On FortiCloud, click on **Mange User** at the left hand side, then a list of users will display.



3. Click on add user button  on the right hand side:



4. Fill in the **User Name**, **E-mail**, and **Telephone** for the user you would like to set up.
5. **a.** Select **Full Access** to grant the user full permissions, including the ability to create/access/assign companies and business units.
   b. Select **Limited Access** to only grant the user basic access. Then click **Save**.
6. If **Limited Access** is selected, click on **Add More Products** to select a license.



7. Click **Save**.
   Repeat this process to create more users.

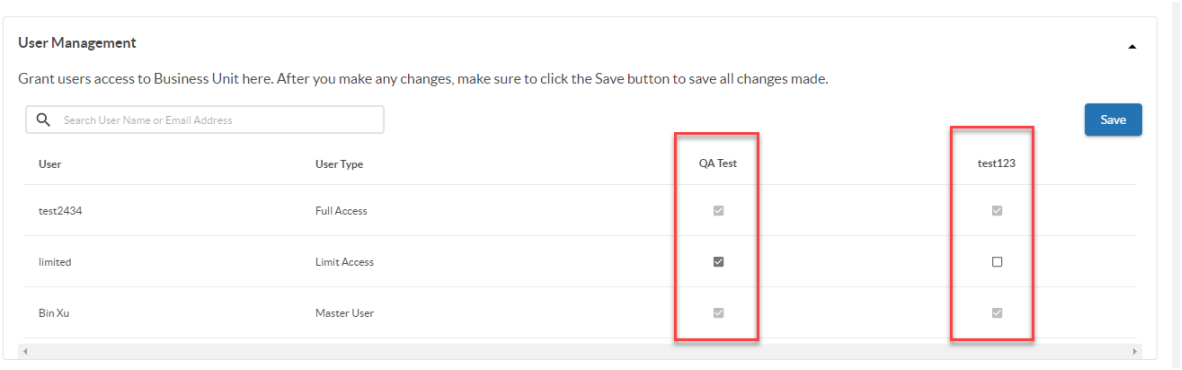
After business user(s) are created, you may assign the new users to the business units through Assign users to a business unit on page 29.

Assign users to a business unit

After you create business users on FortiCloud, they will appear in **User Management** on FortiCASB.

(If you just created the user on FortiCloud, make sure you log out of FortiCASB and log back in to see the new users in User Management.)

1. Log into FortiCASB with your primary FortiCloud account.
2. At the **FortiCASB Dashboard**, click **Company** at the top right hand corner.
3. Scroll down to **User Management** section, grant the user access to a business unit by checking the business unit check box, uncheck the check box to remove the user.



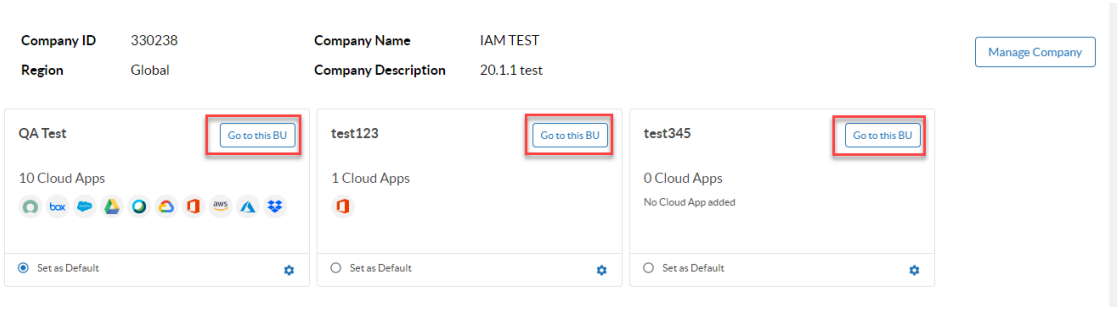
4. Click **Save** to save the configurations.

Switch between business units

Only **Business Unit** users created by FortiCloud primary account are able to access FortiCASB. If you have not created an user, please contact your administrator to help you create one.

1. Go to FortiCASB, at the sign-in page, sign in with your business user account.
2. Select a FortiCASB user account (if applicable).
3. Select your business unit, then you will be brought to the FortiCASB dashboard.
4. If you need to switch to different business unit, click on Company at the top right hand side.

5. Look for the Business unit that you want to switch to and click **Go to this BU**.



If your account hasn't been assigned to a business unit, an error message will appear. Please contact your administrator with primary FortiCloud account to add you into the business unit.

FortiCASB User Type Classification

There are two major types of user classification in FortiCASB:

FortiCLoud Full Access Users and **IAM Admin Users** - these type of users have full permission in FortiCASB Company and Business Unit management.

FortiCloud Limit Access Users and **IAM Read/Write Users** - these type of users have limited permissions in Company and Business Unit management.

User Permission Chart

User Type	Permission Type	Need to assign BU first in Company page	Manage Company page	Add BU in Company page	Modify Business Units	Add Applications in Business Unit
IAM user	Admin	No (It has access to all BU)	Yes	Yes	Yes	Yes
IAM user	Read/Write	Yes	No	No	No	Yes
Sub Account User	Limited	Yes	No	No	No	Yes
Sub	Full	No (It has	Yes	Yes	Yes	Yes

User Type	Permission Type	Need to assign BU first in Company page	Manage Company page	Add BU in Company page	Modify Business Units	Add Applications in Business Unit
Account User		access to all BU)				

Microsoft Entra ID Administrative Units Integration

Introduction

Microsoft Entra ID Administrative Units allow users to be grouped together with the same management scope.

Instead of monitoring all cloud account users' activities, create Microsoft Entra ID Administrative Units to define the list of users that should be monitored for user activities.

If this is your first time using Microsoft Entra ID AU Management in FortiCASB, please first update your Azure Storage account. Please see Update Azure Storage Account on page 69

Steps to monitor through Microsoft Entra ID Administrative Unit

1. Create Administrative Unit and add users on a Microsoft Entra ID account.
   Detailed instructions provided by Microsoft - https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-manage?tabs=ms-powershell
2. **Add New Microsoft Entra Administrative Unit To FortiCASB on page 32**
3. **Add Microsoft Entra ID AU to Business Unit on page 33**
4. **Apply Microsoft Entra ID Administrative Units to Cloud Account on page 36**

List of Supported Cloud Accounts

Currently, only the following cloud accounts support Microsoft Entra ID Administrative Units Integration in FortiCASB.

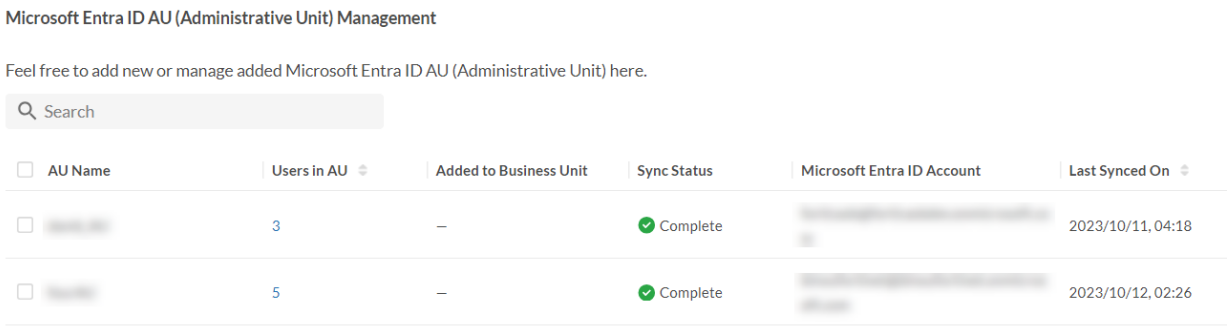
Supported Cloud Accounts
Salesforce

Supported Cloud Accounts
Office365
Box
Dropbox
Google
Jira
Webex
GitHub
Zoom
ServiceNow
Egnyte
Confluence
SAP IAS

Add New Microsoft Entra Administrative Unit To FortiCASB

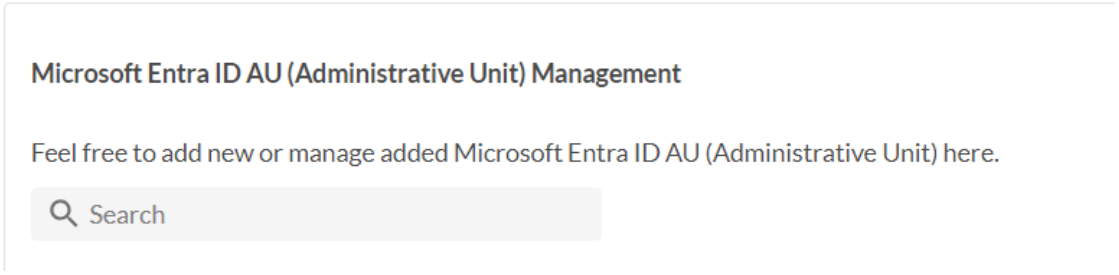
Microsoft Entra ID AU (Administrative Unit) Management

Microsoft Entra ID (formerly known as Azure AD) Administrative Unit management allows you to manage all the Microsoft Entra ID administrative units in one place and add them to different FortiCASB Business units. When a Microsoft Entra ID administrative unit is added to the Microsoft Entra ID AU Management, all users under the administrative unit will be added simultaneously.

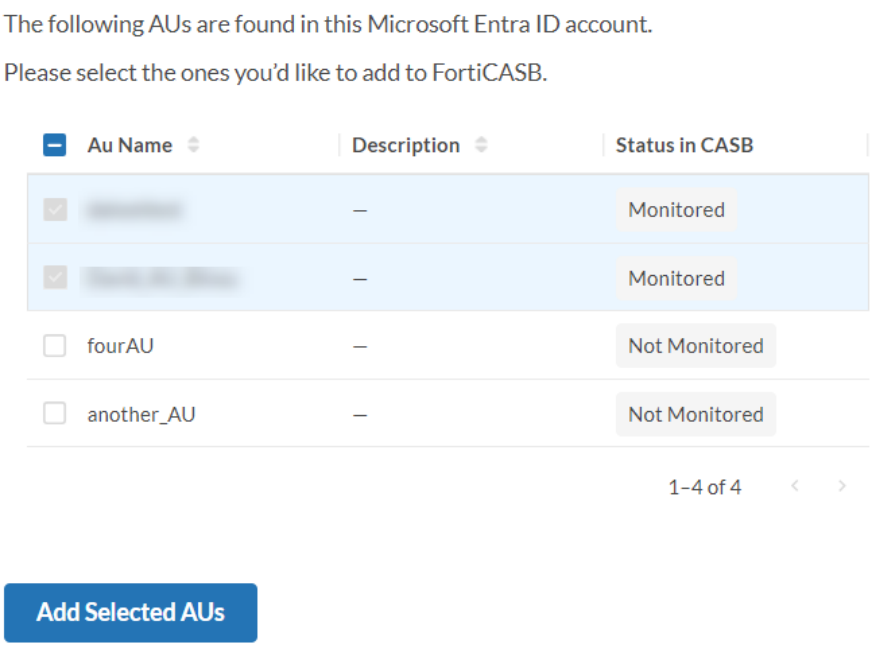


Before the Microsoft Entra Administrative Unit can be added to a FortiCASB Business unit, it needs to be added to FortiCASB first.

1. Log into FortiCASB, and click on Company button .
2. Scroll down to **Microsoft Entra ID AU (Administrative Unit) Management** and click **+ Add New**.



3. Click **Login @Microsoft Entra ID** to grant FortiCASB access to the Microsoft Entra ID account.
4. Once you sign in with your Azure admin account, you will be re-directed back to FortiCASB to select the Microsoft Entra ID Administrative Unit to be added to FortiCASB.



5. Select the administrative unit(s) to be added and click **Add Selected AUs**.
6. Click **Done** and wait for a few minutes to sync all users in those Administrative Units.

Add Microsoft Entra ID AU to Business Unit

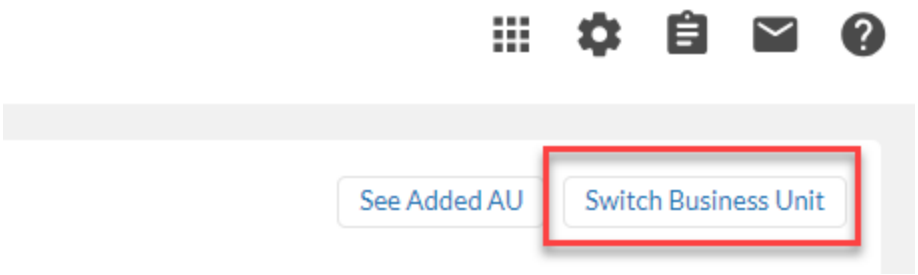
Add To BU is a feature to add Microsoft Entra ID Administrative Unit to FortiCASB Business Unit.

Steps to Add Microsoft Entra ID AU to Business Unit

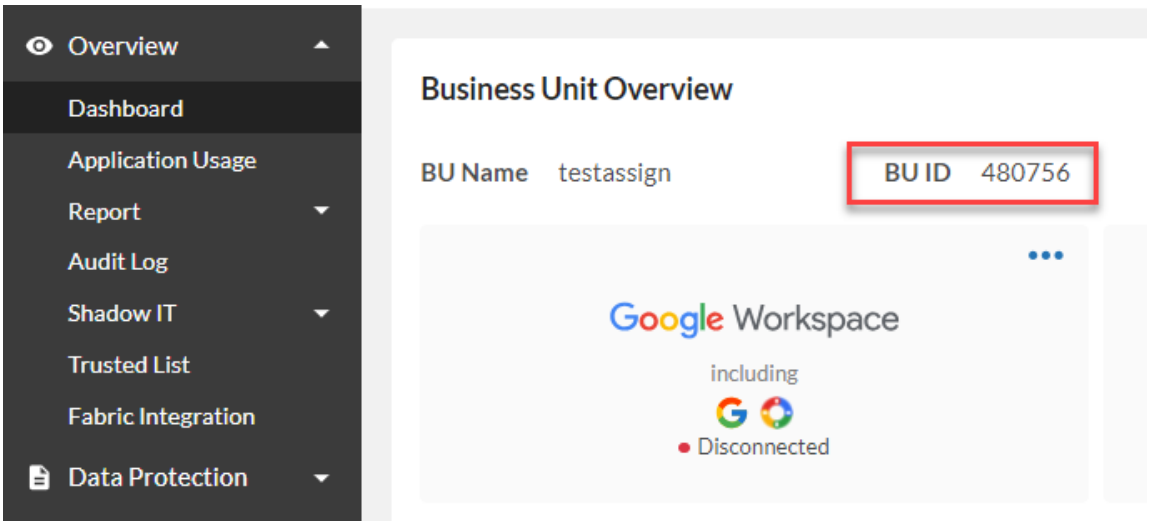
1. Obtain FortiCASB Business Unit ID

Before adding the Administrative Unit to Business Unit, first obtain the **Business Unit ID** (BU ID).

1. Switch to the Business Unit where the Administrative Unit is going to be added to.

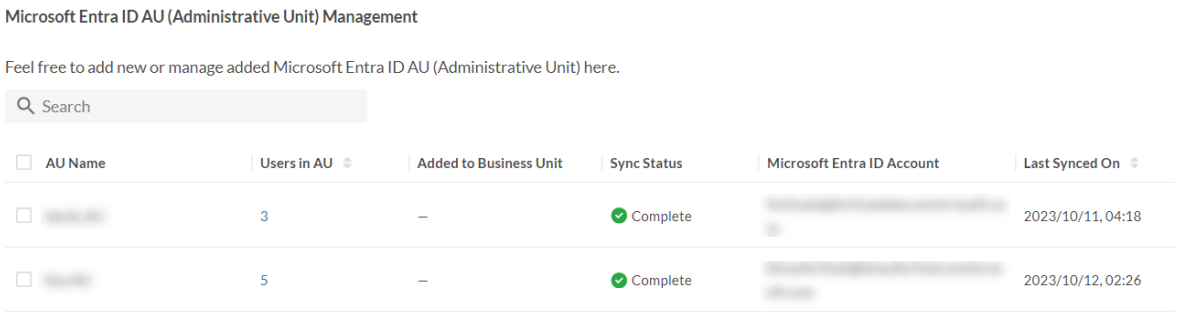


2. Record down the **Business Unit ID** located in the Dashboard.

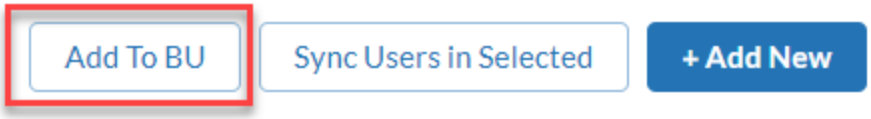


2. Add the Administrative Unit to the Business Unit

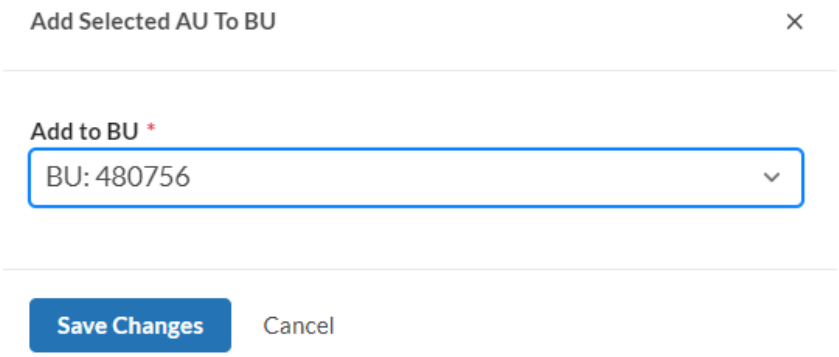
1. Go to Company Management, scroll down to **Microsoft Entra ID AU (Administrative Unit) Management**



2. Select an Administrative Unit to add from the list.
3. Click **Add To BU** to add the Administrative Unit.



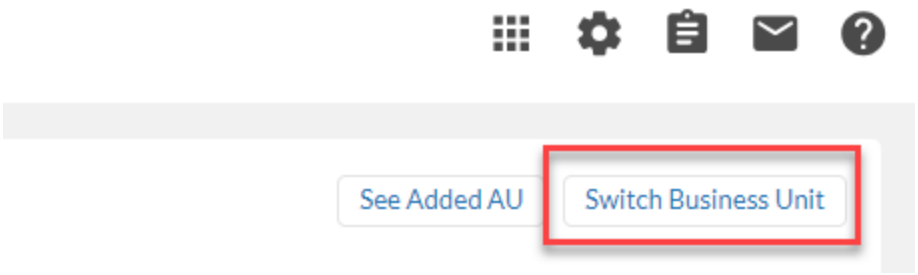
4. Click **Select BU** drop down button and select the Business Unit ID that the Administrative Unit will be added to.



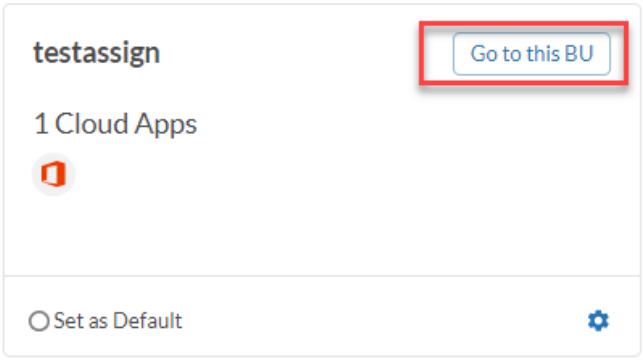
5. Click **Save Changes** to finish.

3. Check the Administrative Unit added to Business Unit

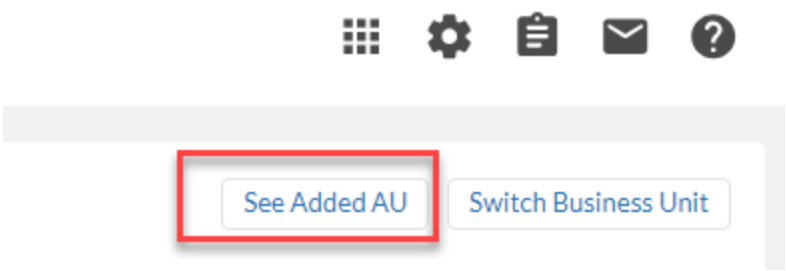
1. In FortiCASB Dashboard, click **Switch Business Unit** in the upper right corner.



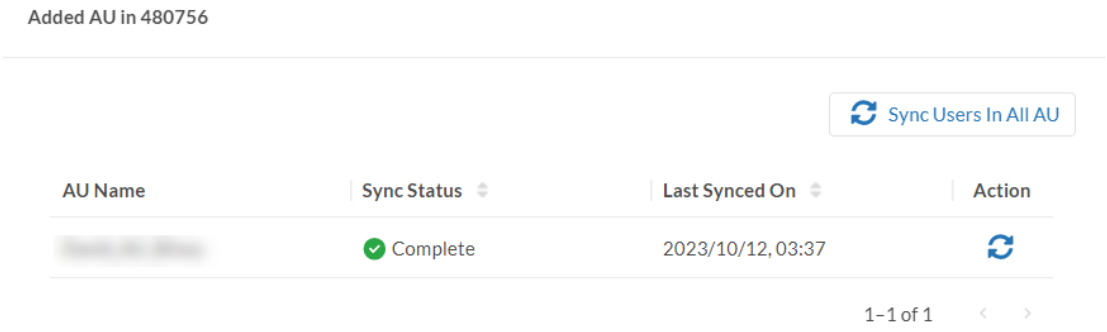
2. Scroll down to the Business Unit that the Administrative Unit is added to, and click **Go to this BU**.



3. When switched to the new Business Unit click **See Added AU** in Dashboard.



4. The newly added Administrative Unit should be in the list.



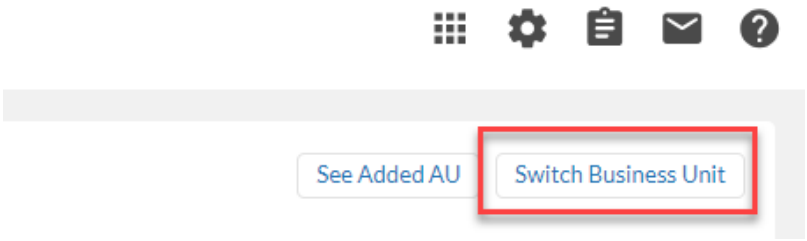
Apply Microsoft Entra ID Administrative Units to Cloud Account

After a Microsoft Entra ID Administrative Unit is added to a FortiCASB Business Unit, it is ready to be applied to the supported cloud applications in a Business Unit.

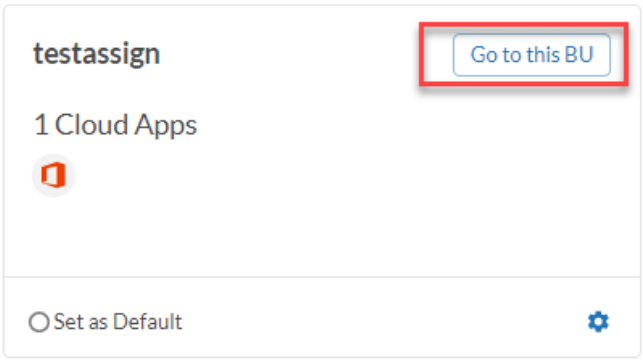
There are two methods to apply the Microsoft Entra ID administrative units - **Add** or **Update** cloud account.

Method 1 - Apply Microsoft Entra ID Administrative Units through Add Cloud Account

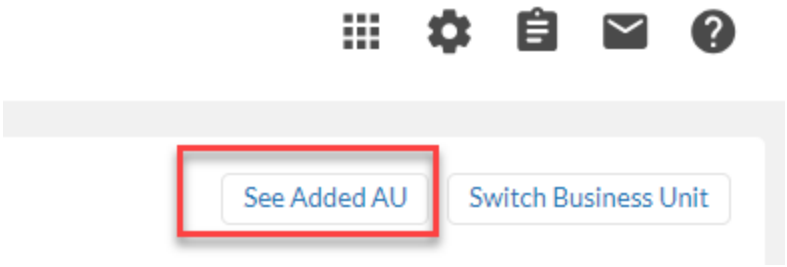
1. In FortiCASB Dashboard page, click on **Switch Business Unit**.



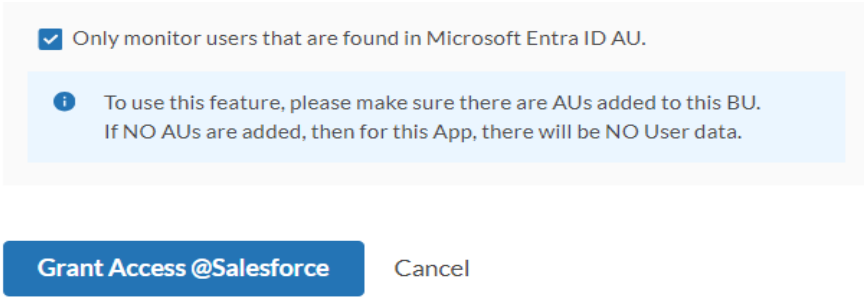
2. In **Company**, go to the Business Unit that has the Microsoft Entra ID Administrative Unit added.



3. Check the Administrative Units by clicking **See Added AU** to verify that the Administrative Units are added.



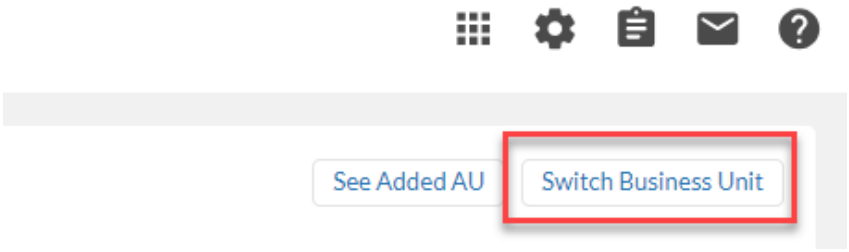
4. In **Business Unit Overview**, click **Add New** cloud account.
5. Select the supported cloud application, e.g., Salesforce, and click **Add Selected Cloud App**.
6. Click the checkbox for **Only monitor users that are found in Microsoft Entra ID AU**.



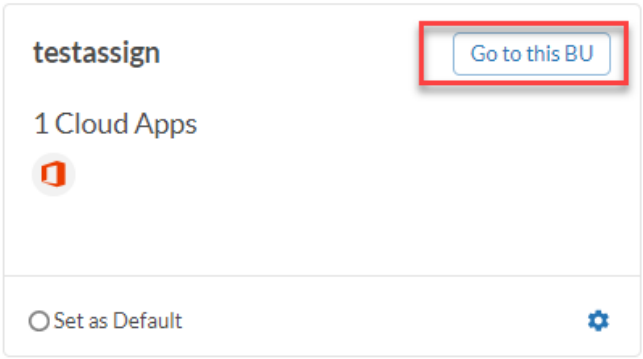
7. Continue with the rest of the Add Cloud Account steps to finish.

Method 2 - Apply Microsoft Entra ID Administrative Units through Update Cloud Account

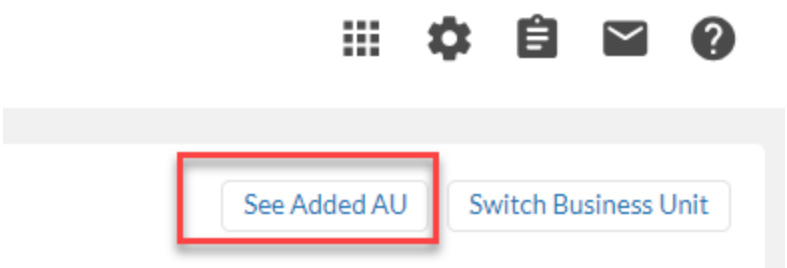
1. In FortiCASB Dashboard page, click on **Switch Business Unit**.



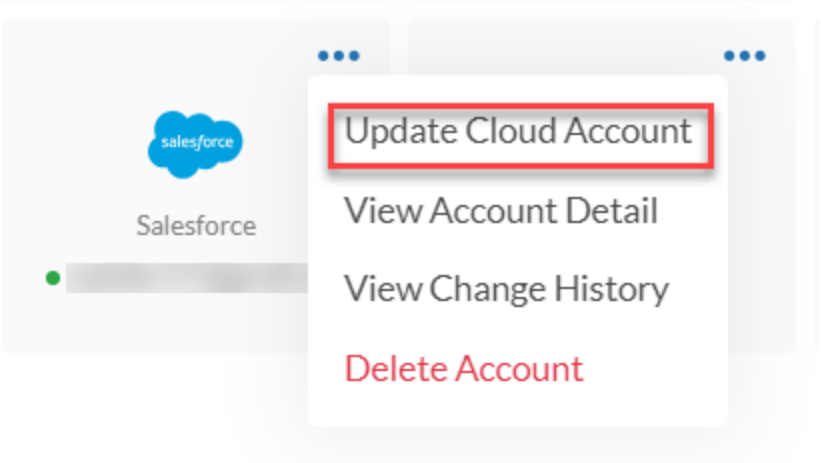
2. In **Company**, go to the Business Unit that has the Microsoft Entra ID Administrative Unit added.



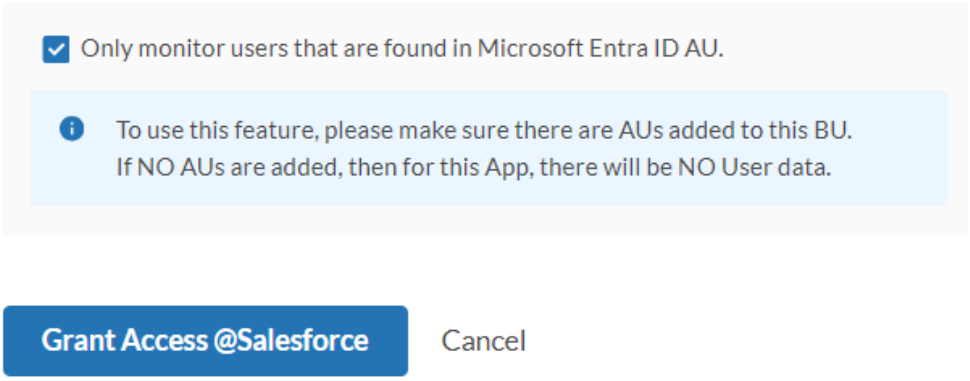
3. Check the Administrative Units by clicking **See Added AU** to verify that the Administrative Units are added.



4. In **Business Unit Overview**, Select the supported cloud application, e.g., Salesforce, and click the setting button and select **Update Cloud Account**.



5. Click the checkbox for **Only monitor users that are found in Microsoft Entra ID AU**.



6. Continue with the rest of the Update Cloud Account steps to finish.

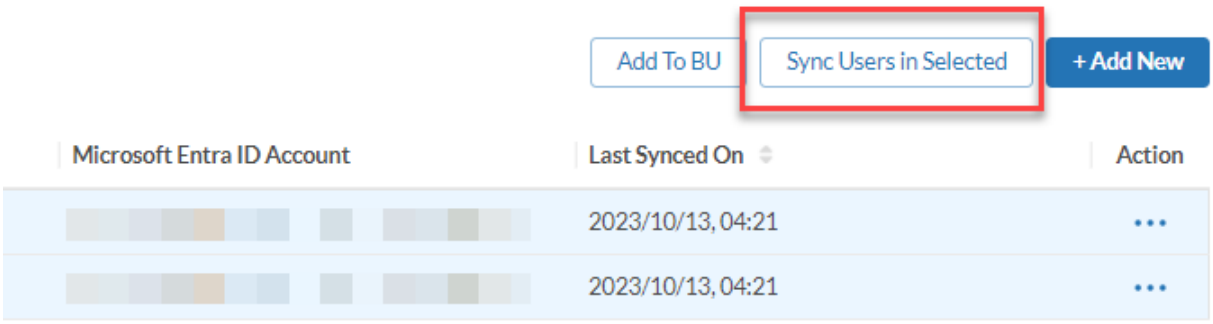
Synchronize Microsoft Entra ID Administrative Unit Users

After the Microsoft Entra ID AU (Administrative Unit) is added to FortiCASB. When users under each administrative unit is updated, the administrative unit can be manually synchronized.

There are two methods to synchronize administrative users.

1. Synchronize Microsoft Entra ID Administrative Unit users in Company

In **Company > Microsoft Entra ID AU (Administrative Unit) Management**, administrative users can select and synchronize AU units through **Sync Users in Selected** button.

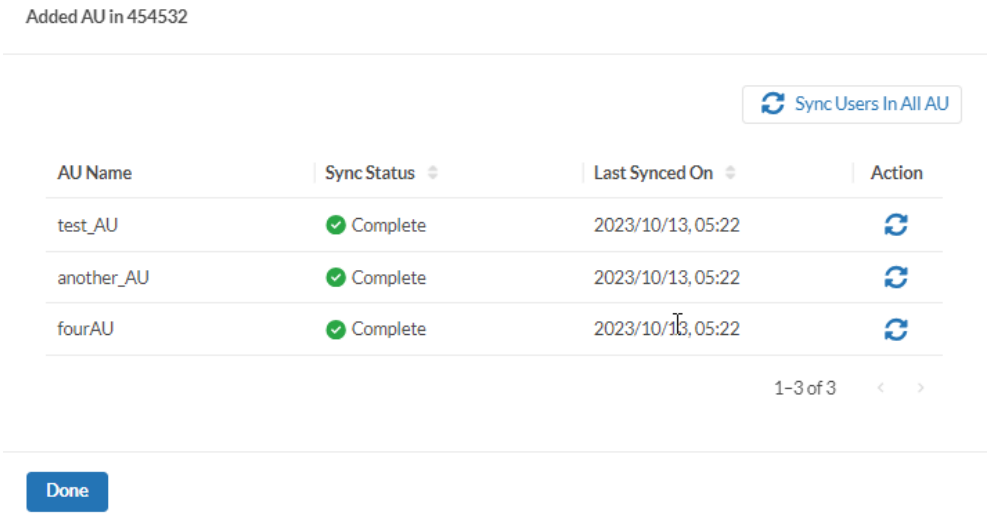


2. Synchronize All Microsoft Entra ID Administrative Units users in the same Business Unit

This method will synchronize all users in all administrative units within the same Business Unit.

1. Go to **Overview > Dashboard**
2. Click on **See Added AU** in the Business Unit.

3. Click **Sync Users In All AU** to synchronize all administrative units' users.



FortiCASB NAT IP Address

The FortiCASB NAT IP address is the public IP address that is being used to connect to your SaaS accounts or added cloud accounts. The IP address can be added to your cloud account security white list to avoid alerts being triggered when FortiCASB requests updates through API calls on the cloud accounts.

Depending on where you are located, the IP address is different for Global (US) and European Union (EU) users:

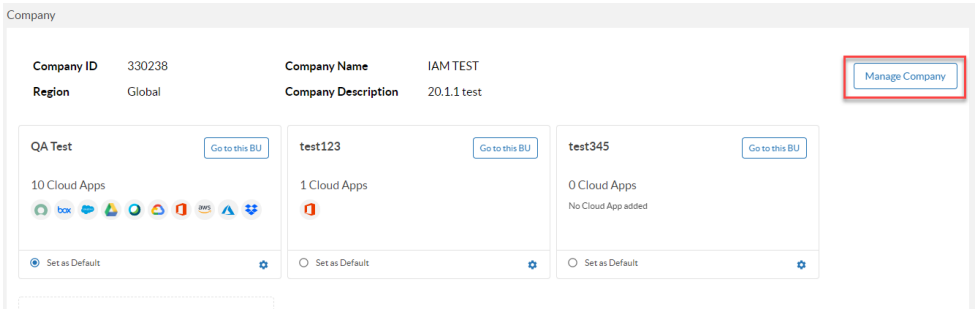
Region	FortiCASB Site Address	NAT IP Address
Global (US)	https://www.forticasb.com	52.41.24.220
European Union (EU)	https://eu.forticasb.com	34.247.192.72

Generate API Credential

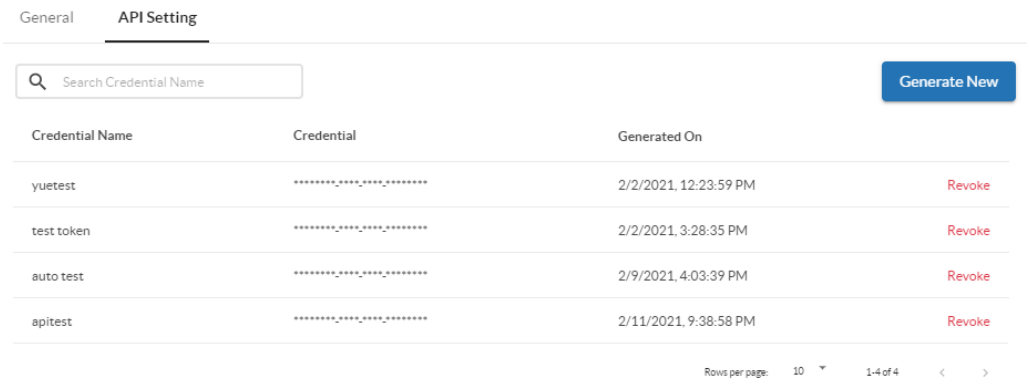
FortiCASB REST API resources are free and available for development purpose. To use these API resources, an OAuth 2.0 bearer token is required in the Authorization header. One method to get OAuth 2.0 bearer token is to call **Get Credentials Token**. Before calling Get Credentials Token API, follow the steps below to generate a credential.

1. Log into FortiCASB with your account.
2. Click on Switch Company from the top right hand side.

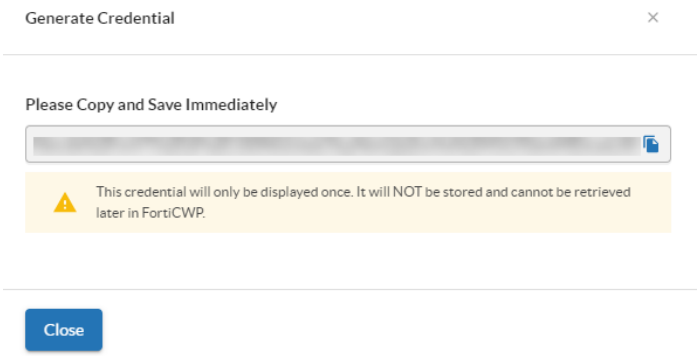
3. In Company, click **Manage Company** to access company setting.



4. Click on **API Setting** tab.
5. Click **Generate New** to generate a new API credential.



6. Enter a name for the new credential and click **Generate Credential**.
7. Copy down the credential to be used to call any FortiCASB API later.



Note: The credential will only be shown once, please keep it at a private and secured place.

The generated credential can be used repeatedly as long as it is not revoked on FortiCASB.

Cloud Application Onboarding

Both FortiCASB administrators and users can onboard the cloud applications to a business unit. Once added, all users in the business unit can view the cloud application.

AWS S3

FortiCASB offers an API-based approach, pulling data directly from AWS S3 via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track AWS S3 user activities, provides DLP Data Analysis for files stored on AWS S3.

Prerequisites

1. Account Requirement

Before adding your AWS S3 account to FortiCASB, make sure the AWS account user you use is an Administrator User. For instructions on creating an "Administrative User" in your AWS account, please refer to:

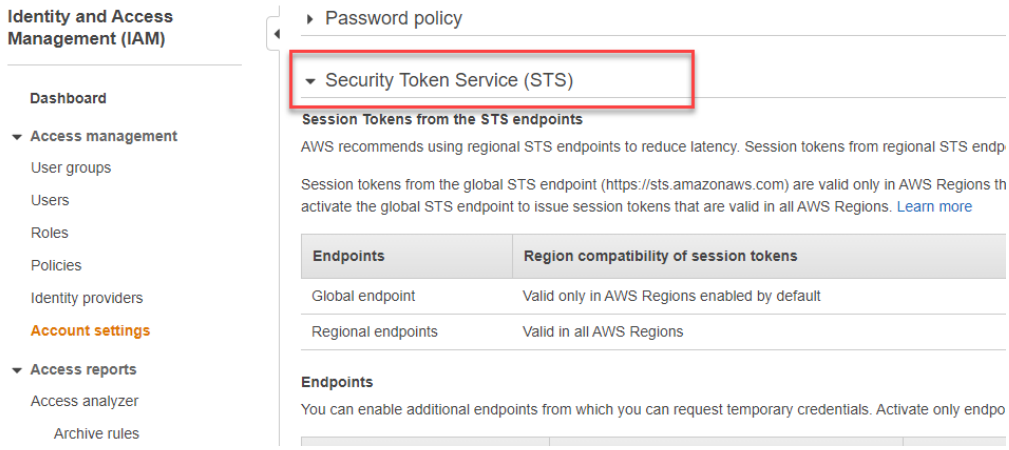
https://docs.aws.amazon.com/mediapackage/latest/ug/setting-up-create-iam-user.html

2. Activate Security Token Service (STS)

FortiCASB uses regional Security Token Service (STS) to reduce latency and provide smoother user experience.

Follow these steps to turn on Security Token Service (STS) on AWS console.

1. From your AWS console dashboard, go to **Identity and Access Management (IAM)**.
2. Click **Account settings** from the left navigation panel, and click to expand **Security Token Service (STS)**.



3. Based on your location, activate **EU (Ireland)** if you are located in European Union, otherwise, activate **US West (Oregon)**.

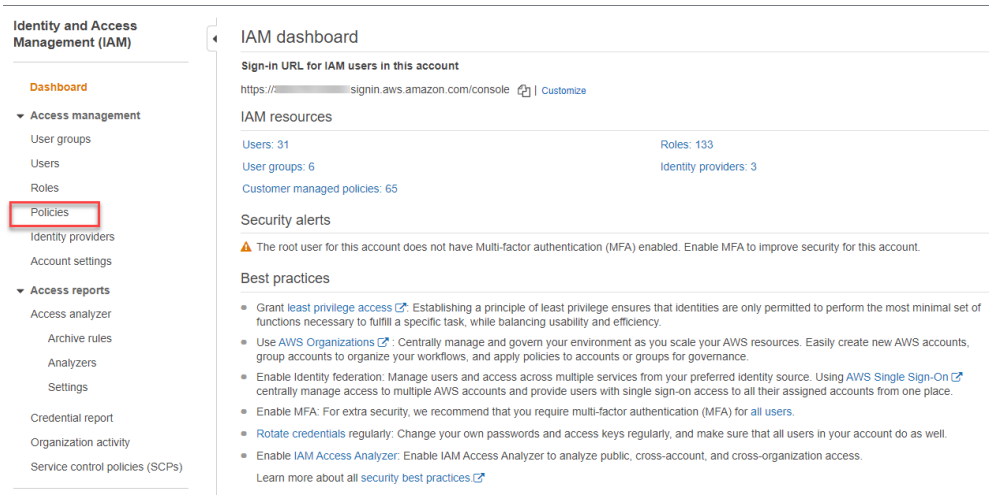
Add AWS S3 Account

Use the Administrator User to create new AWS Policy, Role, and configure the CloudTrail setting:

1. **AWS Policy Creation on page 45**
2. **AWS Role Creation on page 47**
3. **Update AWS Role External ID (optional) on page 51**
4. **AWS Configure CloudTrail Setting on page 52**
5. **Add AWS S3 Account on page 55**

AWS Policy Creation

1. Go to your AWS console dashboard, search and click **IAM**.
2. Click **Policies** from the left navigation menu.



3. Click **Create policy**, and go to **JSON** tab.
4. Replace the existing JSON code with the following:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
      "Action": [
         "s3:Get*",
         "s3:List*",
         "s3:Put*",
         "s3:Delete*",
         "s3:CreateBucket",
         "iam:List*",
         "iam:Get*",
         "cloudtrail:LookupEvent
               s",
         "cloudtrail:GetTrailStatu
               s",
         "cloudtrail:DescribeTrail
               s",
         "cloudtrail:ListTags",
         "cloudtrail:GetEventSelec
               tors",
         "config:Get*",
         "config:Describe*",
         "config:Deliver*",
         "config:List*"
      ],
      "Resource": "*",
      "Effect": "Allow"
      }
   ]
}
```

5. Click **Review policy.**
6. Name the new policy, e.g. , "forticasb_authentication".
7. Click **Create policy.**

Your new policy will be created.

Please keep your policy name later for role creation.

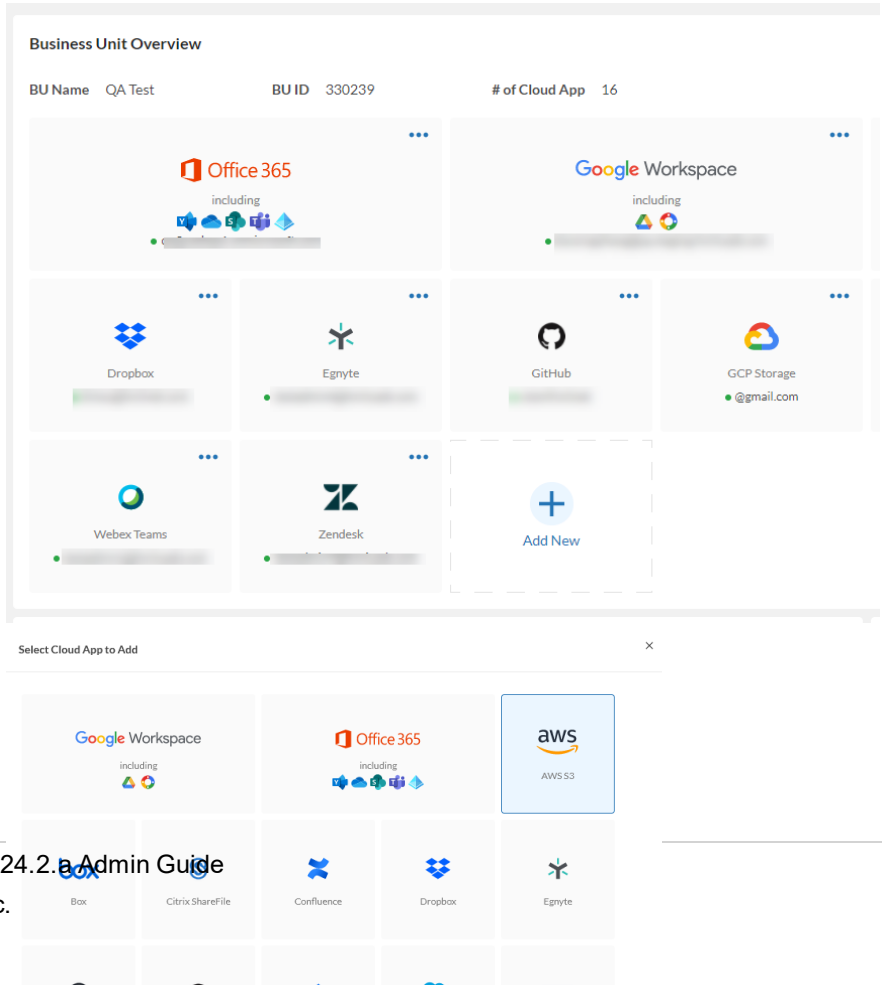
For the purpose behind the AWS services being used to create the custom policy, please refer to Appendix A - Amazon Policy Usage on page 536.

AWS Role Creation

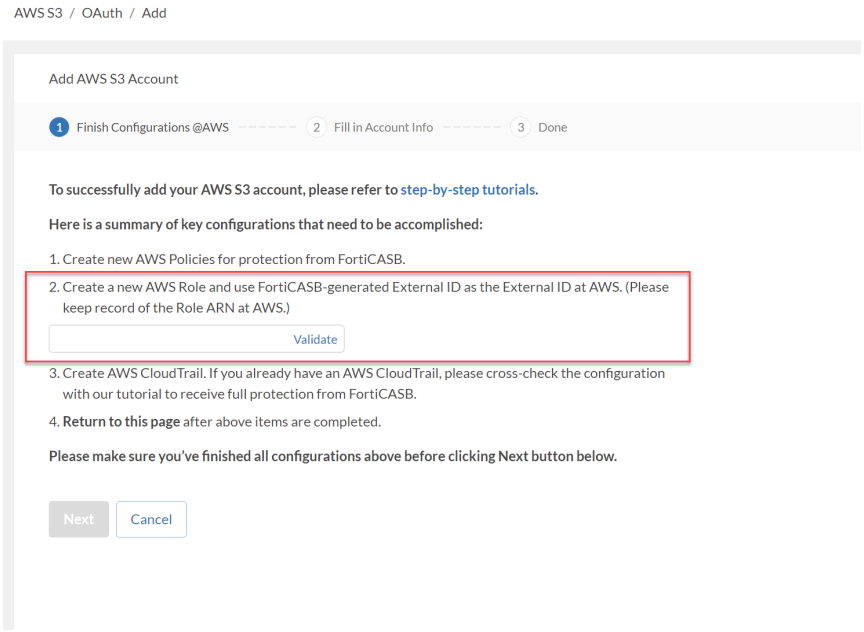
Obtain External ID from FortiCASB

Before creating an AWS Role, you will need an **external-ID** generated from FortiCASB. The External ID is an unique 32-bit token that meets AWS security requirement that protects the AWS Role.

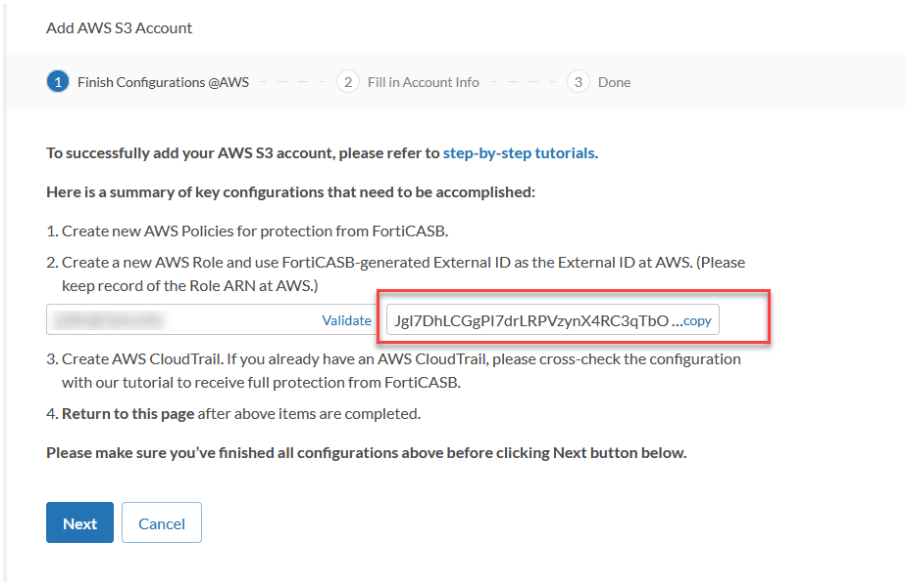
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **AWS S3**, then click **Add Selected Cloud App**.



3. Enter your AWS Account ID and click **Validate** to generate External ID for AWS role creation.



4. The external ID will be appear on the right, click **copy** to copy the 32-bit external ID token.

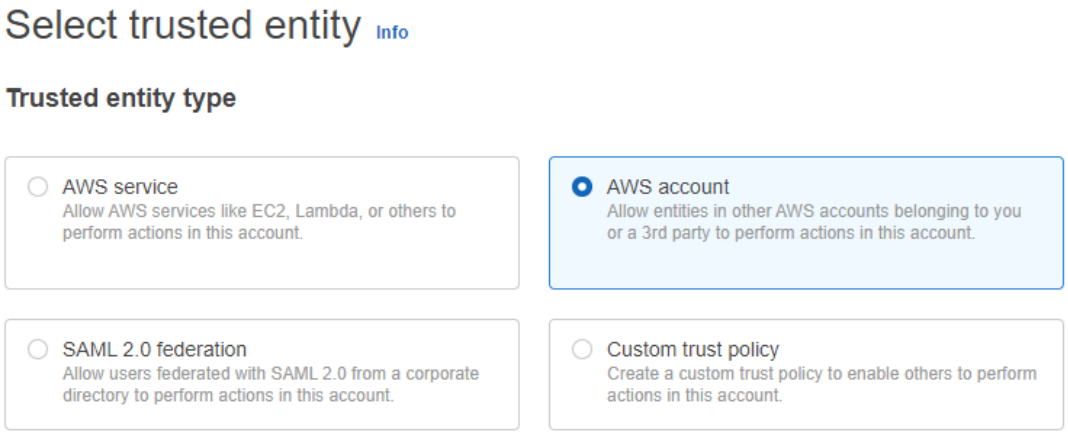


If you already have an AWS Role associated with FortiCASB, and only need to update the External ID. Please refer to Update AWS Role External ID (optional) on page 51

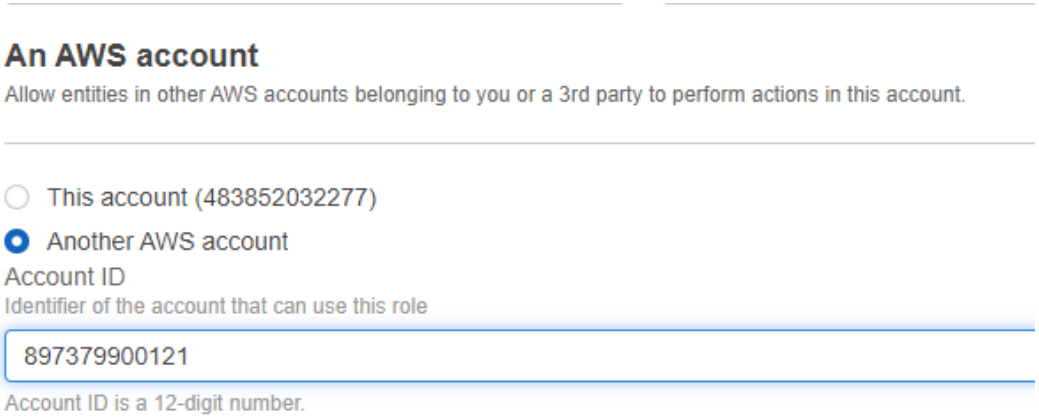
Create AWS Role.

1. Click **Roles** from the menu on the left.
2. Click **Create role**.

3. In Select trusted entity, select **AWS account.**

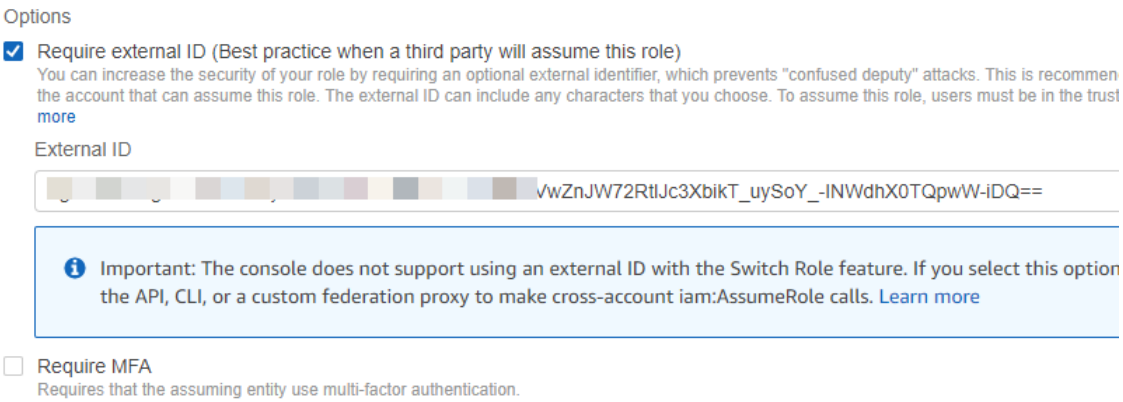


4. Choose Another AWS account, and enter the following Account ID: 897379900121.



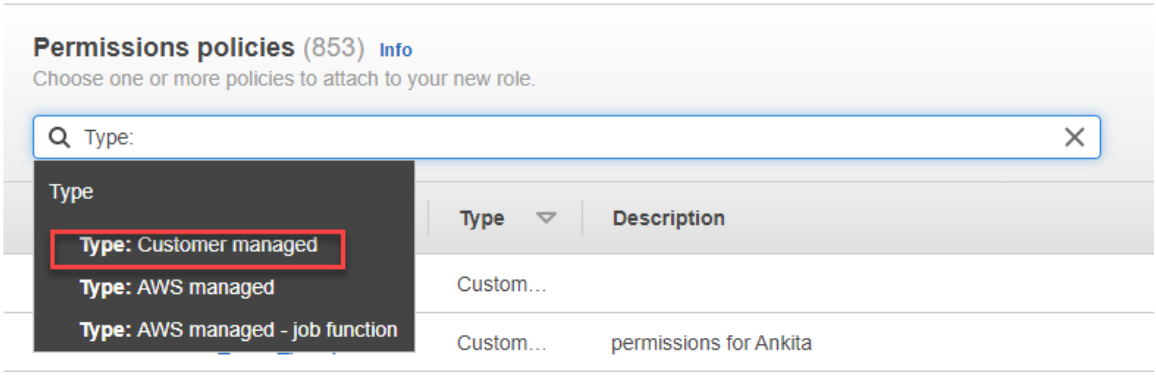
Note: This is the Amazon AWS account that FortiCASB uses to monitor the new role that is being created.

5. Select the box **Require external ID** and enter in the **External ID token** generated earlier.

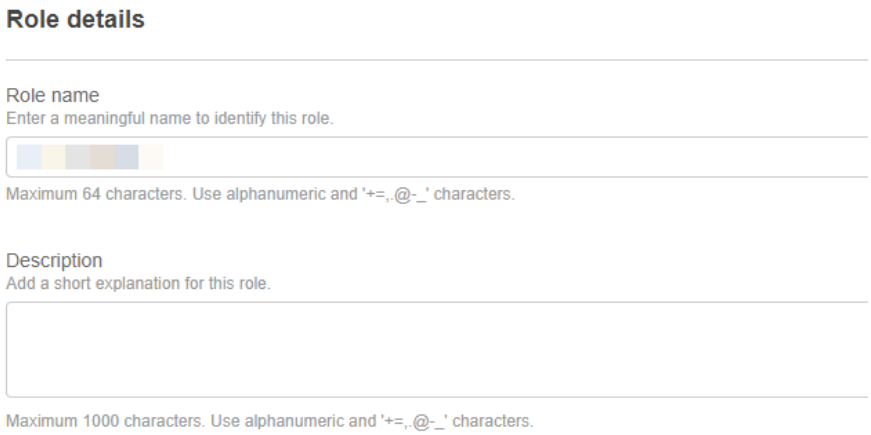


The External ID token must be the one generated earlier through FortiCASB using the same AWS account. If the External ID is not generated from FortiCASB, the AWS account cannot be added to FortiCASB.

6. Make sure the box **Require MFA** is not selected. Click **Next** to continue.
7. Click **Filter**, select **Type**, and then select **Type: Customer managed**.

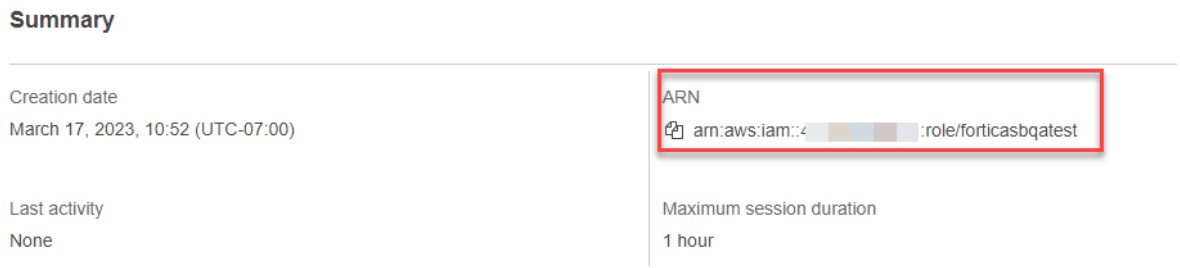


8. Select the policy you created earlier.
9. Click **Next**.
10. Enter a role name of your preference.



11. Click **Create role**.
12. Click the role name created, and copy the **AWS Role ARN**.

Example of AWS Role ARN: arn:aws:iam::123456123456:role/FortiCASBTester



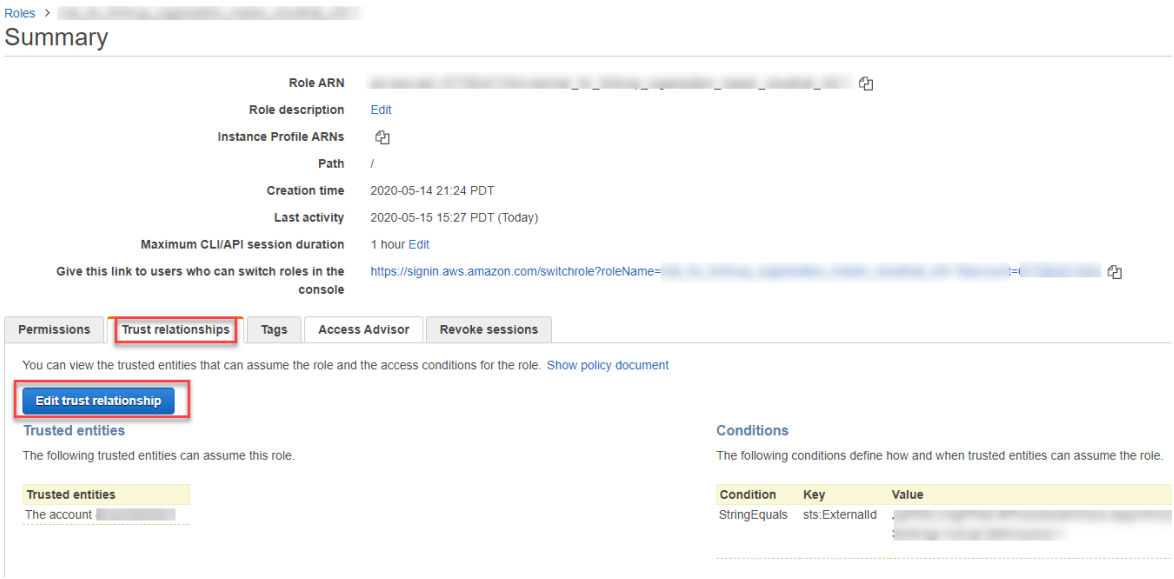
Please keep the AWS Role ARN later for AWS authentication during installation.

Update AWS Role External ID (optional)

If you have previously created an AWS role, you will only need to update the old External ID to the new FortiCASB generated 32-bit External ID token without creating a new AWS role.

Follow the steps below to update the External ID:

1. Log into your AWS account portal using your **Administrator User**.
2. Search and click on **IAM** (Manage Access to AWS resources) from the AWS portal page.
3. Click on **Roles**, search and click on the AWS Role you created for adding the AWS S3 account to FortiCASB.
4. Click **Trust Relationships** tab and click on **Edit trust relationship**.

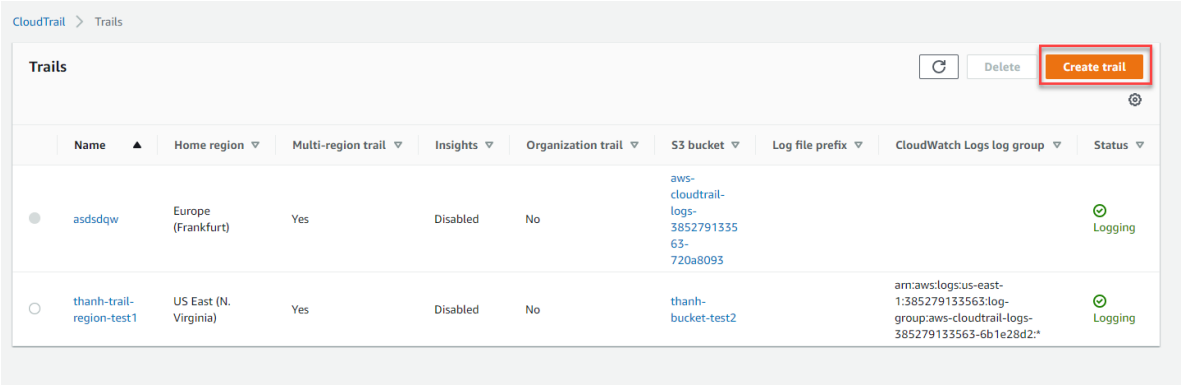


5. Replace the External ID value in the line "**sts:ExternalId**" with the FortiCASB generated 32-bit External ID.

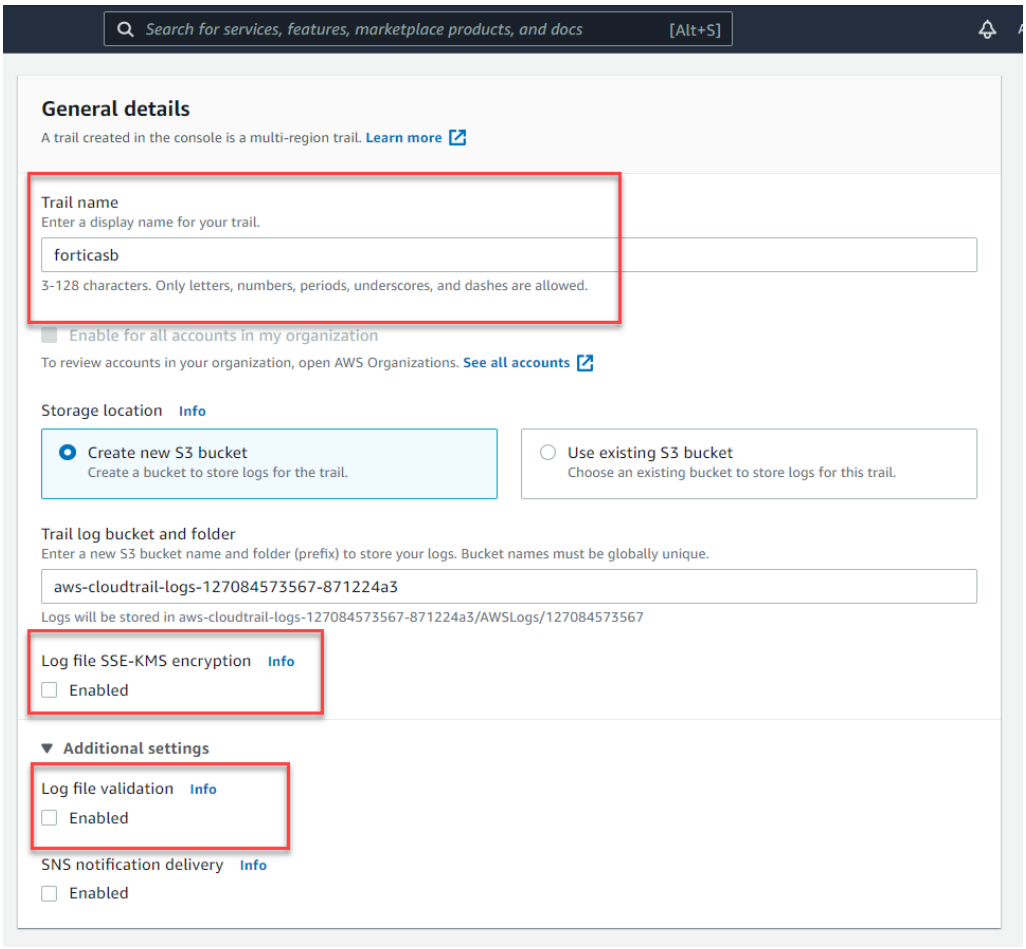
6. Click **Update Trust Policy** to finish updating the External ID.

AWS Configure CloudTrail Setting

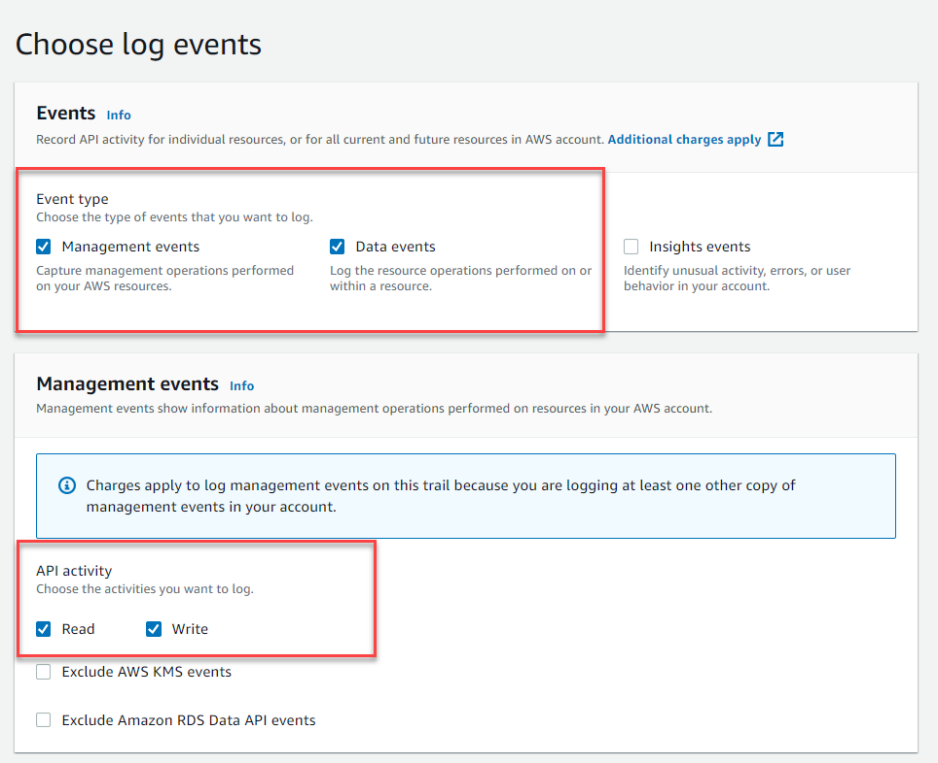
1. From AWS console dashboard, search and go to "**CloudTrail**"
2. Click on **Trails** in the left navigation pane, and click **Create trail**.



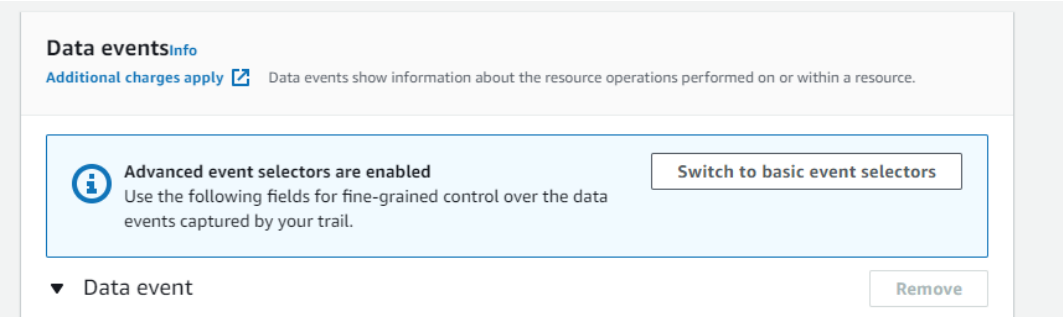
3. In **General details** page, enter a **Trail name** based on your preference, keep the default selection to **Create a new S3 bucket.**



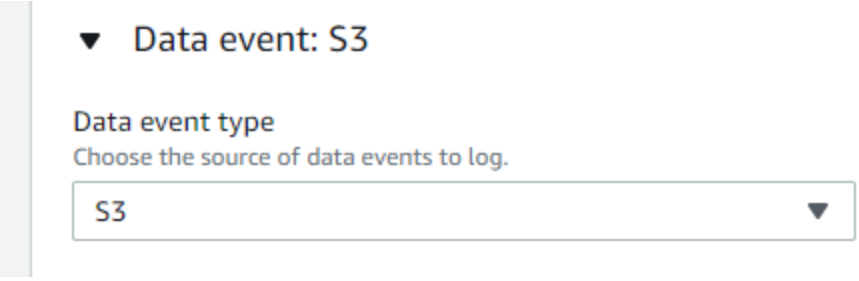
4. **Uncheck** the options to enable **Log file SSE-LMS encryption** and **Log file validation**.
5. Scroll down and click **Next** to continue.
6. In **Choose log events**, **Events** > **Event type**, select **Mangement events** and **Data events** types.



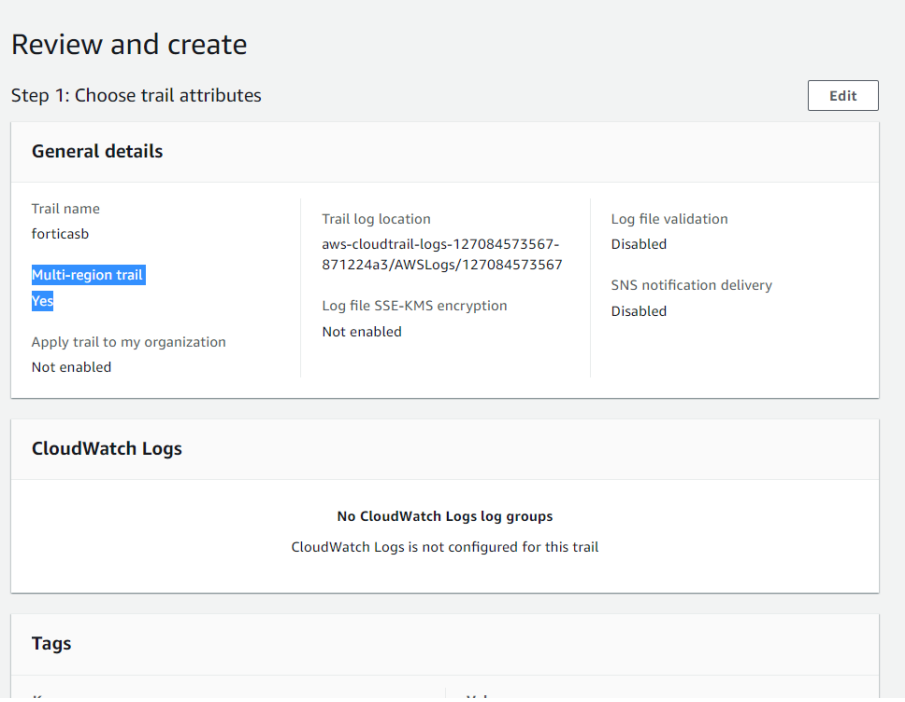
7. In **Manage events** > **API activity**: keep **Read** and **Write** options selected.
8. In **Data events**, click **Switch to basic event selectors**.



9. In **Data event source**, select **S3**, then click **Next**.



10. Review the trail settings, make sure it is configured as **multi-region trail**, scroll down and click **Create Trail**.

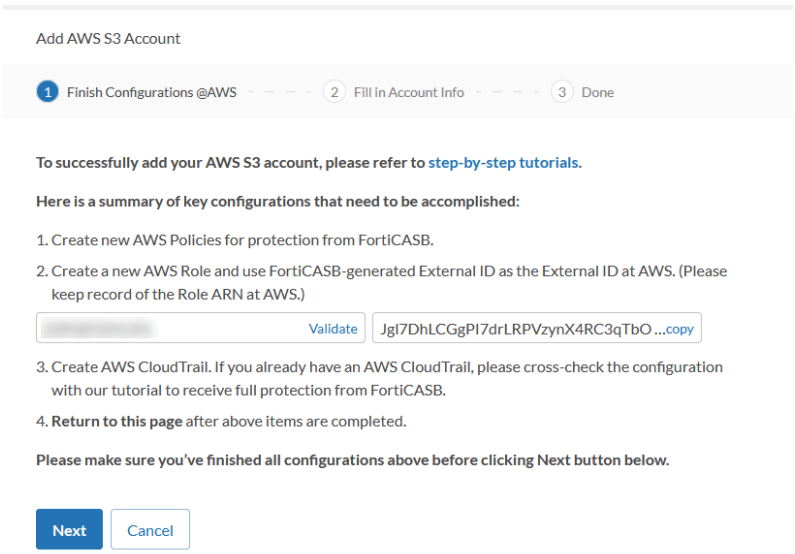


You have finished all the preliminary steps to add your AWS account. Now go back to FortiCASB and click **Next**.

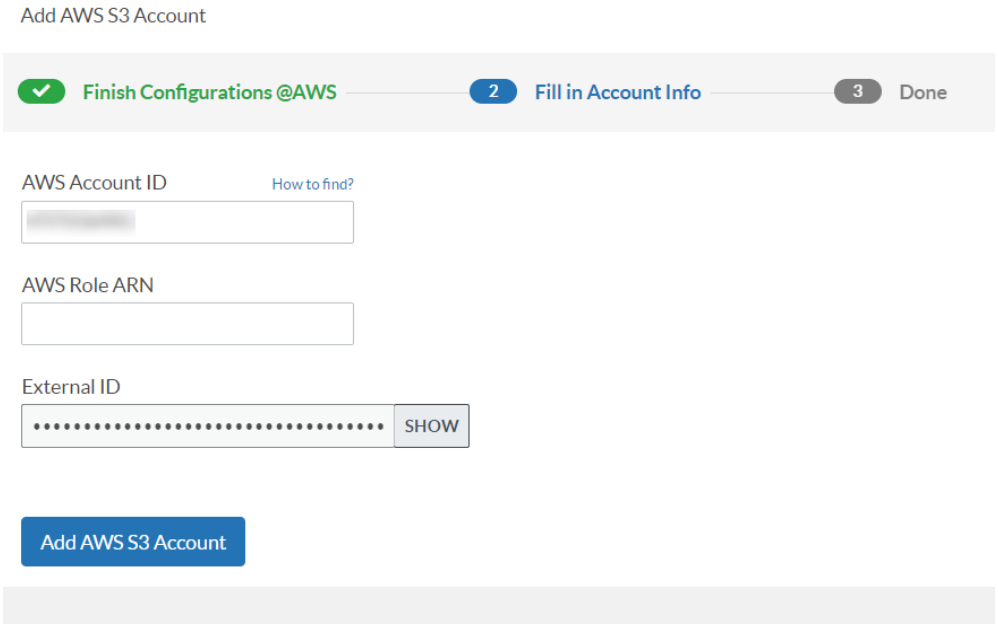
Add AWS S3 Account

After all the AWS S3 configurations are completed from previous sections, follow these steps to add your AWS S3 account on FortiCASB.

1. Go back to **Add AWS S3 Account** page, review the key configurations list to see if they are completed, then click **Next**.



2. Enter the "AWS Role ARN" from the AWS CloudTrail Configuration that you have completed earlier.



3. Click **Add AWS S3 Account** to complete adding the account.

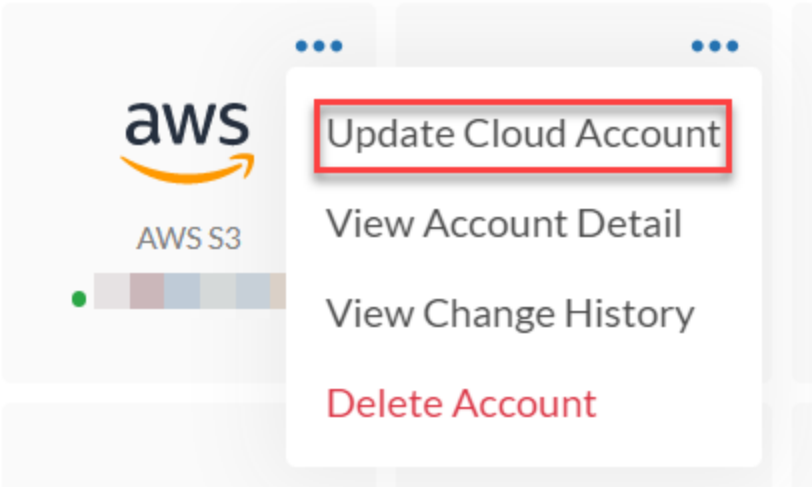
Update AWS S3 Account

Before updating the AWS S3 account on FortiCASB, use the AWS Administrator User to complete the same AWS configurations.

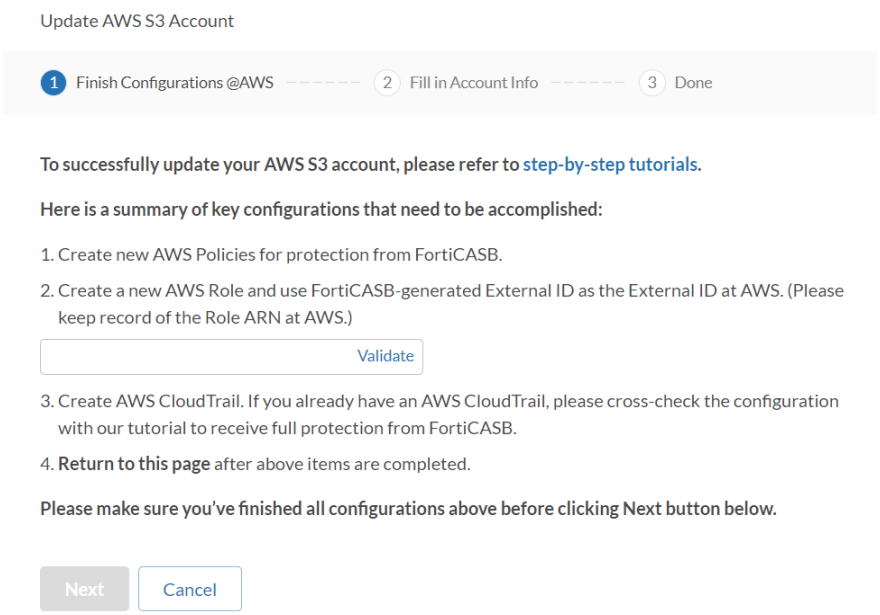
1. **AWS Policy Creation on page 45**
2. **AWS Role Creation on page 47**
3. **Update AWS Role External ID (optional) on page 51**
4. **AWS Configure CloudTrail Setting on page 52**

After all 3 steps are completed, go back to FortiCASB to finish updating the AWS S3 account.

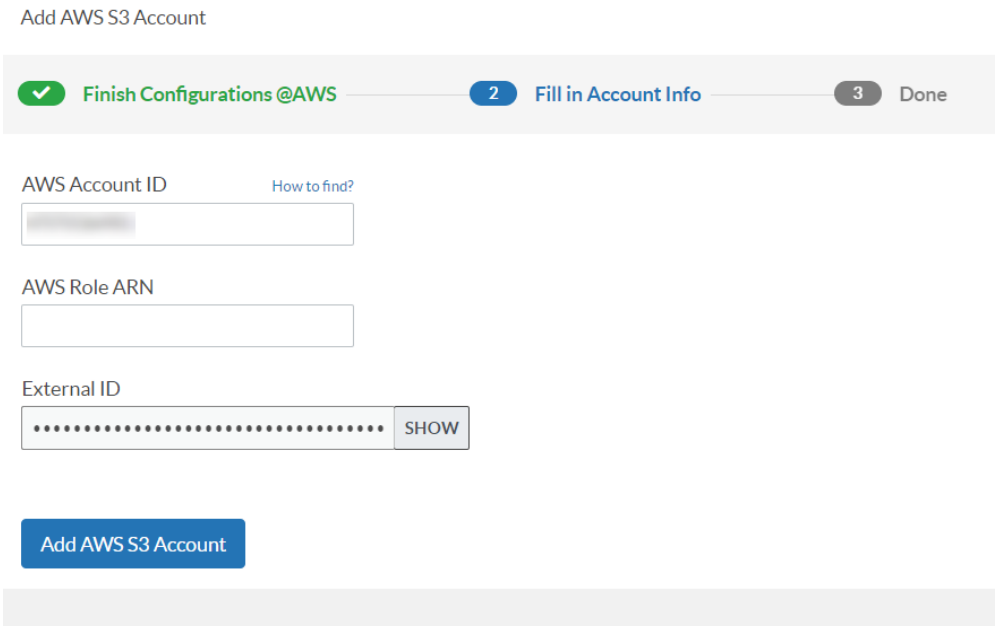
1. In FortiCASB, go to **Overview > Dashboard**.
2. Click on the AWS S3 account menu and select **Update Cloud Account**.



3. At the **Update AWS S3 Account** page, review the key configurations list to see if they are completed, then click **Next**.



4. Enter the "AWS Role ARN" from the AWS CloudTrail Configuration that you have completed earlier.



5. Click **Update AWS S3 Account** to complete Updating the account.

Azure Storage

FortiCASB offers an API-based approach, pulling data directly from Azure Storage via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Azure Storage user activities, provide DLP Data Analysis for files on Azure Storage.

Prerequisites

You may use an existing **Azure AD** account or create a new account. If you create a new account, wait for at least 24 hours for the new account to take effect before granting access to FortiCASB.

Make sure the user account that will be used on FortiCASB has a **Global Administrator role** or **Cloud Application Administrator + Global Reader roles**.

You will also need to set up the Azure AD Privileged Identity Management application. For more information on how to do so, go to:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure.

FortiCASB supports all types of Azure AD licenses. However, depending on the features supported by the Azure AD license, FortiCASB will only integrate features available to that license. For example, a free Azure AD license does not include sign-in activity report, thus FortiCASB cannot provide sign-in activities from the free Azure AD account.

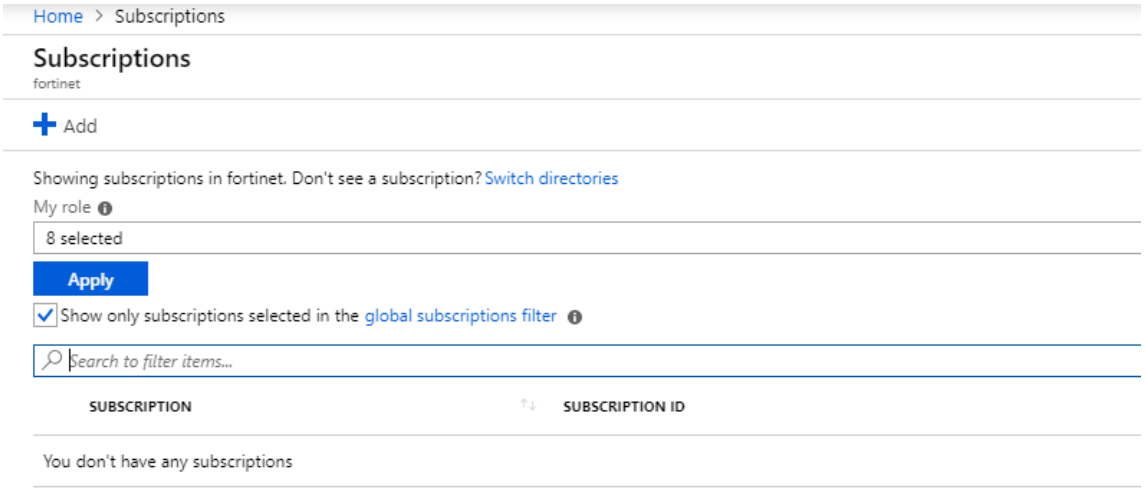
Follow each section below to help you setup the Azure Subscription, Roles, and configure the Blob Storage in preparation to add the Azure Subscription to FortiCASB:

1. **Setup Azure Subscription on page 60**
2. **Add Reader role to the Subscription on page 61**
3. **Add Reader roles to multiple subscriptions simultaneously (optional) on page 62**
4. **Collect Subscription and Tenant IDs on page 64**
5. **Setup Blob Storage on page 65**
6. **Enable Blob Log Monitoring on page 66**
7. **Setup Storage Blob Data Reader on page 67**
8. **Add Azure Storage Account on page 68**

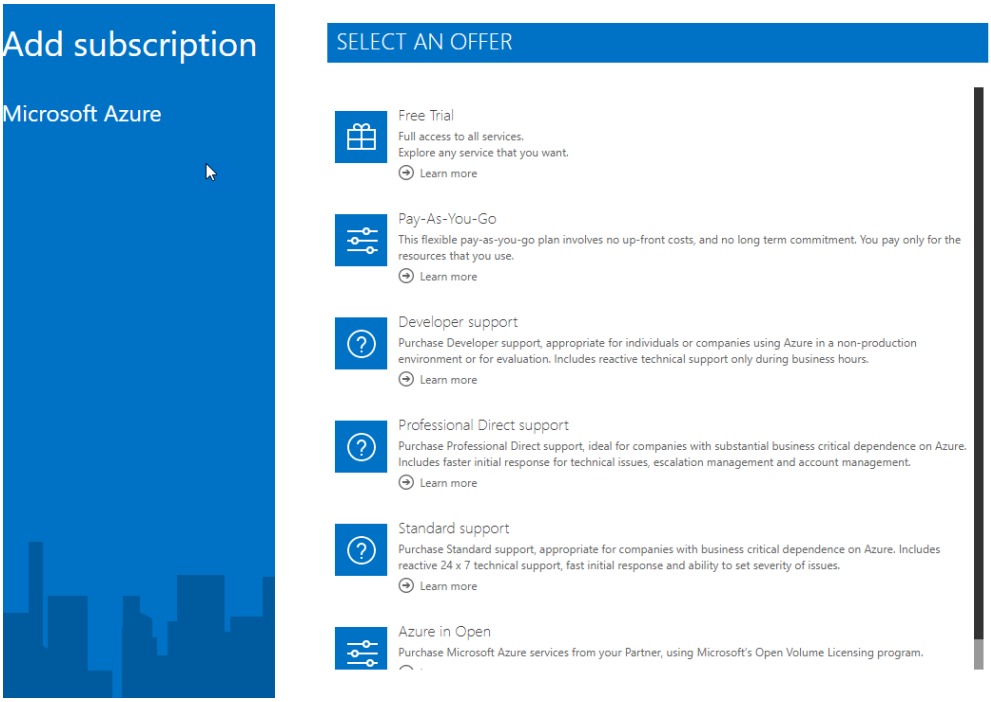
Setup Azure Subscription

Once you have your Azure license ready, you will need a subscription ID to use FortiCASB. If you do not have a subscription yet, please follow these steps:

1. Log into the Azure Portal using your Azure account.
2. Search and click on **Subscriptions**.
3. Click on **+Add** button to add a subscription.



4. Select the subscription desired and complete the rest of the billing steps.

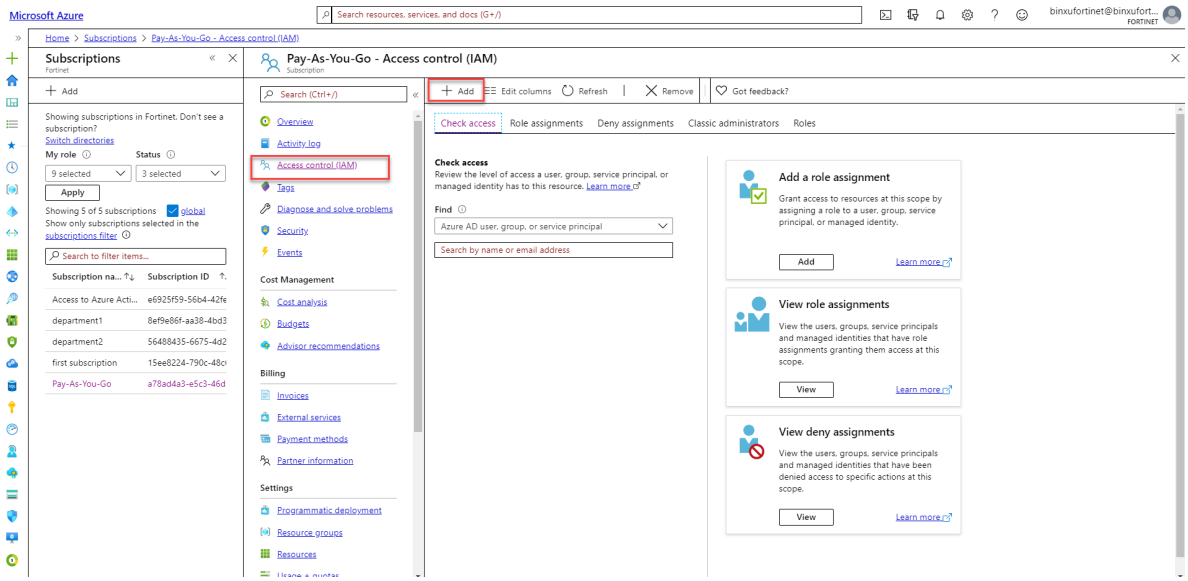


Note: You will need a minimum of "Pay-As-You-Go" subscription to use FortiCASB.

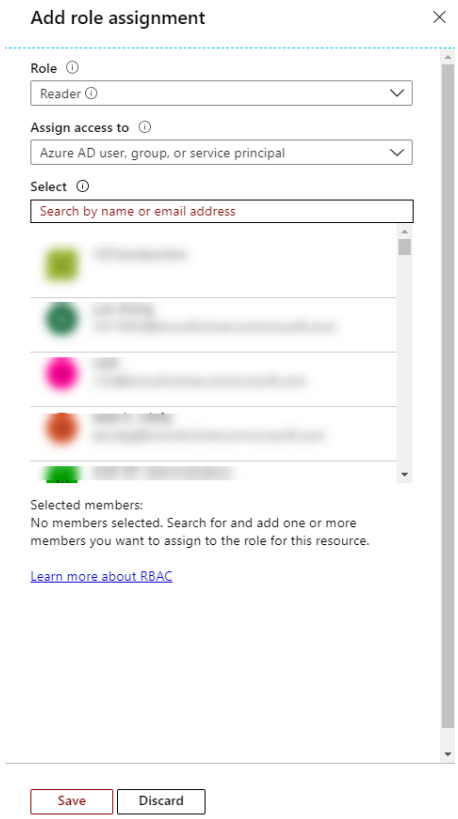
Add Reader role to the Subscription

Add a Reader role to the Subscription that is going to be added FortiCASB. The purpose is to provide FortiCASB with read access to the resources under the Subscription.

1. Search and click on **Subscriptions**.
2. Click on the Subscription that is going to be used on FortiCASB.
3. In the Subscription menu, click on **Access control (IAM)**.



4. Click on **+Add** and select **Add role assignment**.
5. In **Add role assignment** drop down menu, click on **Select a role** and select **Reader**.
6. Leave **Assign access** to as **User, group, or service principal**.



7. In Select field, search and select a member (user account) that will be associated with the role.

The member (user account) should have a **Global Administrator role** or **Cloud Application Administrator + Global Reader roles**.

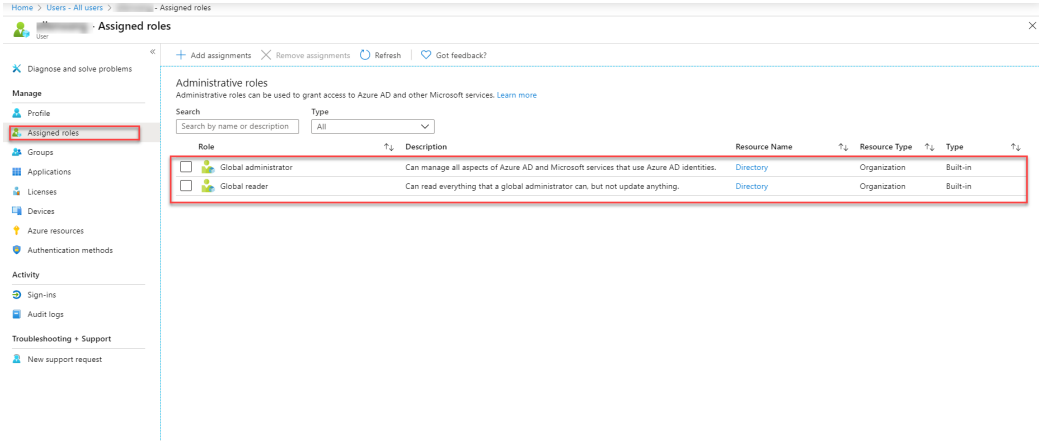
8. Click **Save** to finish creating the Reader role.

Add Reader roles to multiple subscriptions simultaneously (optional)

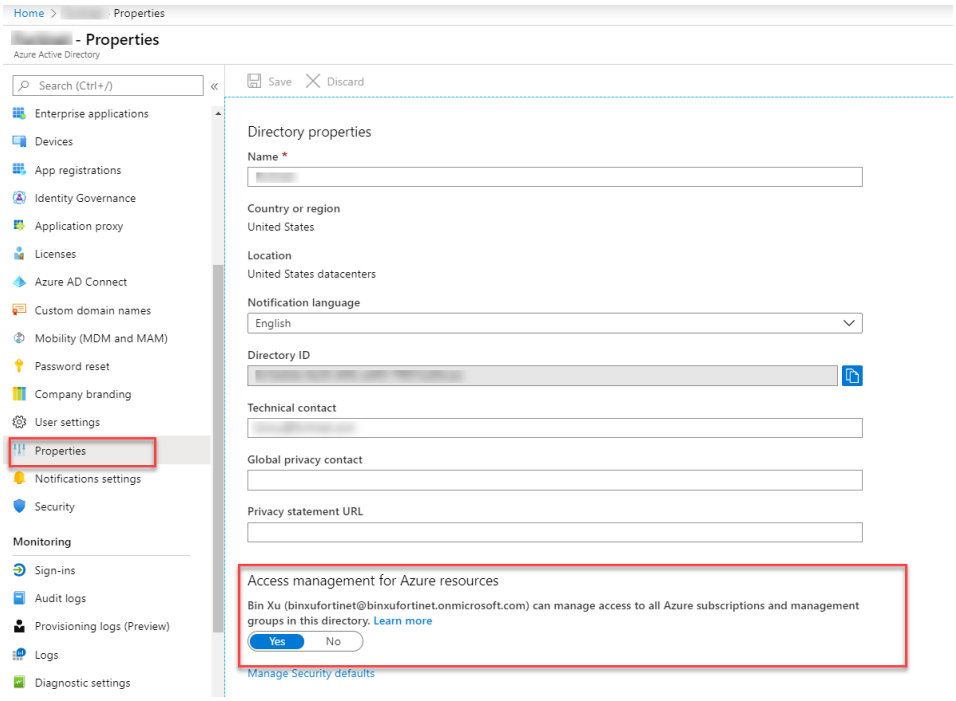
To add multiple subscriptions to FortiCASB with one user account simultaneously, follow these steps to configure the subscriptions with read access. If the user account has **Global Administrator role**, only do step 6-9.

1. Log in to Azure portal as the master account user.
2. In the search field, search and click on "users".
3. Click on the user that will be used when adding the Subscriptions to FortiCASB.
4. In the middle Profile navigation menu, click on **Assigned roles**.

5. Click +**Add assignments** to add **Global reader role** and **Global Administrator role** to the user. (Global Administrator role will be removed later)



6. Log out of the master account user, and log back in as the user whom the new roles are assigned to.
7. Search and click on "Azure Active Directory".
8. In the middle Azure Active Directory navigation menu, click on **Properties**.
9. Click **Yes** under **Access management for Azure resources**, and click **Save**. This step allows the user to manage access of all Subscriptions under the Azure account.



10. Log out of the user account, and log back in as the master account.
11. Follow the steps 2-4 above, and remove the **Global administrator role**.

Now all the Subscriptions under the user account have Reader role, and you can add multiple Azure Subscriptions at the same time.

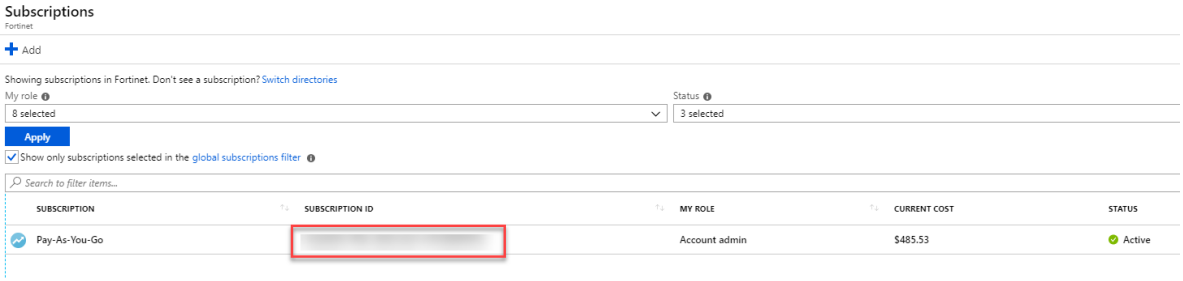
Collect Subscription and Tenant IDs

For Azure Authentication during installation, please find and record down Azure **Subscription ID** and **Tenant ID**.

View Subscription ID

To view your subscription ID after you have setup subscription, please follow these steps:

1. From the portal page, search and click on **Subscriptions**.
2. Once Subscriptions page opens, record down the **subscription ID**.

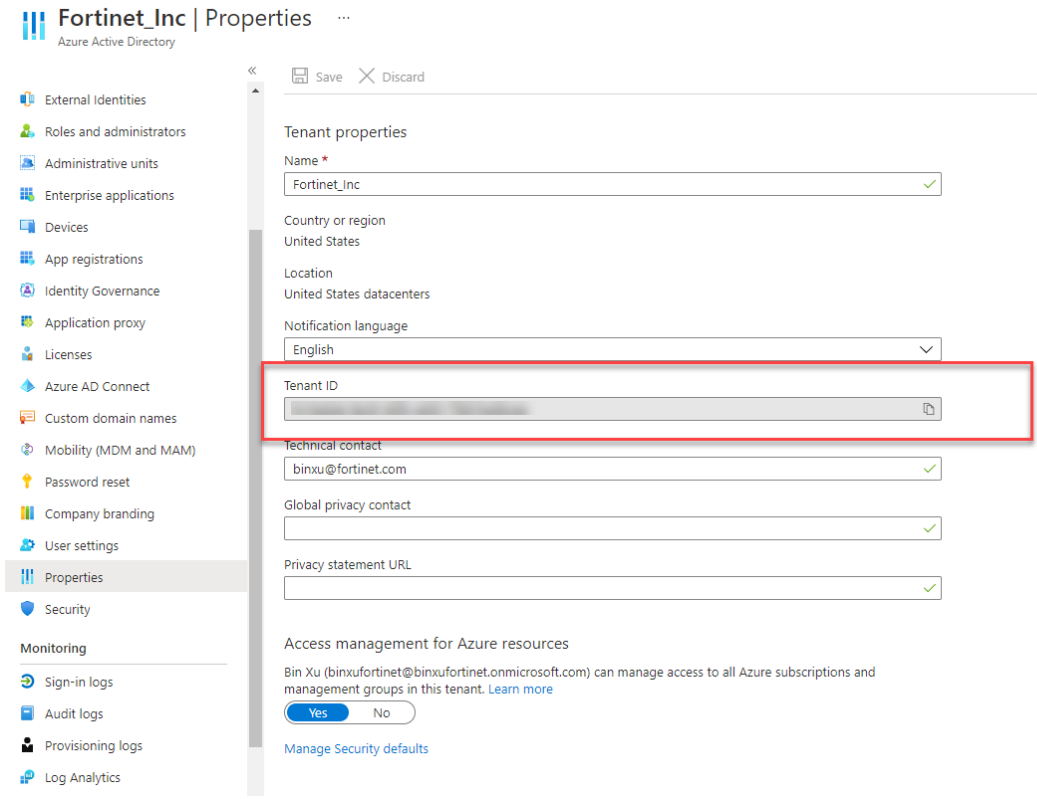


View Tenant ID

Obtain **Tenant ID** following the steps below:

1. From the portal page, search and click on **Azure Active Directory**.
2. Click on **MANAGE > Properties**.

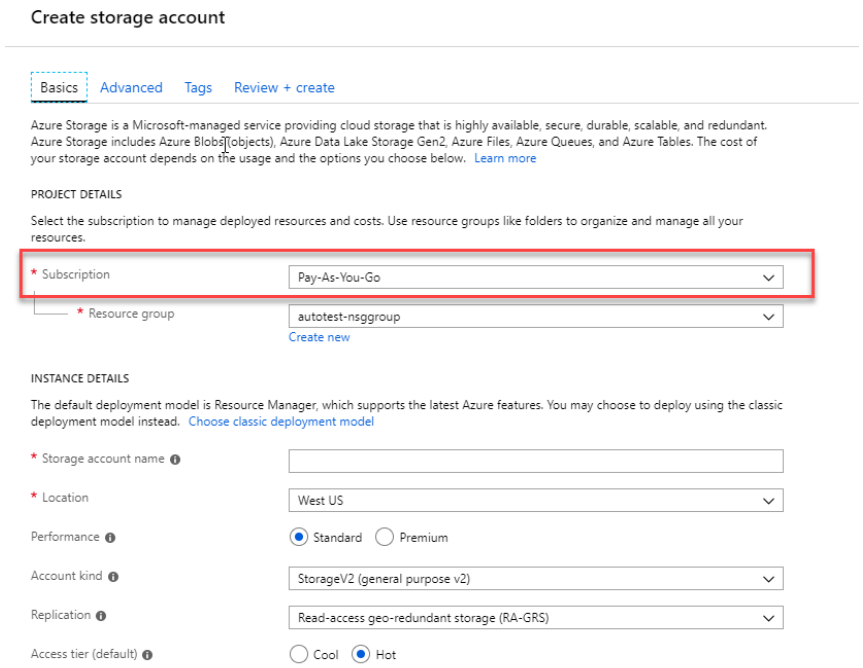
3. Under **Directory properties**, you will find Tenant ID.



Setup Blob Storage

An Azure storage account with blob log monitoring enabled is required to before adding the account FortiCASB. If you do not have a storage account yet, please follow the steps below to create a storage account:

1. From the portal page, search and click on **storage accounts**.
2. Click **+Create** to create a storage account.
3. In **Basics** tab, under **Project details**, select the subscription that is linked to your subscription ID.



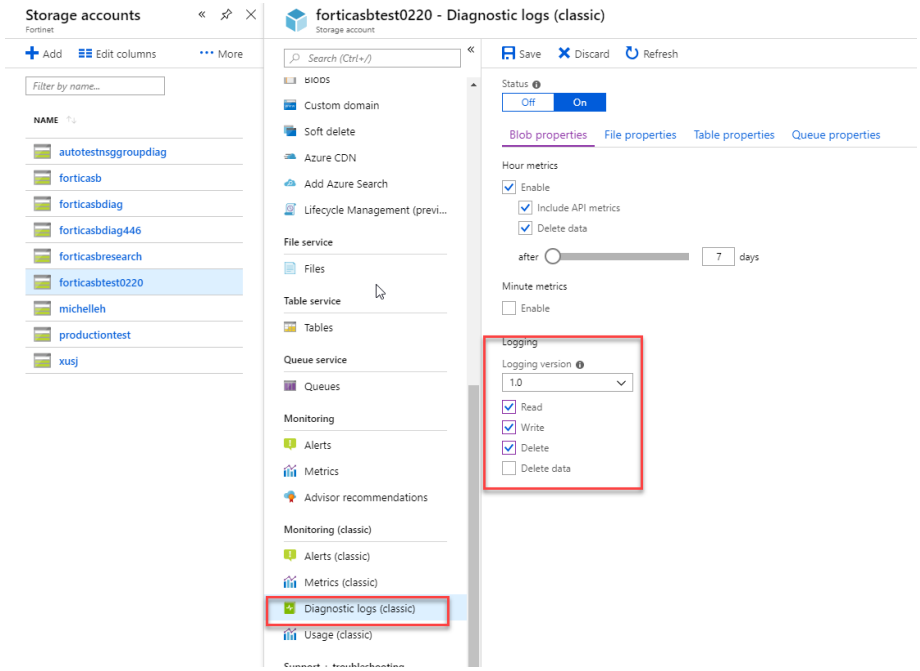
4. In **Resource group** field, select a resource group based on your preference or create a new one.
5. In **Instance details** > **Storage account name** field , enter an account name based on your preference.
6. Click **Review + create**. Once validation passed, click **Create**.

Enable Blob Log Monitoring

Once storage account is created, now you can enable blob log monitoring:

1. Select the storage account created earlier.
2. In the middle pane, scroll down to **Monitoring (classic)** and click on **Diagnostic settings (classic)**.
3. Turn **On** diagnostic logs. In **Blob properties** tab, under **Logging**, select **Read/Write/Delete**.

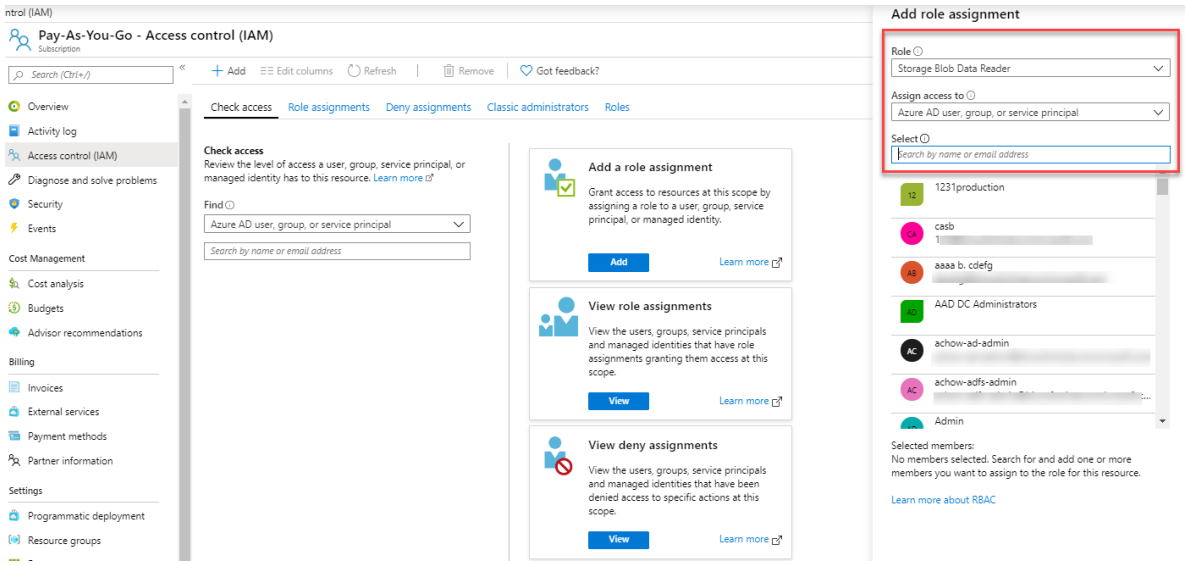
4. Click **Save** to finish the configuration.



Setup Storage Blob Data Reader

The last step is to grant Storage Blob Data Reader permission to the Azure AD user. This is a necessary step for FortiCASB DLP Data Analysis and virus scan to read and analyze the data stored in the Storage Blob account as well as integrating Azure cloud traffic in FortiCASB.

1. From the Azure portal page, search and click **Subscriptions**.
2. Select your subscription.
3. Select **Access Control (IAM)**, and click **+Add,** then **Add role assignment** pane will pop-up.
4. In **Role** field, type and select **Storage Blob Data Reader**.
5. In **Assign access to** field, leave it as **User, group, or service principal**.
6. In **Select** field, type and select the name or e-mail address of the Azure AD user.

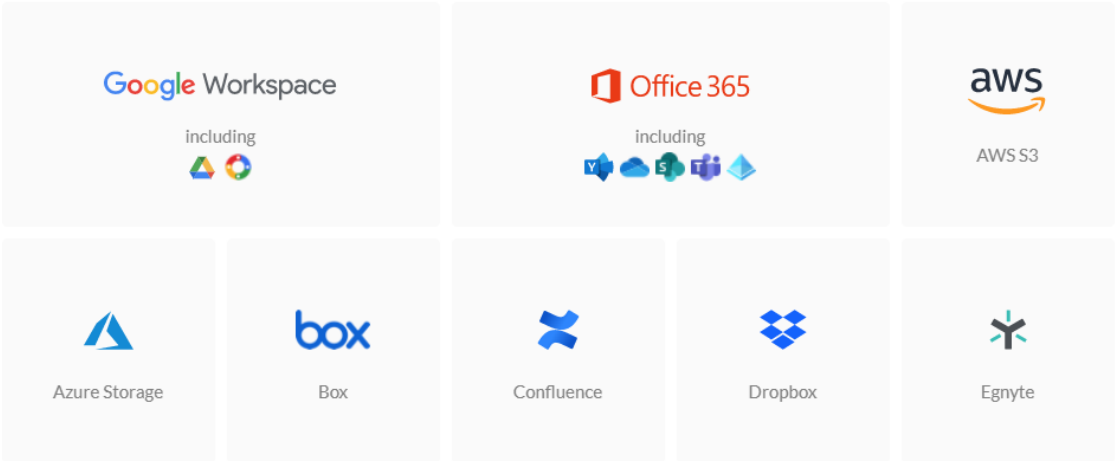


7. Click **Save** to complete granting the role to the Azure AD user.

Add Azure Storage Account

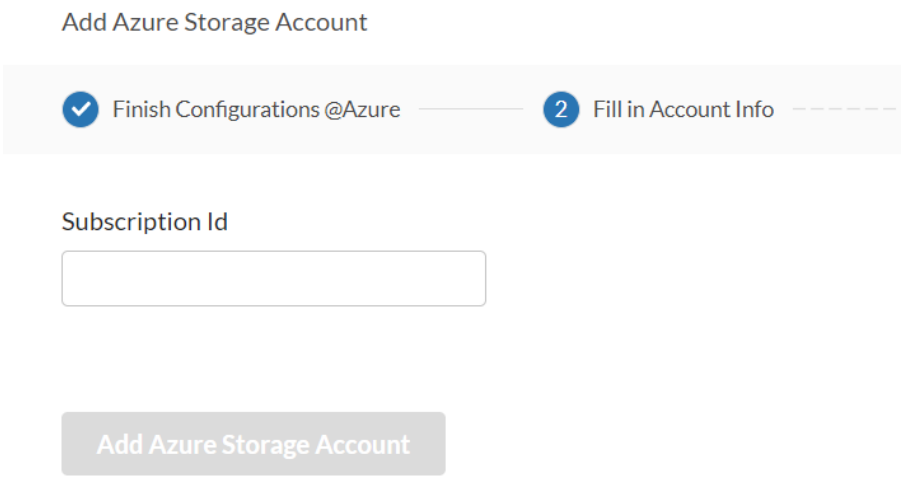
Once you have all the Azure Storage Configurations, you can add Azure Storage account on FortiCASB following these following steps:

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Azure Storage**, then click **Add Selected Cloud App**.



3. Review the key configurations list to see if you have finish all the required configurations, then click **Next**.

4. Enter your subscription ID you saved earlier in **Subscription ID** field.



5. Click **Add Azure Storage Account**.

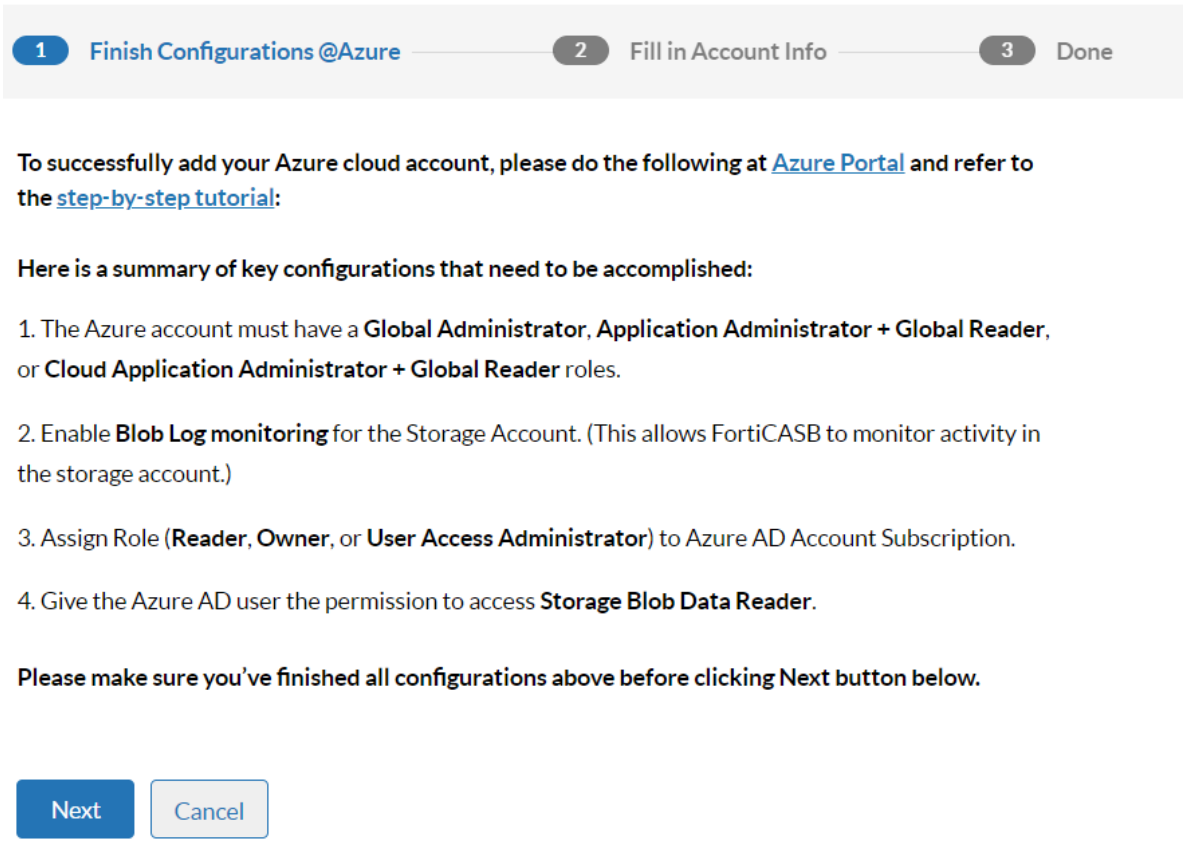
Update Azure Storage Account

Before updating the Azure Storage account on FortiCASB, complete the same Azure Storage Configurations.

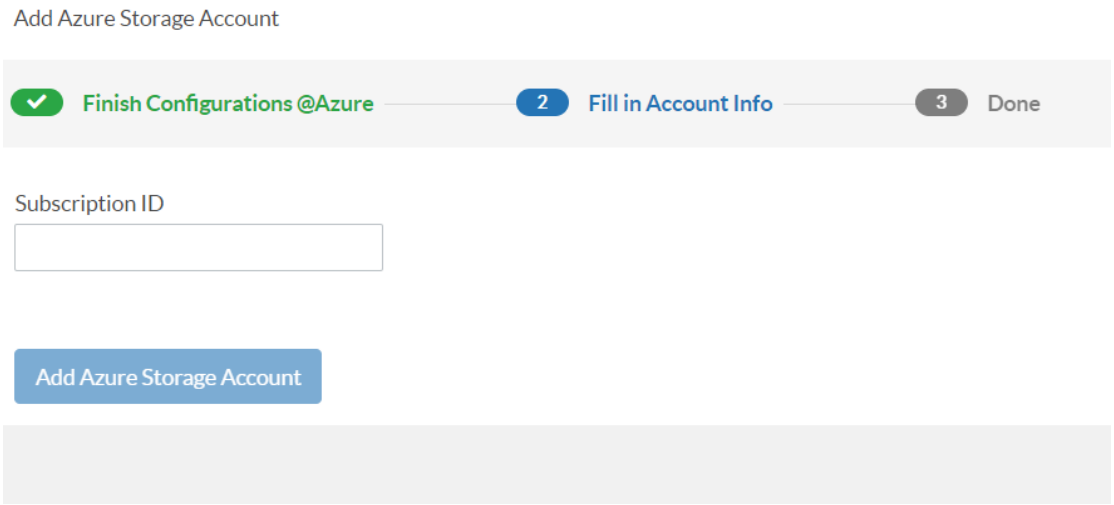
1. **Setup Azure Subscription on page 60**
2. **Add Reader role to the Subscription on page 61**
3. **Add Reader roles to multiple subscriptions simultaneously (optional) on page 62**
4. **Collect Subscription and Tenant IDs on page 64**
5. **Setup Blob Storage on page 65**
6. **Enable Blob Log Monitoring on page 66**
7. **Setup Storage Blob Data Reader on page 67**

Once you finish all the Azure Storage Configurations, follow these stesp to update the Azure Storage account.

1. In FortiCASB, go to **Overview > Dashboard**.
2. Click on Azure Storage Account menu and select **Update Cloud Account**.
3. Review the key configurations list to see if you have finish all the required configurations, then click **Next**.



4. Enter your subscription ID you saved earlier in **Subscription ID** field.



5. Click **Update Azure Storage Account**.

Box

FortiCASB offers an API-based approach, pulling data directly from Box via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Box user activities, provides DLP Data Analysis for files stored on Box.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- **Business Edition**
- **Enterprise Edition**
- **Developer Edition**

The user account installed in FortiCASB must have the following permissions:

- **Read and write all files and folders stored in Box**
- **Manage users**
- **Manage groups**
- **Manage enterprise properties**

You may either use an existing account or create a new account. If you create a new account, wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

The following features require "Admin User" permission as well:

- User login tracking
- User IP address tracking
- Geographical location tracking
- User password change tracking
- Change admin role tracking

Without "Admin User" permissions, FortiCASB cannot obtain user login IPs. Therefore, any user activity will not appear on the Activity map.

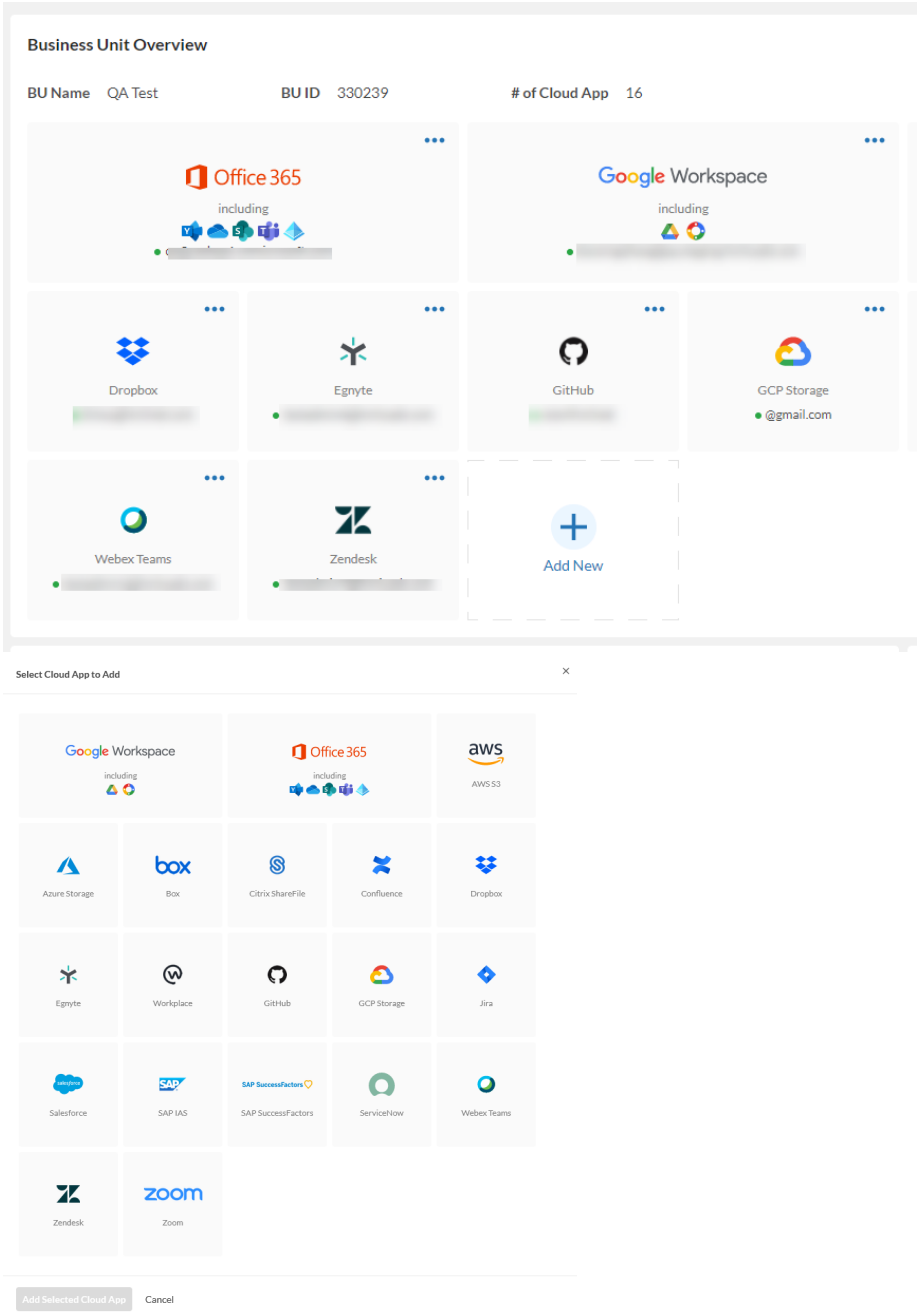
After you have verified the account prerequisite, follow the guides below to **Add** or **Update** the account on FortiCASB:

Add Box Account on page 73

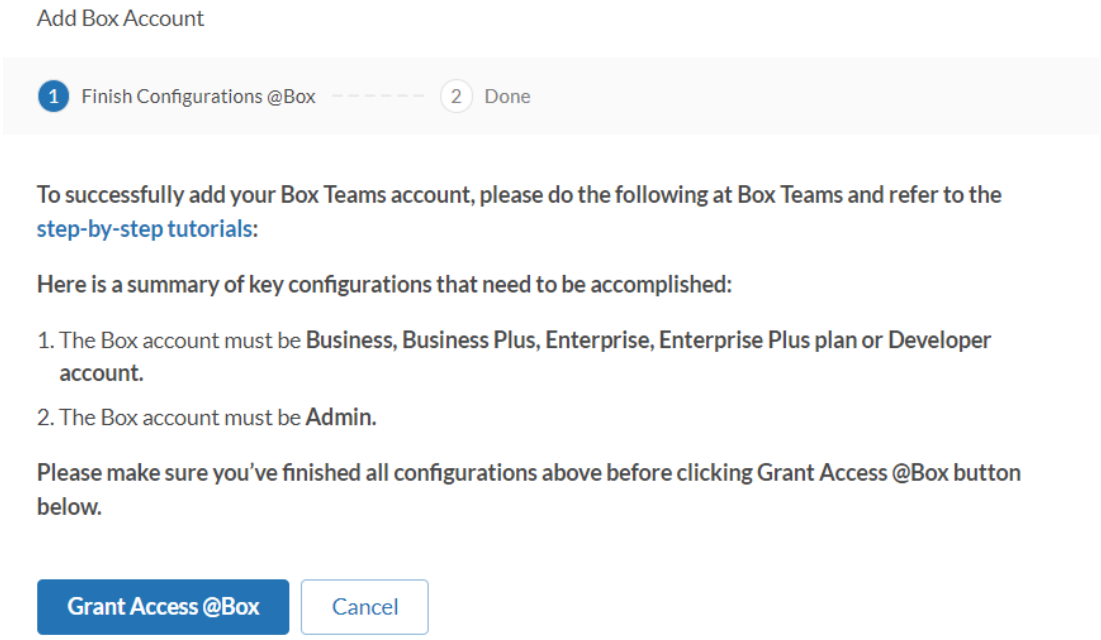
Update Box Account on page 75

Add Box Account

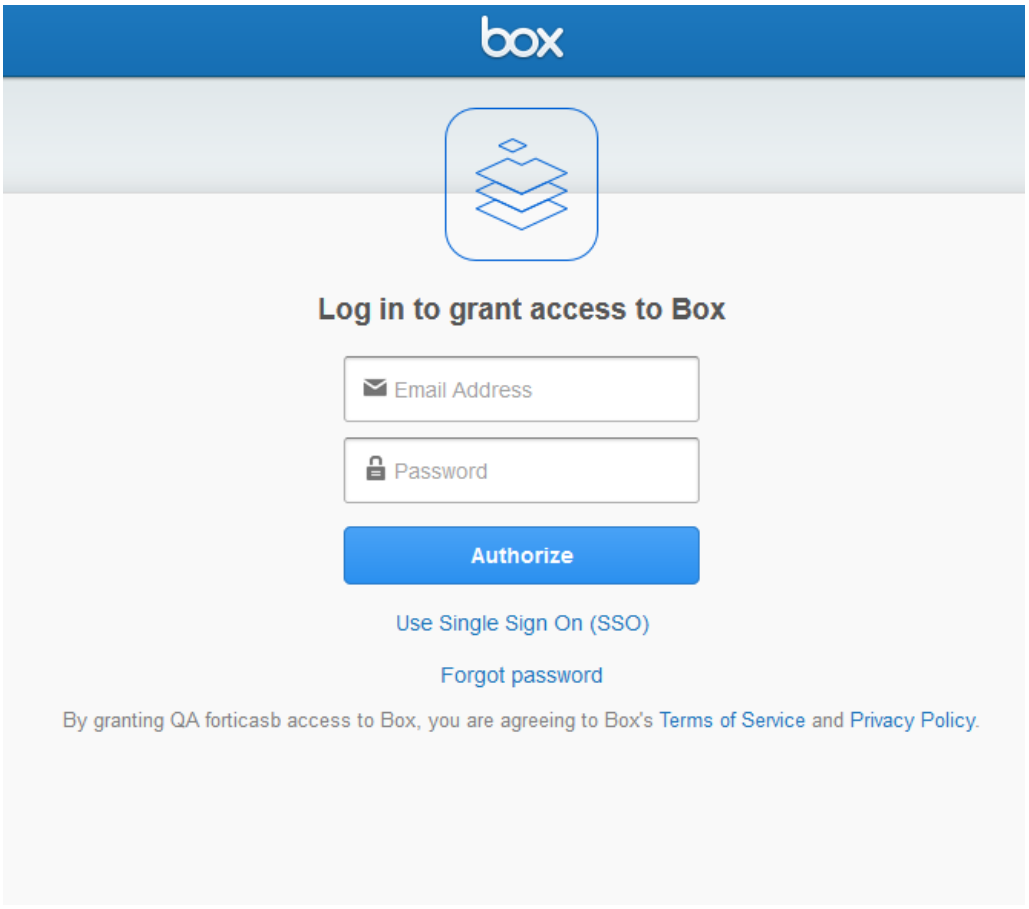
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Box**, then click **Add Selected Cloud App**.



3. Click **Grant Access @Box** to authenticate the account



4. You will be navigated to the Box website for authentication. Log in to authenticate.



Box will prompt you to **allow** or **deny** access.

5. Click **Allow** to grant FortiCASB permissions to monitor your Box application.

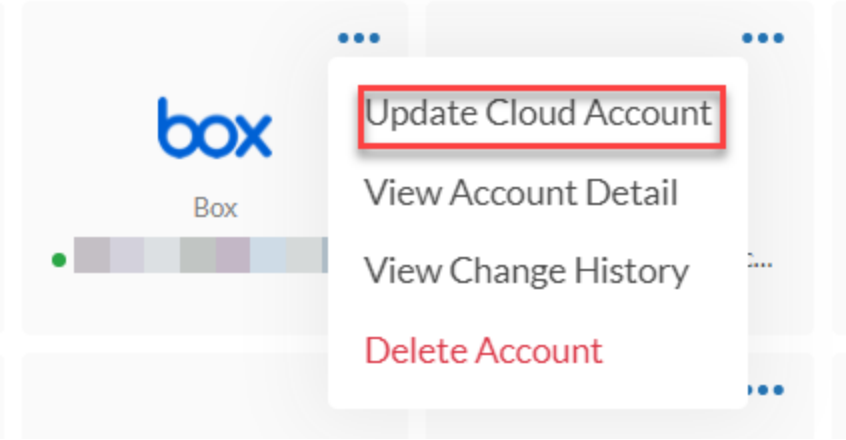
After you click **Allow**, you will be redirected back to the FortiCASB dashboard.

You can check the installation checklist and monitoring status in the Box dashboard.

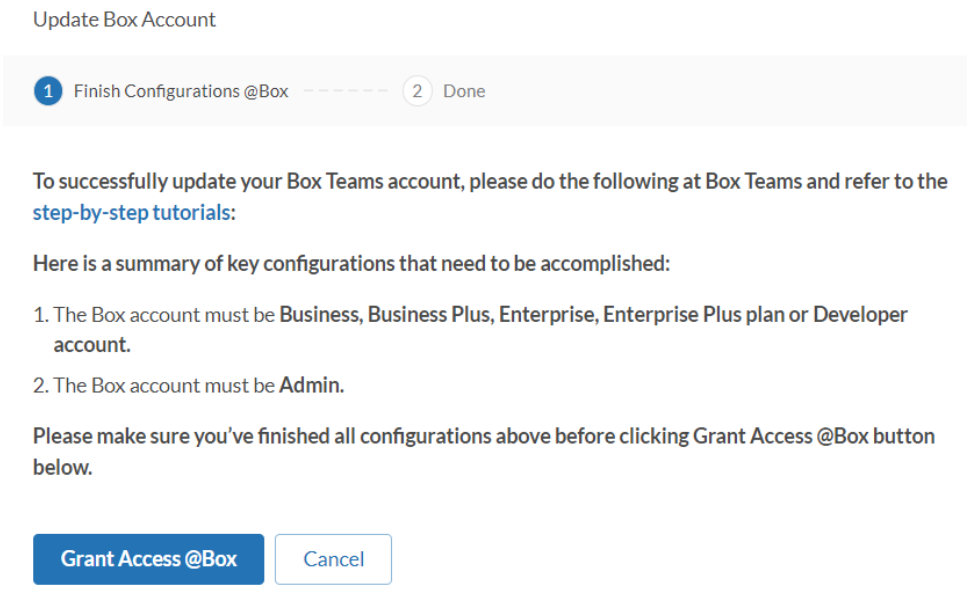
For more information on common installation issues, see Troubleshooting on page 515.

Update Box Account

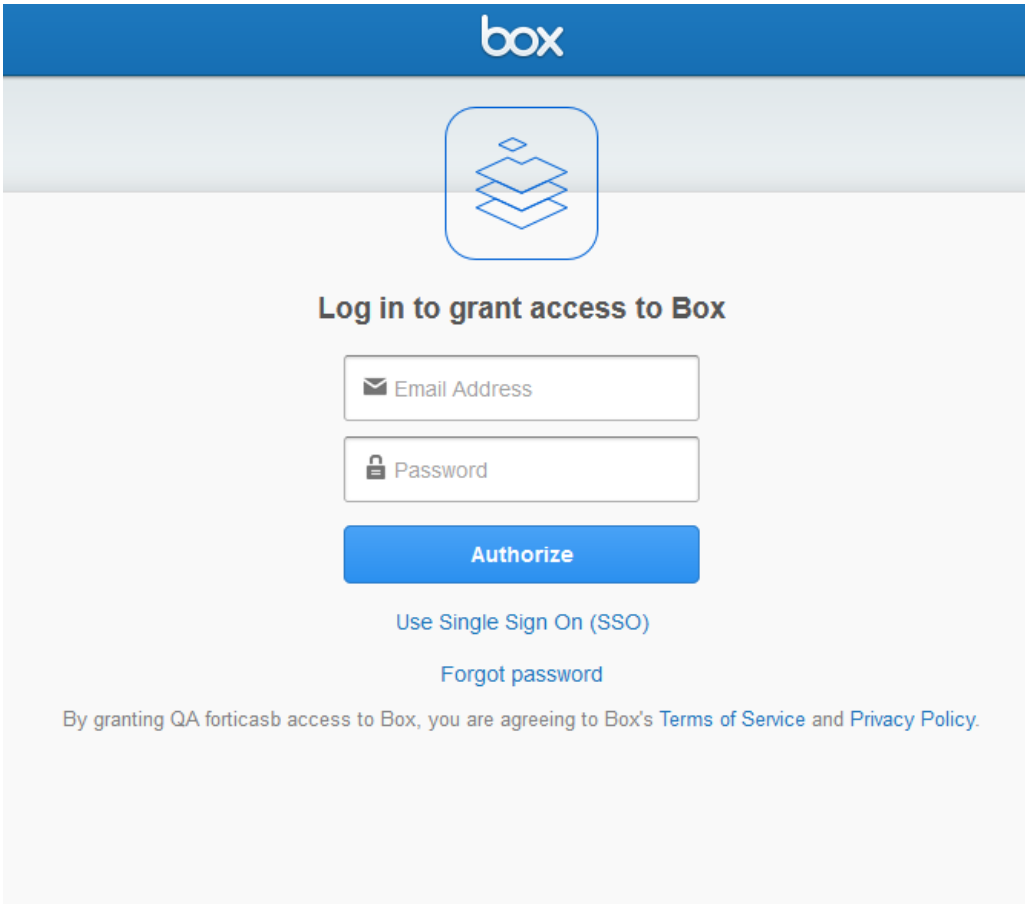
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**,
3. Click on the Box account menu, and select **Update Cloud Account**.



4. Click **Grant Access @Box** to re-authenticate the account.



5. You will be navigated to the Box website for authentication. Log in to authenticate.



Box will prompt you to **allow** or **deny** access.

6. Click **Allow** to grant FortiCASB permissions to monitor your Box application.

After you click **Allow**, you will be redirected back to the FortiCASB dashboard.

You can check the installation checklist and SaaS platform monitoring status in the Box dashboard.

For more information on common installation issues, see Troubleshooting on page 515.

Citrix ShareFile

FortiCASB offers an API-based approach, pulling data directly from Citrix ShareFile via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Citrix ShareFile user activities, provides DLP Data Analysis for files stored on Citrix ShareFile.

Follow the guides below to add or update the account on FortiCASB:

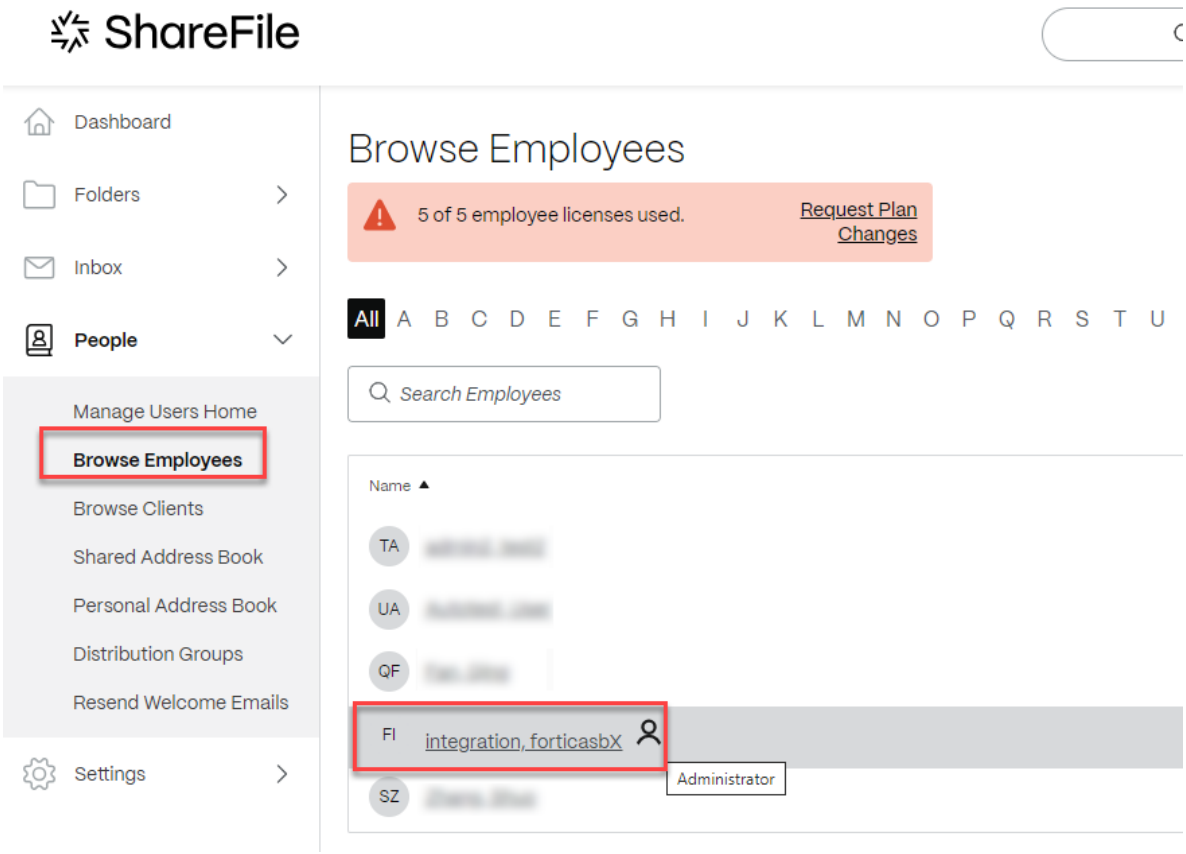
Add Citrix ShareFile Account on page 77

Update Citrix ShareFile Account on page 80

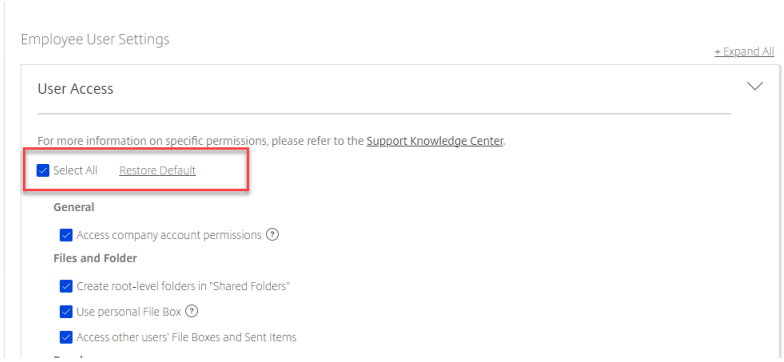
Add Citrix ShareFile Account

Follow these steps to add the Citrix ShareFile on FortiCASB:

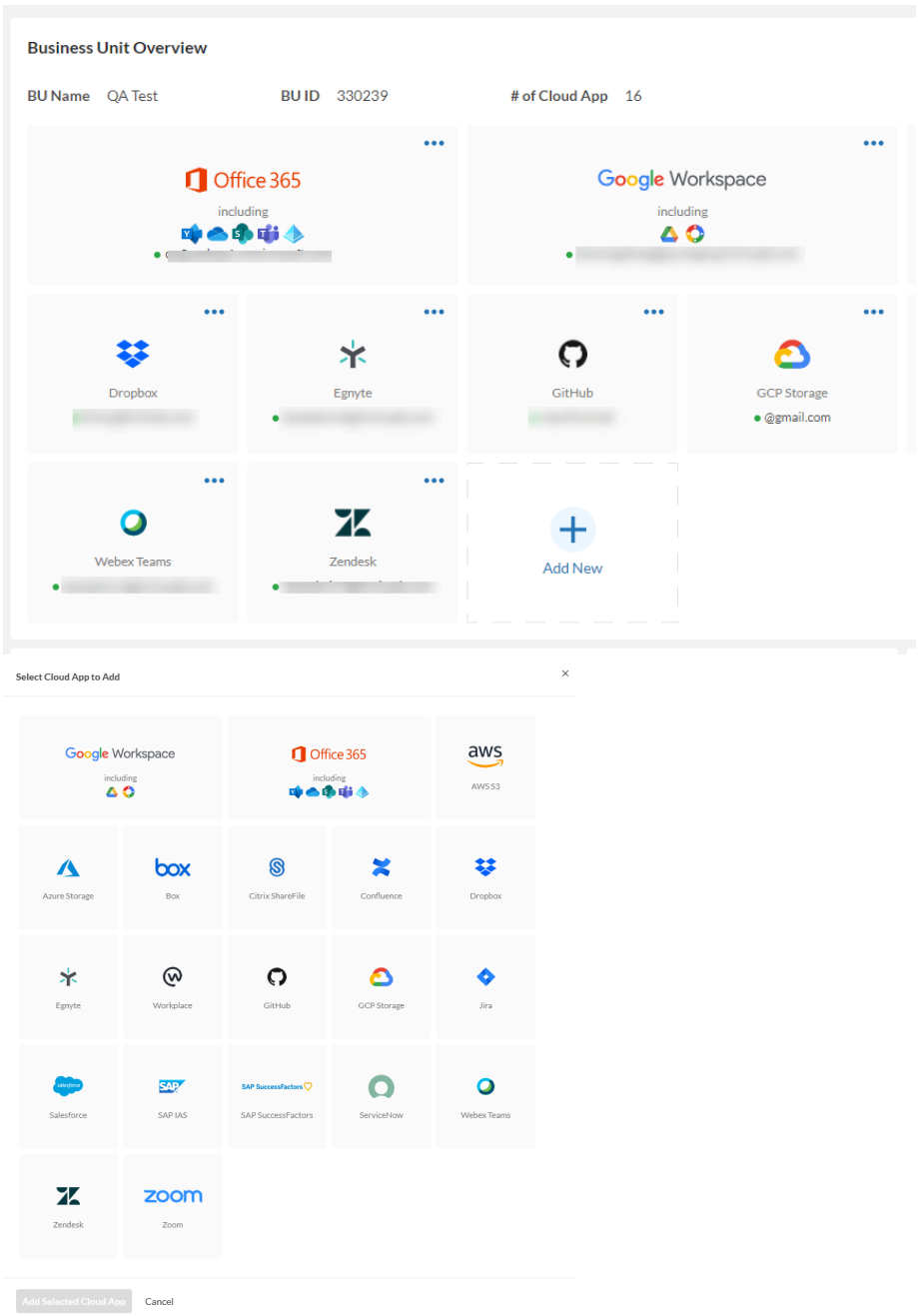
1. Log into Citrix ShareFile with your account.
2. In the left navigation menu, click **People** drop down menu and then select **Browse Employees**.



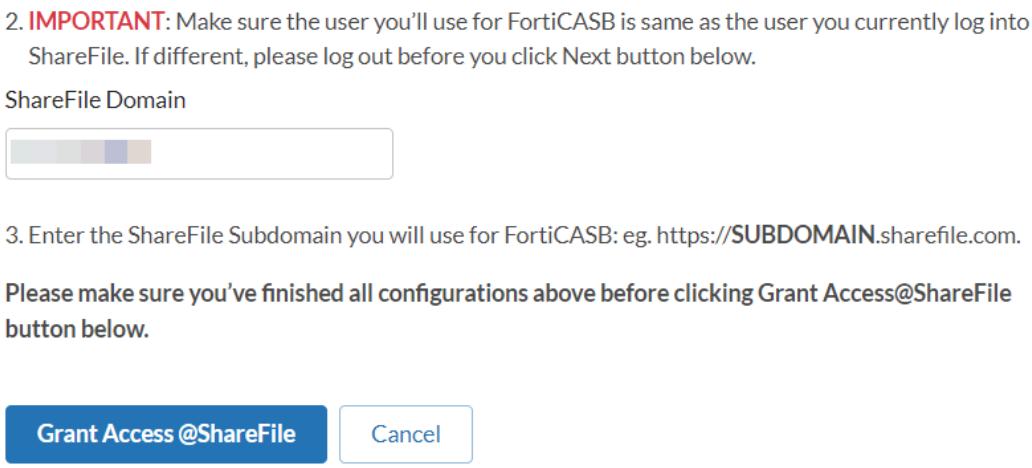
3. In **Browse Employees**, click on the user with administrator privilege to be added on FortiCASB.
4. Scroll down to **Employee User Settings**, click and expand **User Access** section, check **Select All** to include all permissions.



5. Scroll down more and click **Save Changes** to save the configurations.
6. Now go back to FortiCASB, go to **Overview > Dashboard**, click on **Add New**, select **Citrix ShareFile**, then click **Add Selected Cloud App**.

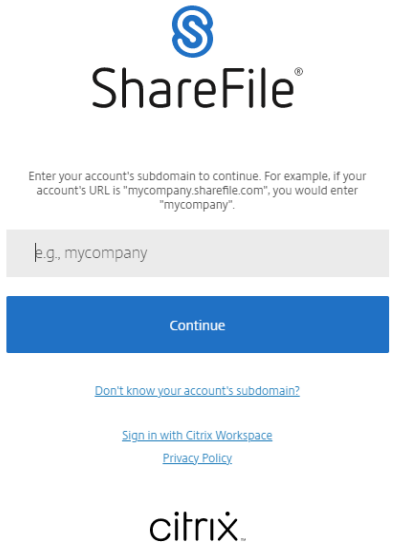


7. Enter the **ShareFile Subdomain** you will use for FortiCASB: e.g. https://**SUBDOMAIN**.sharefile.com.



Important: Make sure the user your are adding to FortiCASB is the same user you are currently logged into ShareFile. If different, please log out and log back in with the right user.

8. Click **Grant Access@ShareFile** to add the ShareFile account. You will be re-directed to ShareFIle OAuth page for validation.
9. Enter your ShareFile domain and credentials to sign in to complete the validation.

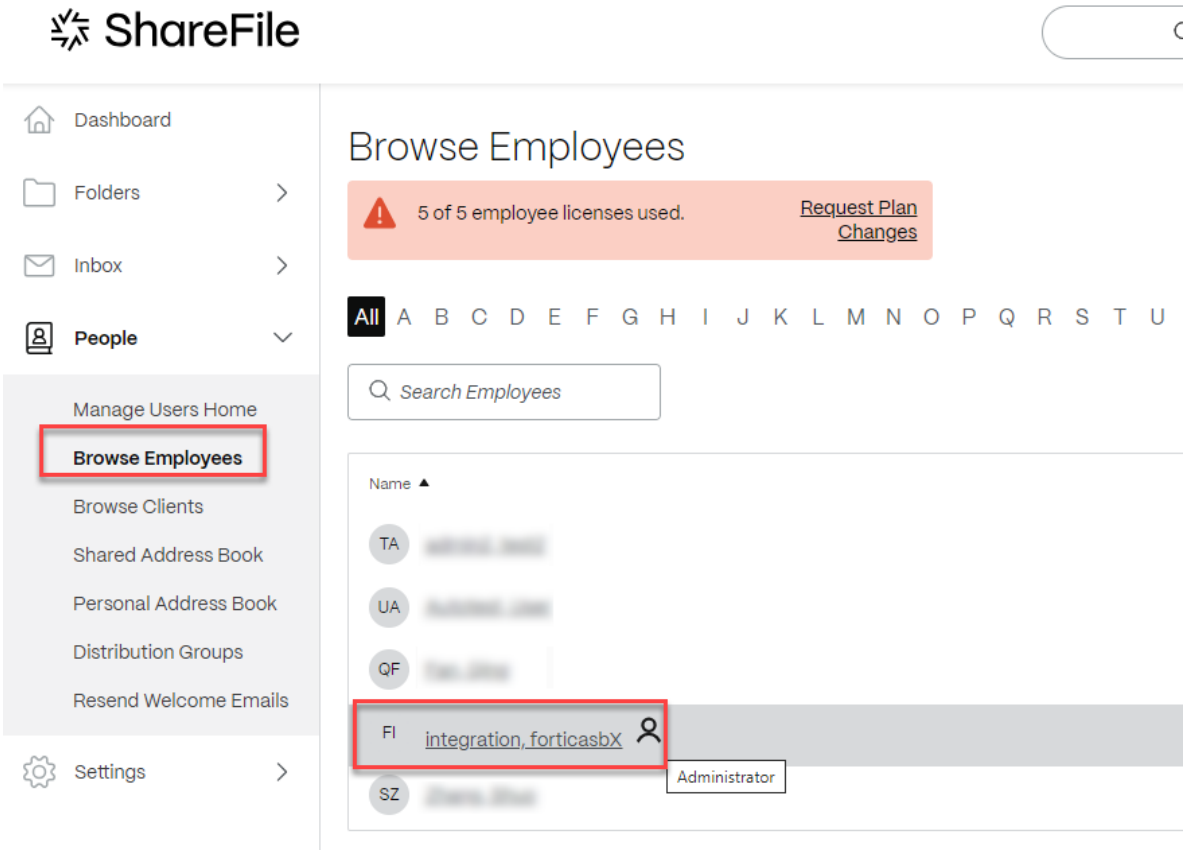


The add account process may take 15 minutes to complete. You may check the status in **Overview > Dashboard.**

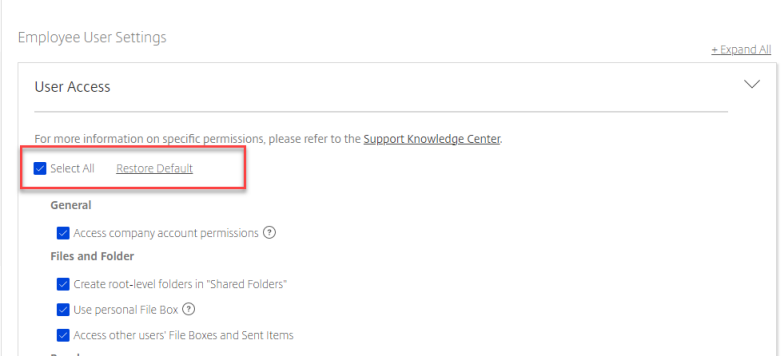
Update Citrix ShareFile Account

Follow these steps to update the Citrix ShareFile on FortiCASB:

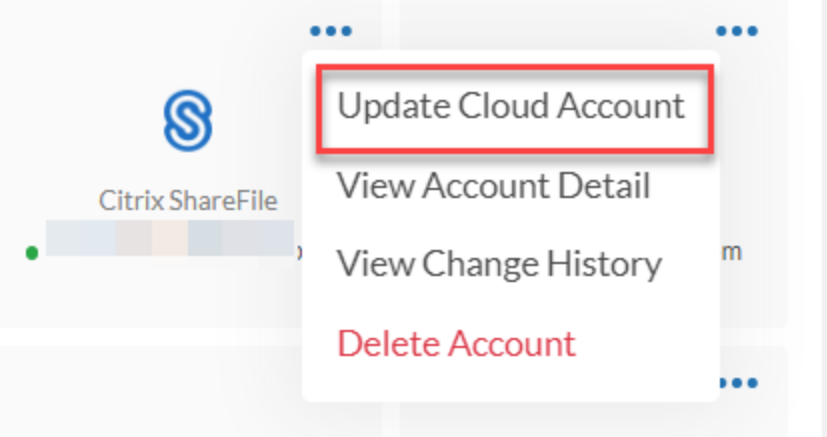
1. Log into Citrix ShareFile with your account.
2. In the left navigation menu, click **People** drop down menu and then select **Browse Employees**.



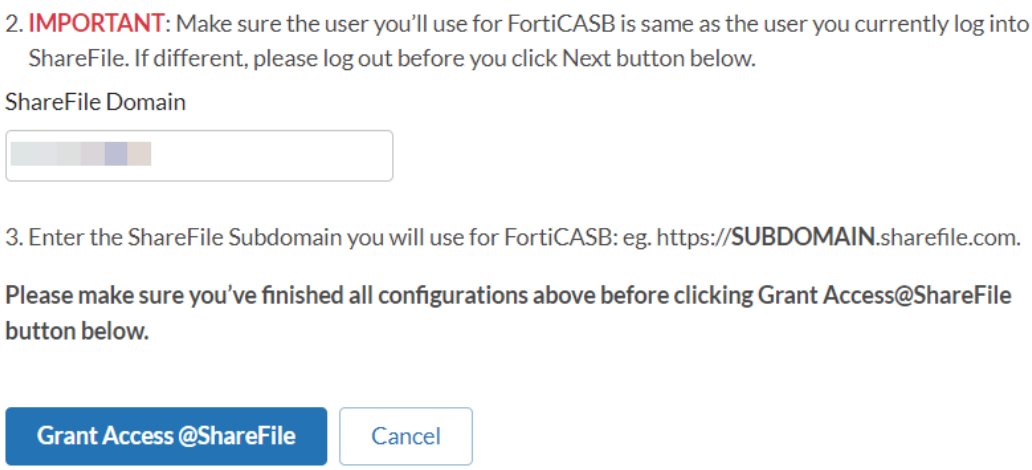
3. In **Browse Employees**, click on the user with administrator privilege to be added on FortiCASB.
4. Scroll down to **Employee User Settings**, click and expand **User Access** section, check **Select All** to include all permissions.



5. Scroll down more and click **Save Changes** to save the configurations.
6. Now go back to FortiCASB, go to **Overview > Dashboard**
7. Click on the Citrix ShareFile account menu, and select **Update Cloud Account**.

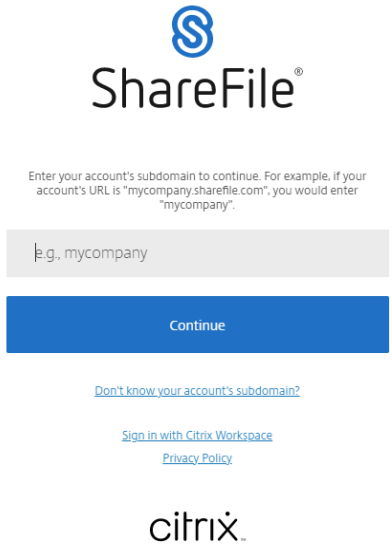


8. Enter the **ShareFile Subdomain** you will use for FortiCASB: e.g. https://**SUBDOMAIN**.sharefile.com.



Important: Make sure the user your are adding to FortiCASB is the same user you are currently logged into ShareFile. If different, please log out and log back in with the right user.

9. Click **Grant Access@ShareFile** to add the ShareFile account. You will be re-directed to ShareFIle OAuth page for validation.
10. Enter your ShareFile domain and credentials to sign in to complete the validation.



The add account process may take 15 minutes to complete. You may check the status in **Overview > Dashboard.**

Confluence

FortiCASB offers an API-based approach, pulling data directly from Confluence via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Confluence user activities, provides DLP Data Analysis.

Before adding the Confluence account to FortiCASB, configure the Confluence account to grant FortiCASB read access permission to monitor account activities and provide other security measures on the account. Make sure the Confluence account that will be added on FortiCASB is the **same** account that is configured.

Prerequisite

- The Confluence plan must be **Standard**, **Premium** or **Enterprise**. Free plan is NOT supported.
- The account must be the **Organization and Site Admin** of the Confluence site you will use on FortiCASB.

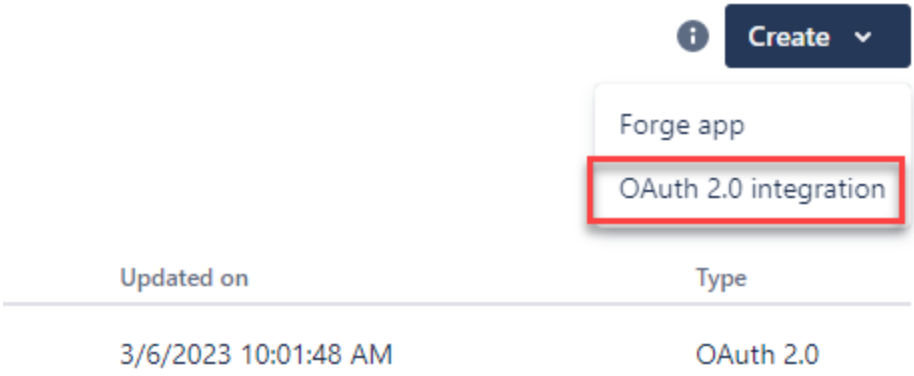
Add Confluence account to FortiCASB:

1. **Confluence Account Configuration on page 84**
2. **Add Confluence Account on page 87**

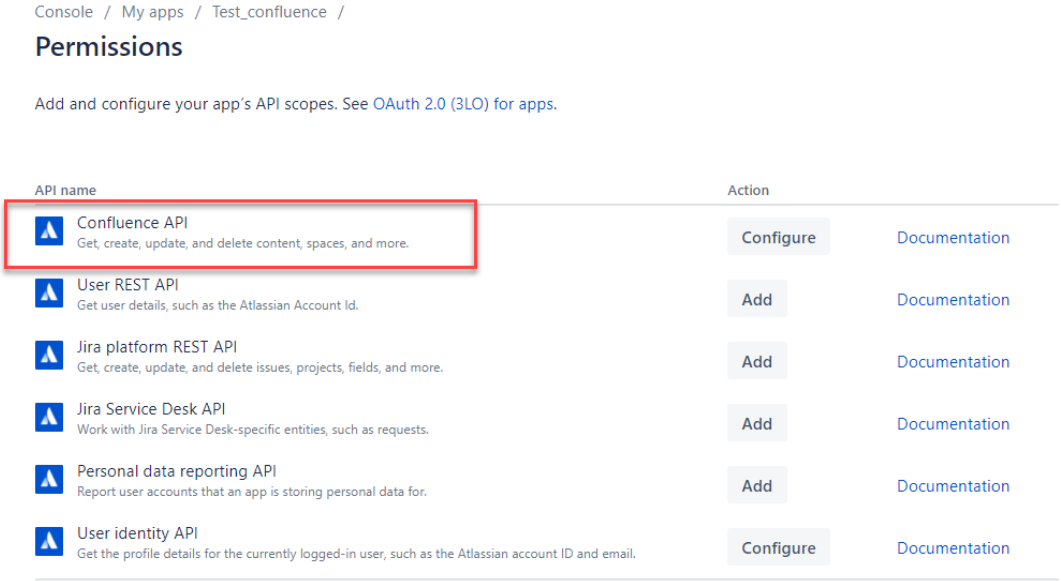
Confluence Account Configuration

Follow the instructions below to create and configure an App on Confluence:

1. Login to Atlassian Developer Console as the **Organization and Site Admin.**
2. Click **Create App** drop down menu and select **OAuth 2.0 integration**.



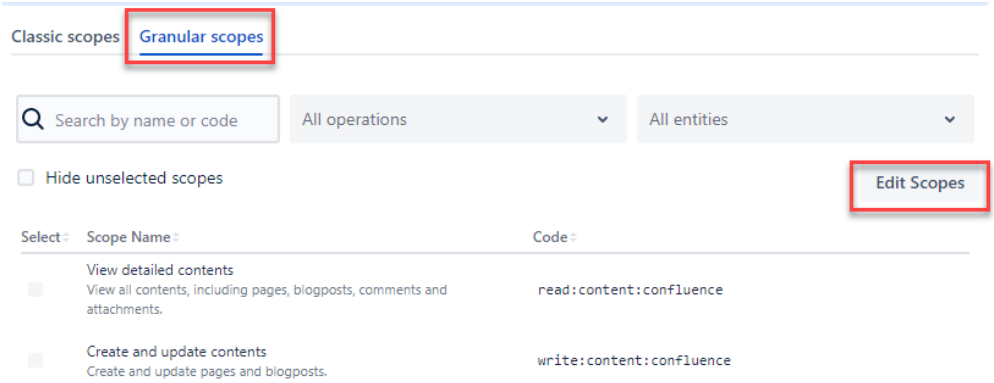
3. Fill in an **App name**, agree to Atllassian's developer terms, and click **Create**.
4. In the left navigation menu, click **Permission**.
5. In **API name**, find **Confluence API**, then click **Add**.



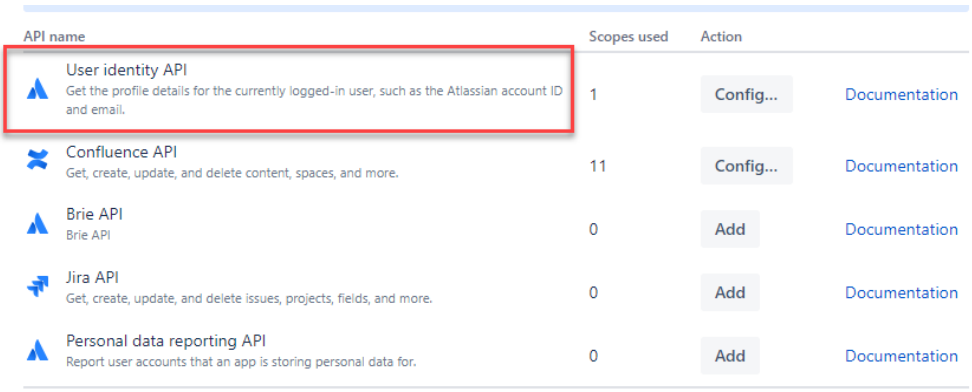
When the **Add** button turns into **Configure**, click **Configure**.

6. In **Classic scopes** tab, click **Edit Scopes** to add scopes for the Confluence API.

7. Select the following scopes and click **Save**.
   - **Read Confluence space summary**
   - **Read Confluence content properties**
   - **Read Confluence detailed content**
   - **Read Confluence content summary**
   - **Read content permissions in Confluence**
   - **Read user**
   - **Read user groups**
   - **Download content attachments**
8. Click the **Granular scopes** tab, then click **Edit Scopes** to add granular scopes.

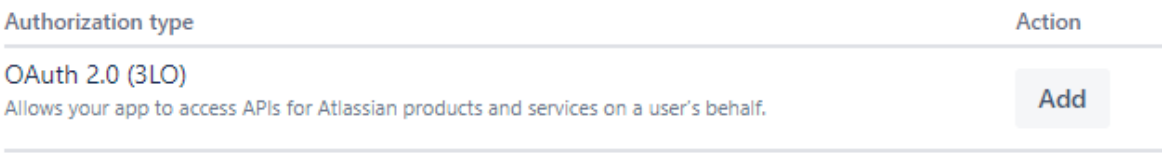


9. Select the following scopes and click **Save**.
   - **View audit records**
   - **View and download content attachments**
   - **View user details**
10. In the left navigation menu, click **Permissions** again, find **User Identity API**, then click **Add**.

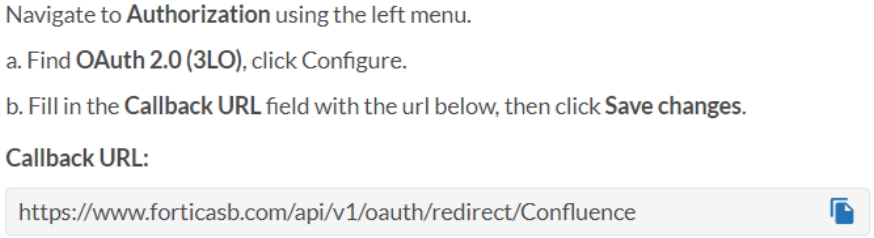


When the **Add** button turns to **Configure**, click **Configure**.

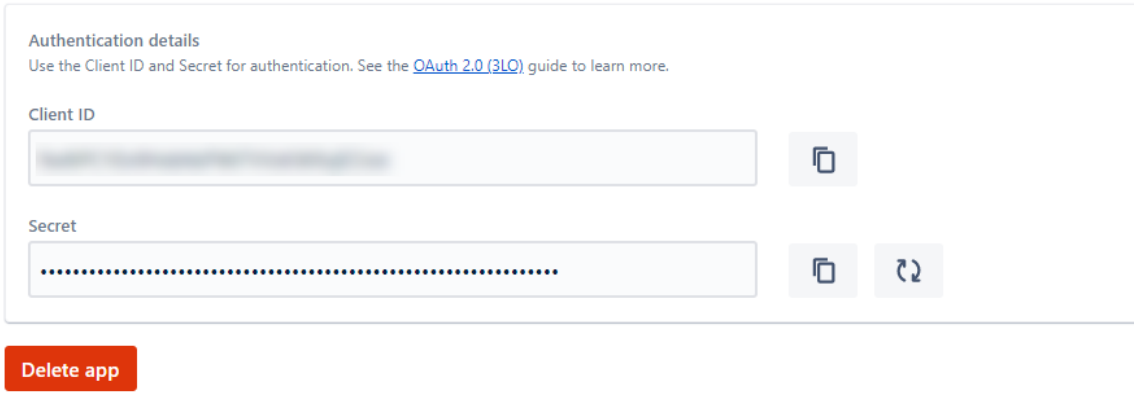
11. Click **Edit Scopes** to add the following scopes and click **Save**.
    - View active user profile
    - View user profiles
12. Go back to the navigation menu, click **Authorization**.
13. In **Authorization type** > **OAuth 2.0 (3LO)**, click **Add**.



14. In the **Callback URL**, enter the callback URL provided by FortiCASB, then click **Save Changes** to save the settings.



15. In the left navigation menu, click **Settings**, then scroll down to **Authentication details**, make a note of the **Client ID** and **Secret** for later in FortiCASB authentication.



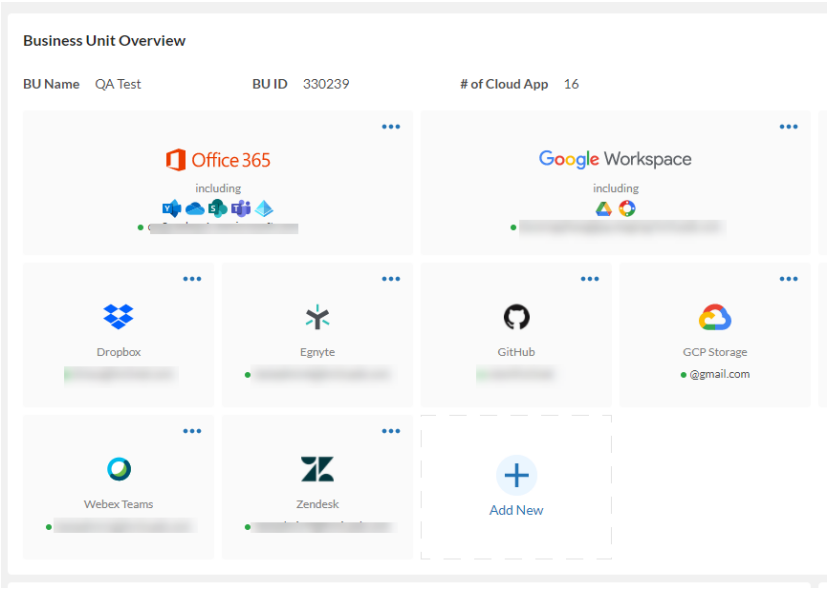
Please make sure the Confluence account that will be added on FortiCASB is the same account that is configured.

Add Confluence Account

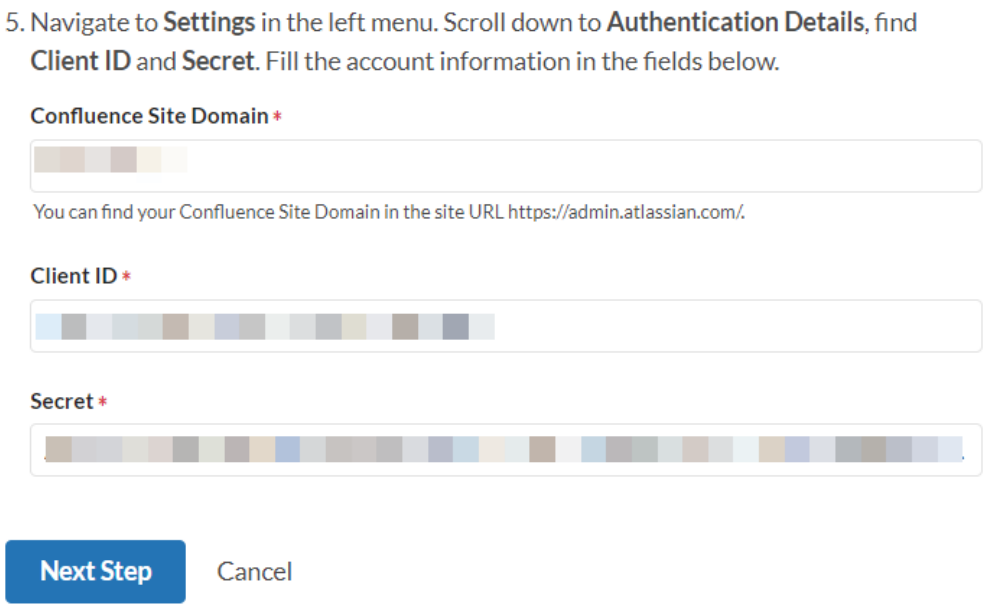
After completing Confluence Account Configuration on page 84, follow the steps below to create a Confluence Webhook and add Confluence account on FortiCASB.Webhook

Webhook are automated messages sent from Confluence to FortiCASB. They are much faster than API calls and are sent automatically when targeted Confluence events are triggered.

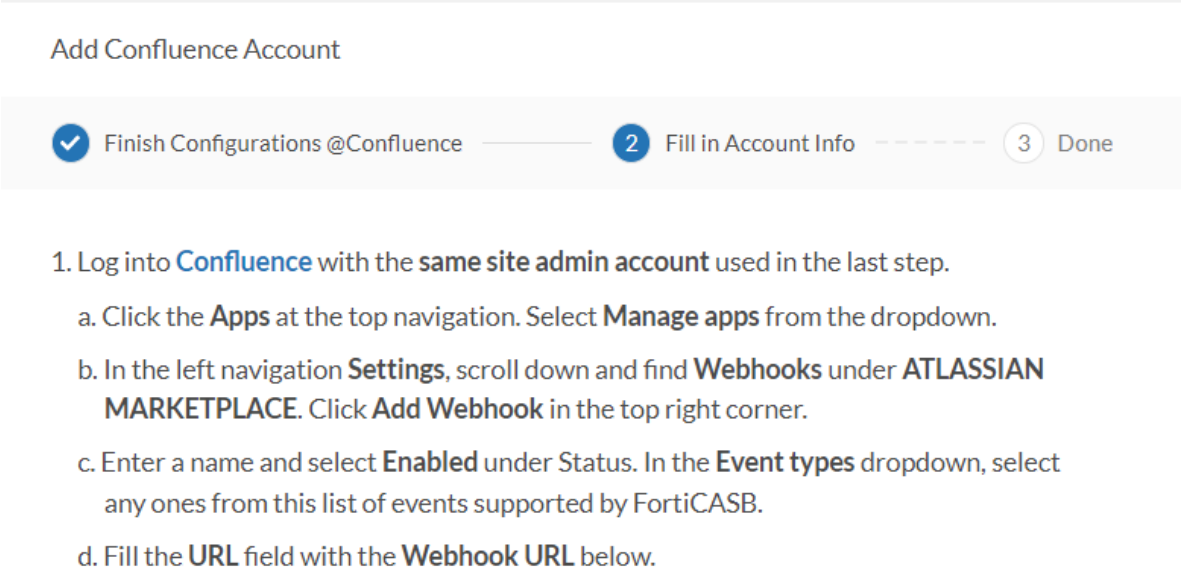
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Confluence**, then click **Add Selected Cloud App**.



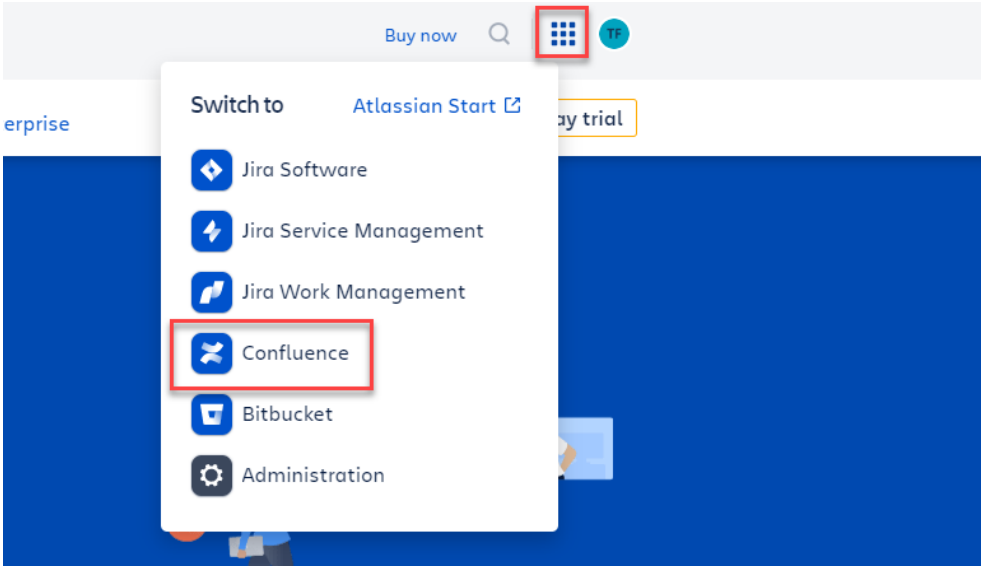
3. Scroll down to fill in the **Confluence Site Domain name** which the Confluence account associates with, the **Client ID** and **Client Secret** recorded down from Confluence Account Configuration. Your Confluence site domain name is the site domain prefix.
For example: for https://mydomain.atlassian.net/, the Confluence site domain name is "mydomain".



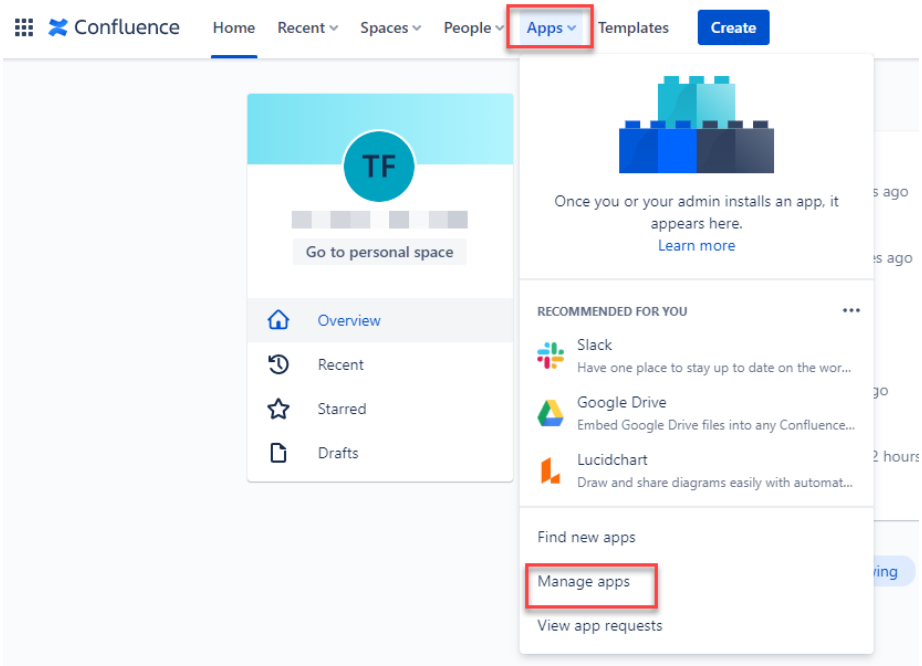
4. Click **Next Step** to continue.
5. In **Add Confluence Account** page 2, click the **Confluence** link to be re-directed to Atlassian main page.



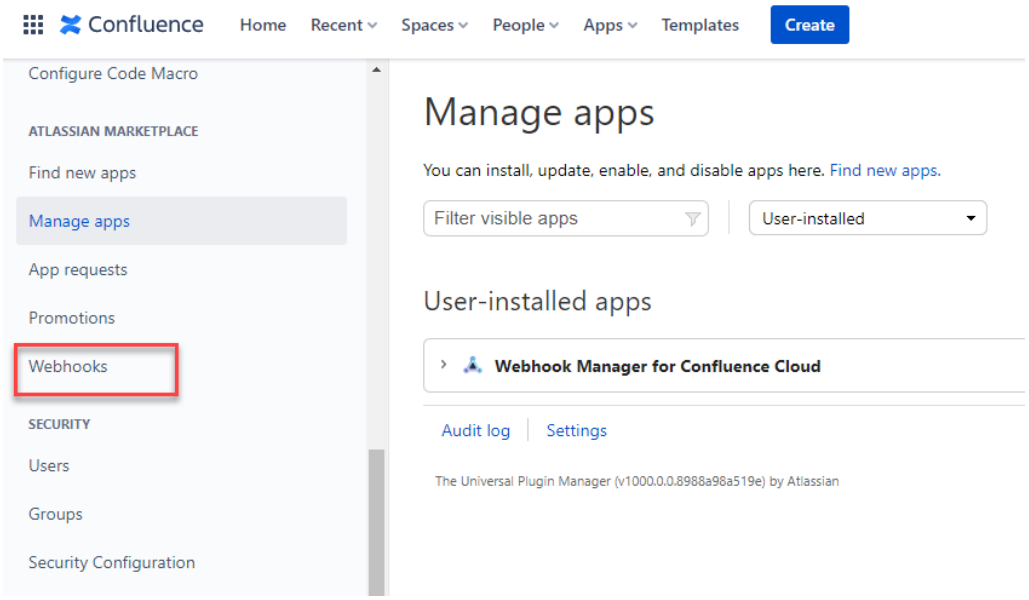
6. In the Atlassian main page, click the apps menu button and select **Confluence**.



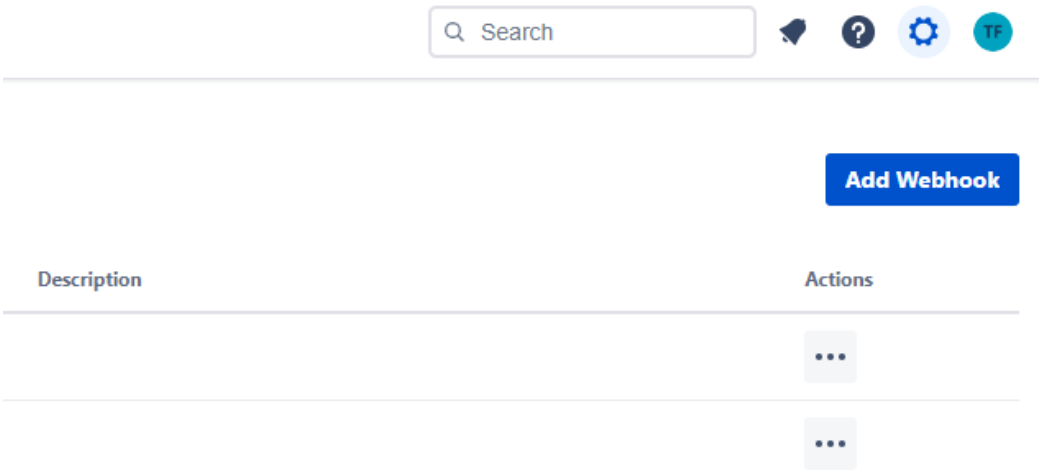
7. In Confluence main page, click **Apps** drop down menu and select **Manage apps**.



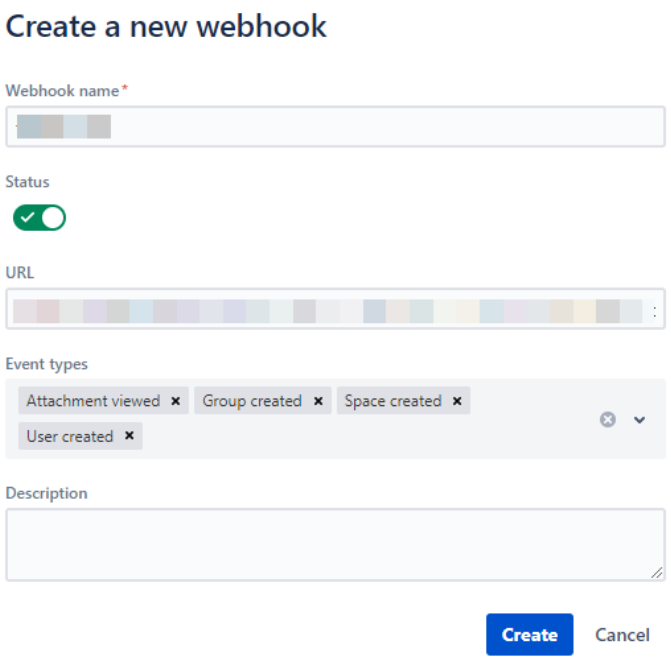
8. In the left navigation menu, scroll down to select **Webhooks**.



9. Click **Add Webhook** to create a Webhook.

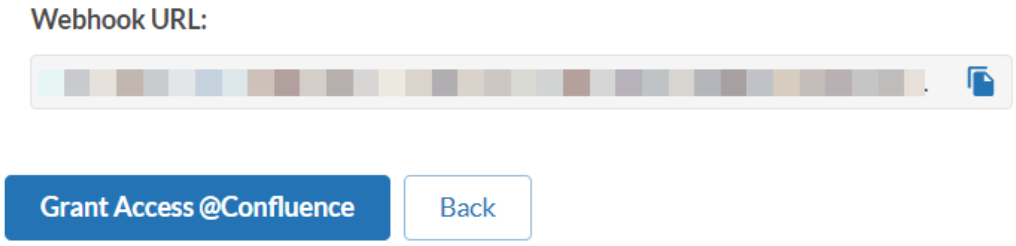


10. Fill in a name for the Webhook and enable the Webhook status.
11. Click **Event types** drop down menu and select the event types to monitor.

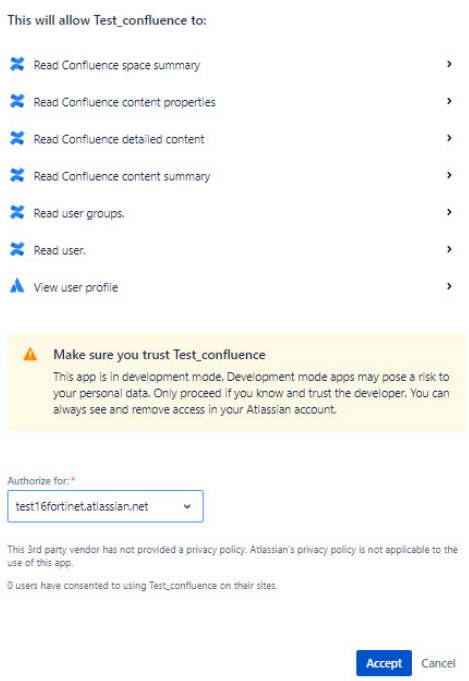


For the list of Webhook events supported by FortiCASB, please see **Confluence Events on page 309**.

12. Copy and paste the **Webhook URL** from the FortiCASB **Add Confluence Page** to the URL field.



13. Click **Grant Access @Confluence** to continue.
14. You will be re-directed to Confluence OAuth validation site, click **Authorize for** drop down menu, and select **Confluence Site domain**.



15. Click **Accept** to finish adding the Confluence account. Then you will be re-directed back to FortiCASB. It may take 15 minutes to finish adding the account. You may check the status in **Overview > Dashboard.**

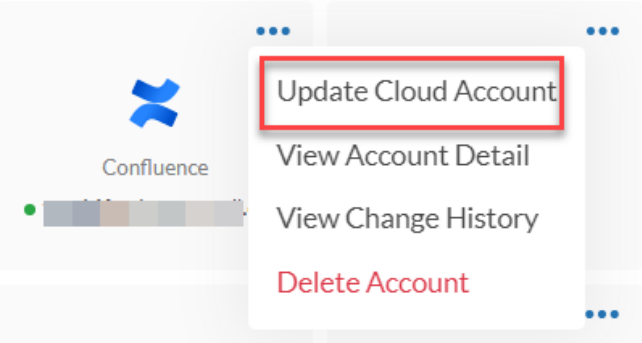
Update Confluence Account

Before updating the Confluence account on FortiCASB, complete the same Confluence Configurations:

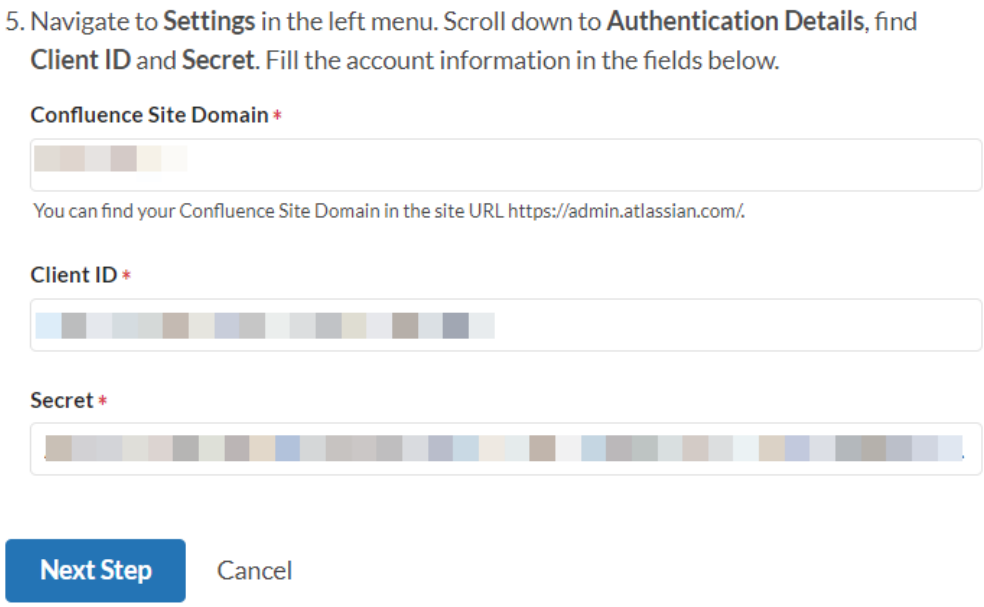
Confluence Account Configuration on page 84

After the Confluence account is configured, go back to FortiCASB to update the Confluence account.

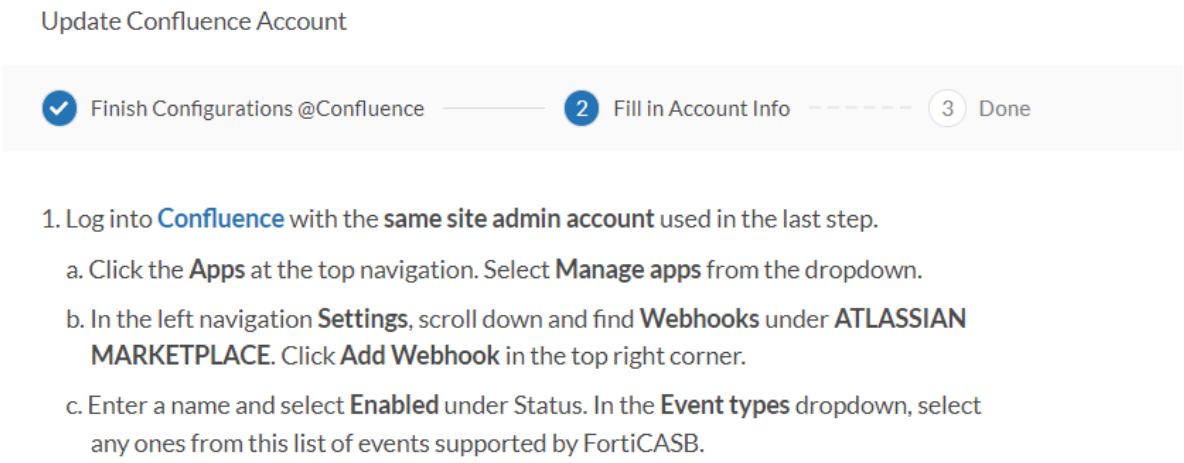
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on Confluence Account and menu and select **Update Cloud Account**.



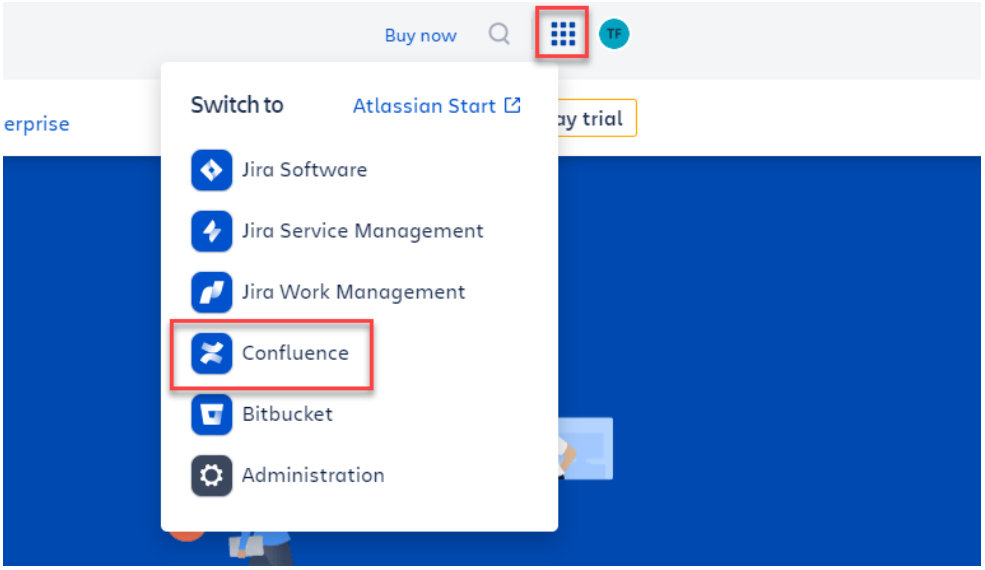
4. Scroll down to fill in the **Confluence Site Domain name** which the Confluence account associates with, the **Client ID** and **Client Secret** recorded down from Confluence Account Configuration. Your Confluence site domain name is the site domain prefix.
For example: for https://mydomain.atlassian.net/, the Confluence site domain name is "mydomain".



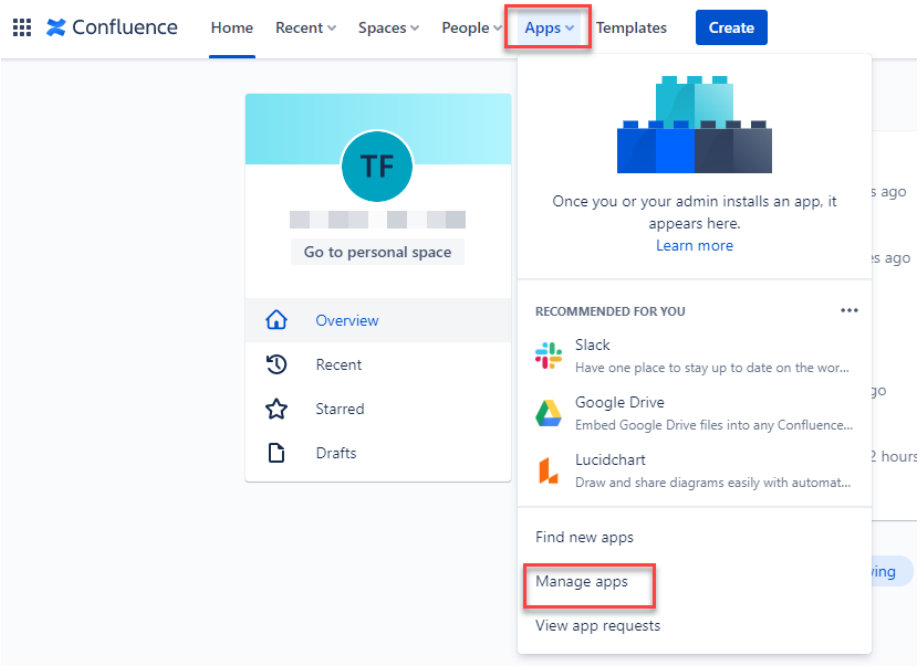
5. Click **Next Step** to continue.
6. In **Update Confluence Account** page 2, click the **Confluence** link to be re-directed to Atlassian main page.



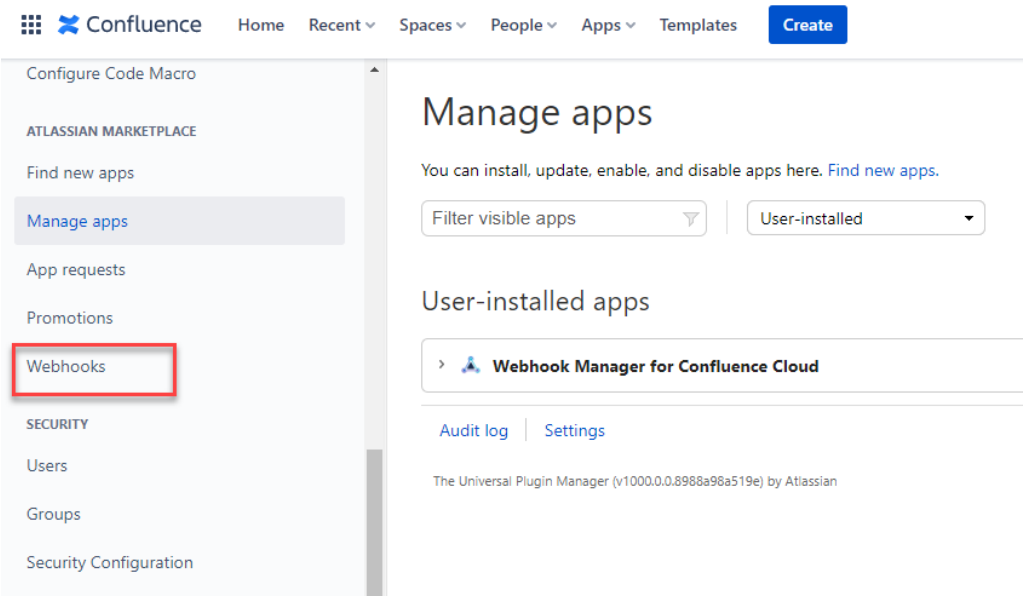
7. In the Atlassian main page, click the apps menu button and select **Confluence**.



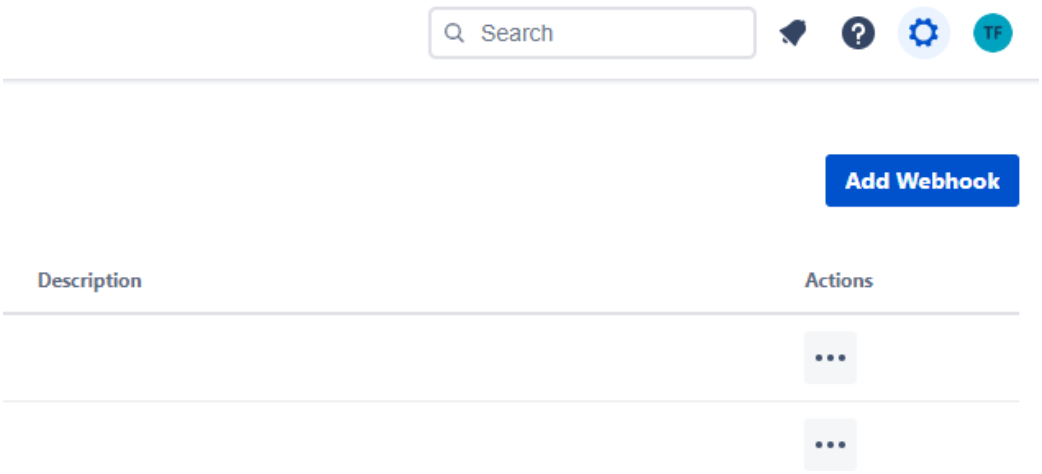
8. In Confluence main page, click **Apps** drop down menu and select **Manage apps**.



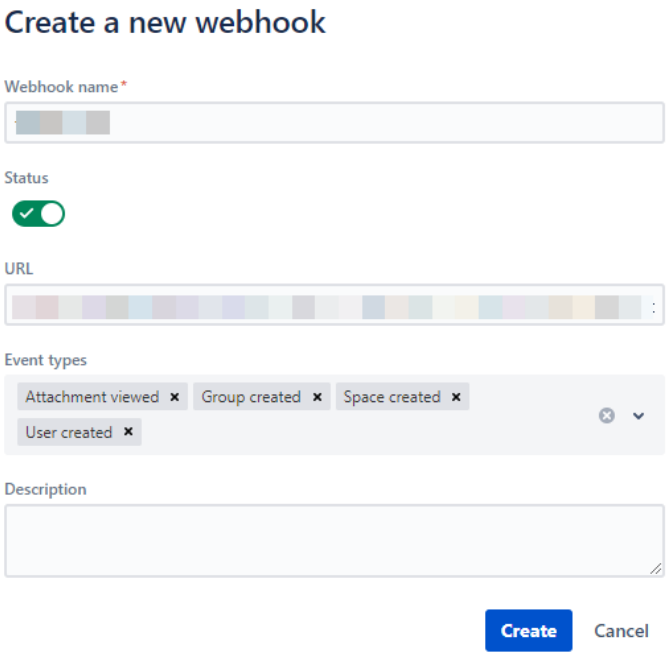
9. In the left navigation menu, scroll down to select **Webhooks**.



10. Click **Add Webhook** to create a Webhook.

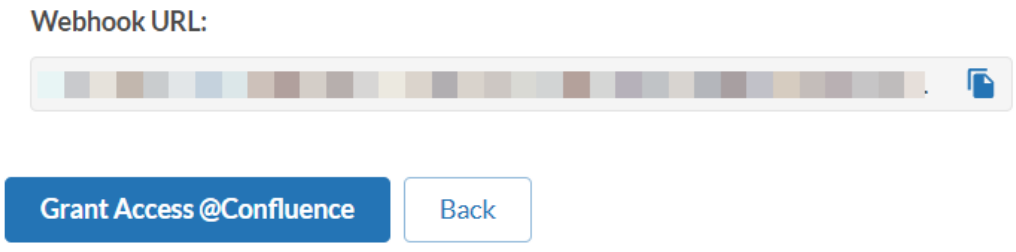


11. Fill in a name for the Webhook and enable the Webhook status.
12. Click **Event types** drop down menu and select the event types to monitor.



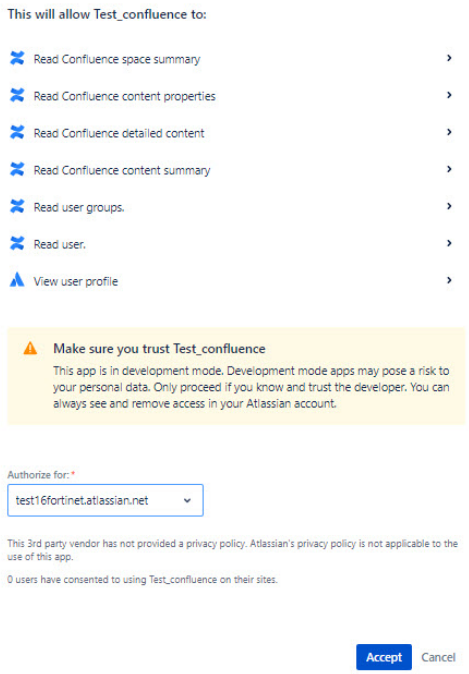
For the list of Webhook events supported by FortiCASB, please see **Confluence Events on page 309**.

13. Copy and paste the **Webhook URL** from the FortiCASB **Update Confluence Page** to the URL field.



14. Click **Grant Access @Confluence** to continue.

15. You will be re-directed to Confluence OAuth validation site, click **Authorize for** drop down menu, and select **Confluence Site domain**.



16. Click **Accept** to finish updating the Confluence account. Then you will be re-directed back to FortiCASB. It may take 15 minutes to finish updating the account. You may check the status in **Overview > Dashboard.**

Dropbox Business

FortiCASB offers an API-based approach, pulling data directly from Dropbox Business via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Dropbox Business user activities, provides DLP Data Analysis for files stored on Dropbox Business.

Prerequisites

To use API access, your organization must be using one of the following Dropbox Business plans:

- **Standard Plan**
- **Advanced Plan**
- **Enterprise Plan**

The user account added on FortiCASB must have the following permission:

- **Team Admin**

You may either use an existing account or create a new account.

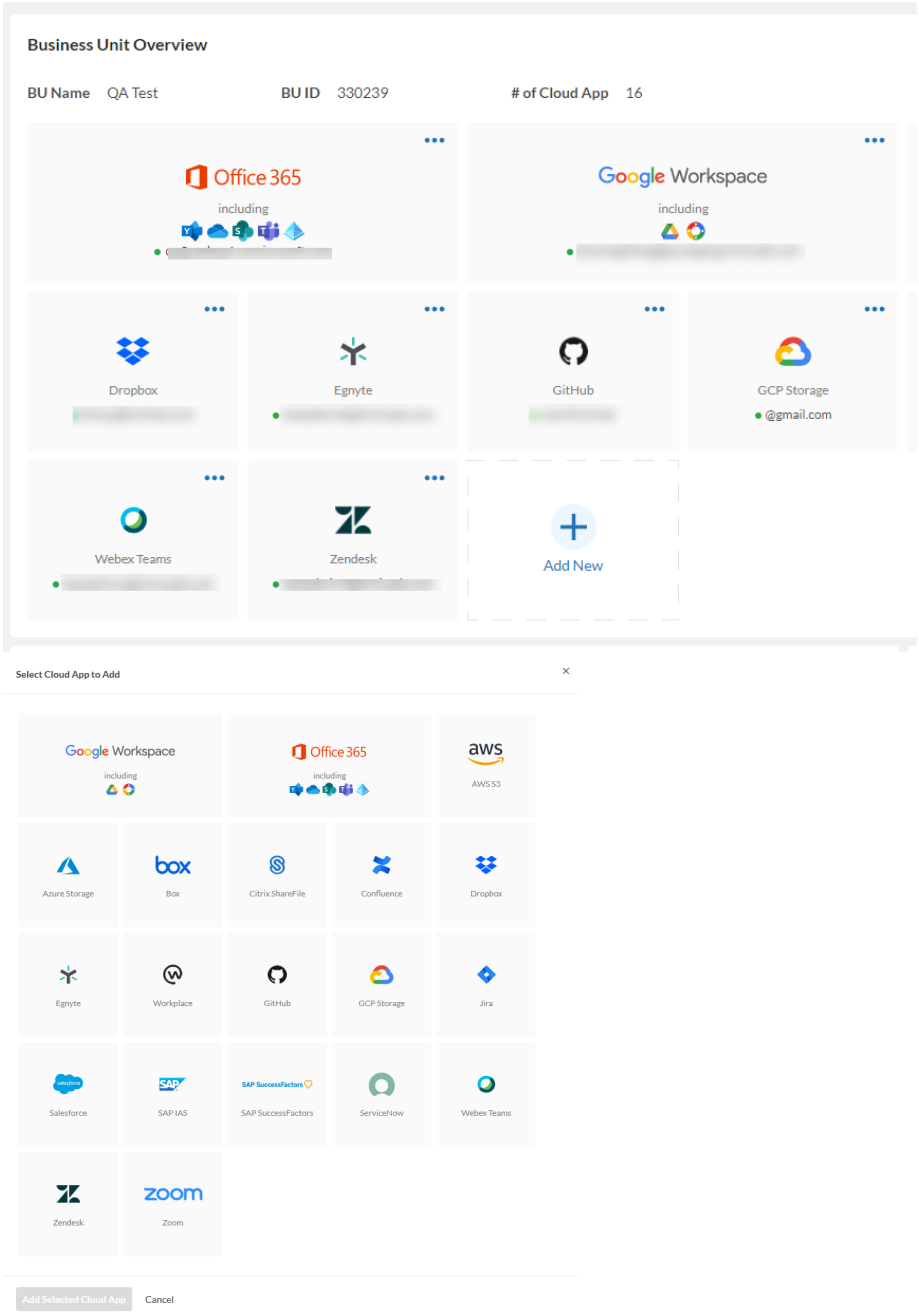
After you have verified account prerequisite, follow the guides below to **Add** or **Update** the account on FortiCASB:

Add Dropbox Business on page 99

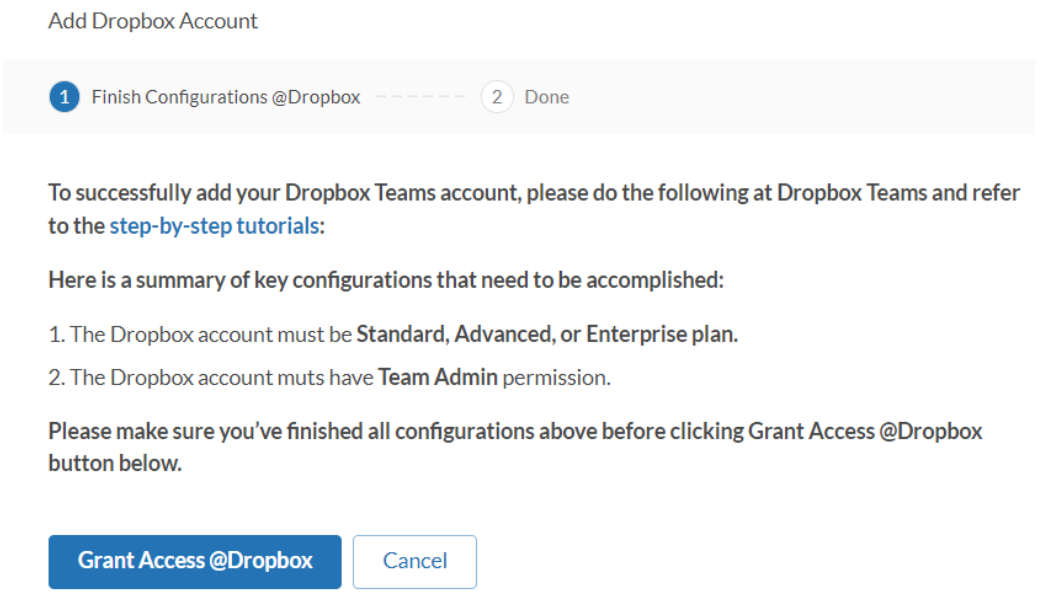
Update Dropbox Business on page 101

Add Dropbox Business

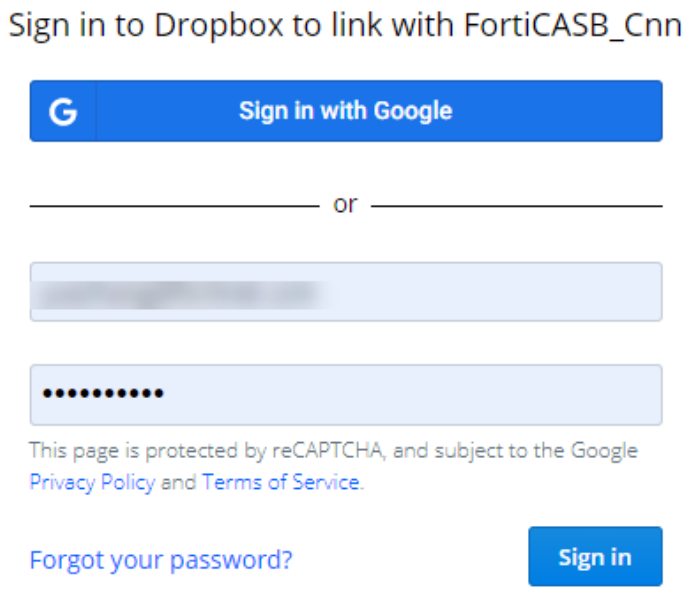
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Dropbox**, then click **Add Selected Cloud App**.



3. Click **Grant Access @Dropbox** to be re-directed to Dropbox website.



4. Log in to authenticate. Dropbox will prompt you to **allow** or **deny** access.



5. Click **Allow** to grant FortiCASB permissions to monitor your Dropbox application.

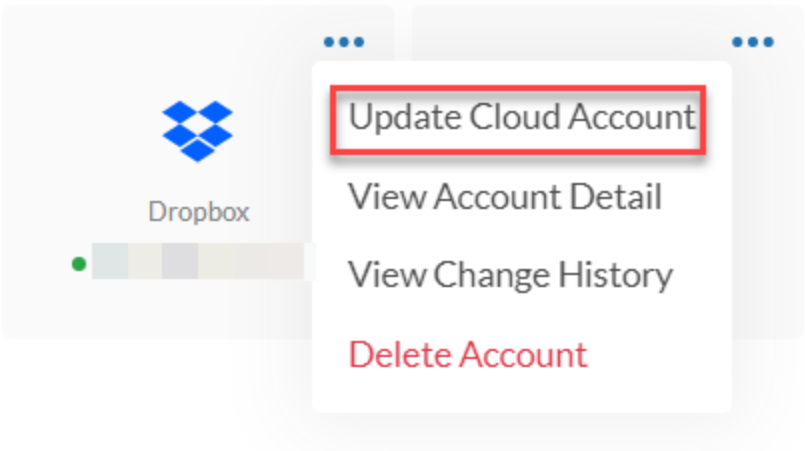
After you click **Allow**, you will be redirected back to the FortiCASB dashboard.

You can check the installation result and SaaS platform monitoring status in the Dropbox dashboard.

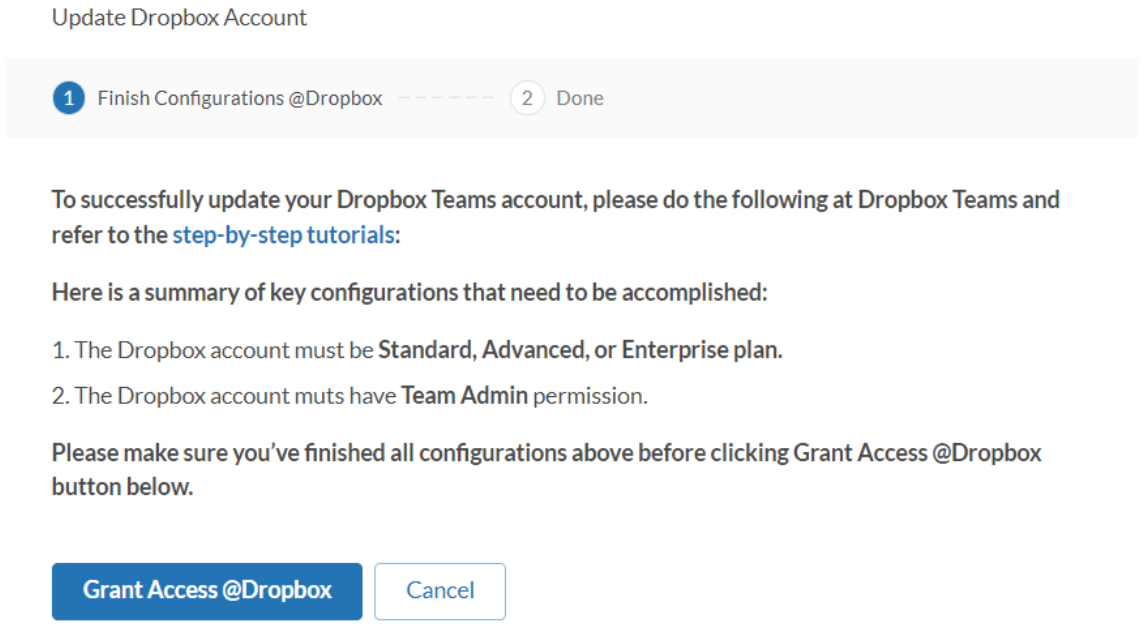
For more information on common installation issues, see Troubleshooting on page 515

Update Dropbox Business

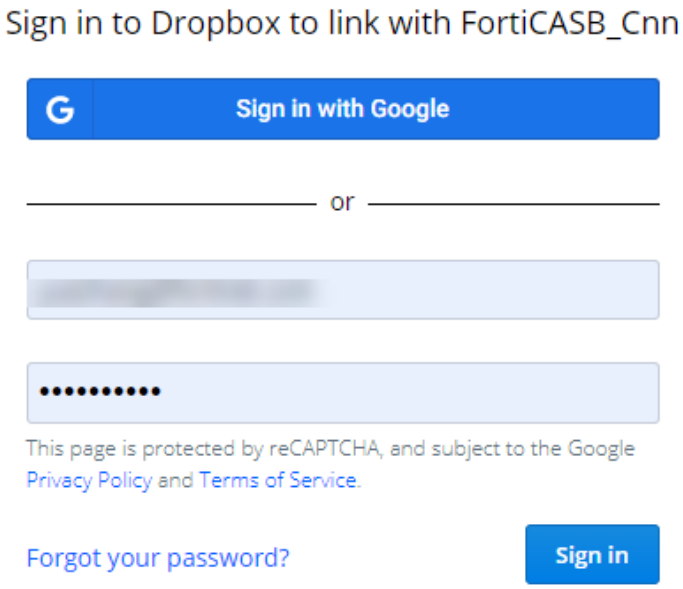
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**
3. Click on Dropbox account menu, and select **Update Cloud Account**.



4. Click **Grant Access @Dropbox** to be re-directed to Dropbox website.



5. Log in to authenticate. Dropbox will prompt you to **allow** or **deny** access.



6. Click **Allow** to grant FortiCASB permissions to monitor your Dropbox application.

After you click **Allow**, you will be redirected back to the FortiCASB dashboard.

You can check the account checklist and platform monitoring status in the Dropbox dashboard.

For more information on common installation issues, see Troubleshooting on page 515

Egnyte

FortiCASB offers an API-based approach, pulling data directly from Egnyte via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Egnyte user activities, provides DLP Data Analysis for files stored on Egnyte.

Prerequisites

The Egnyte account must be an **Administrator**, all other roles are NOT supported.

After you have verified the prerequisites, continue to **Add** or **Update** the account:

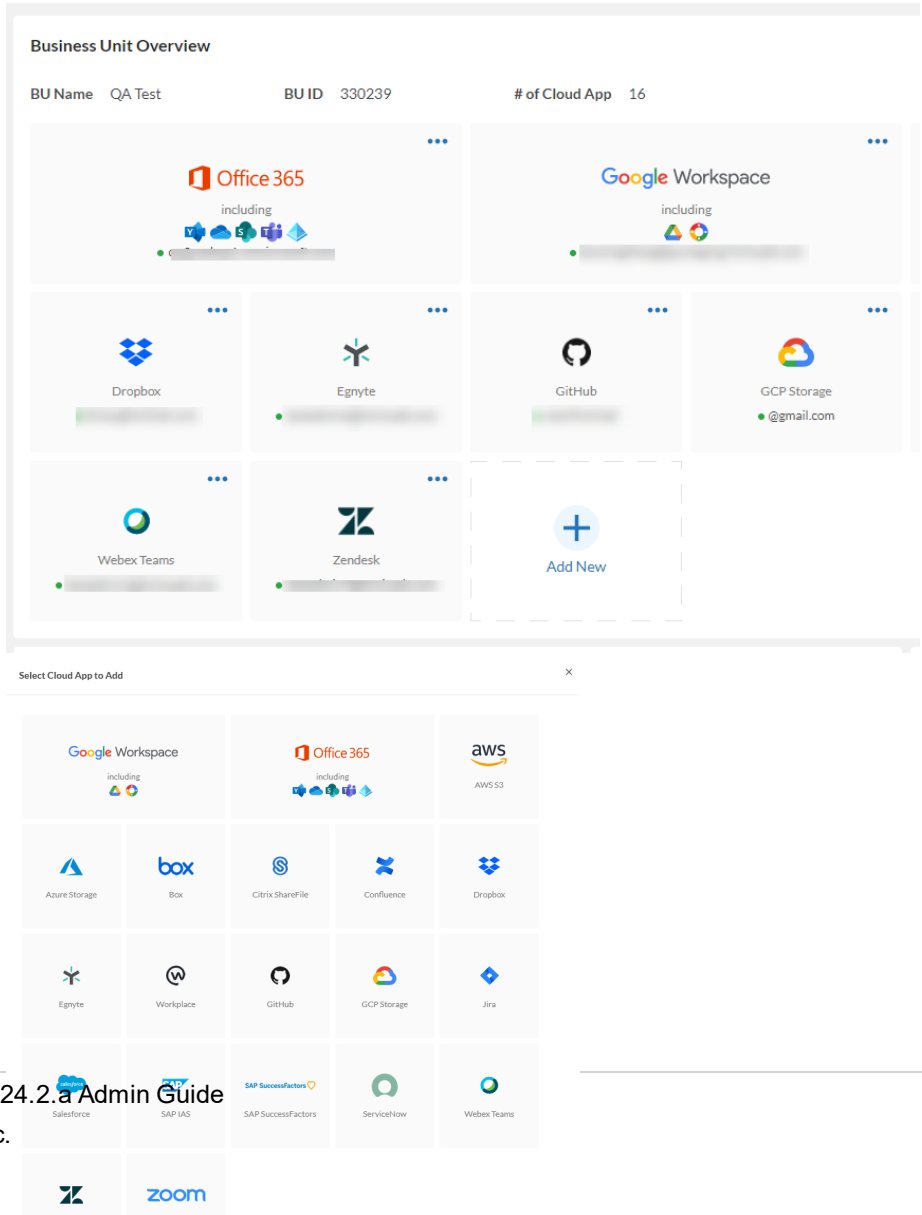
Add Egnyte Account on page 103

Update Egnyte Account on page 105

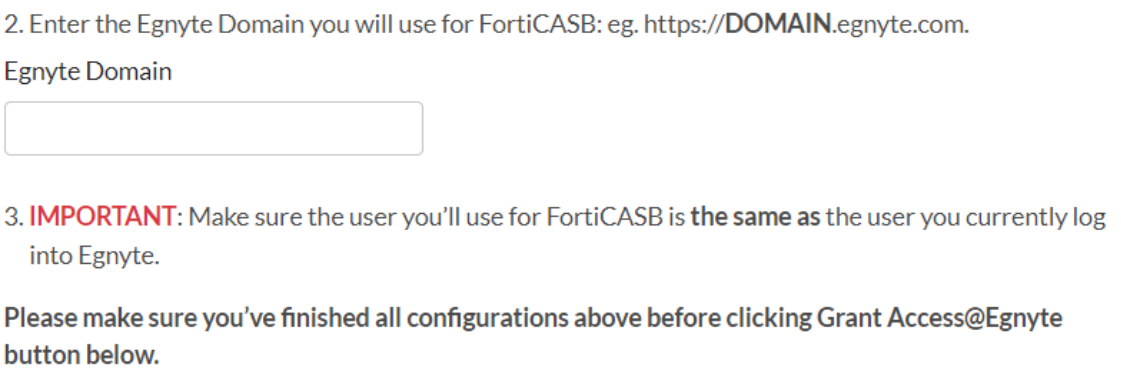
Add Egnyte Account

Follow these steps to add Egnyte account on FortiCASB:

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Egnyte**, then click **Add Selected Cloud App**.

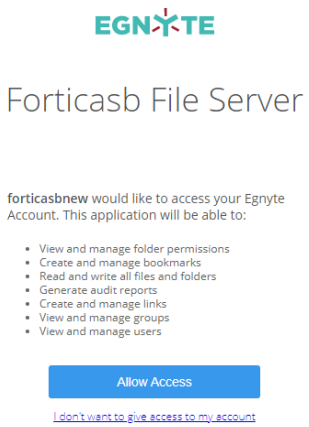


3. Enter the Egnyte Domain you will use on FortiCASB: e.g. https://**DOMAIN**.egnyte.com.



Important: Make sure the user you'll add on FortiCASB is the same user you are currently logged in on Egnyte.

4. Click **Grant Access@Egnyte**.
5. You will be re-drected to Egnyte OAuth page to ask you to grant FortiCSB access to the Egnyte account. Click **Allow Access**.

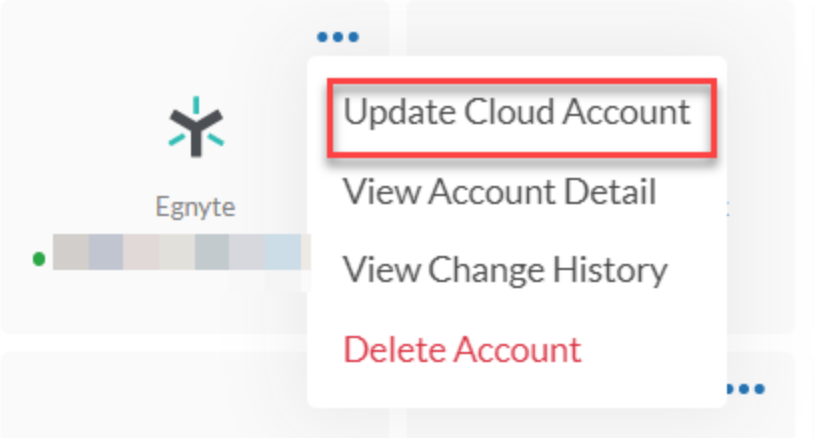


After the Egnyte OAuth validation, the add account process may take 15 minutes to complete. You may check the status in **Overview > Dashboard.**

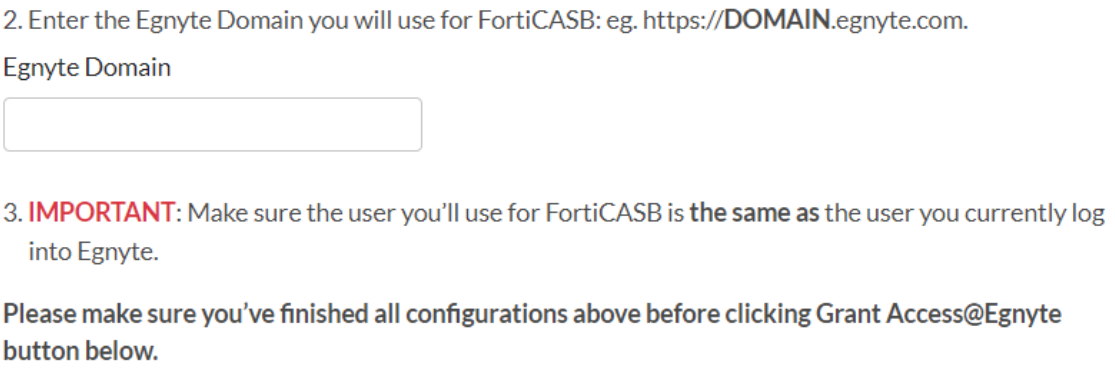
Update Egnyte Account

Follow these steps to udpate Egnyte account on FortiCASB:

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**
3. Click on the**Egnyte** account menu, and select **Update Cloud Account**.

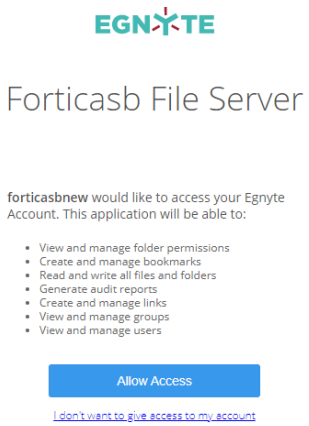


4. Enter the Egnyte Domain you will use on FortiCASB: e.g. https://**DOMAIN**.egnyte.com.



Important: Make sure the user you'll add on FortiCASB is the same user you are currently logged in on Egnyte.

5. Click **Grant Access@Egnyte**.
6. You will be re-drected to Egnyte OAuth page to ask you to grant FortiCSB access to the Egnyte account. Click **Allow Access**.



After the Egnyte OAuth validation, the add account process may take 15 minutes to complete. You may check the status in **Overview > Dashboard.**

Facebook Workplace

FortiCASB offers an API-based approach, pulling data directly from Facebook Workplace via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Facebook Workplace user activities, conducts DLP Data Analysis for files shared on Facebook Workplace.

Prerequisites

The Facebook Workplace plan must be **Advanced** or **Enterprise**, free plan is NOT supported.

The Facebook Workplace account to be added on FortiCASB must be the **System Administrator** user.

After you have verified the prerequisites, continue to **Add** or **Update** the account:

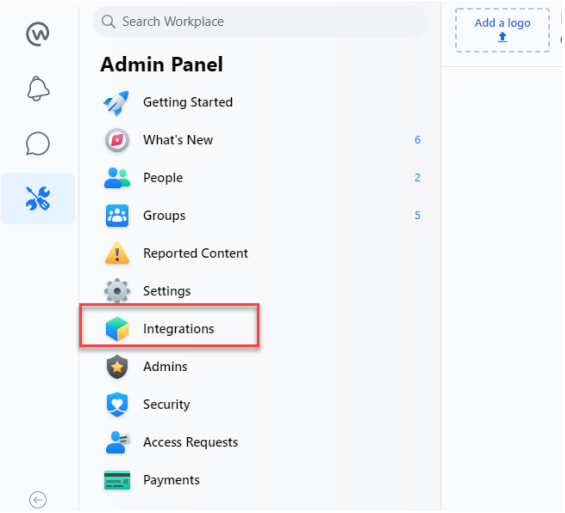
Add Facebook Workplace Account on page 107

Update Facebook Workplace Account on page 110

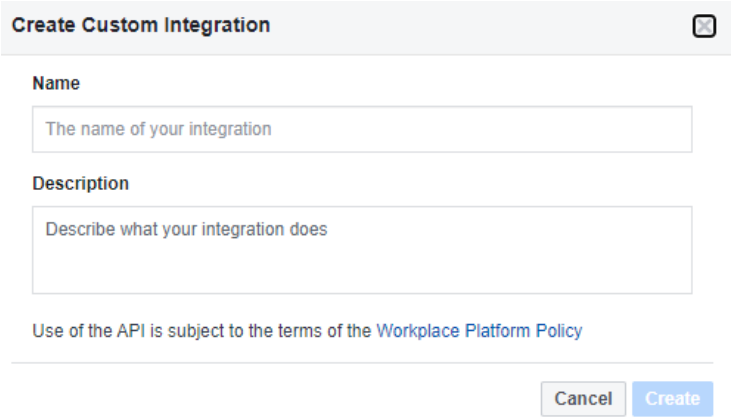
Add Facebook Workplace Account

Follow these steps to configure Workplace account before adding the Workplace account on FortiCASB:

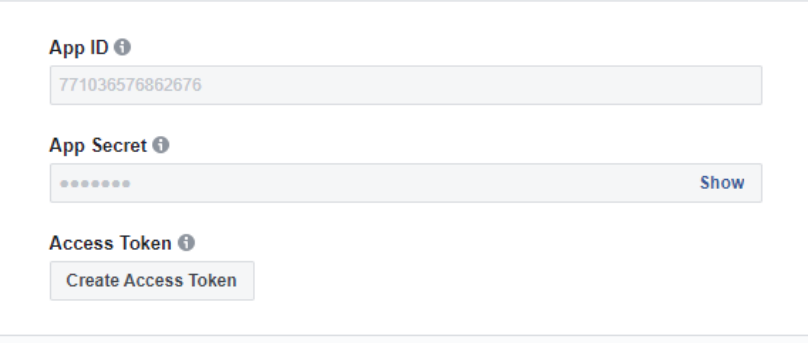
1. Log into Facebook Workplace with the System Administrator account.
2. Navigate to **Admin Panel** on the left navigation bar and click **Integrations**.



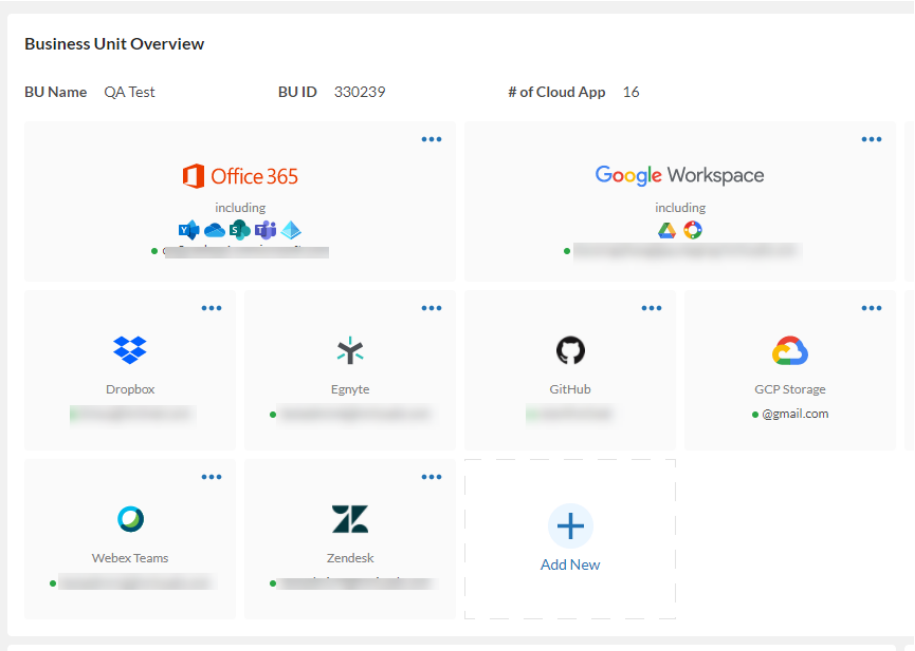
3. Click **Create Custom Integration**, fill in the **Name** and **Description** fields, then click **Create**.

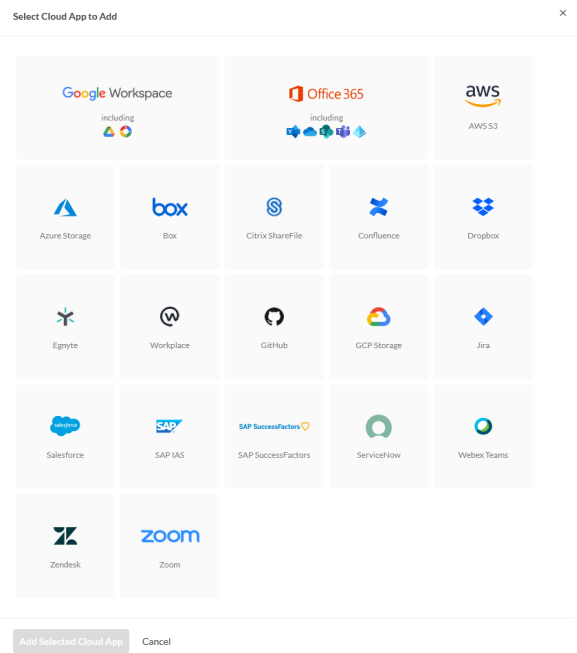


4. Under the **Integration Details**, make a note of **App ID** and **App Secret**, click **Create Access Token** and copy the generated token to be used later.

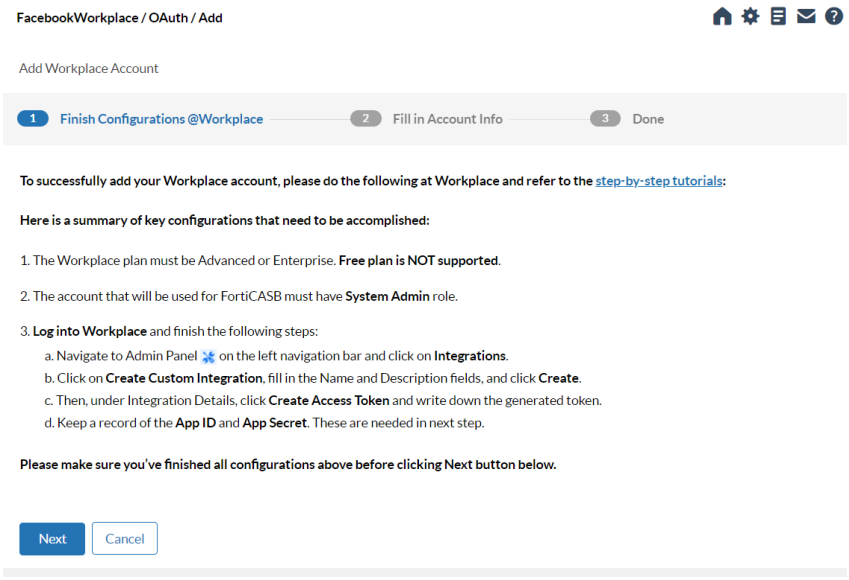


5. Now go back to FortiCASB, go to **Overview > Dashboard**, click on **Add New**, select **Workplace**, then click **Add Selected Cloud App**.

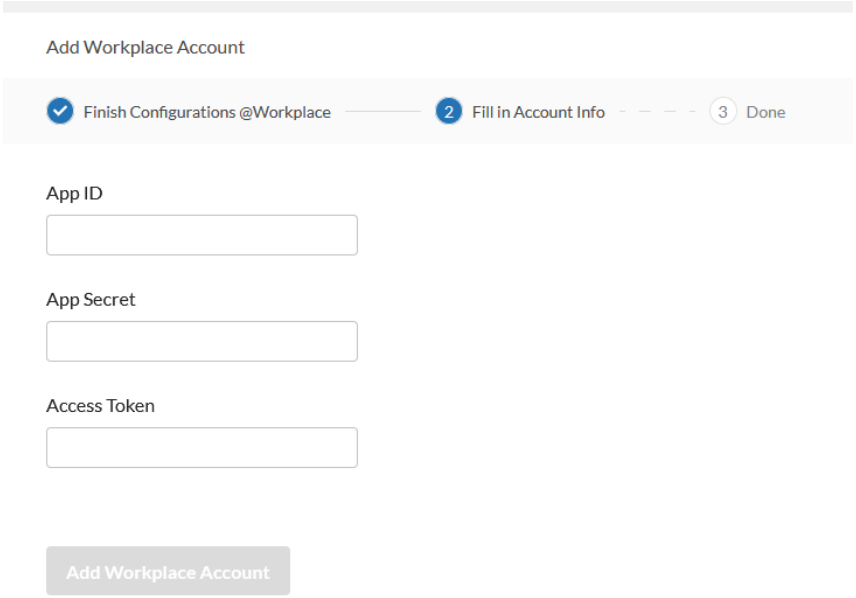




6. Click **Next** on the FortiCASB **Add Workplace Account** page to proceed:



7. Enter the **App ID**, **App Secret**, and **Access Token**, and click **Add Workplace Account**.

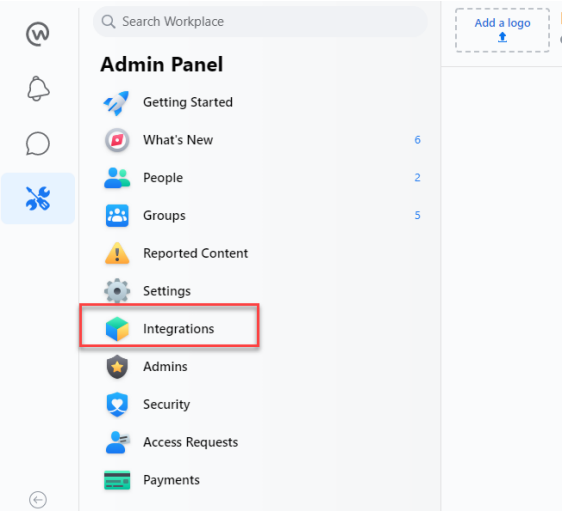


The add account process may take 15 minutes to complete. You may check the status in **Overview > Dashboard.**

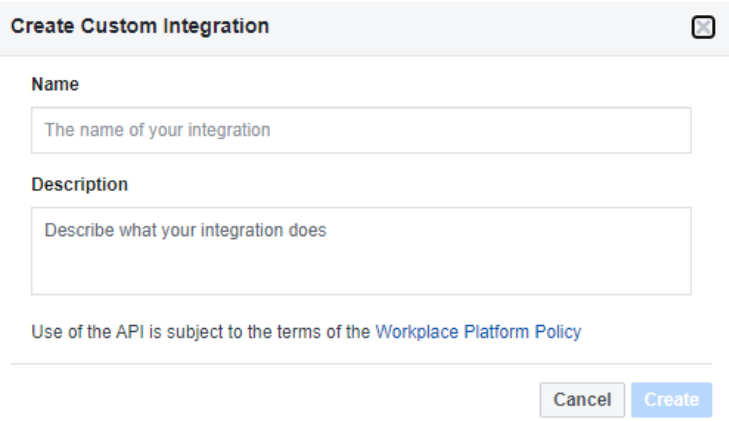
Update Facebook Workplace Account

Follow these steps to configure Workplace account before updating the Workplace account on FortiCASB:

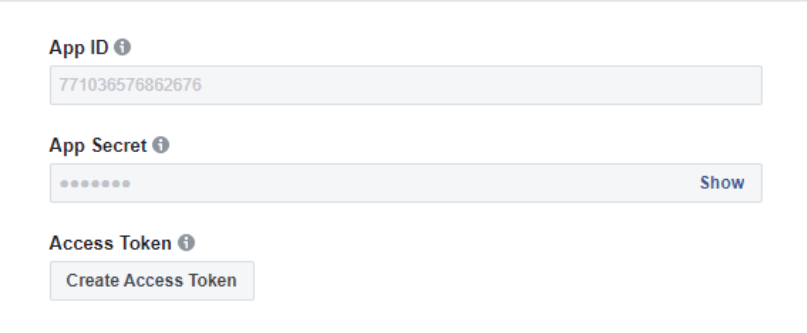
1. Log into Facebook Workplace with the System Administrator account.
2. Navigate to **Admin Panel** on the left navigation bar and click **Integrations**.



3. Click **Create Custom Integration**, fill in the **Name** and **Description** fields, then click **Create**.

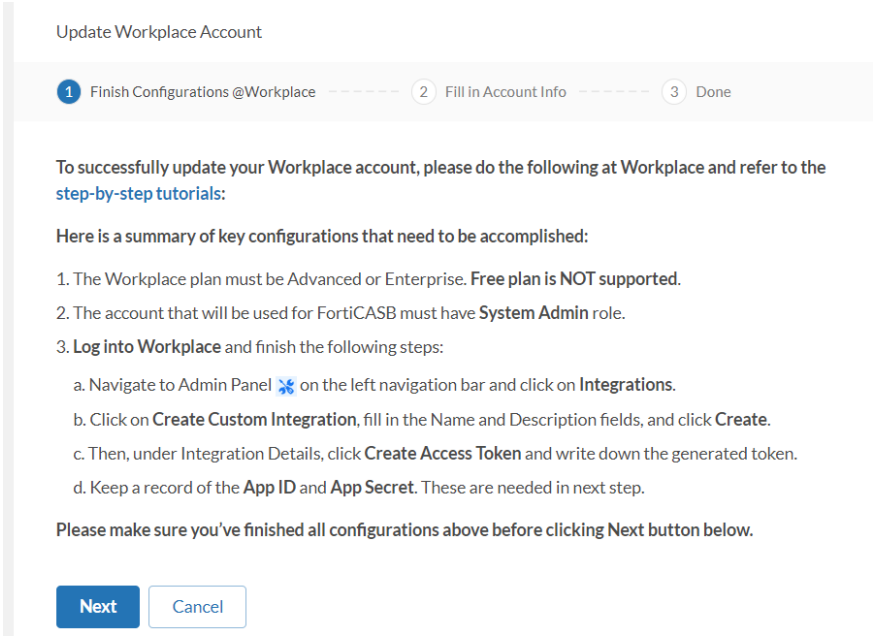


4. Under the **Integration Details**, make a note of **App ID** and **App Secret**, click **Create Access Token** and copy the generated token to be used later.

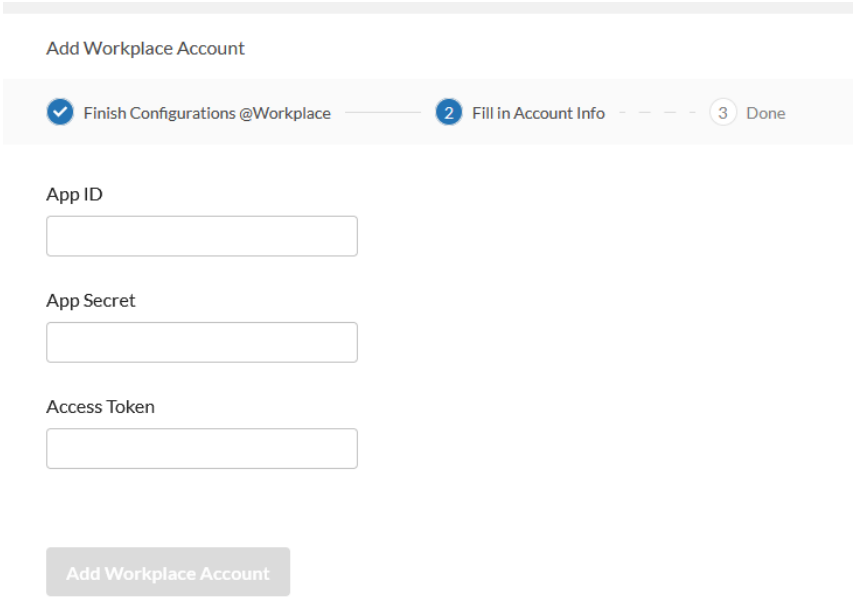


5. Now go back to FortiCASB, go to **Overview > Dashboard.**

6. Click on the **Workplace** account menu, and select **Update Cloud Account**.
7. Click **Next** on the FortiCASB **Update Workplace Account** page to proceed:



8. Enter the **App ID**, **App Secret**, and **Access Token**, and click **Add Workplace Account**.



The add account process may take 15 minutes to complete. You may check the status in **Overview > Dashboard.**

Github

FortiCASB offers an API-based approach, pulling data directly from Github via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Github user activities, provides DLP Data Analysis for files stored on Github.

Prerequisites

The GitHub account must be one of these **organization plans**: **Free** , **Team**, or **Enterprise**. (Personal User account is NOT supported)

The GitHub account to be added to FortiCASB must be the **Organization Owner**, all other roles are not supported.

After you have verified the prerequisites, continue to **Add** or **Update** the account:

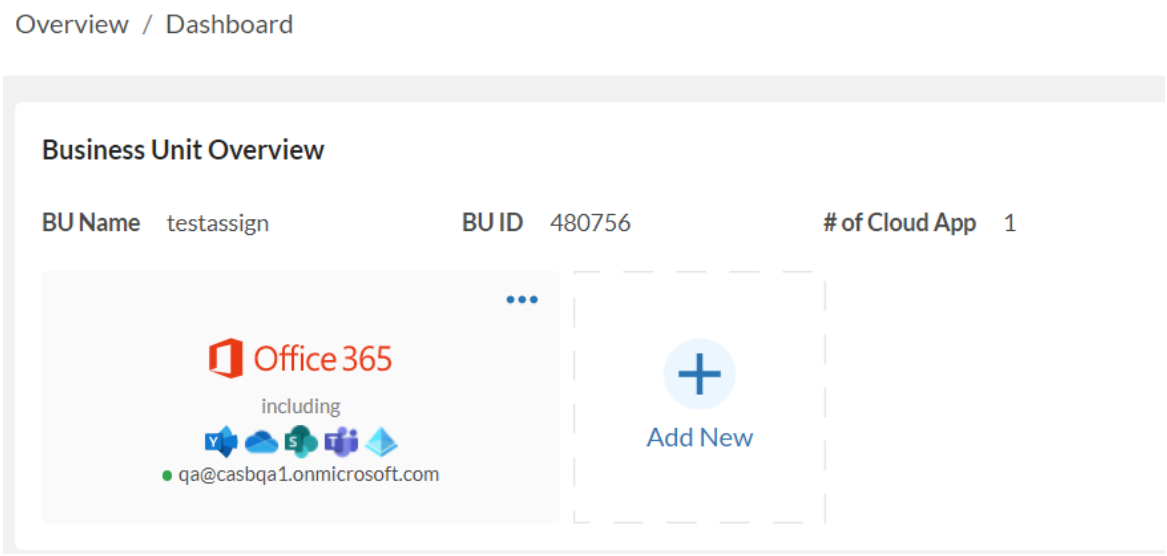
Add GitHub Account on page 112

Update GitHub Account on page 115

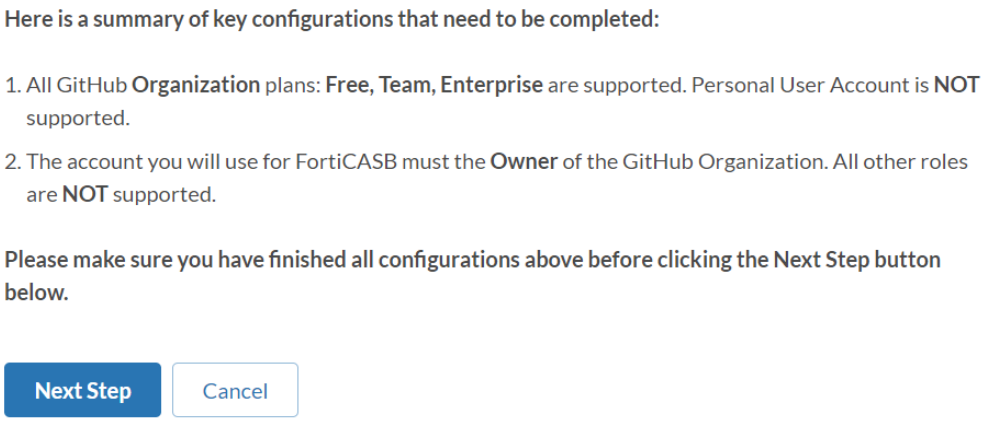
Add GitHub Account

Follow the steps below to update GitHub account on FortiCASB:

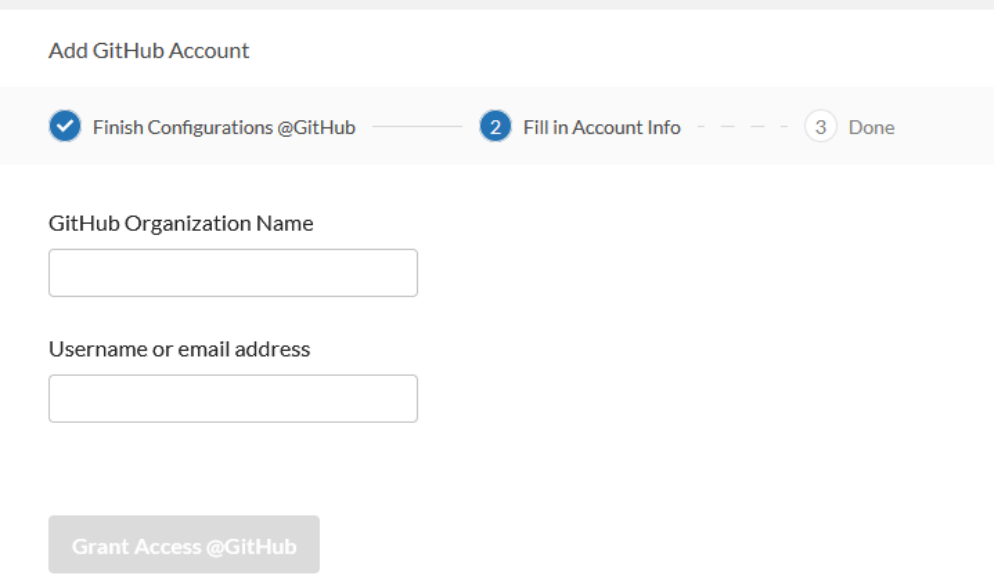
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**,
3. click on **Add New**, select **GitHub**, then click **Add Selected Cloud App**.



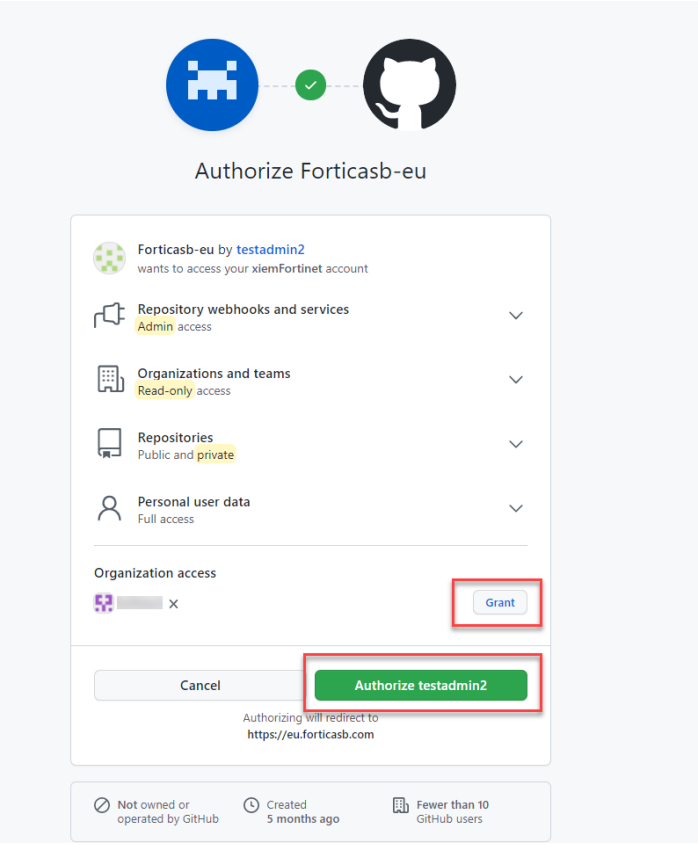
4. Verify that the your Github account fulfills the requirement and click **Next Step**.



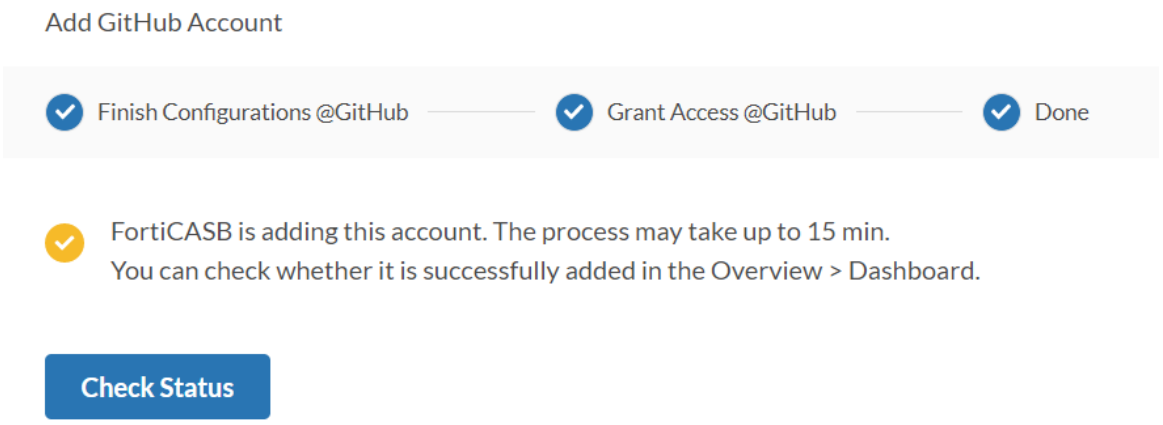
5. Fill in **GitHub Organization Name** and **Username or e-mail address** of the account, then click **Grant Access@GitHub**.



6. You will be redirected to GitHub OAuth page with request to authorize FortiCASB access to the Organization.
7. In **Organization Access**,
   a. Click **Grant** to grant the user to access the organization, then
   b. Click **Authorize (username)** to authorize the request. Then you will be re-direct back to FortiCASB.



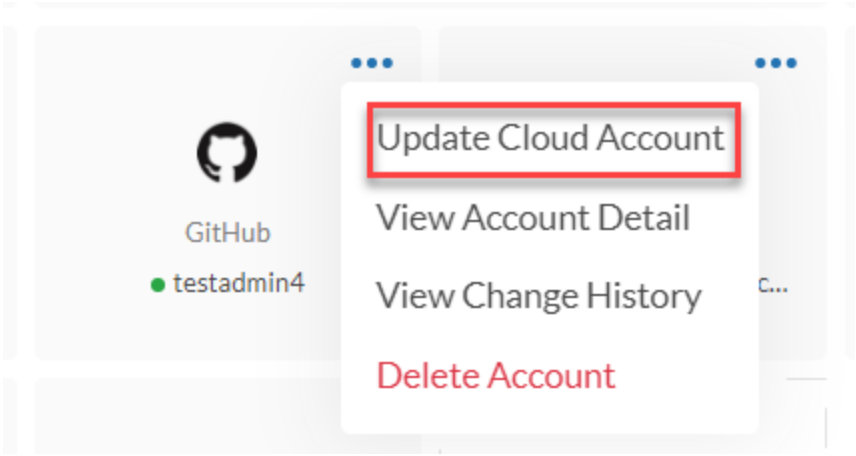
The add account process is completed, please wait 15 minutes and check on the status of the account.



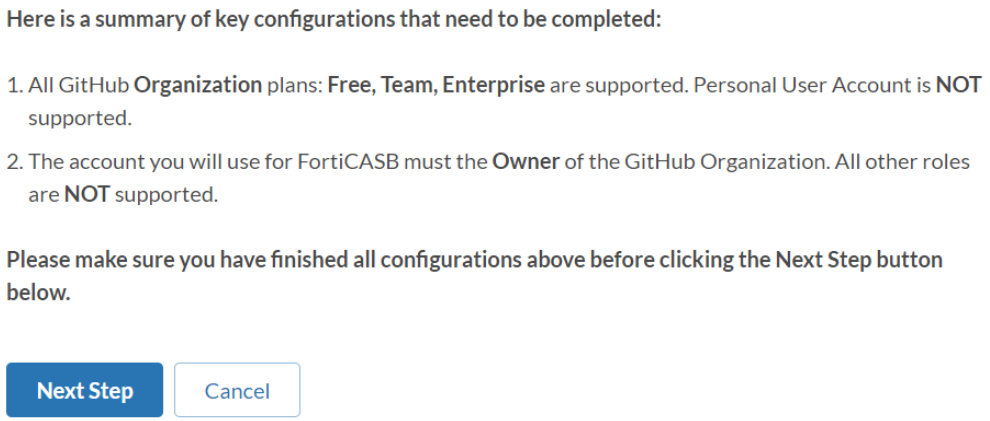
Update GitHub Account

Follow the steps below to add GitHub account on FortiCASB:

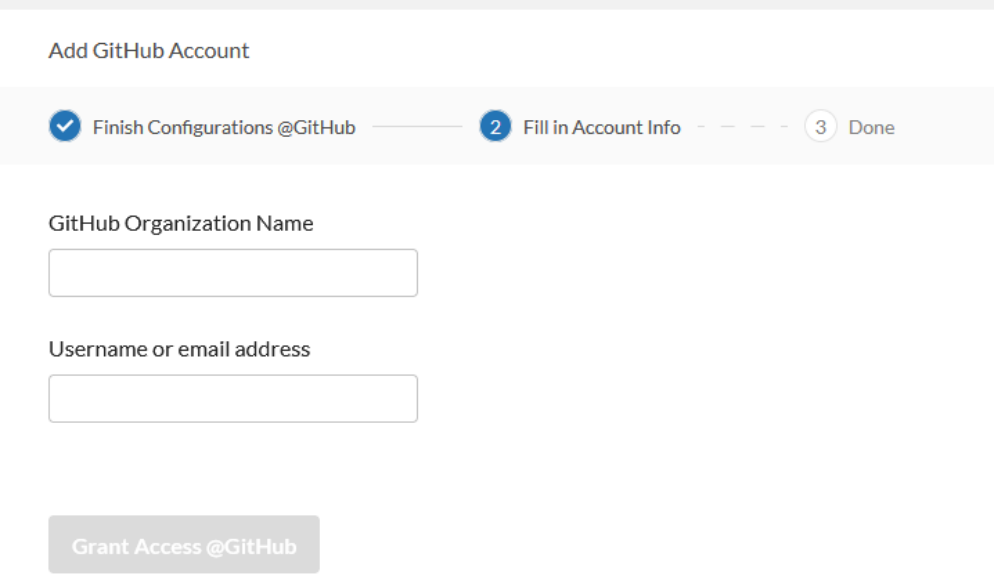
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**,
3. Click on the **GitHub** account menu, and select **Update Cloud Account**.



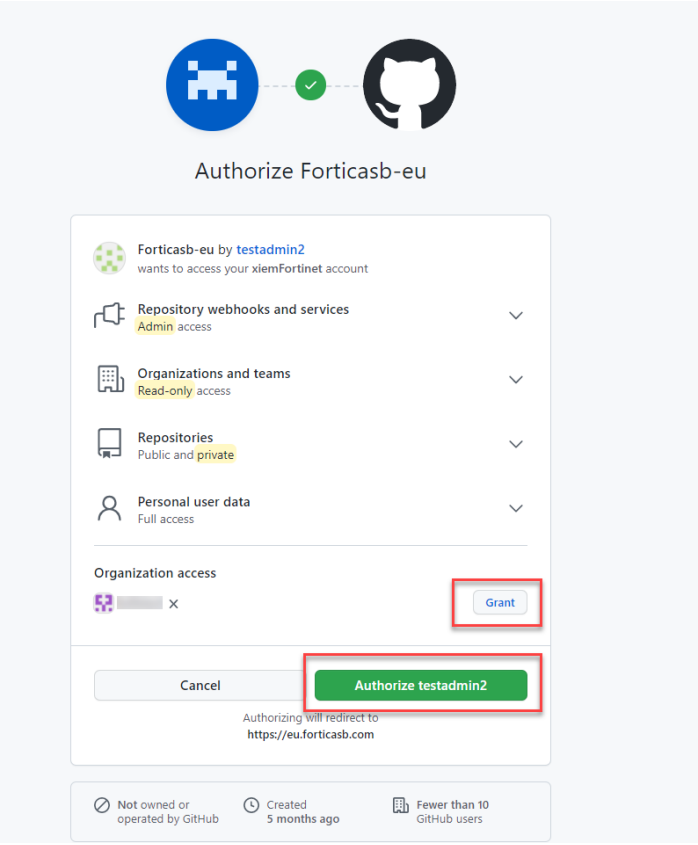
4. Verify that the your GitHub account fulfills the requirement and click **Next Step**.



5. Fill in **GitHub Organization Name** and **Username or e-mail address** of the account, then click **Grant Access@GitHub**.



6. You will be redirected to GitHub OAuth page with request to authorize FortiCASB access to the Organization.
7. In **Organization Access**,
   a. Click **Grant** to grant the user to access the organization, then
   b. Click **Authorize (username)** to authorize the request. Then you will be re-direct back to FortiCASB.



The update account process is completed, please wait 15 minutes and check on the status of the account.

Google Cloud Storage

FortiCASB offers an API-based approach, pulling data directly from Google Cloud Storage via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Google Cloud Storage user activities, conducts DLP Data Analysis for files stored on Google Cloud Storage.

Prerequisites

To use FortiCASB with Google Cloud Platform, you must have a **Google Workspace account**, **Service Account**, and the **JSON private key** associated with the service account. The service account must have "**Google Workspace Domain-wide Delegation**" enabled and **Project Owner/Organization Administrator roles** for monitoring.

Steps to Add Google Cloud Account

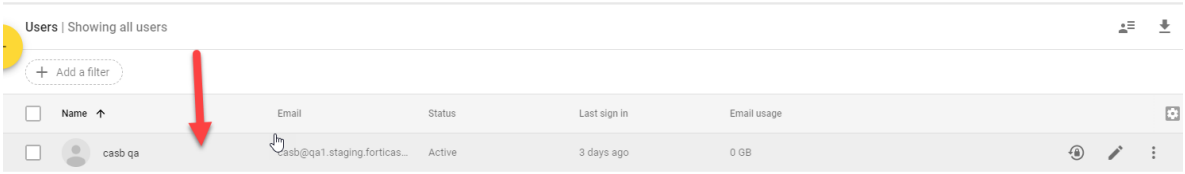
1. **Configure Google Workspace Account on page 119**
2. **Configure OAuth Consent Screen on page 120**
3. **Create Service Account on page 126**
4. **Grant Service Account API Access on page 129**
5. **Grant Service Account Owner and Organization Administrator Role on page 131**
6. **Enable required APIs on page 133**
7. **Enable activity and alert monitoring on page 135**
8. **Add Google Cloud Storage Account on page 136**

Your Google Workspace account can be either an existing account or a new account. If you have just created a new account, you must wait for at least 24 hours for the account to take effect before granting it access to FortiCASB. The Google Workspace account which you connect from with FortiCASB must have the **Super Admin role**.

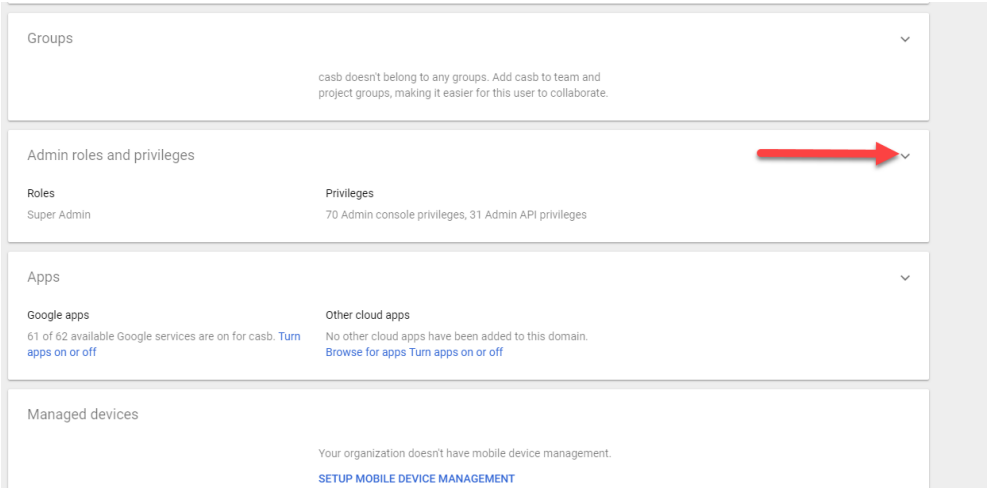
Configure Google Workspace Account

Use the following steps to check if your account has the Super Admin role:

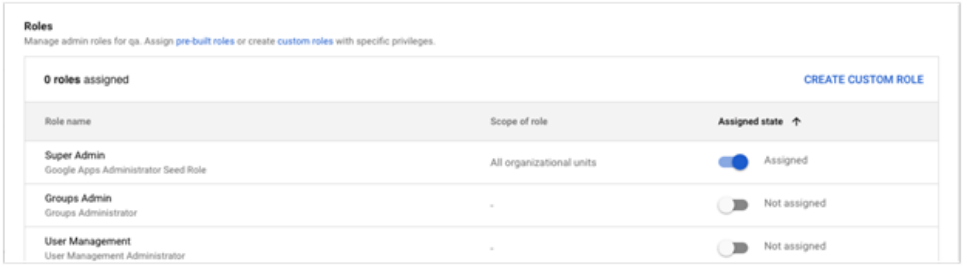
1. Log into Google Admin with your **Google Workspace** account credentials.
2. In the upper-left corner, click the **navigation menu** ☰, and select **Directory** > **Users**.
3. Click on the user account of interest.



4. Scroll down to the **Admin roles and privileges** section, and click on the expand button.



5. In the **Roles** section, make sure that the **Super Admin role** has been assigned. If not, assign the **Super Admin** role by clicking on the toggle switch butoon.

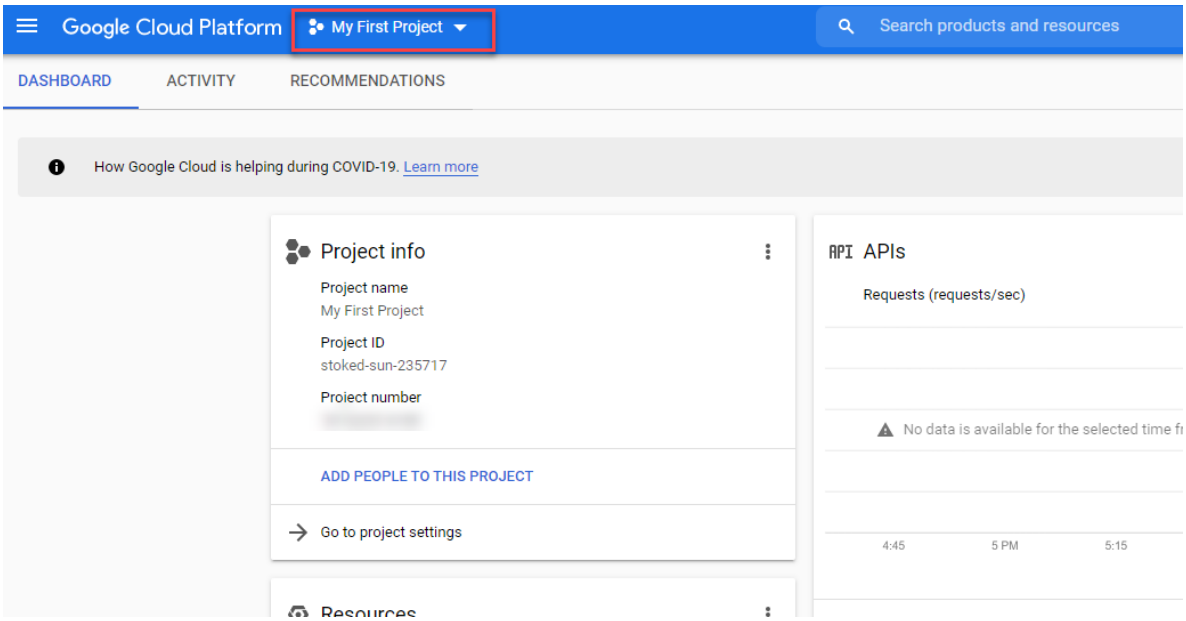


Configure OAuth Consent Screen

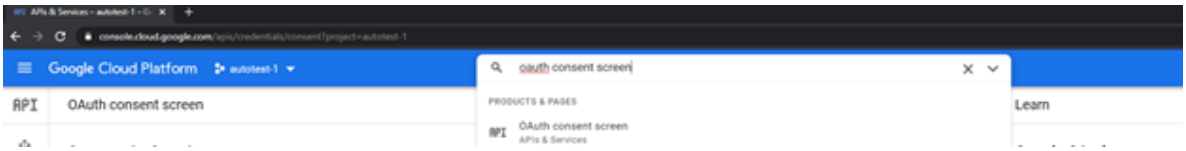
The Google project needs to have **OAuth Consent Screen** created and configured to enable **Google Workspace Domain-Wide Delegation** when service account is created.

Note: If you have already configured OAuth Consent Screen for the project, you can skip this section.

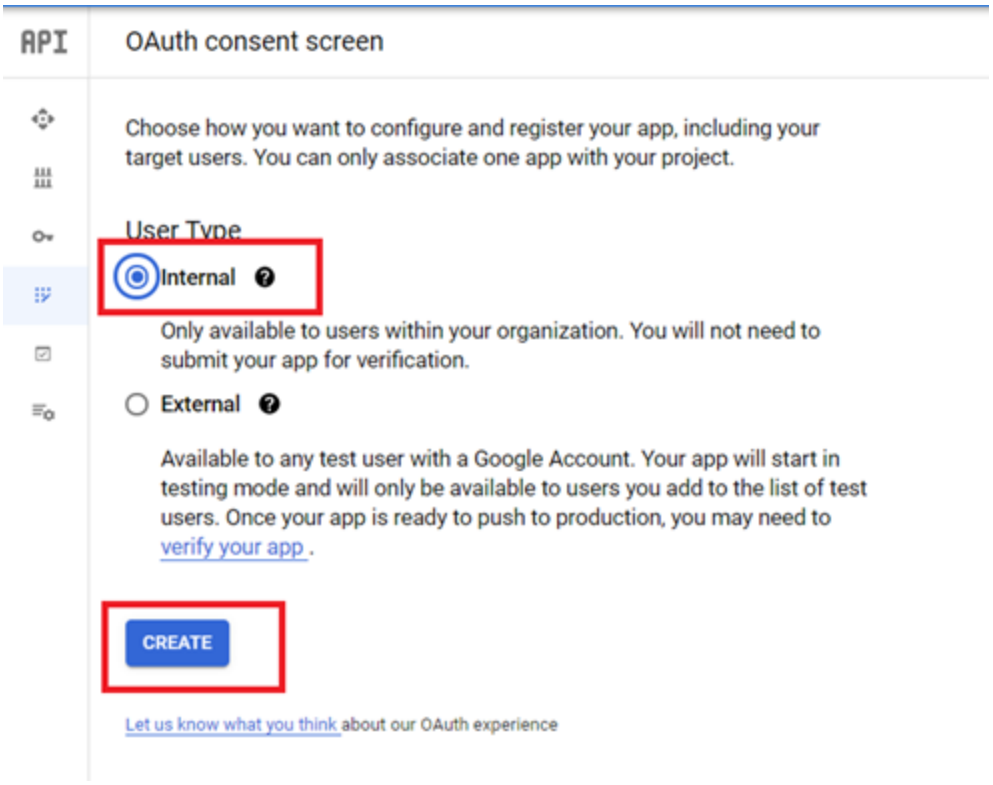
1. Go to Google Cloud Platform and log in with your **Google Workspace account**.
2. Click on the project drop-down menu > **Select a project**. Select an existing project you want to monitor or create a new project by selecting **New Project**.



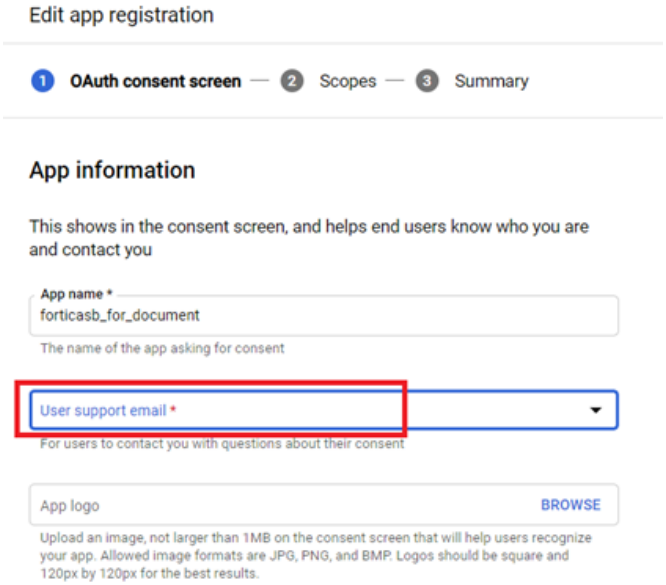
3. With your project selected, search and click on **OAuth Consent Screen**.



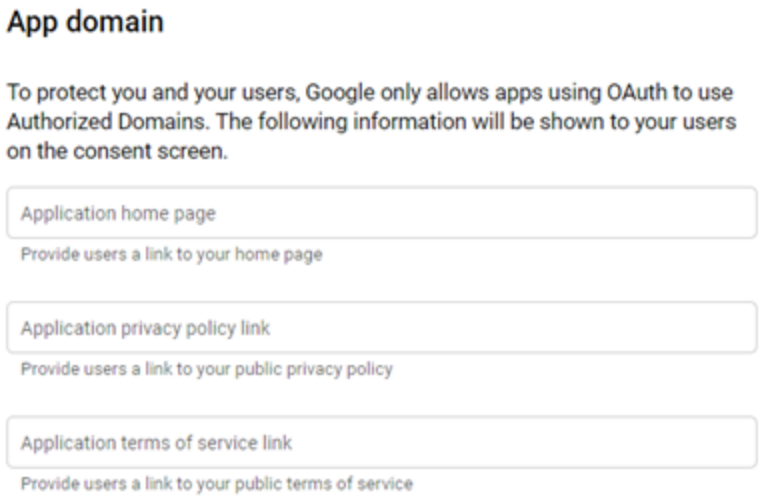
4. When you get started with OAuth Consent Screen configuration, choose **Internal** user type, then click **CREATE**.



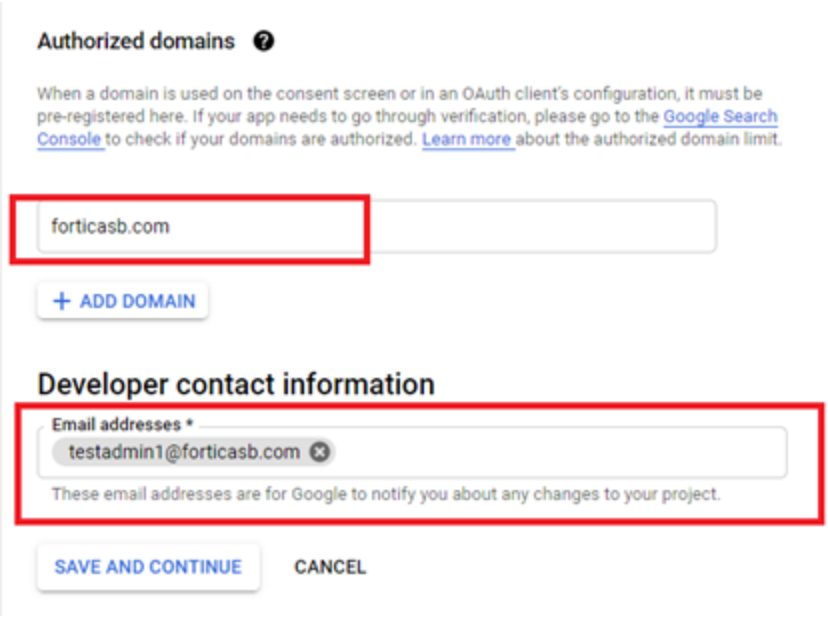
5. **Step 1: OAuth Consent Screen:**
   a. Name the app and choose the user that will manage the app within the Google Cloud Platform account.



   b. For the App domain, leave it as blank since it will only be for internal use.

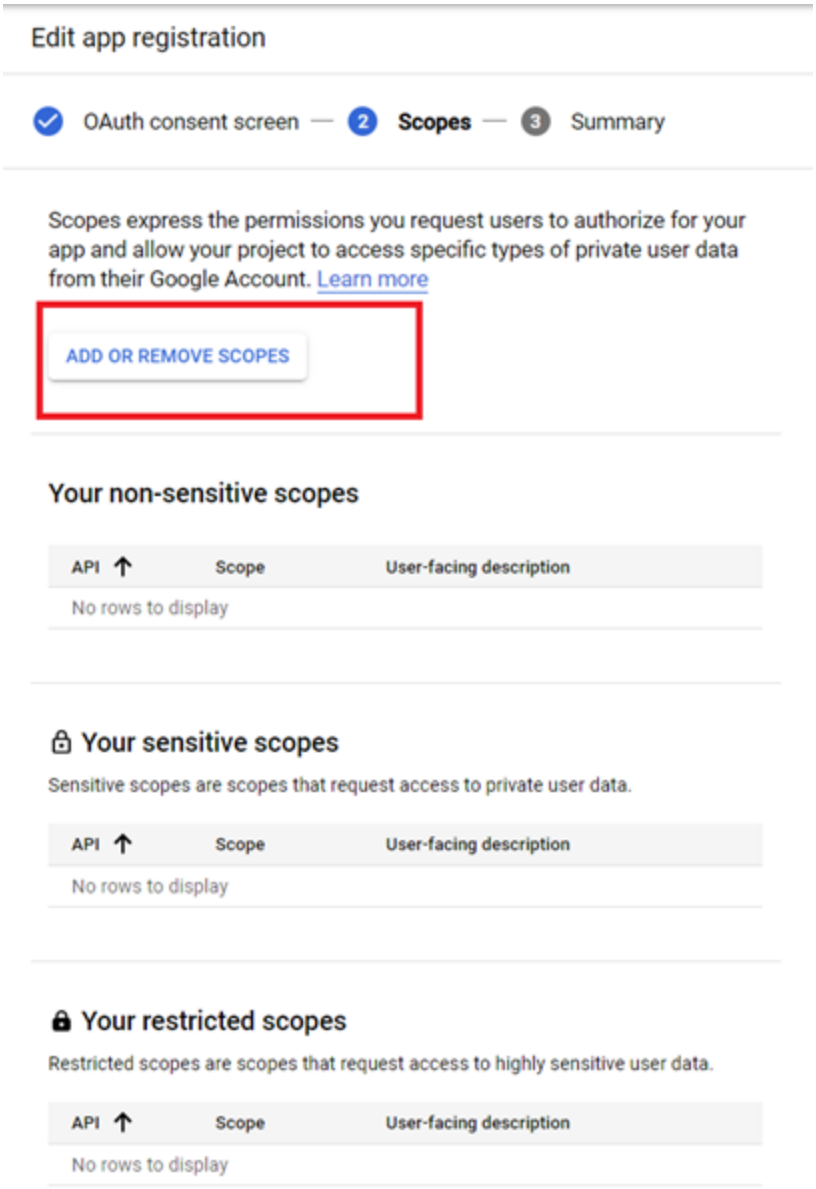


c. Click **+ADD DOMAIN** and enter the domain of this Google Cloud Platform account.
For example, if the Google Cloud Platform account I am using is @forticasb.com, then the domain is forticasb.com.

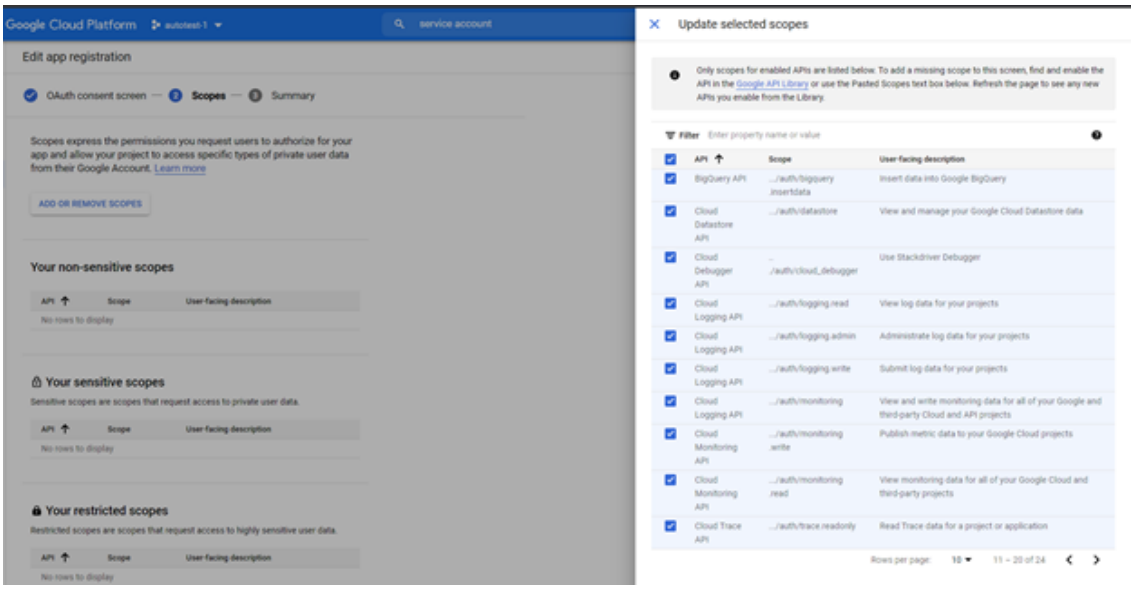


d. In **Developer contact information**, enter the e-mail of the person managing the app.
e. Click **SAVE AND CONTINUE**.

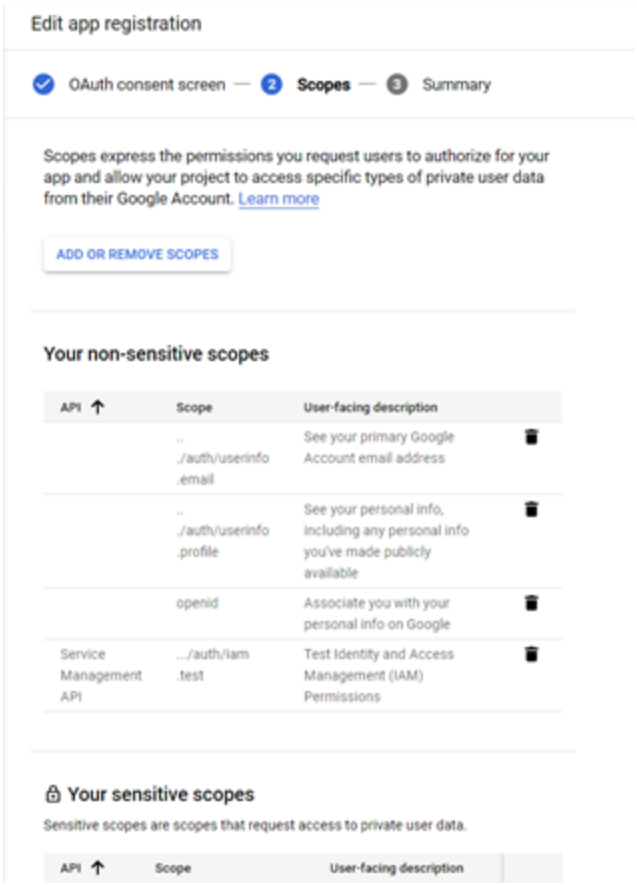
6. **STEP 2: Scopes:**
   a. Click **ADD OR REMOVE SCOPES**.



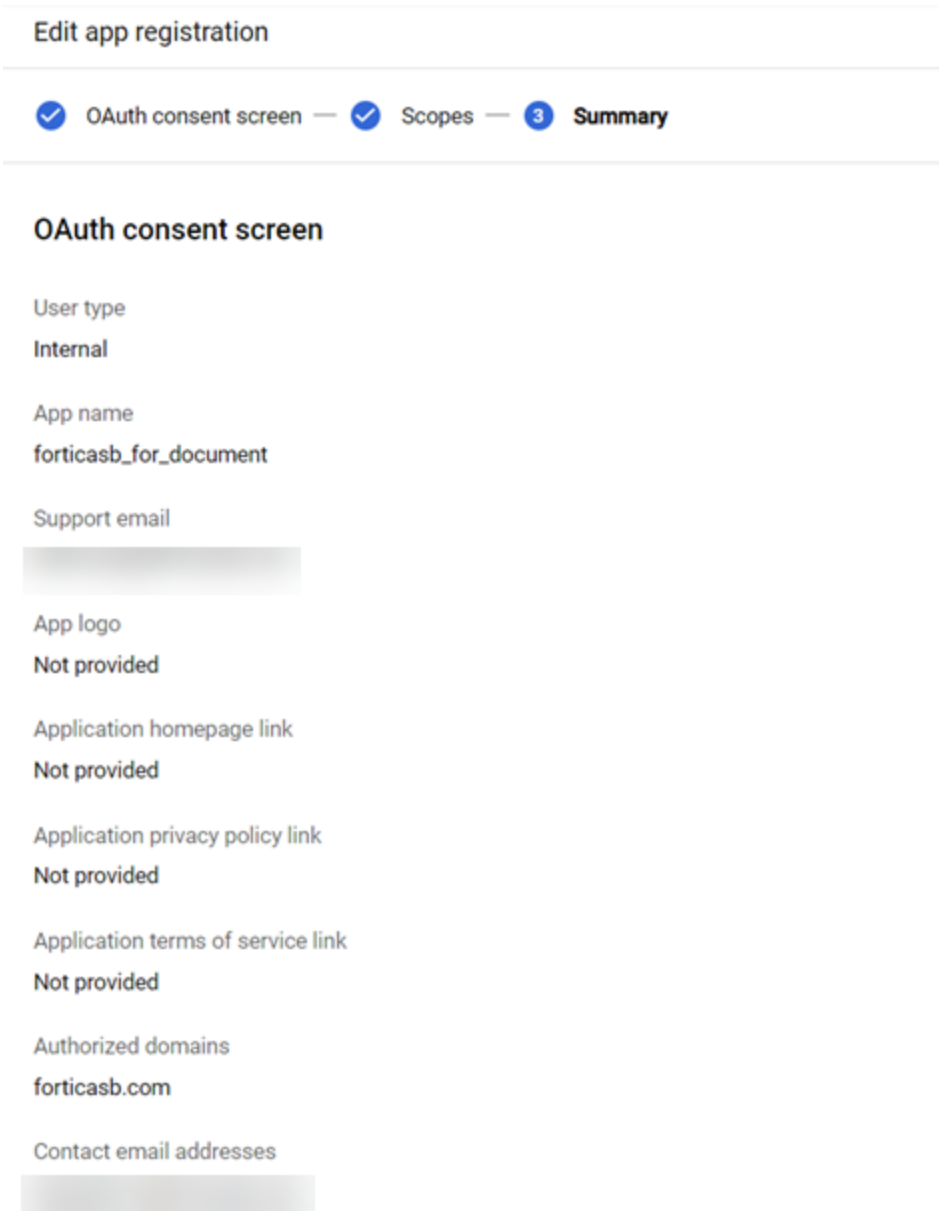
   b. Select **all scopes** of this App and click **update** to apply the settings.



c. Review the scopes selected, then click **SAVE AND CONTINUE**.



d. Review and confirm all settings are correct in the Summary page, then click **BACK TO DASHBOARD**, the OAuth consent screen should now be added to the project.

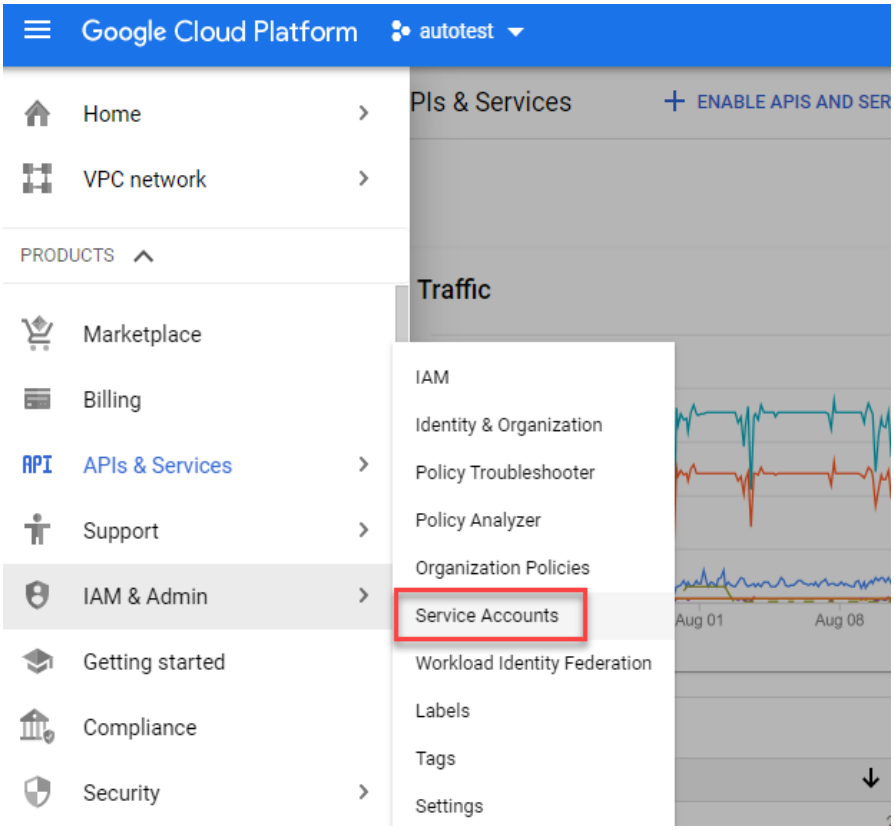


Now **Google Workspace Domain-wide Delegation** can be enabled in Create Service Account on page 126.

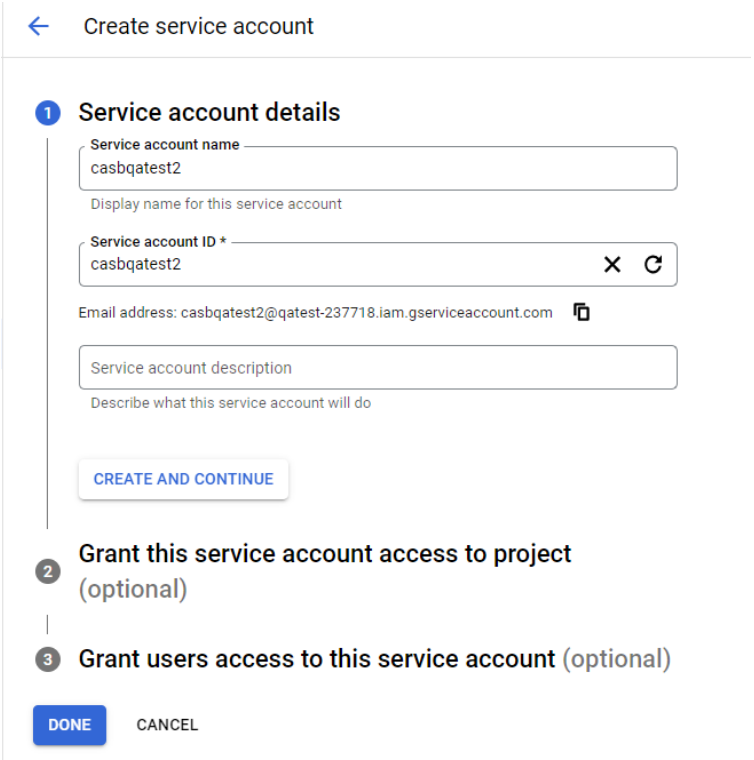
Create Service Account

For your service account, you may either use an existing or create a new service account. The service account needs to be created in the project that has **OAuth Consent Screen** created.

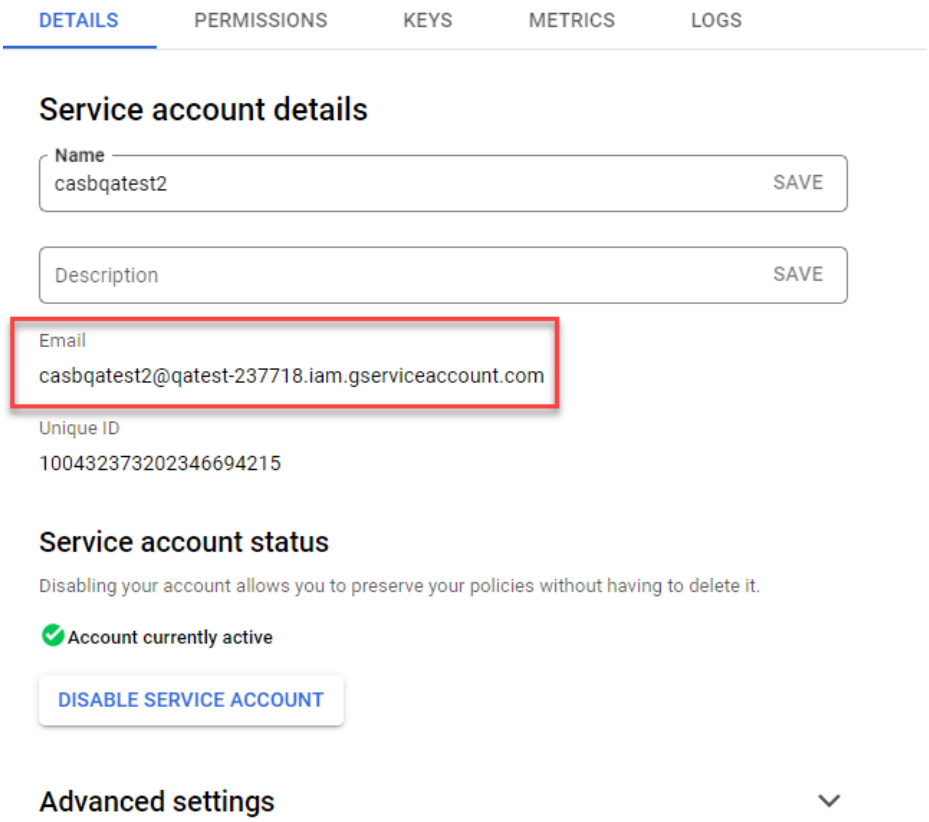
1. Go to the Google Cloud Platform portal and log in with your **Google Workspace account**.
2. With the project selected, click the Navigation Menu ☰ on the top left corner, go to **IAM & Admin > Service accounts.**



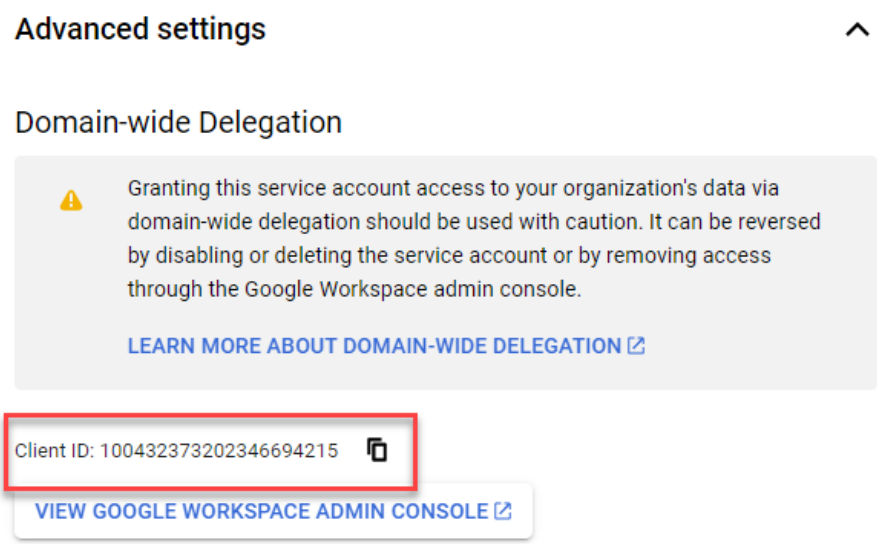
3. Click **+Create service account**, then enter a **Service account name** of your preference and click **CREATE AND CONTINUE**.
   Skip the optional steps, and click **Done**.



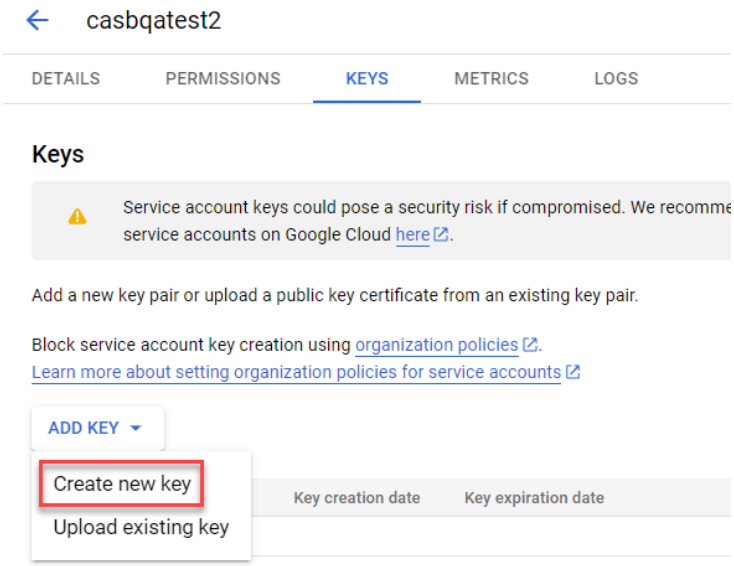
4. In **Service Accounts** page, click on the service account you created to enter the **Details** page, keep a record of the **Service Account ID** (Email).



5. Click on **Advanced settings** drop down menu, and keep a record of the **Client ID** for use later in Grant Service Account API Access on page 129.



6. Click the **KEYS** tab, then click **ADD KEY** drop down menu and select **Create new Key**. Then select **JSON** key format and click **CREATE**. The **JSON** private key will be downloaded automatically.



Keep the **Service Account ID** and **JSON key** later for Google cloud authentication during installation.

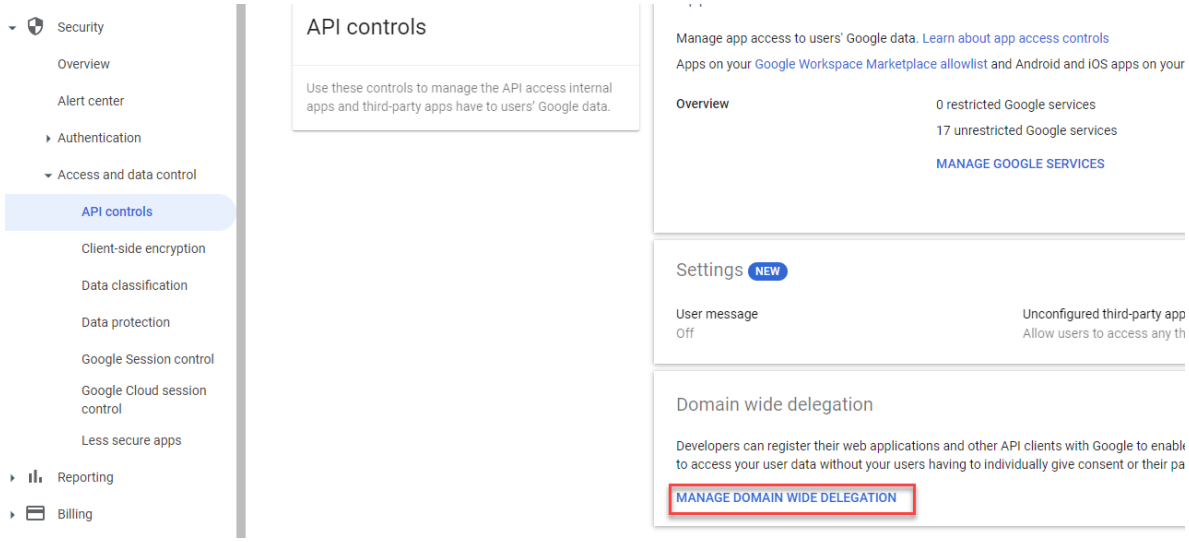
The **Client ID** will be used later in Grant Service Account API Access on page 129.

Grant Service Account API Access

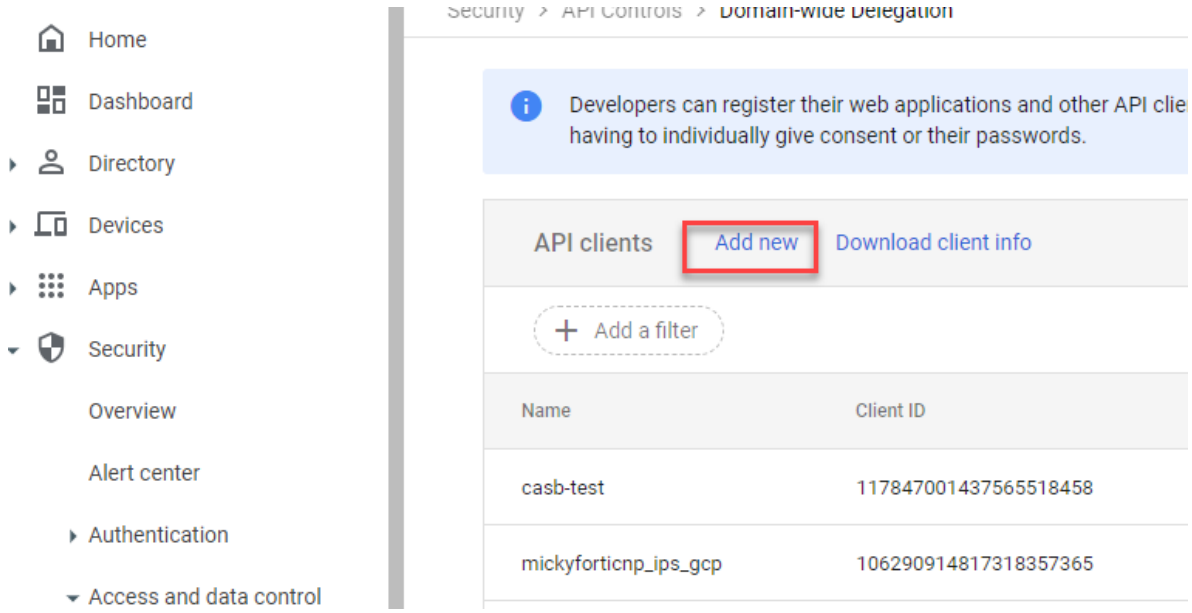
Google Administrator requires Google Workspace account with Super Admin Role to grant the service account with API access.

The account with Super Admin role only needs to perform this one time configuration for the Google Workspace account to be added to FortiCASB.

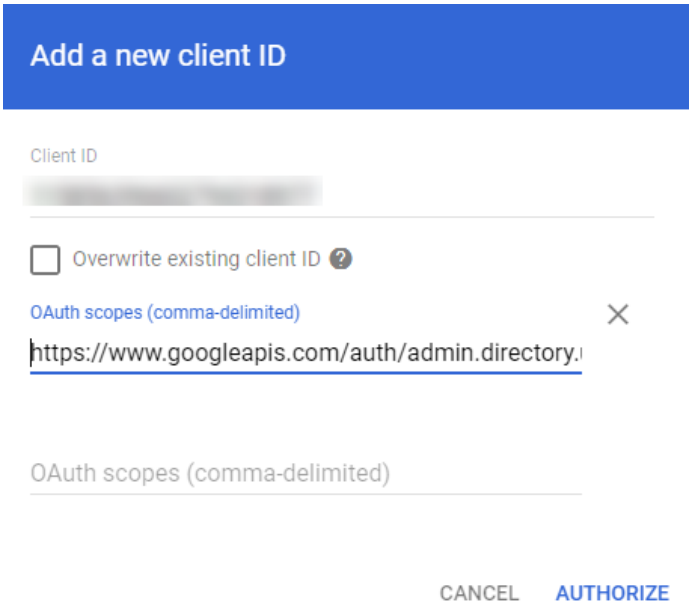
1. Log into Google Admin with the same Google account.
2. Go to **Security > Access and data control > API Controls**, scroll down and click **Manage Domain wide Delegation**.



3. Click **Add new** to authorize the registered client to access your user data.



4. In the **Client ID** field, enter the Client ID saved from Create Service Account on page 126. Your Client ID must be a string of numbers.



5. In the **OAuth scopes** field, enter:

   "https://www.googleapis.com/auth/admin.directory.user,https://www.googleapis.com/auth/admin.reports.audit.readonly".

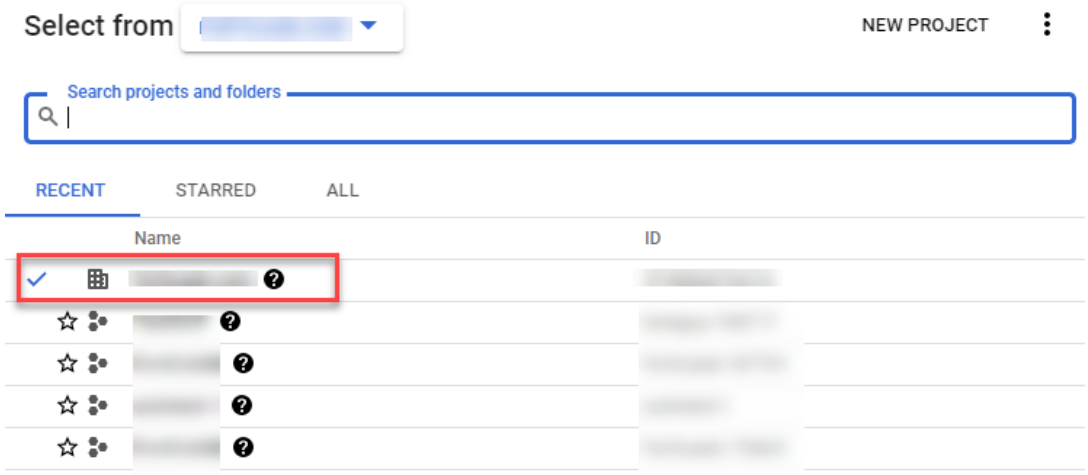
Grant Service Account Owner and Organization Administrator Role

The service account is created under a project of a organization in the Google Cloud account. FortiCASB requires the service account to be granted with one of the following roles in the scope of organization level to provide security monitoring across all projects under the organization:

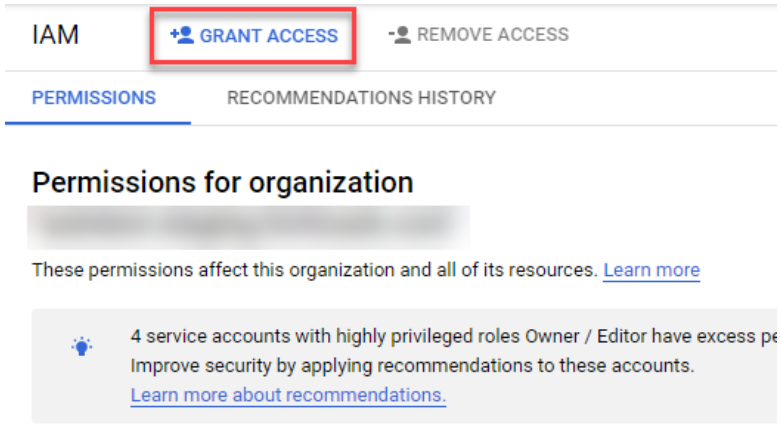
1. **Organization Administrator** and **Owner** roles.
2. **Basic > Viewer** and **Tag Viewer** and **Log View Accessor**

Steps to Grant Service Account and Organization Roles

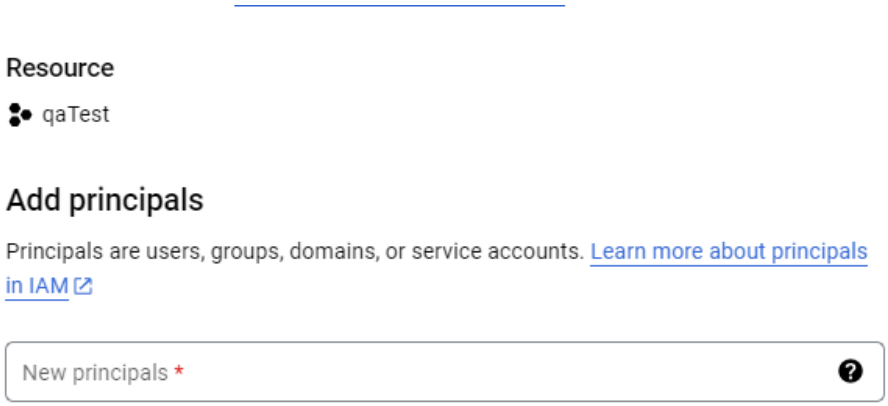
1. In Google Cloud Portal, first select the organization which the project is under.



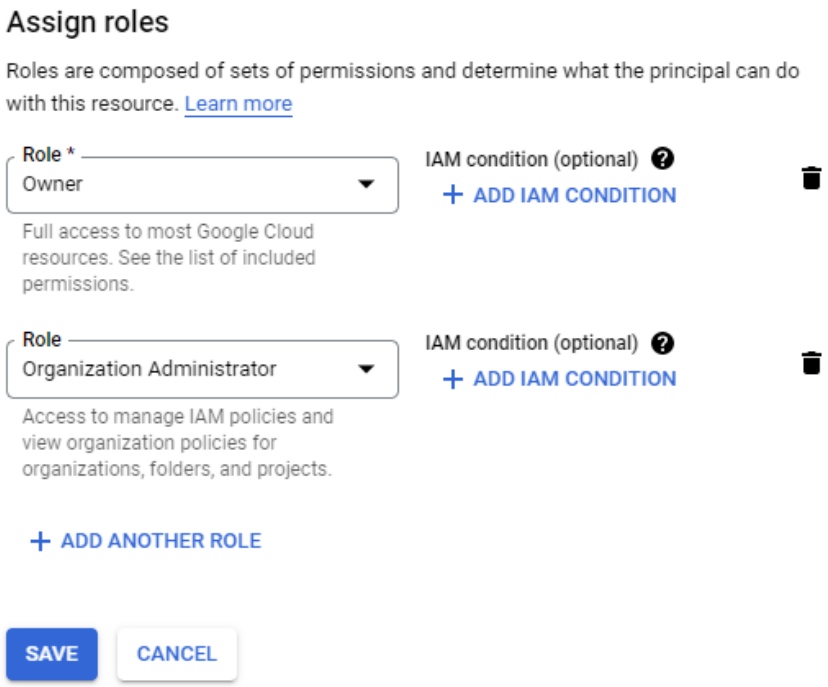
2. Click the **Navigation Menu** , select **IAM & admin > IAM**.
3. Click the **+Grant Access** button on the top.



4. In the **Add Principals > New principals** field, enter the service account ID created earlier.

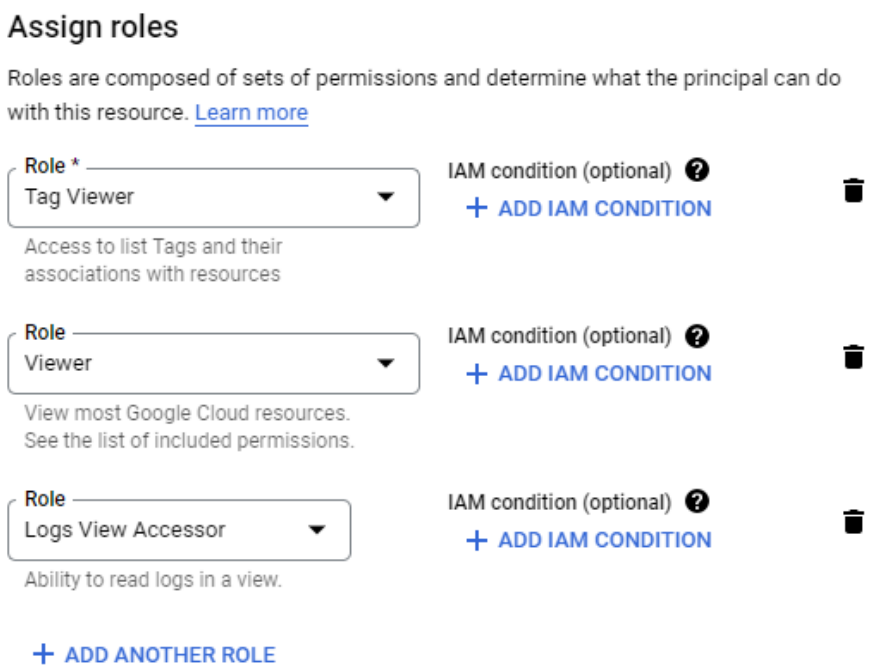


5. In **Assign roles**, choose one of the options and add the appropriate roles:
   a. **Option 1**: In the **Select a role** field, select **Project > Owner** or **Viewer**.
   b. Then click **+ ADD ANOTHER ROLE**, select **Resource Manager > Organization Administrator**.



   c. **Option 2**: In the **Select a role** field, select **Resource Manager > Tag Viewer**.
   d. Then click **+ ADD ANOTHER ROLE**, select **Basic > Viewer**.

e. Click **+ ADD ANOTHER ROLE** again, select **Logging > Log View Accessor**.



6. Click the **SAVE** button to finish.

Enable required APIs

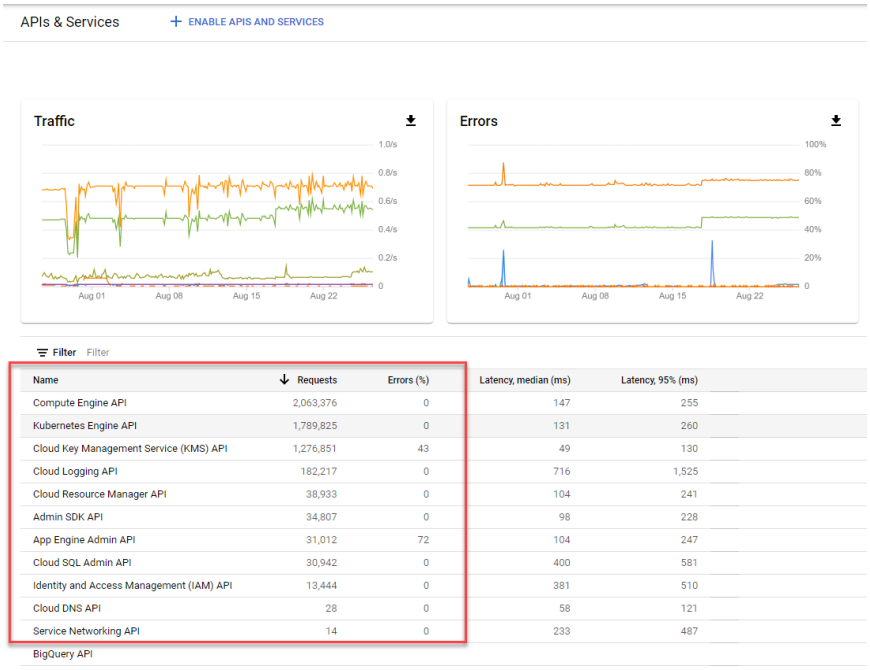
After adding roles to the service account, you must make sure that the following APIs are enabled on all projects for monitoring. This will ensure that FortiCASB can gather information from the Google Cloud.

- **Cloud Resource Manager API**
- **App Engine Admin API**
- **Cloud Key Management Service (KMS) API**
- **Compute Engine API**
- **Cloud SQL**
- **Google Cloud Storage JSON API**
- **Cloud Storage**
- **Cloud SQL Admin API**
- **Stackdriver API**

- **Admin SDK**
- **Identity and Access Management (IAM) API**

To enable the APIs, do the following:

1. On **Google Cloud Platform Consolel** , first select the project to be monitored.
2. Click the **Navigation Menu** in the upper-left corner, and select **APIs & Services > Enable APIs & services**.
3. In the **API & Services** list, make sure that the required APIs are listed (enabled).



If any of the APIs is not enabled, use the below steps to enable it:

1. Go to the project to be monitored.
2. Click the **Navigation Menu** , and select **APIs & Services**
3. Click **Activate Cloud Console** in the upper right hand corner.

4. Copy and paste the shell command to enable the required services:

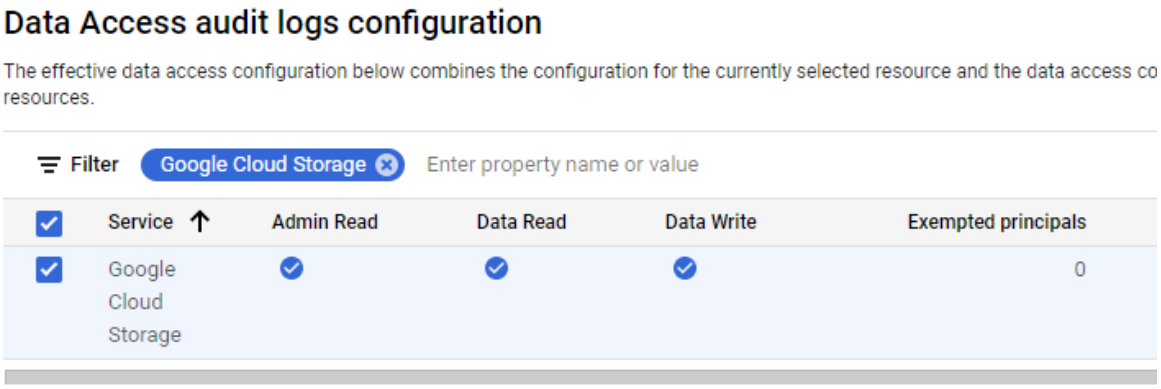
```
gcloud services enable \
cloudresourcemanager.googleapis.com \
appengine.googleapis.com \
cloudkms.googleapis.com \
compute.googleapis.com \
sql-component.googleapis.com \
storage-api.googleapis.com \
storage.googleapis.com \
sqladmin.googleapis.com \
stackdriver.googleapis.com \
admin.googleapis.com \
iam.googleapis.com
```

Note: Repeat the steps above to enable APIs for other projects under the same organization.

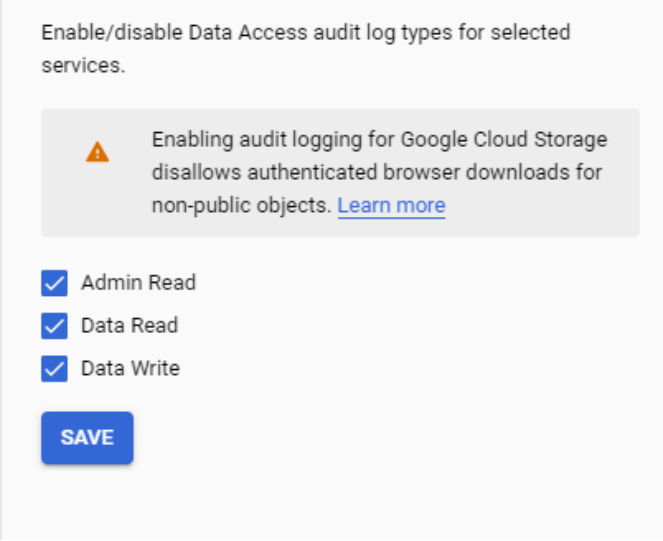
Enable activity and alert monitoring

If you would like to enable FortiCASB activity and alert monitoring, you must turn on audit logging using the following steps:

1. In **Google Cloud Platform Console**, select the project where the service account was created at.
2. Go to the project to be monitored.
3. Click on the **Navigation Menu**, and select **IAM & Admin > Audit Logs.**
4. Search for "Google Cloud Storage" from the list of available resources.



5. Enable all log types, i.e., **Admin Read, Data Read, and Data Write.**

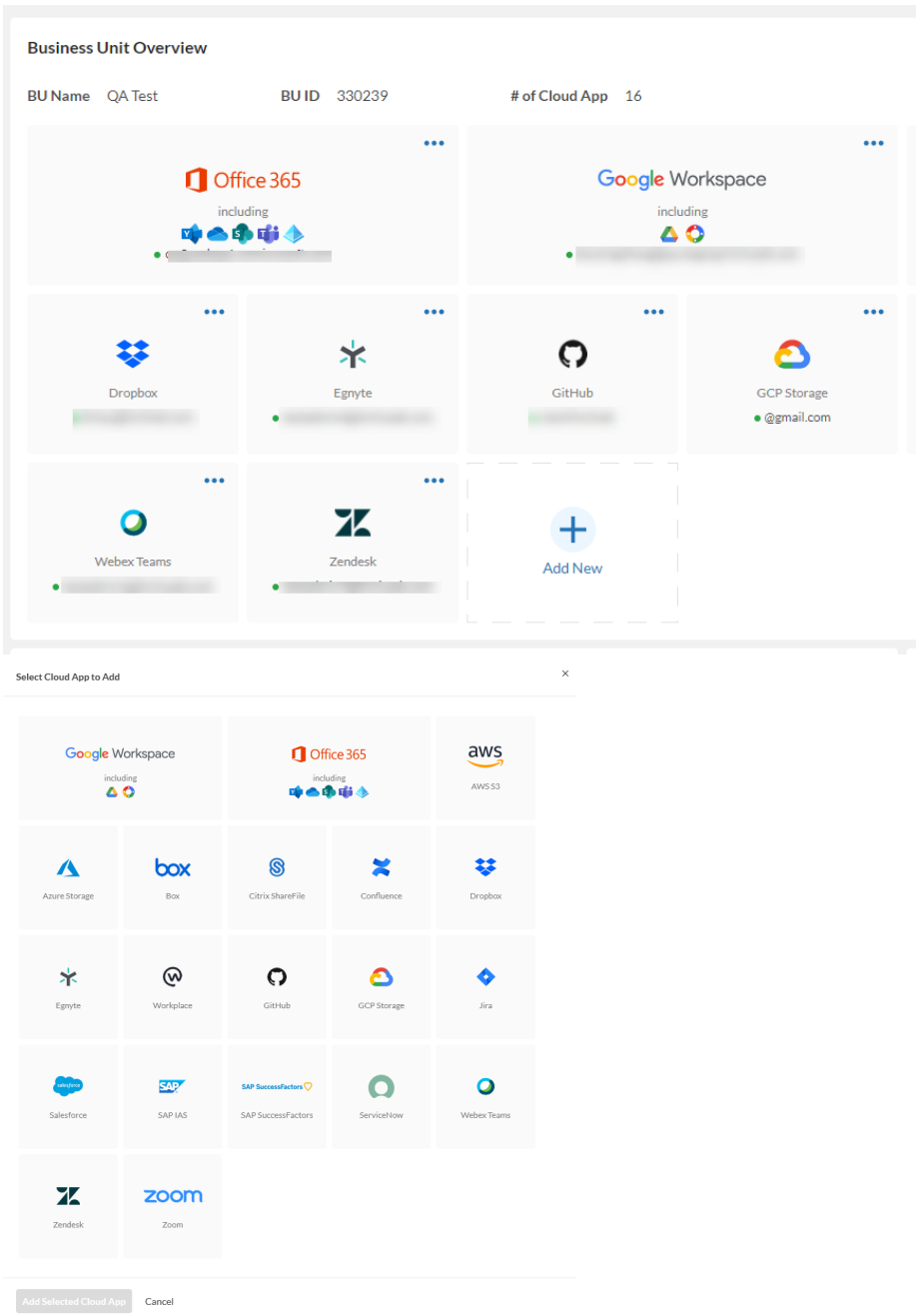


6. Click the **SAVE** button.

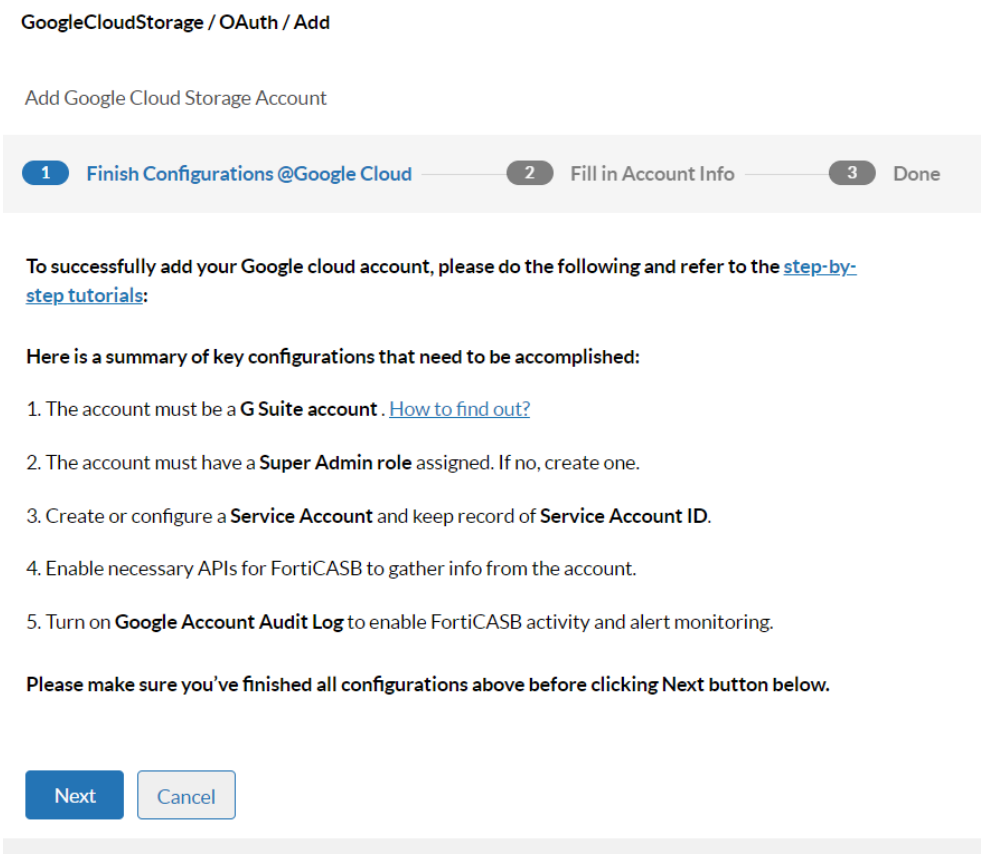
Add Google Cloud Storage Account

After all the Google Cloud Storage configurations are completed, follow these steps to add your Google Cloud Storage account on FortiCASB.

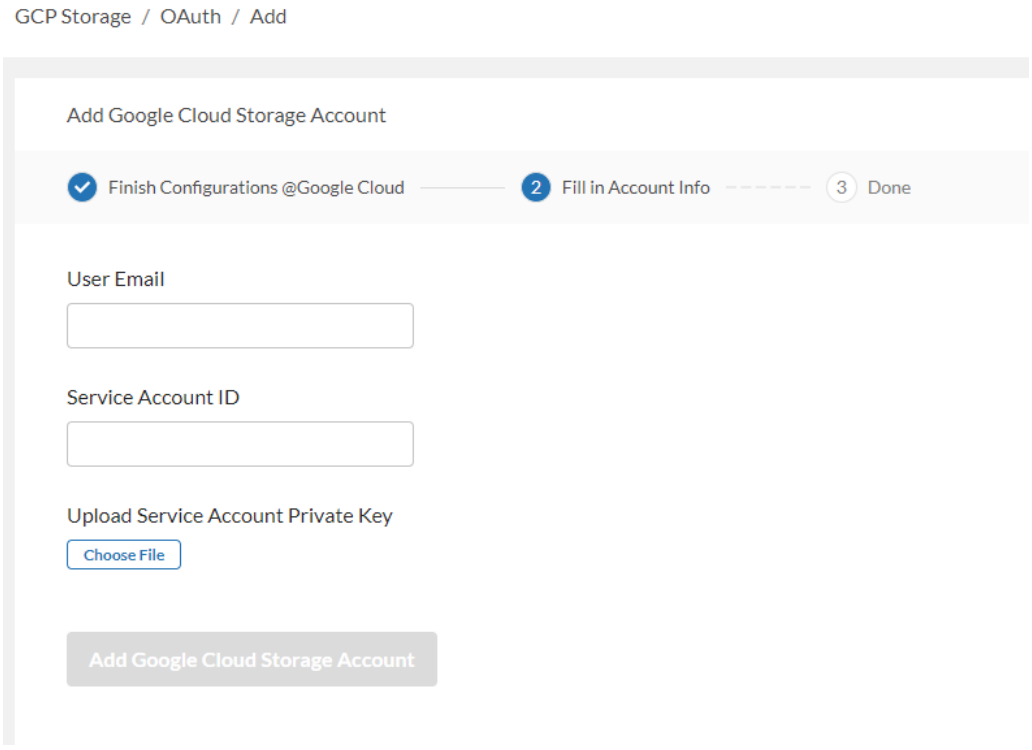
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Google Cloud Storage**, then click **Add Selected Cloud App**.



3. Review the key configurations list to see if you have finish all the required configurations, then click **Next**.



4. In **User Email** field, enter your Google Workspace account which you used to create the service account.



5. In **Service Account ID** field, enter the ID of your service account. Your service account ID should end in ".gserviceaccount.com".
6. In **Upload Service Account Private Key**, click **Choose File** to browse and upload your service account's private key (i.e., a JSON file).
7. Click **Add Google Cloud Storage Account** to complete adding your Google Cloud Storage account.

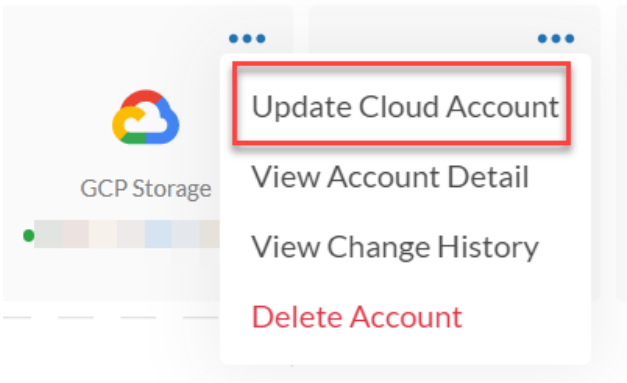
Update Google Cloud Storage Account

Before updating the Google Cloud Storage account on FortiCASB, complete the same configurations using the same Google Workspace account.

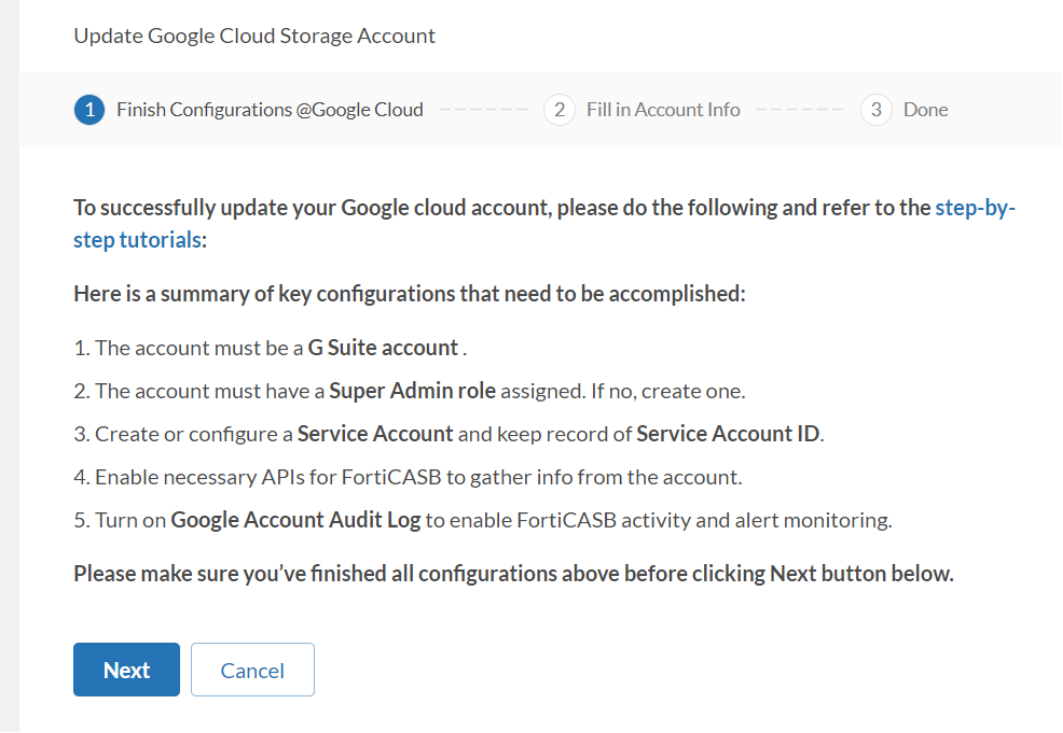
1. **Configure Google Workspace Account on page 119**
2. **Configure OAuth Consent Screen on page 120**
3. **Create Service Account on page 126**
4. **Grant Service Account API Access on page 129**
5. **Grant Service Account Owner and Organization Administrator Role on page 131**
6. **Enable required APIs on page 133**
7. **Enable activity and alert monitoring on page 135**

After all configurations are completed, go back to FortiCASB to update the account.

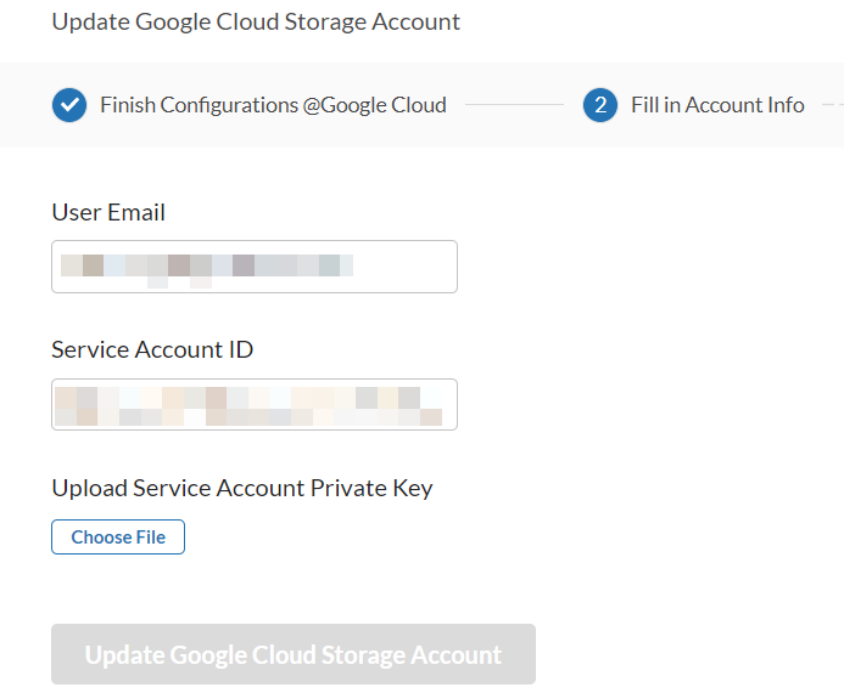
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the Google Cloud Storage menu and select **Update Cloud Account**.



4. Review the key configurations list to see if you have finish all the required configurations, then click **Next**.



5. In **User Email** field, enter your Google Workspace account which you used to create the service account.



6. In **Service Account ID** field, enter the ID of your service account. Your service account ID should end in ".gserviceaccount.com".
7. In **Upload Service Account Private Key**, click **Choose File** to browse and upload your service account's private key (i.e., a JSON file).

8. Click **Update Google Cloud Storage Account** to complete updating your Google Cloud Storage account.

Google Workspace

FortiCASB utilizes and API based approach to monitor your cloud SaaS application. In this example, FortiCASB authenticates itself to your Google Workspaces account using OAuth2.0 credentials, and then utilized the Google Workspaces API to pull information from your cloud accounts. FortiCASB uses this information to monitor and track Google Workspaces user activities and scan data stored in Google Drive.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- **Business Edition**
- **Enterprise Edition**

The user account installed in FortiCASB must be a **Super Administrator** in your Google Workspace account. For steps on how to check if your account is a Super Adminstrator, see Google Workspace connection errors on page 534.

Due to Google requirements, only Google Workspace accounts with a business or enterprise license can use FortiCASB. Google Workspace accounts with a basic license will be not be able to use FortiCASB.

You may either use an existing account or create a new account. Wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

There are four steps you need to setup your Google Workspace account before you can add the Google Workspace account on FortiCASB:

1. **Configure OAuth Consent Screen on page 142**
2. **Create Google Service Account on page 147**
3. **Enable Google Drive API & Authorize Client ID on page 150**

4. **Enable activity and alert monitoring on page 153**
5. **Add Google Workspace Account on page 154**

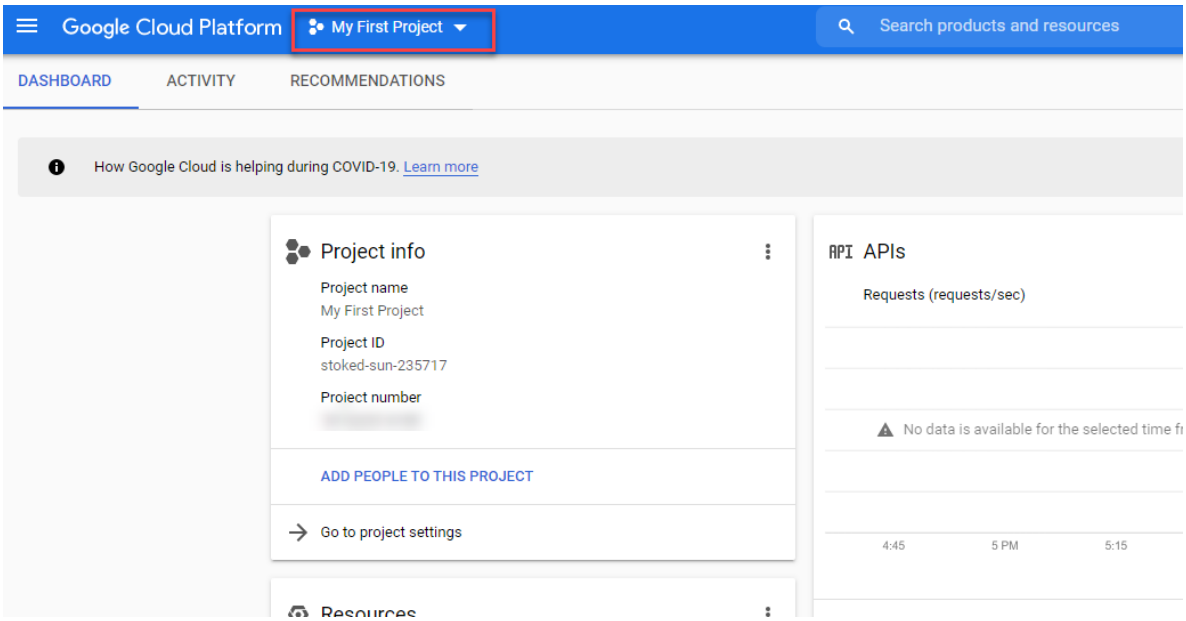
Configure OAuth Consent Screen

The purpose to create an **OAuth Consent Screen** is to enable **Google Workspace Domain-Wide Delegation** when a Google service account is created under a project. Furthermore, with **Google Workspace Domain-Wide Delegation** enabled, the **Google Drive API OAuth** scope can be authorized to be used by the service account. This is critical in authorizing FortiCASB to retrieve data from the Google Workspace account.

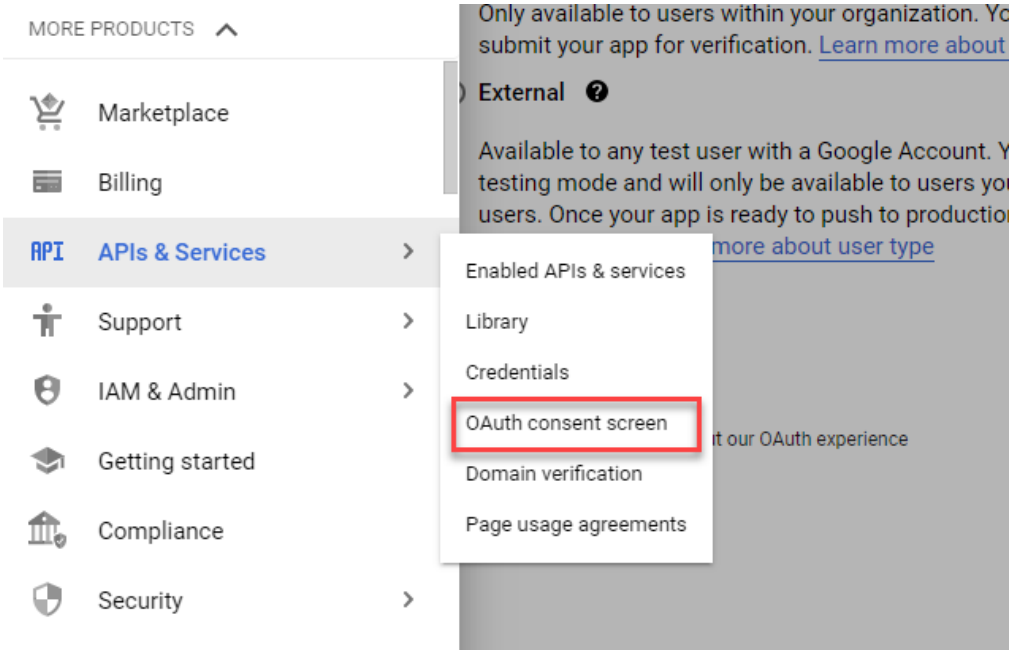
Be mindful the **Google project** that will be hosting the service account will play a critical role in providing the authorization that FortiCASB needs to interact with Google Workspace account.

Note: If you have already configured OAuth Consent Screen for the project, you can skip this section.

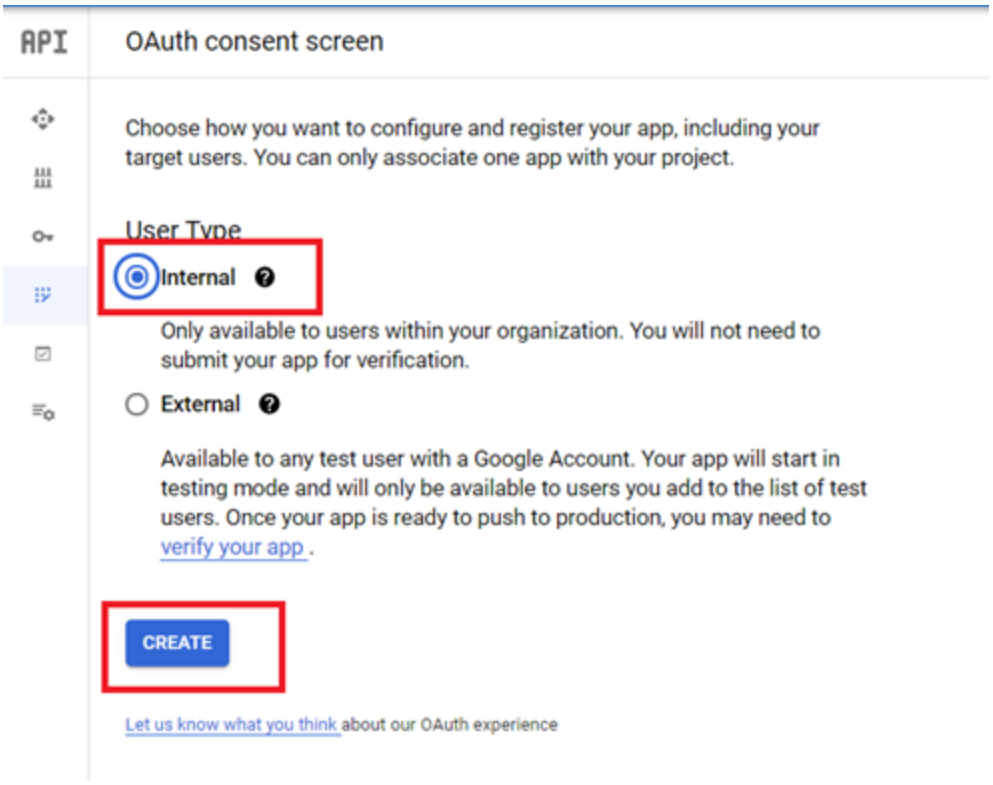
1. Go to **Google Cloud Platform Console** and log in with your **Google Workspace account**.
2. Click on the project drop-down menu > **Select a project**. Select an existing project or create a new project by selecting **New Project**.



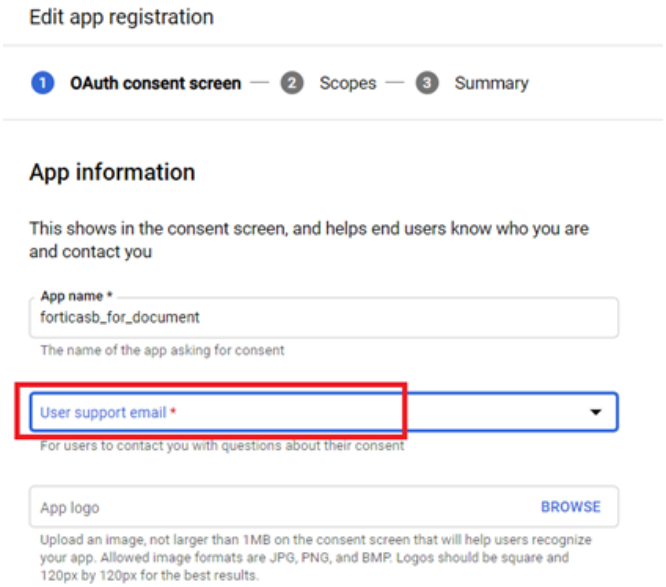
3. With your project selected, click on navigation menu ☰ and go to **APIs & Services > OAuth consent screen**.



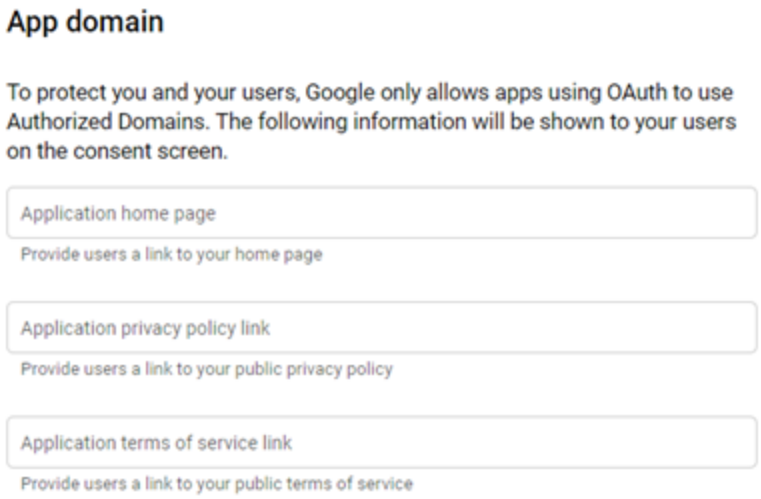
4. When you get started with OAuth Consent Screen configuration, choose **Internal** user type, then click **CREATE**.



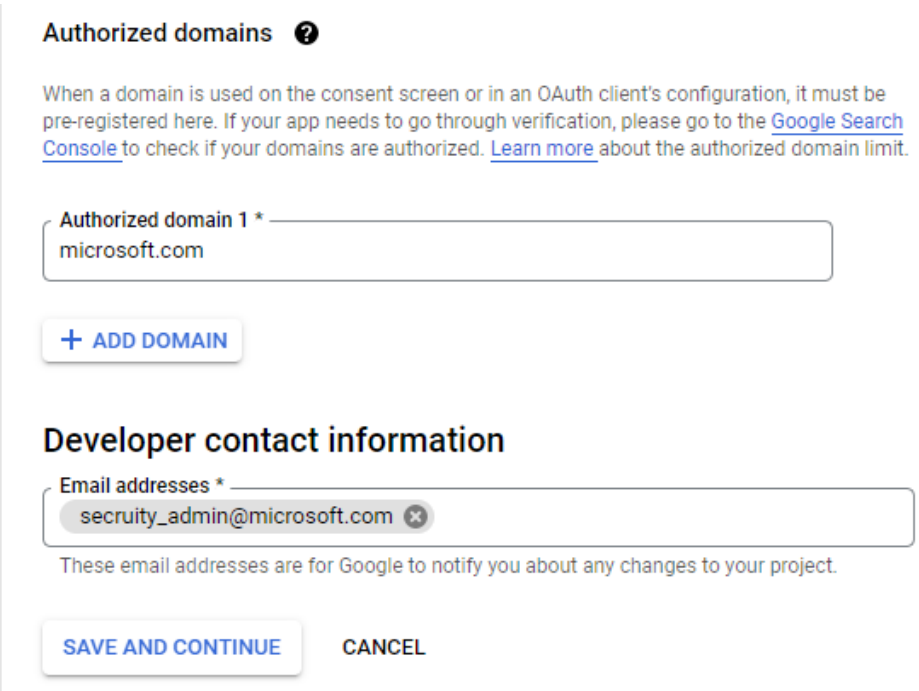
5. In **OAuth Consent Screen** page:
   a. Name the app and choose a user that will manage the app within the Google Workspace account.



   b. For the **App domain**, leave it as blank since it will only be for internal use.

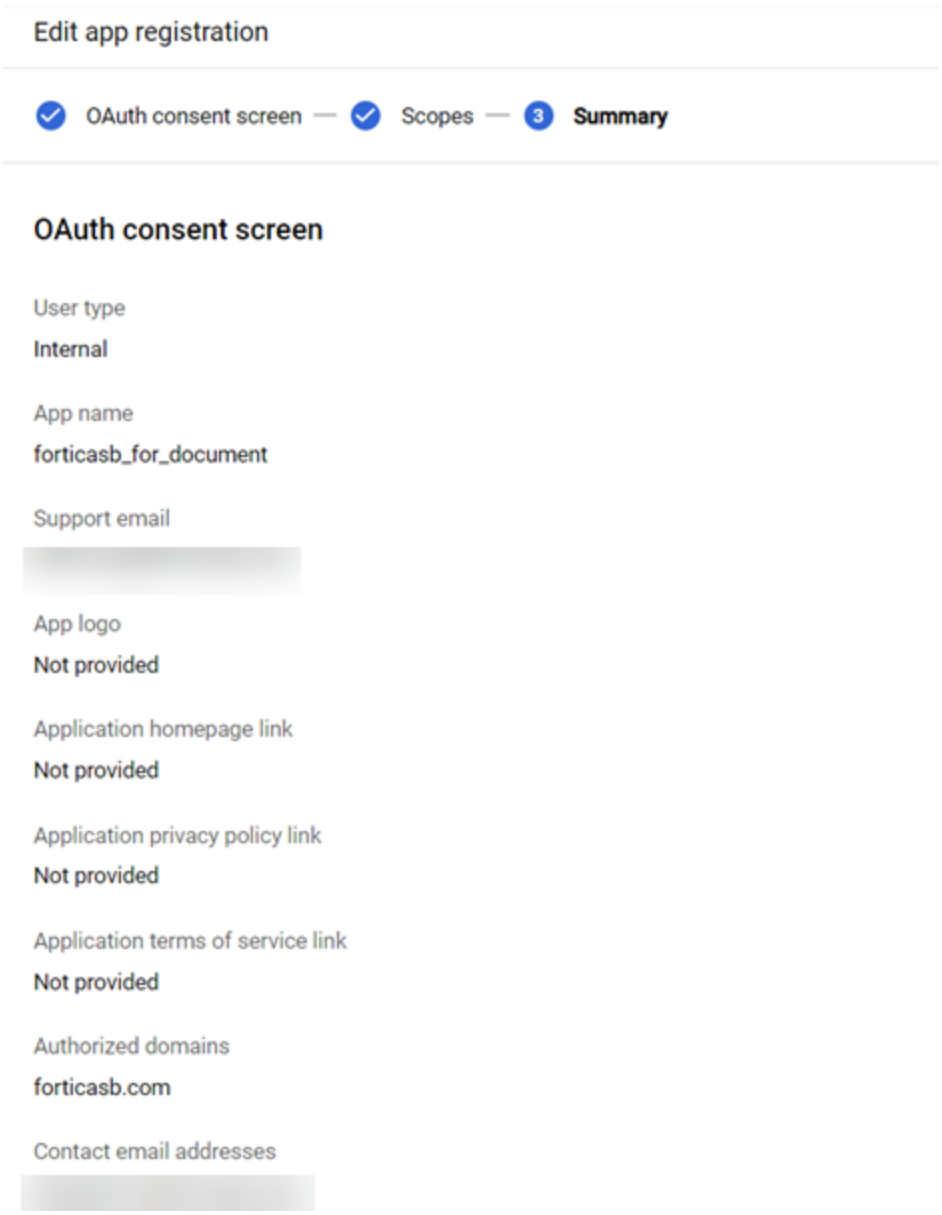


c. Click **+ADD DOMAIN** and enter the domain of this Google Workspace account.
For example, if the Google Cloud Workspace account e-mail is "security_admin@microsoft.com", then the domain is "microsoft.com".



d. In **Developer contact information**, enter the e-mail of the person managing the app.
e. Click **SAVE AND CONTINUE**.

6. In **Scopes** selection page, click **SAVE AND CONTINUE**
7. Review and confirm all settings are correct in the Summary page, then click **BACK TO DASHBOARD**, the OAuth consent screen should now be added to the project.


Edit app registration
OAuth consent screen — Scopes — 3 Summary
OAuth consent screen
User type
Internal
App name
forticasb_for_document
Support email
App logo
Not provided
Application homepage link
Not provided
Application privacy policy link
Not provided
Application terms of service link
Not provided
Authorized domains
forticasb.com
Contact email addresses

Create Google Service Account

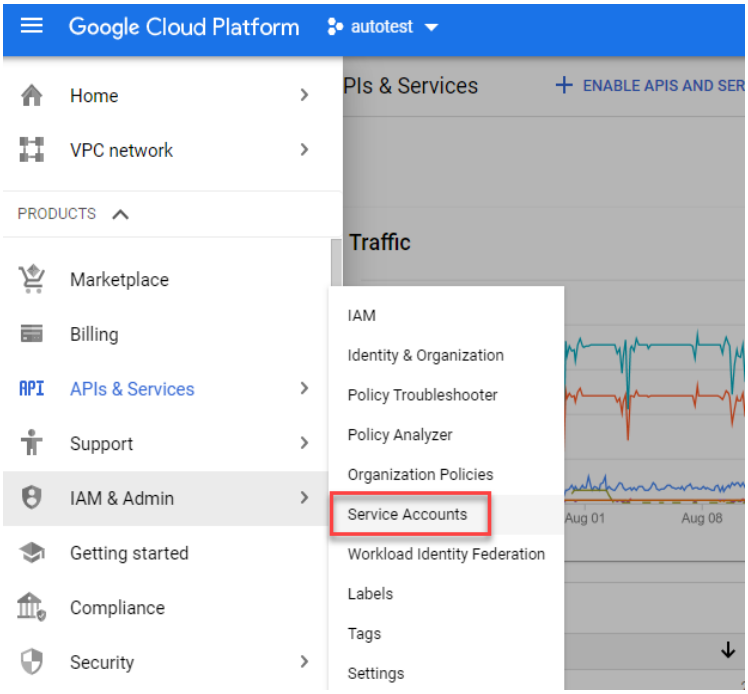
A **service account**created for the Google Workspace account is required to add the account to FortiCASB. The service account needs to be created in the project that has **OAuth Consent Screen** created to activate **Google Workspace Domain-Wide Delegation**. Google Workspace Domain-Wide Delegation is necessary for FortiCASB to visit files in Google Workspace.

Without the service account, you can still use FortiCASB. However, the features related to files in FortiCASB, such as Discovery, will not work.

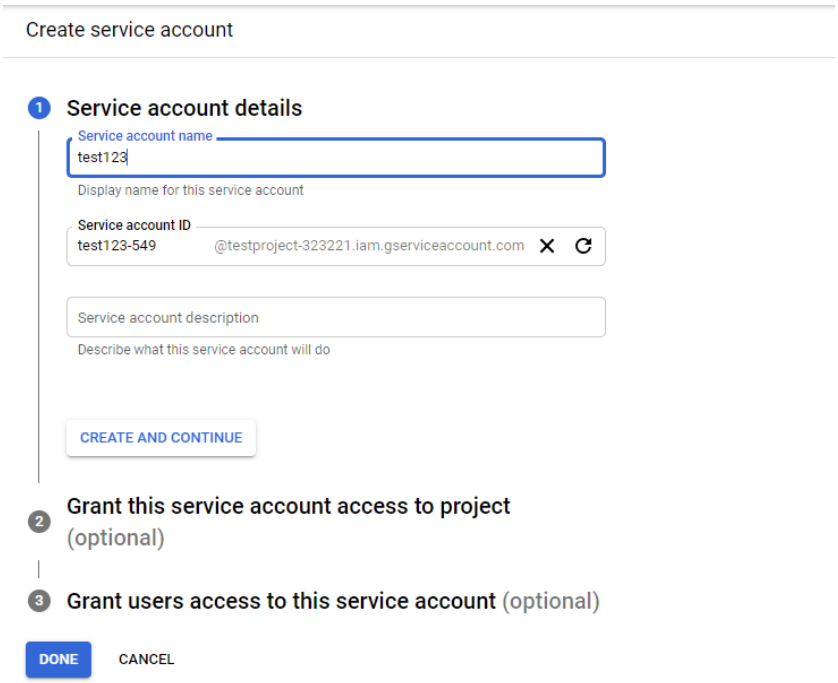
For more information regarding service accounts and domain-wide authority delegation, go to: https://developers.google.com/identity/protocols/OAuth2ServiceAccount#delegatingauthority

Steps to create Google Service Account:

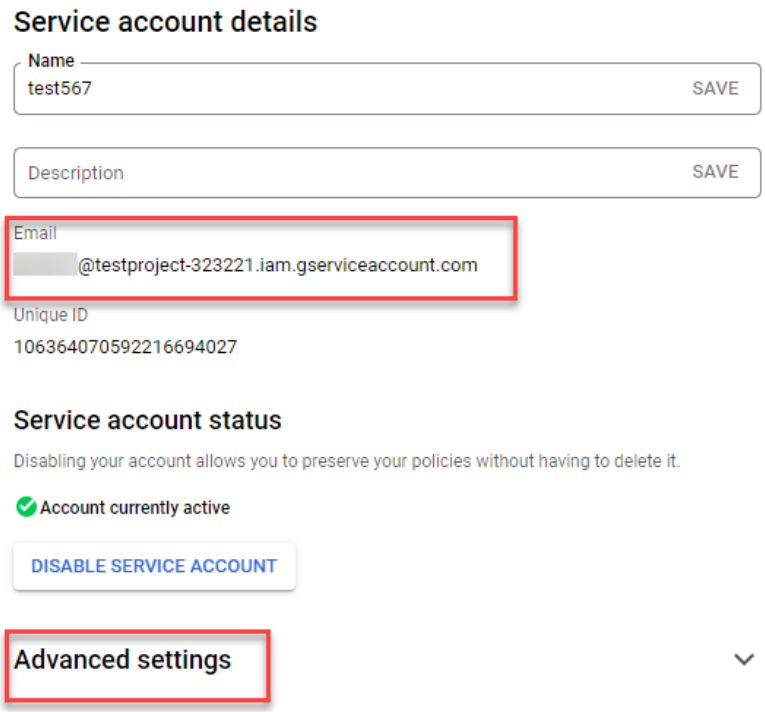
1. Go to the **Google Cloud Platform Console** and log in with your **Google Workspace account**.
2. With the project selected, go to the **Navigation Menu** ☰ **> IAM & Admin > Service accounts**.



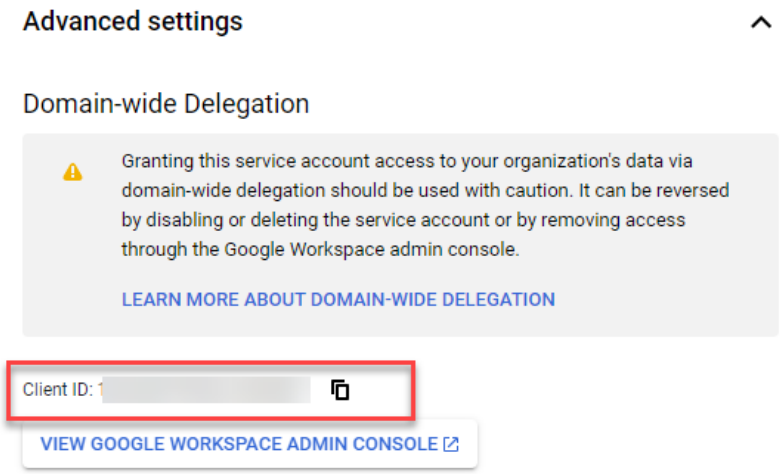
3. Click **+Create service account**, then enter a **Service account name** of your preference and click **CREATE AND CONTINUE**.
   Skip the optional steps, and click **Done**.



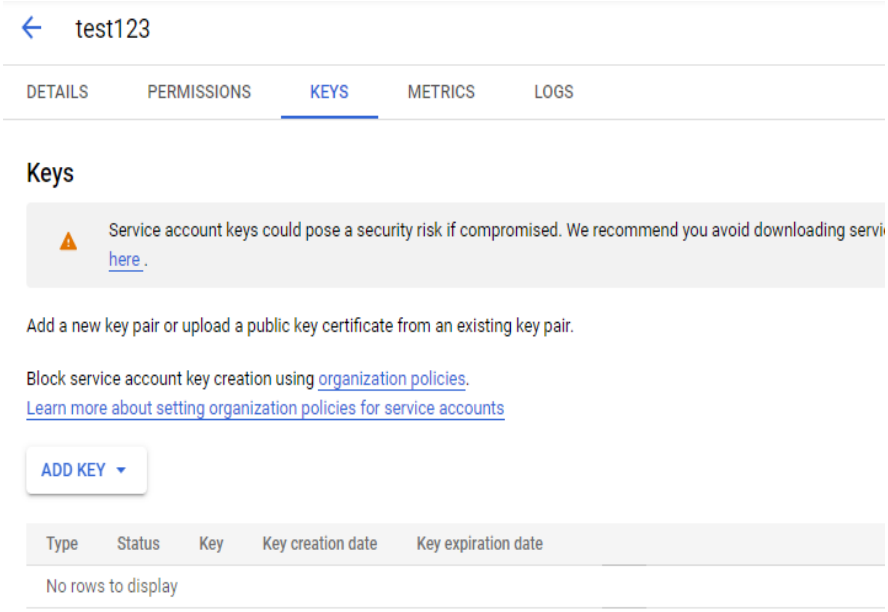
4. In **Service accounts** page, Click on the service account you created to enter the **Details** page, keep a record of the **Service Account ID (Email)**.



5. Click on **Advanced settings** drop down menu, and keep a record of the **Client ID** for use later in Enable Google Drive API & Authorize Client ID on page 150.



6. Click the **KEYS** tab, then click **ADD KEY** drop down menu and select **+Create new Key**. Then select **P12** key format and click **CREATE**. The **P12** private key will be downloaded automatically.

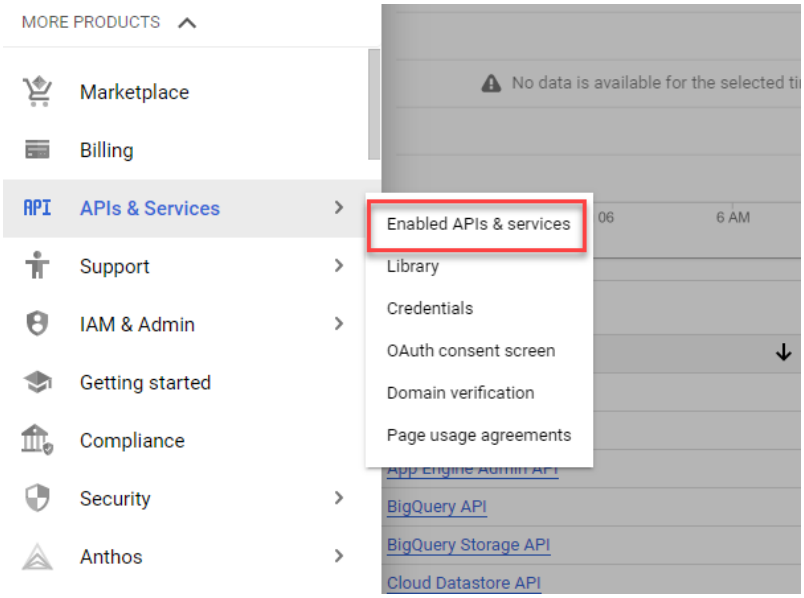


Keep the **Service Account ID** and **P12 private key** later for Google Workspace authentication during installation.

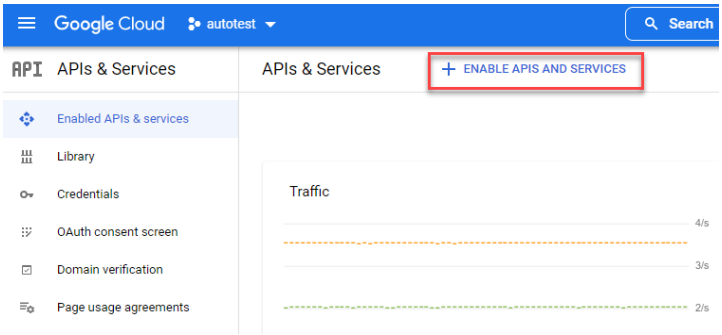
The **Client ID** will be used later in Enable Google Drive API & Authorize Client ID on page 150.

Enable Google Drive API & Authorize Client ID

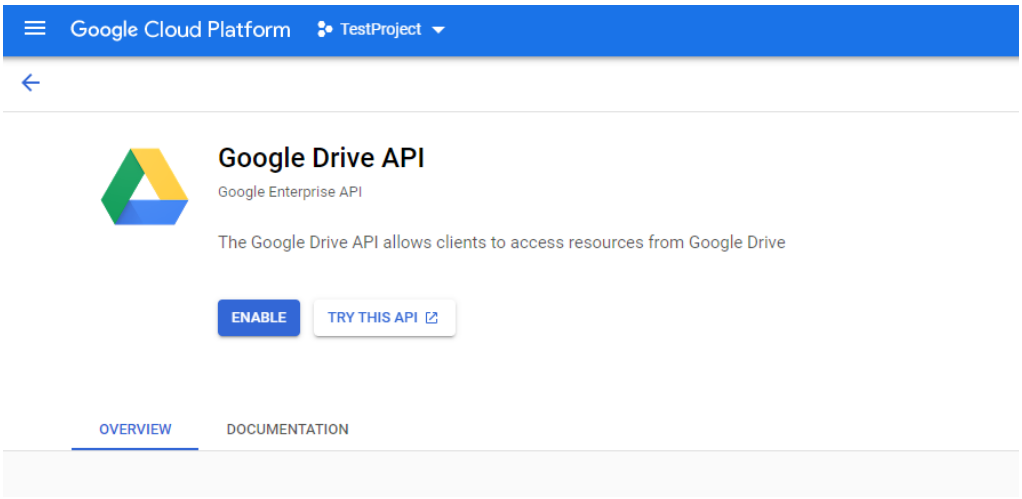
1. In **Google Cloud Platform Console**, select the project where the service account was created at.
2. Go to **Navigation Menu** > **APIs & Services** > **Enabled APIs & services.**



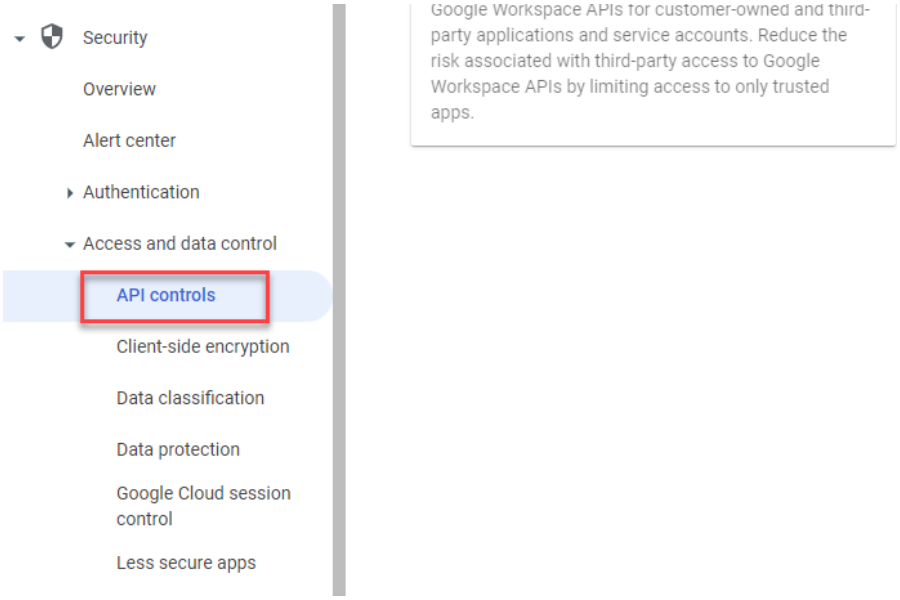
3. Click on **+ENABLE APIS AND SERVICES**.



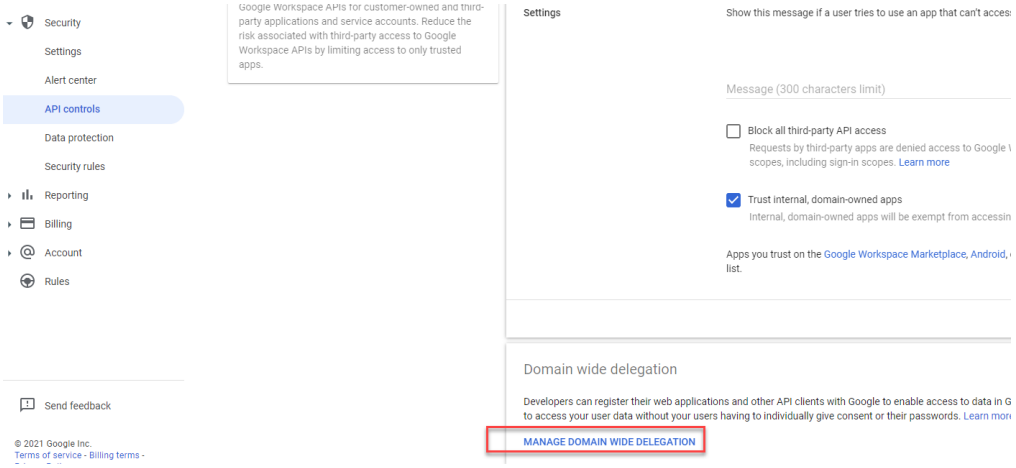
4. Search for the **Google Drive API** and enable it.



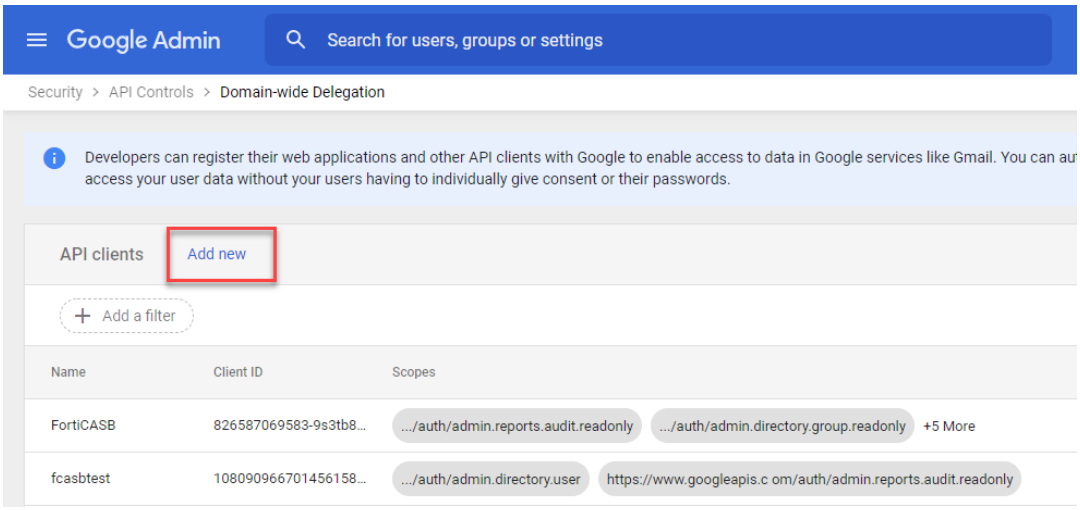
5. Go to **Google Workspace Admin Console** and log in with the same Google Account.
6. Go to **Security > Access and data control > API controls**.



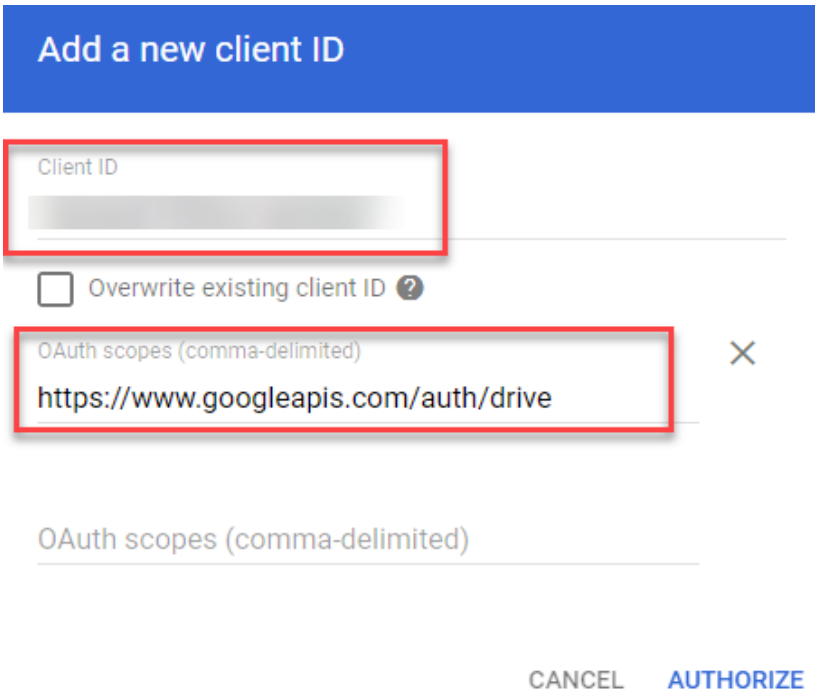
7. In **API controls** page, click **MANAGE DOMAIN WIDE DELEGATION**.



8. Click **Add new** and add the **Client ID** from Create Google Service Account on page 147.



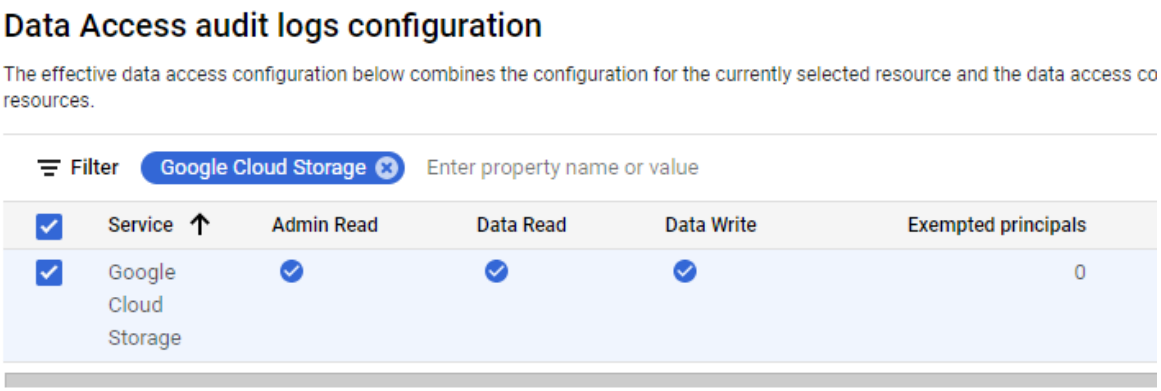
9. Add "https://www.googleapis.com/auth/drive" to **OAuth scope** and click **AUTHORIZE**.



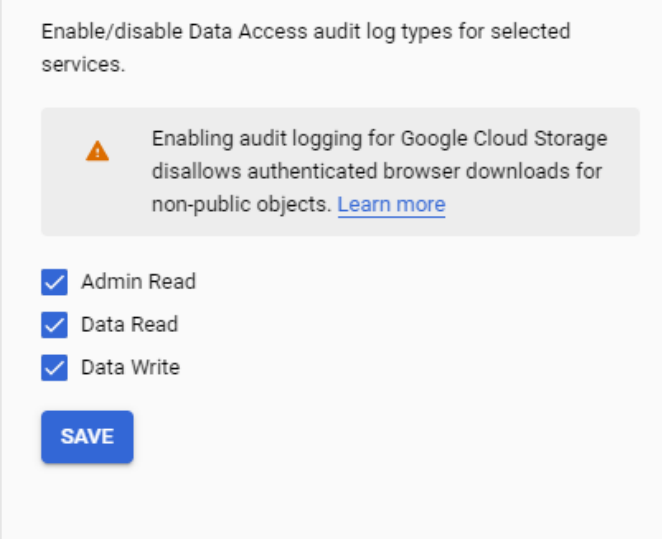
Enable activity and alert monitoring

To enable FortiCASB activity and alert monitoring on the Google Workspace account, audit logging needs to be turned on by the following steps:

1. In **Google Cloud Platform Console**, select the same project as where the service account was created.
2. Go to **Navigation Menu** ☰ **> IAM & Admin > Audit Logs**.
3. Search for "Google Cloud Storage" from the list of available resources.



4. Enable all log types, i.e., **Admin Read, Data Read, and Data Write.**

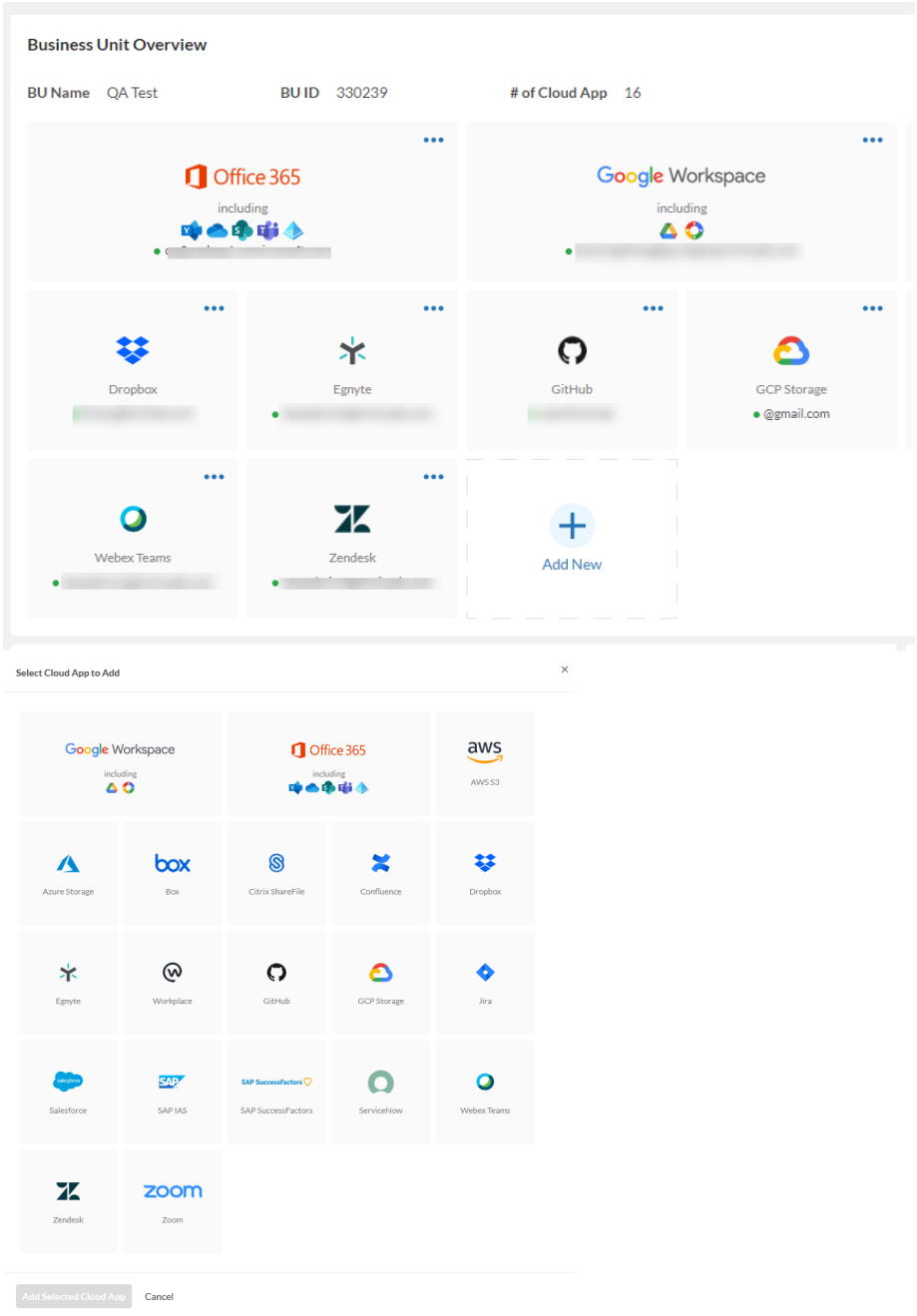


5. Click the **SAVE** button.

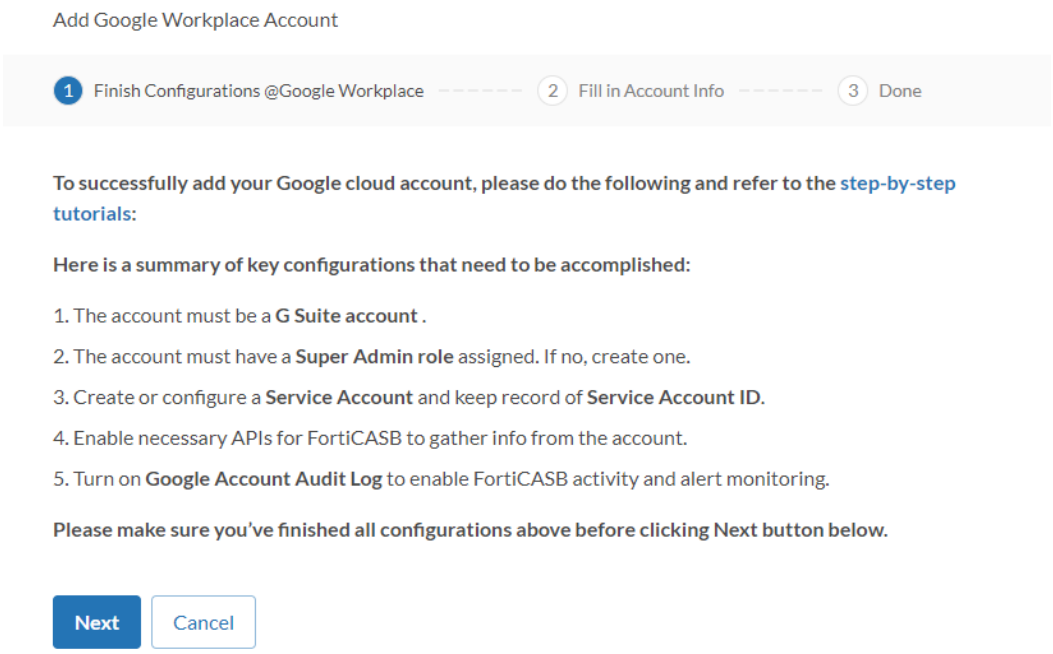
Add Google Workspace Account

After all the Google Workspace configurations are completed from previous sections, follow these steps to add your Google Workspace account on FortiCASB.

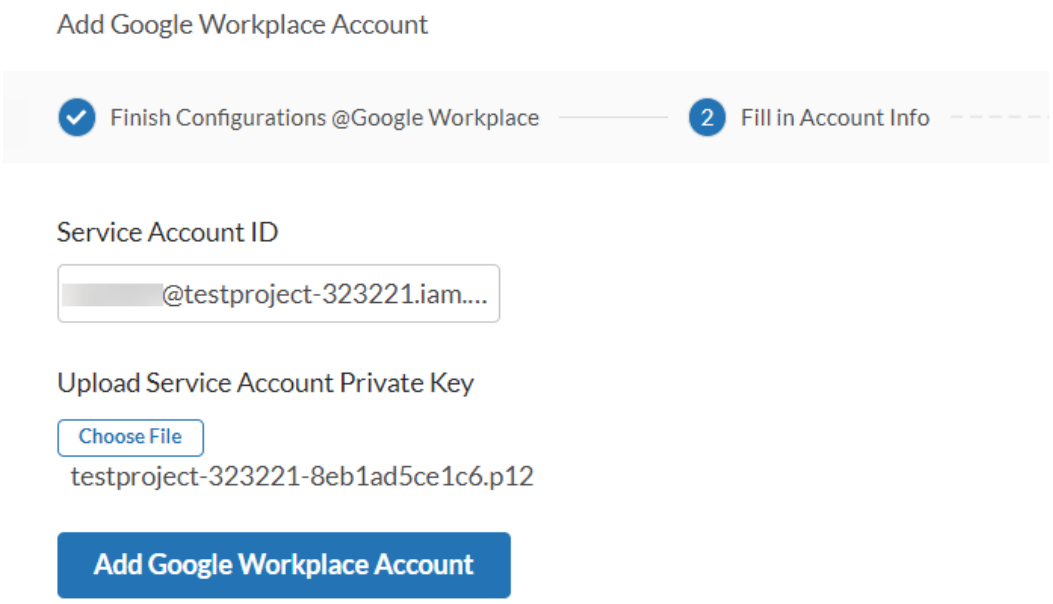
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Google Workspace**, then click **Add Selected Cloud App**.



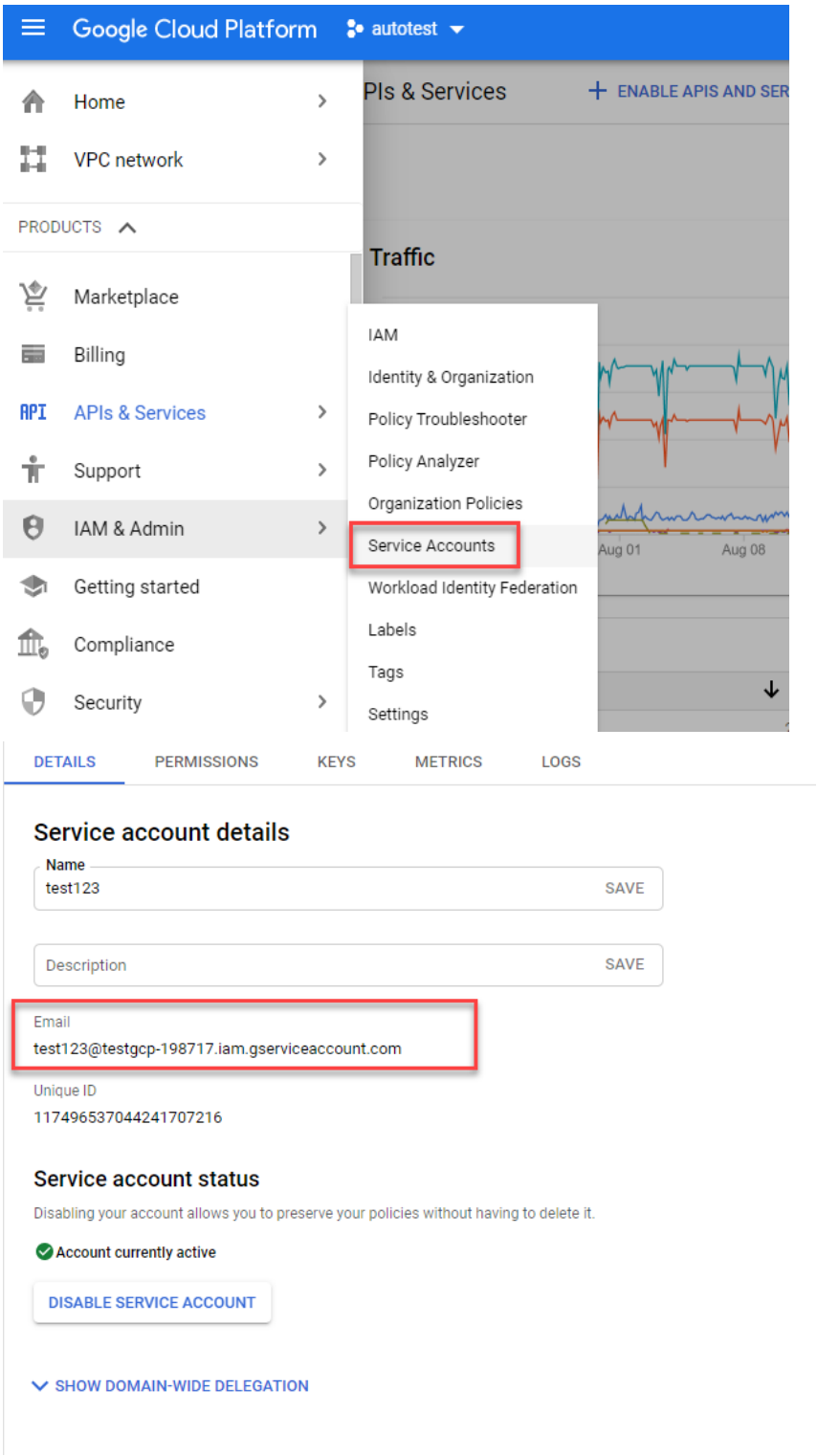
3. Review the summary of key configurations, which should be completed already in previous sections, and click **Next**.



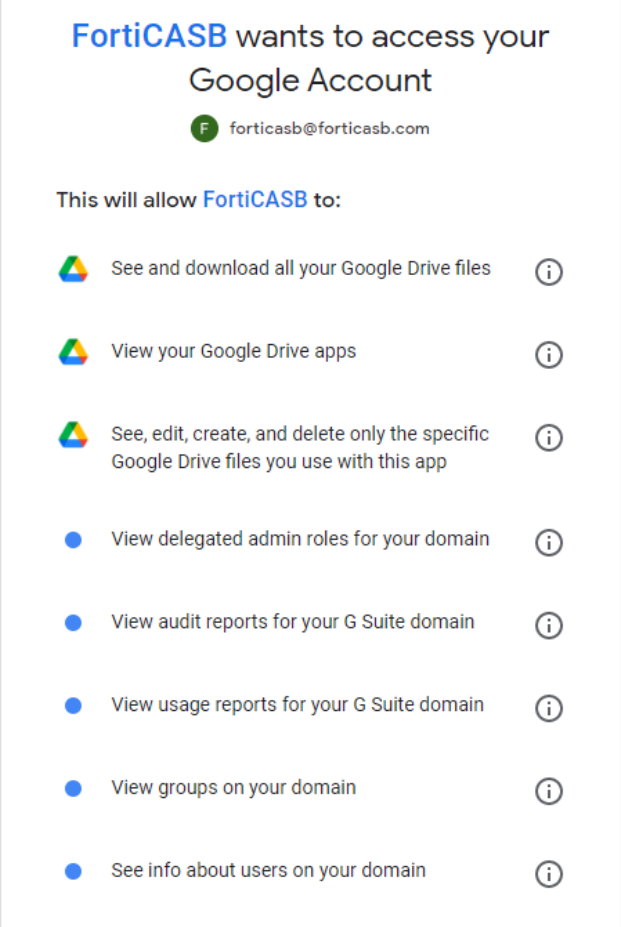
4. Enter the **Service Account ID (Email)** and upload the **Private Key (P12 File)** of the Google Workspace account. Your service account ID should end in ".gserviceaccount.com".



The **Service Account ID** is the email generated from the service account. It is located in **Service account details**.

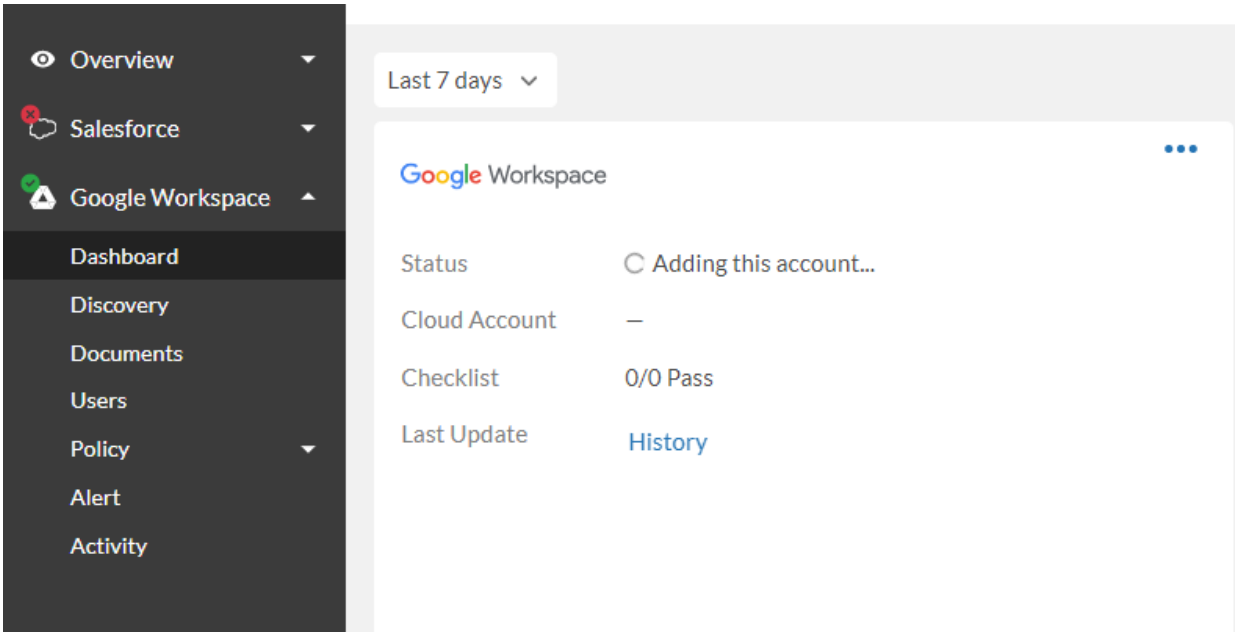


5. Click **Add Google Workspace Account**. You will be navigated to the Google website for authentication. Make sure to use the same Google Workspace account for authentication. If you have a custom Google domain, enter it here.
6. Log in to authenticate. Google will prompt you to **Allow** or **Deny** access.



7. Click **Allow** to grant FortiCASB permission to monitor your Google Workspace application.

You will be redirected back to the FortiCASB dashboard. You can check the installation checklist and platform monitoring status in the Google Workspace dashboard.



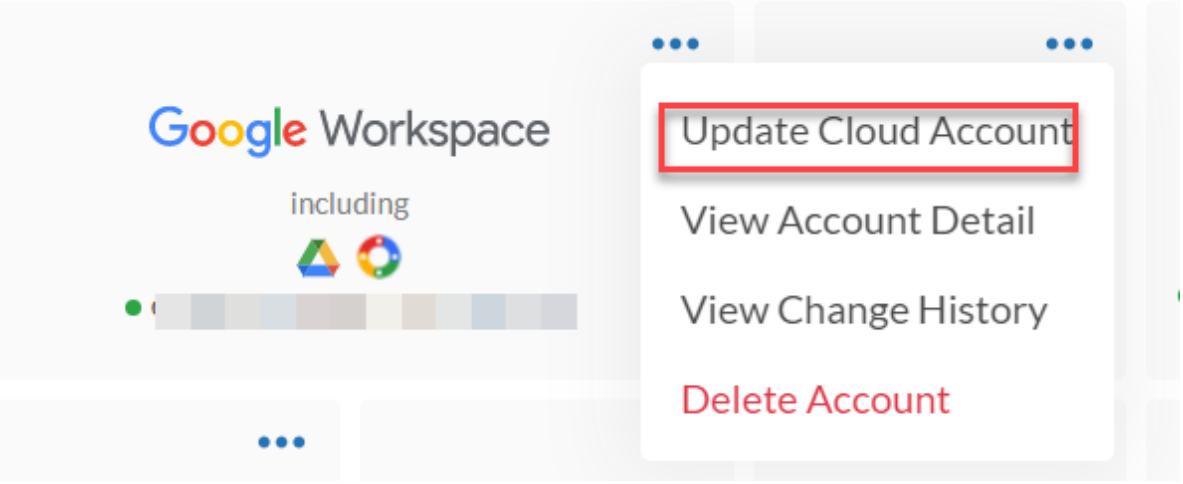
Update Google Workspace Account

Complete the same configurations using the same Google Workspace account before update the Google Workspace account on FortiCASB:

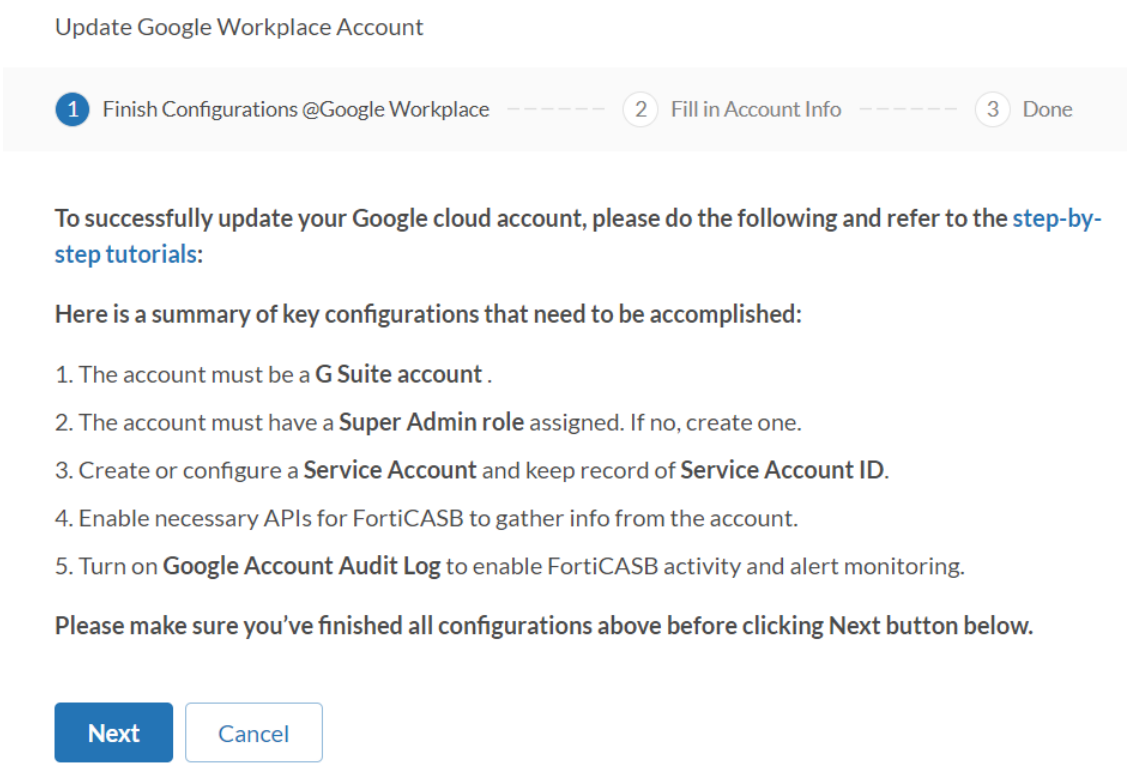
1. Configure OAuth Consent Screen on page 142
2. Create Google Service Account on page 147
3. Enable Google Drive API & Authorize Client ID on page 150
4. Enable activity and alert monitoring on page 153

After all the Google Workspace configurations are completed, follow these steps to update your Google Workspace account on FortiCASB.

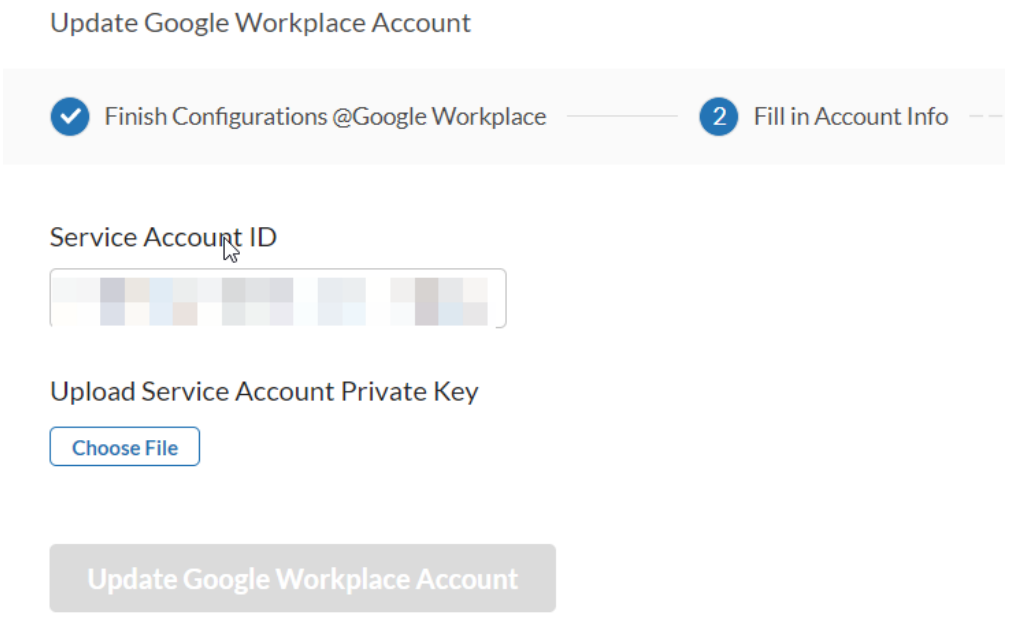
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on Google Workspace menu and select **Update Cloud Account**.



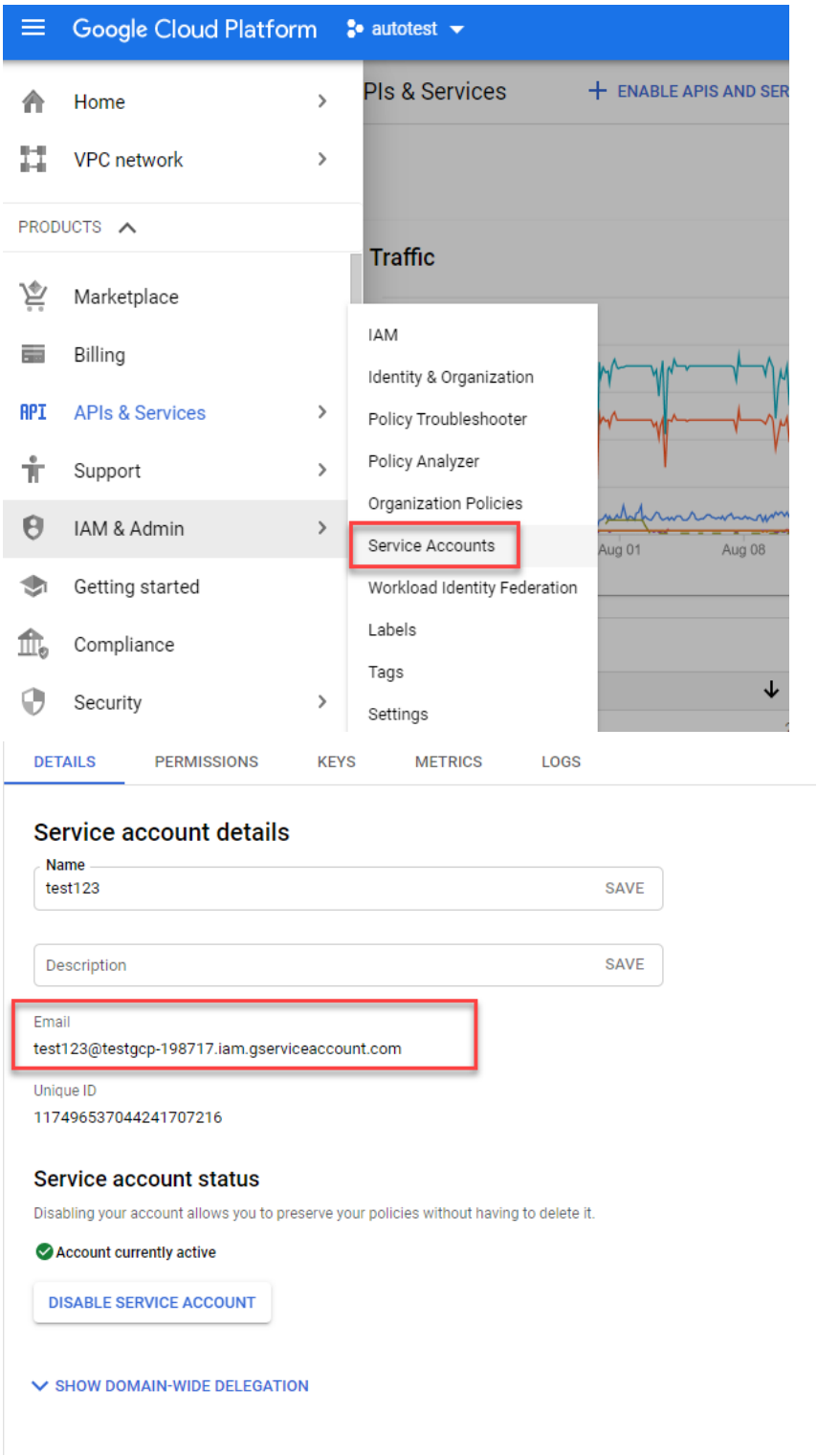
4. Review the summary of key configurations, which should be completed already in previous sections, and click **Next**.



5. Enter the **Service Account ID (Email)** and upload the **Private Key (P12 File)** of the Google Workspace account. Your service account ID should end in ".gserviceaccount.com".



The **Service Account ID** is the email generated from the service account. It is located in **Service account details**.



6. Click **Update Google Workspace Account**. You will be navigated to the Google website for authentication. Make sure to use the same Google Workspace account for authentication. If you have a custom Google domain, enter it here.
7. Log in to authenticate. Google will prompt you to **Allow** or **Deny** access.
8. Click **Allow** to grant FortiCASB permission to monitor your Google Workspace application.

You will be redirected back to the FortiCASB dashboard. You can check the installation checklist and platform monitoring status in the Google Workspace dashboard.

Jira

FortiCASB offers an API-based approach, pulling data directly from Jira via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Jira user activities, provides DLP Data Analysis for files stored on Jira tickets.

Before adding the Jira account to FortiCASB, configure the Jira account to grant FortiCASB read access permission to monitor account activities and provide other security measures on the account. Make sure the Jira account that will be added on FortiCASB is the **same** account that is configured.

Prerequsite

- **All Jira Cloud plans** are supported, including the **Free plan**.
- The account user must be a **Site Admin** of the Jira service site.

Steps to add Jira account to FortiCASB:

1. **Jira Account Configuration on page 164**
2. **Add Jira Account on page 167**

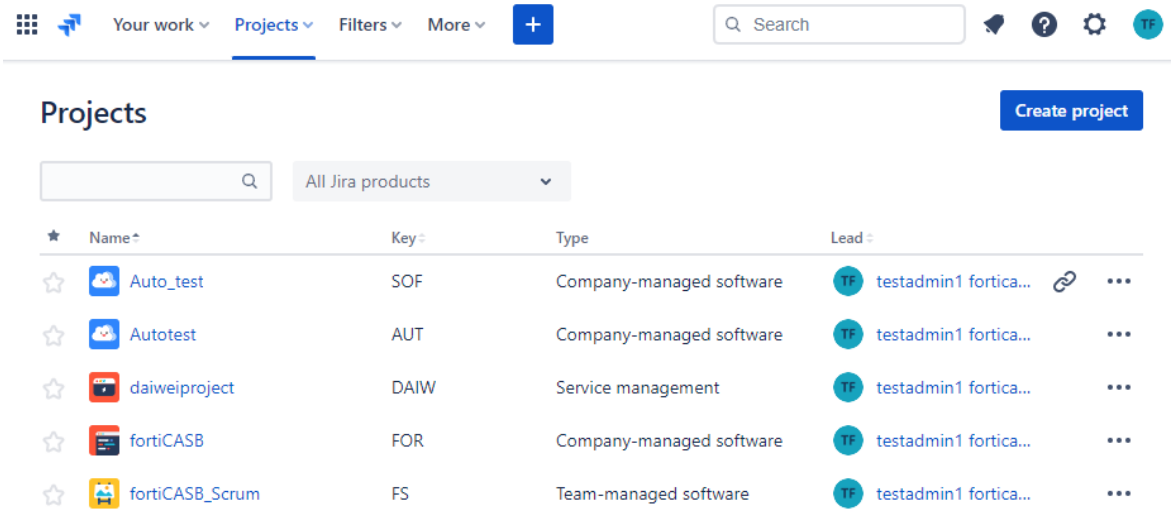
Configure Jira Project Browse Project Permission

The Jira account that will be used to add Jira to FortiCASB needs to be granted **Browse Project permission** to the Jira project to be monitored by FortiCASB. This is so that FortiCASB have sufficient permission to browse the Jira project and the issues within the project as a **site admin**.

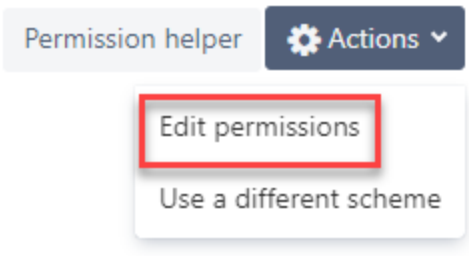
The Jira project must be a **Company-managed software** type to edit the access permission.

Steps to Grant Browse Project Permission to Jira Account

1. Go to your Jira project site.

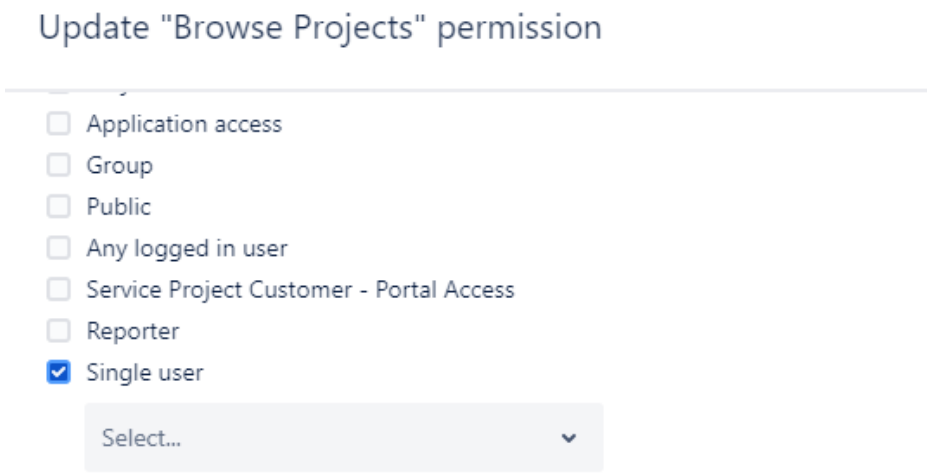


2. Choose the Jira project to be monitor by FortiCASB.
3. Click ••• on the right of the project and select **Project settings**.
4. In **Project settings** menu, click **Permissions**.
5. Click **Actions** drop down menu and select **Edit permissions**



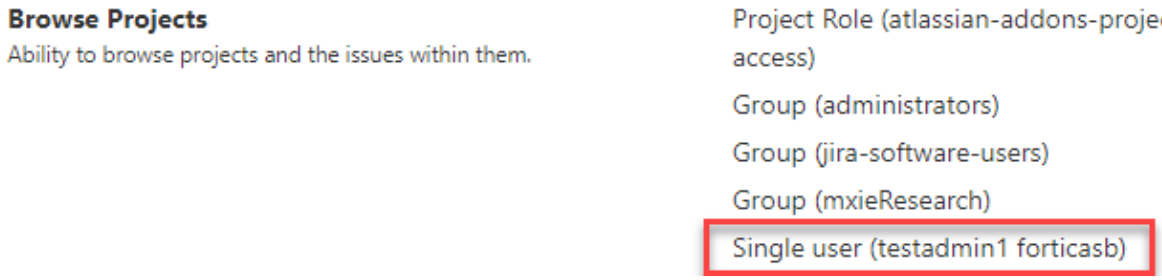
6. In the column **Browse Projects**, click **Update**.

7. Check **Single User**, and type and select the account user that will be used to add Jira to FortiCASB.



8. Click **Update** to finish.

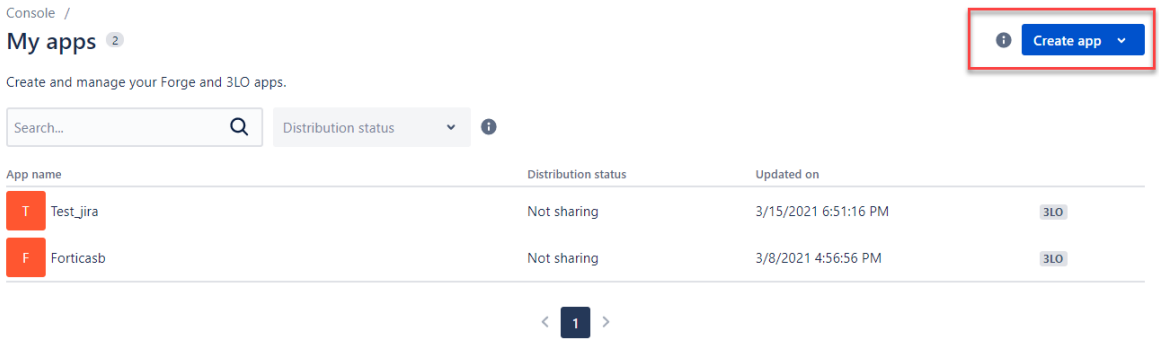
Note the single user added now is one of the user that has **Browse Project permission**.



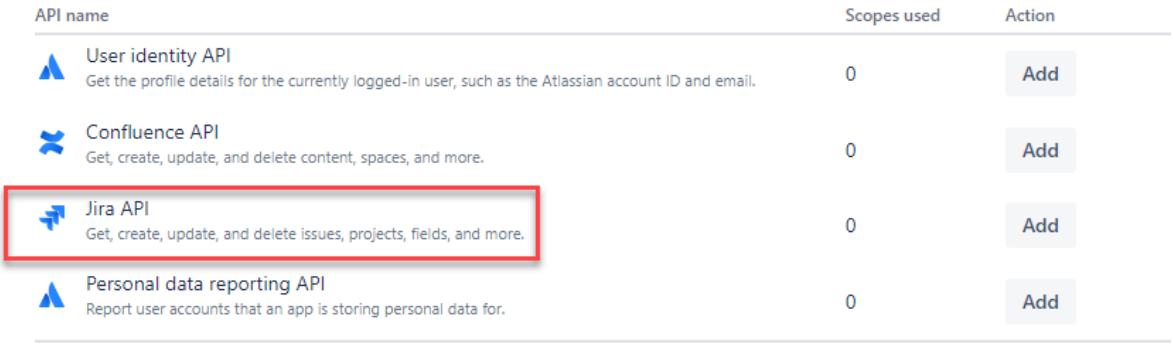
Jira Account Configuration

Follow the instructions below to create and configure an App on Jira:

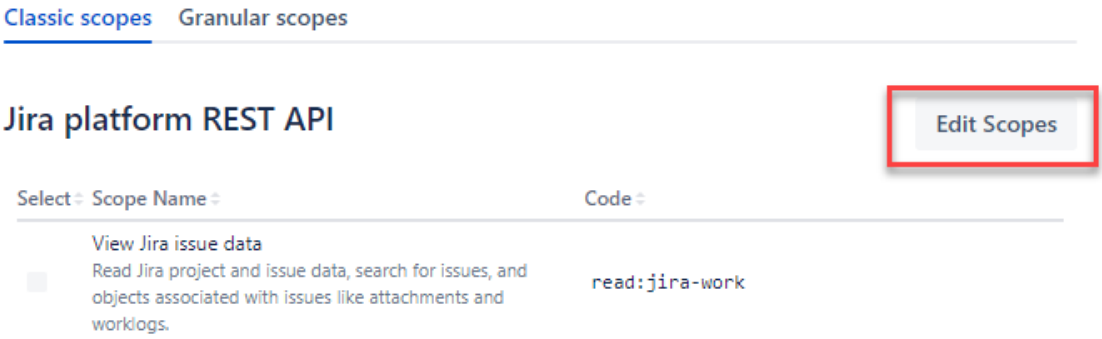
1. Login to Atlassian Developer Console as the **Site Admin**.
2. Click **Create App** drop down menu and select **OAuth 2.0 (3LO) integration**.
3. Fill in a App name, agree to Atllassian's developer terms, and click **Create**.



4. In left navigation menu, click **Permissions**. In **API name** > **Jira API**, click **Add**. When the **Add** button turns to **Configure**, click **Configure**.

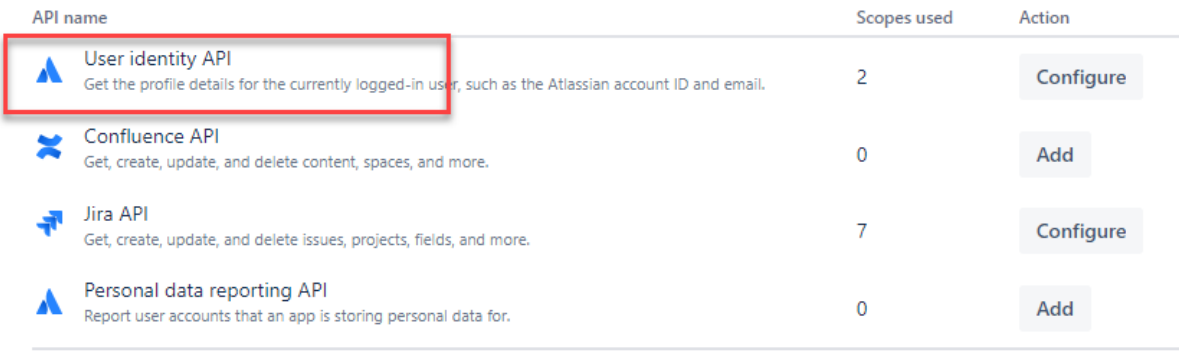


5. In **Classic scopes** tab, go to **Jira Platform REST API** section, and click **Edit Scopes**.

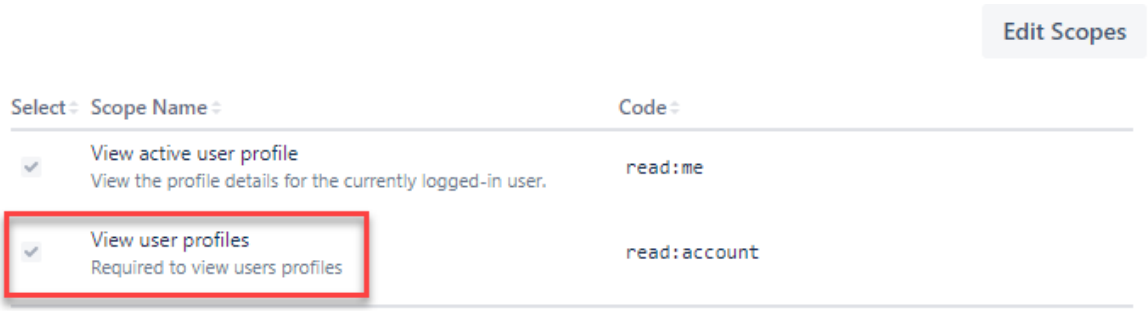


6. Check all scopes in **Edit Jira Platform REST API** and click **Save**.

7. In the left navigation menu, click **Permissions** again, in **API name** > **User Identity API**, click **Add**. When the Add button turns to Configure, click **Configure**.

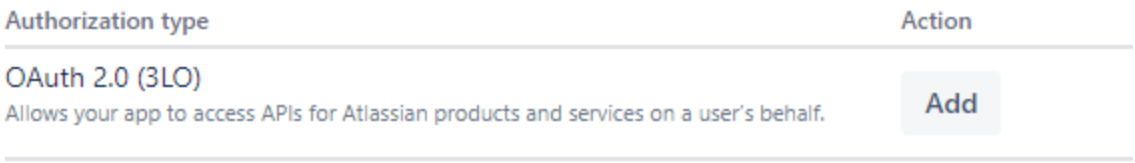


8. Click **Edit Scopes** to add the **View User Profile** scope, and click **Save**

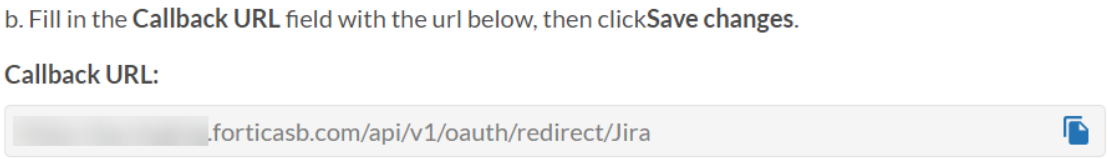


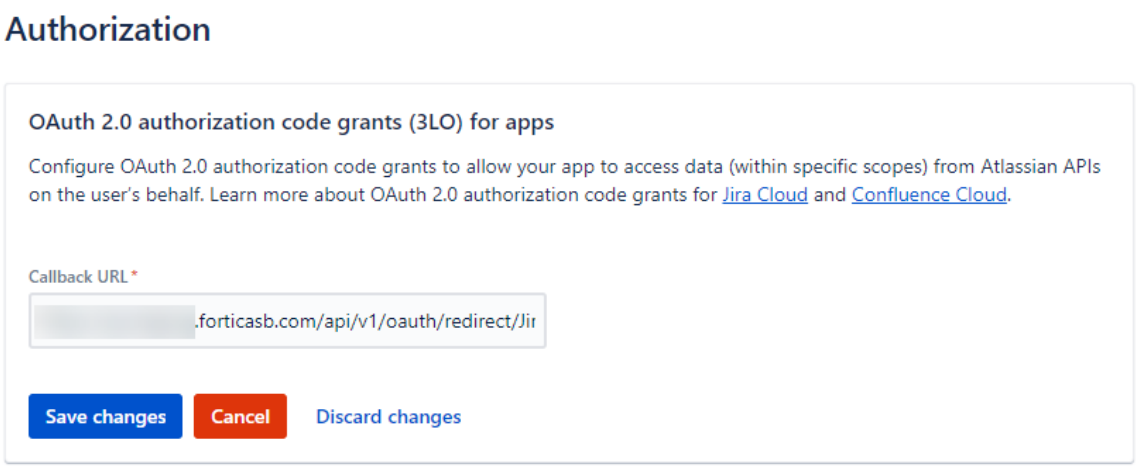
.

9. In the left navigation menu, click **Authorization**,in **Authorization type** > **OAuth 2.0 (3LO)**, click **Add**.



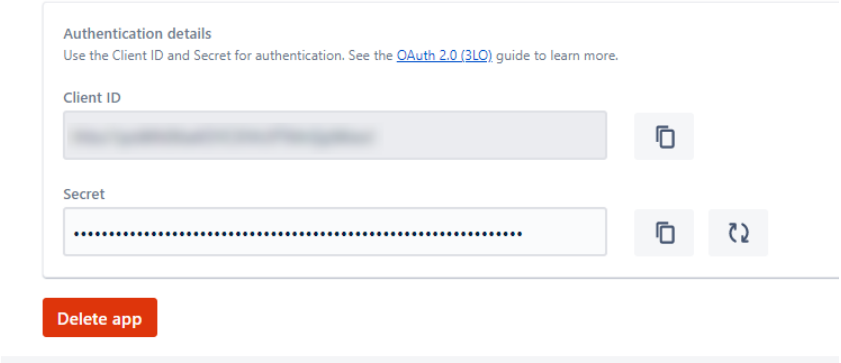
10. In the **Callback URL**, enter the callback URL from FortiCASB **Add Jira Account** page.





Click **Save Changes** to save the settings.

11. In the left navigation menu, click **Settings**, then scroll down to **Authentication details**, make a note of **Client ID** and **Secret** for later in FortiCASB authentication.

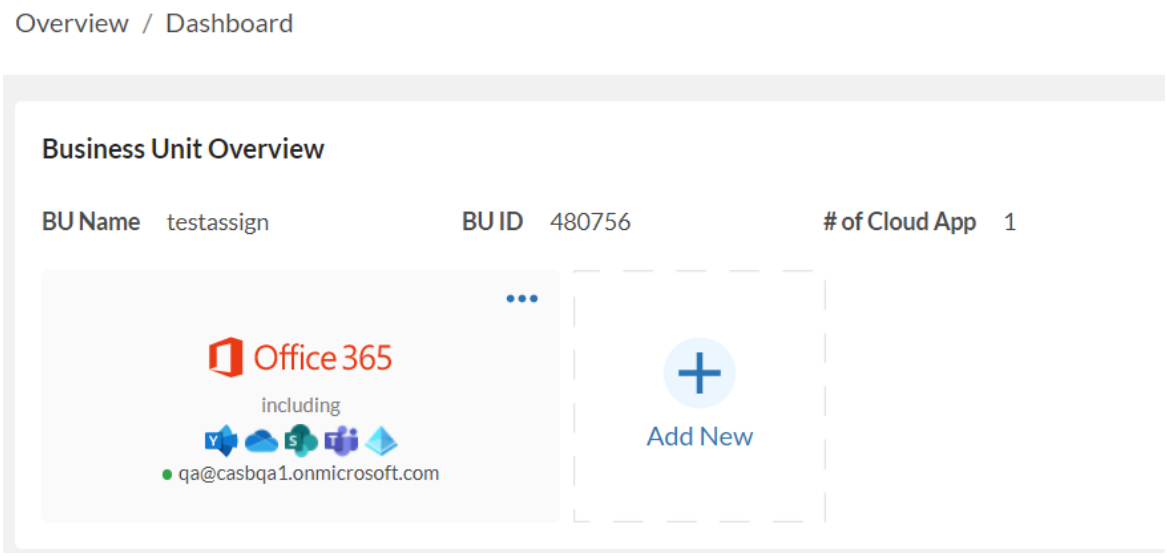


Please make sure the Jira account that will be added on FortiCASB is the same account that is configured.

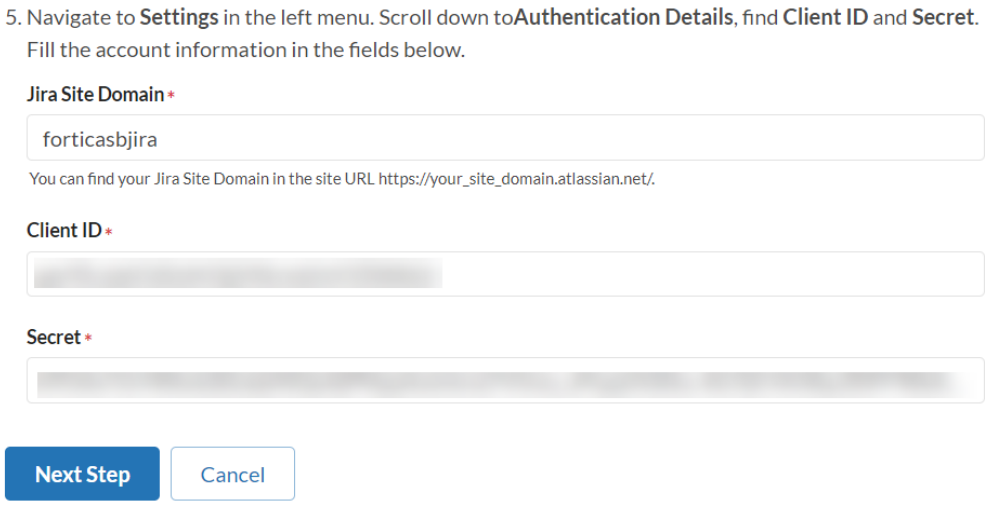
Add Jira Account

After completing Jira Account Configuration on page 164, follow the steps below to add Jira account on FortiCASB.

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **+Add New**, select **Jira**, then click **Add Selected Cloud App**.

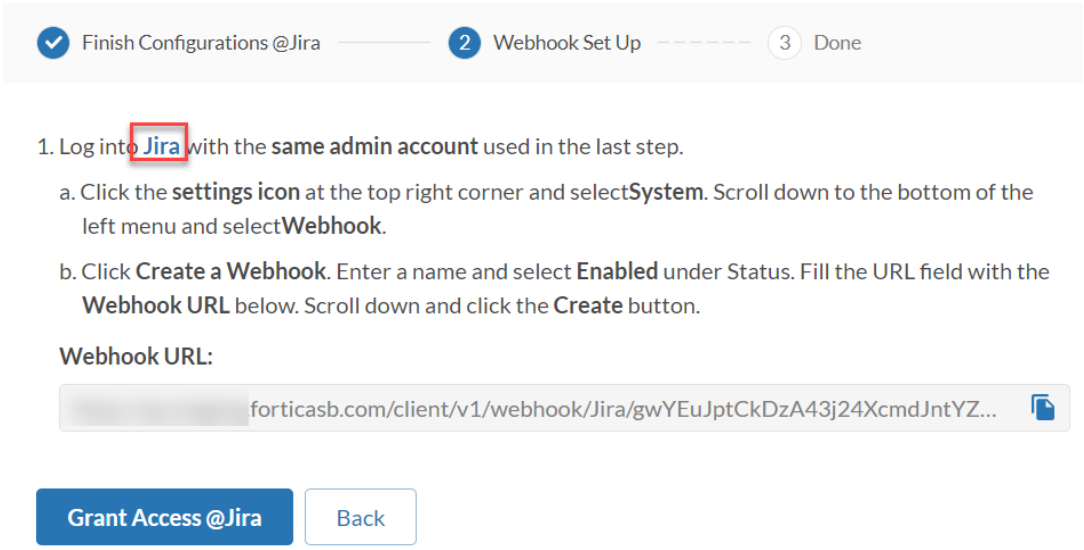


3. Fill in the **Jira Site Domain name** which the Jira account associates with, **Client ID** and **Client Secret** recorded down from Jira Account configuration. Your Jira site domain name is the site domain prefix.
For example: for https://mydomain.atlassian.net/, the Jira site domain name is "mydomain".

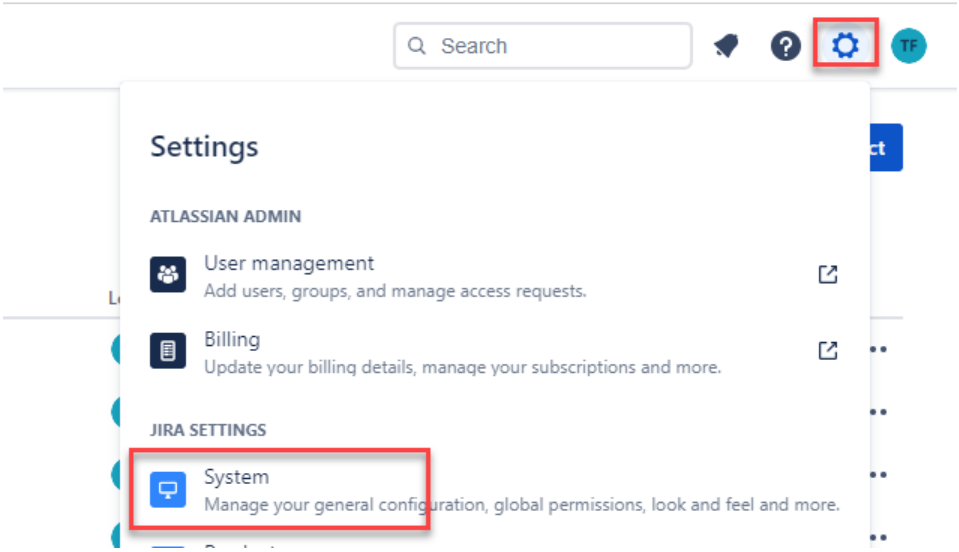


4. Then click **Next Step**.

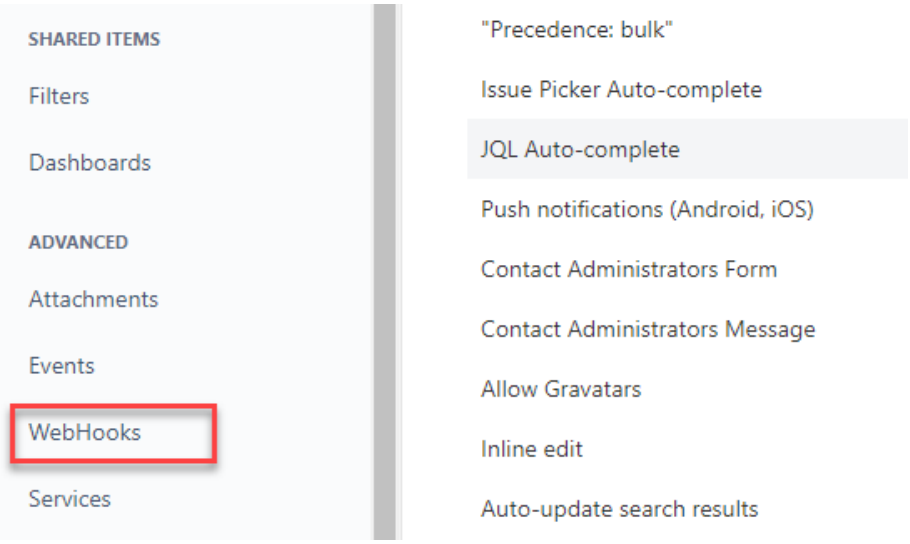
5. Click on the **Jira** link to log into the **Jira Domain Project** page.



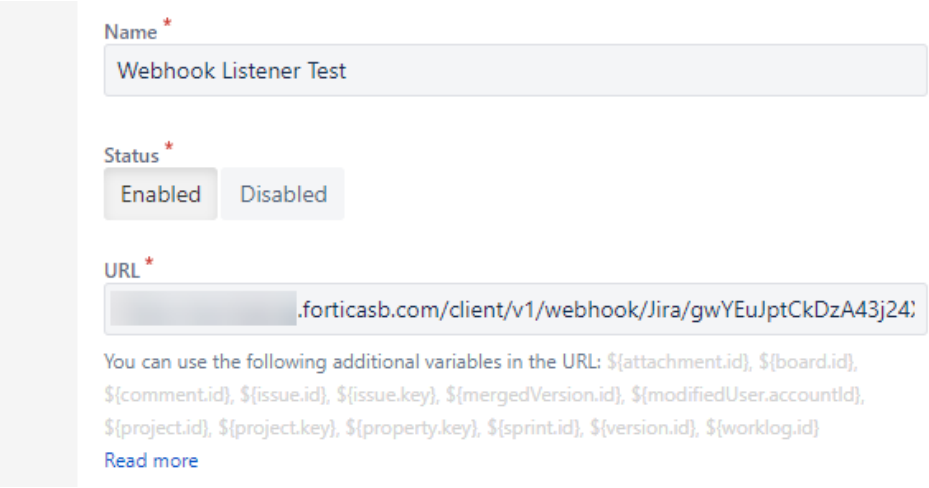
6. In Jira Domain Projects page, click **Settings** in the upper right hand corner, and select **System**.



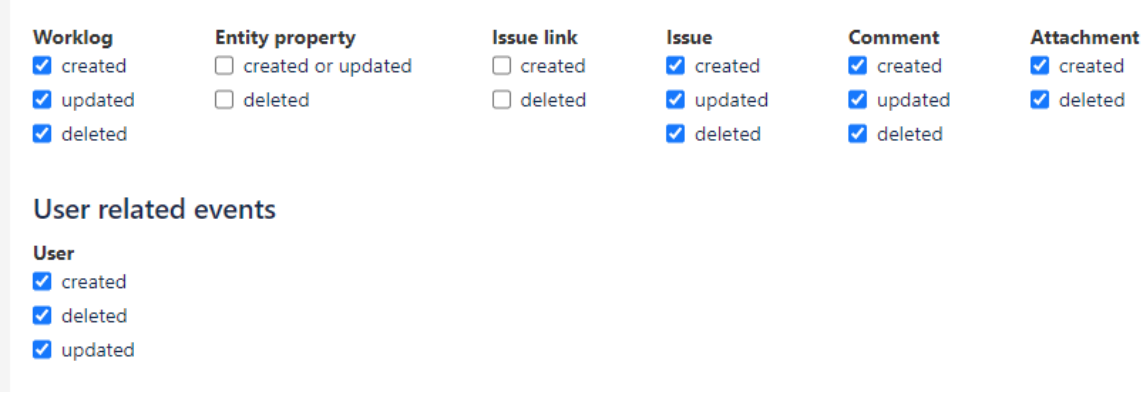
7. In the left menu, scroll down to the bottom of the page and select **Webhooks**.



8. Click **+Create Webhook**.
9. Fill in a **Name** for the Webhook, and select **Enabled** status.

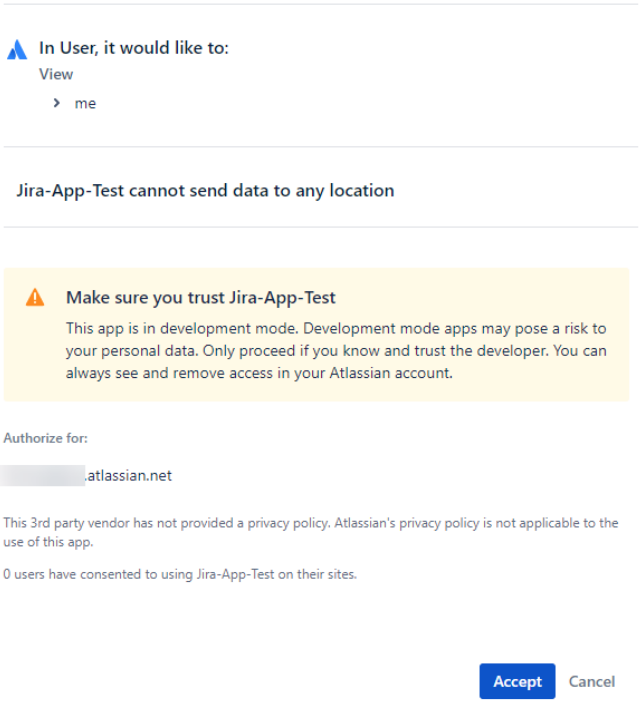


10. Copy the **Webhook URL** from FortiCASB **Add Jira Account** page and paste it in **URL** field.
11. In **Events**, check the issue related events as below.

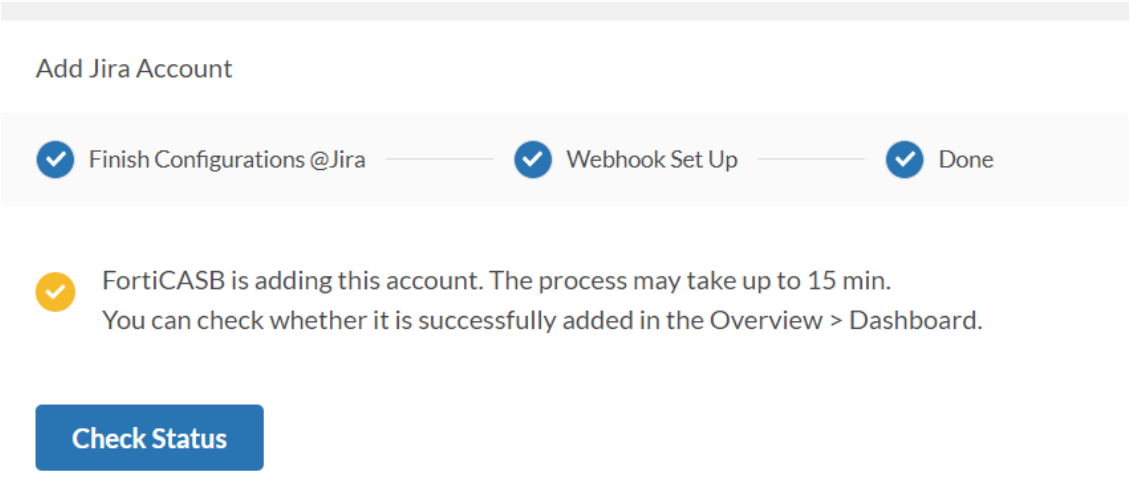


12. Click **Create** to finish.
13. Go back to FortiCASB **Add Jira Account** page, and click **Grant Access @Jira**.

14. You will be re-directed to **Jira OAuth** site, click **Accept** to finish adding the Jira account.



Then you will be re-directed back to FortiCABS. It may take 15 minutes to finish adding the account. You may check the status in **Overview > Dashboard.**



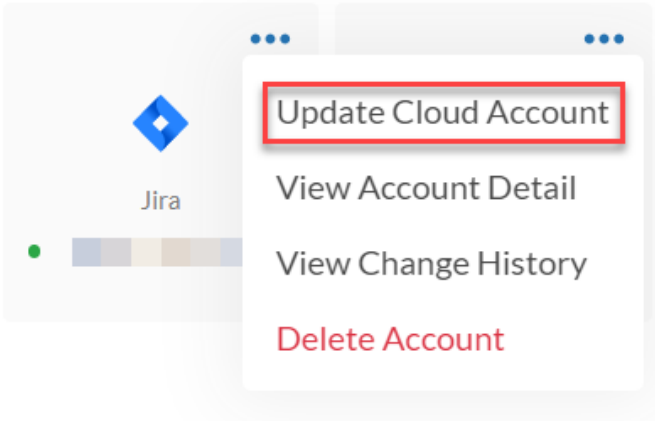
Update Jira Account

Before updating the Jira account on FortiCASB, complete the same configuration using the same Jira account:

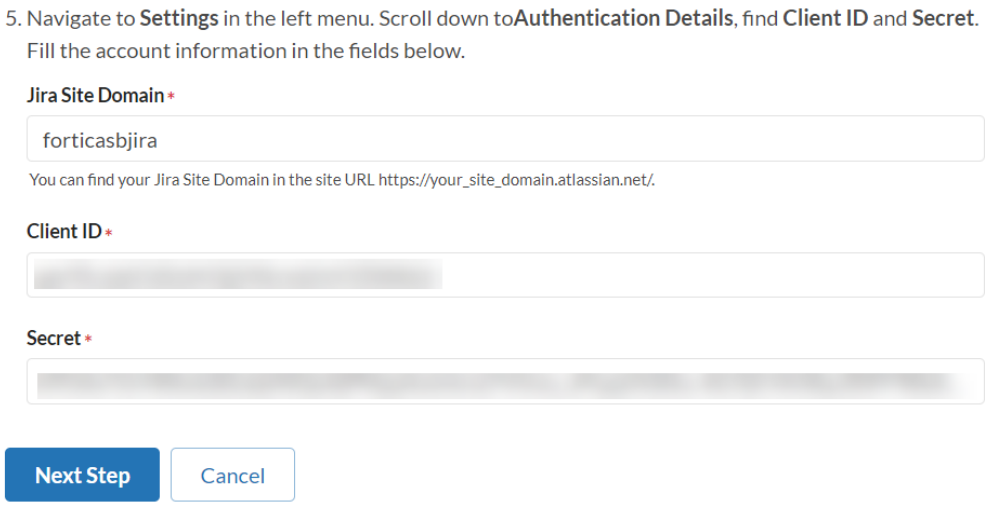
Jira Account Configuration on page 164

After the Jira configuration is completed, follow these steps to update your Jira account on FortiCASB.

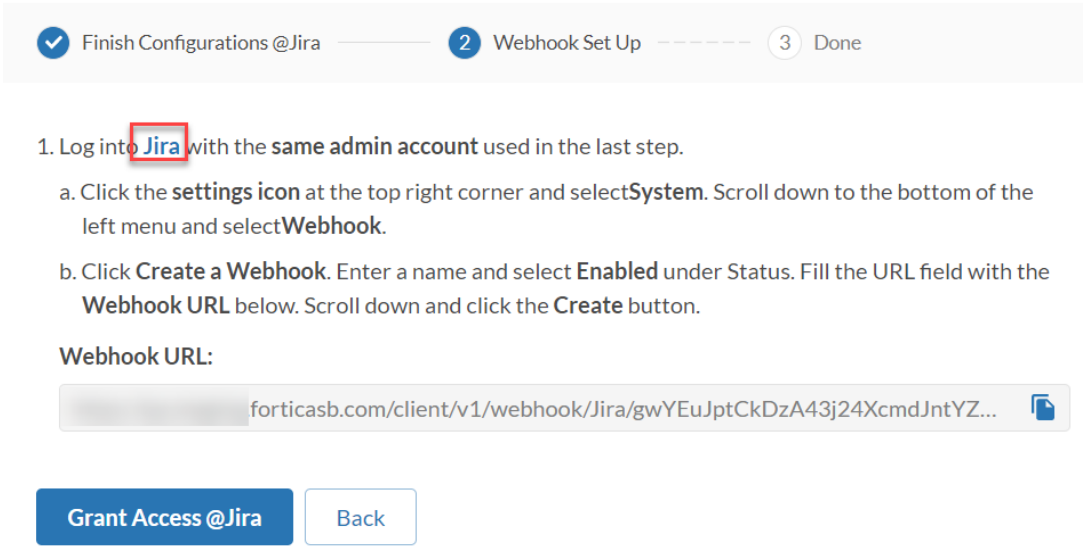
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on Jira account menu and select **Update Cloud Account.**



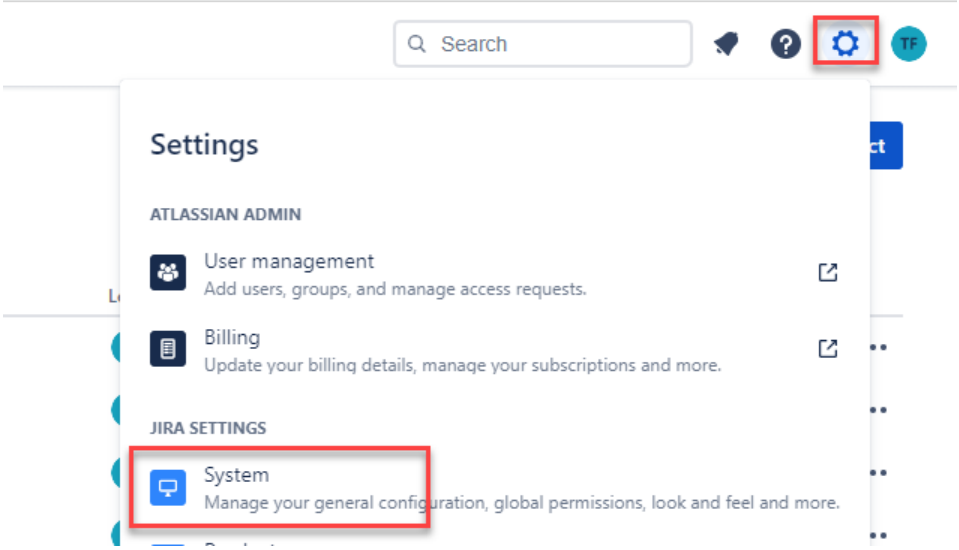
4. Fill in the **Jira Site Domain name** which the Jira account associates with, **Client ID** and **Client Secret** recorded down from Jira Account configuration. Your Jira site domain name is the site domain prefix.
For example: for https://mydomain.atlassian.net/, the Jira site domain name is "mydomain".



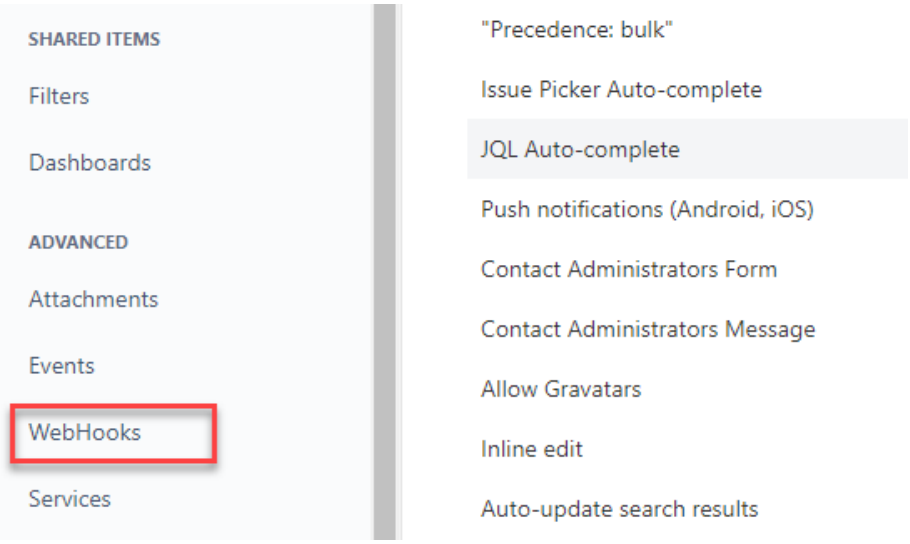
5. Then click **Next Step**.
6. Click on the **Jira** link to log into the **Jira Domain Project** page.



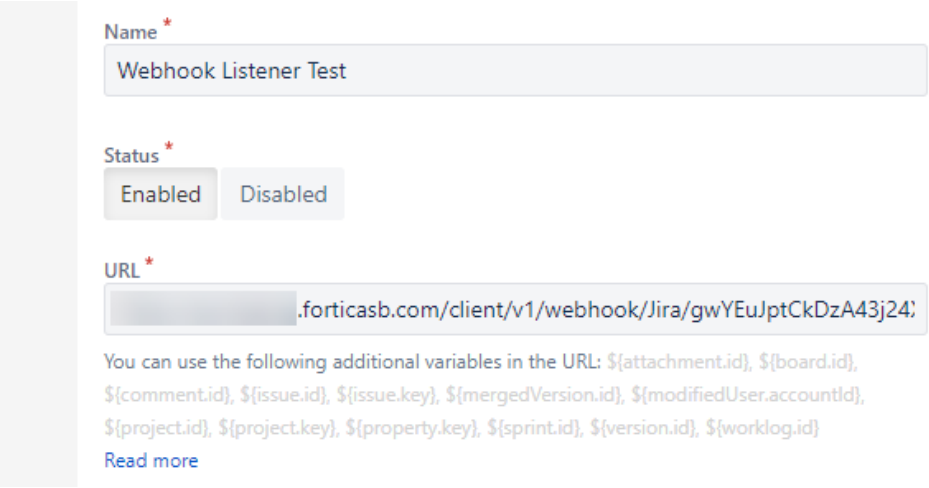
7. In Jira Domain Projects page, click **Settings** in the upper right hand corner, and select **System**.



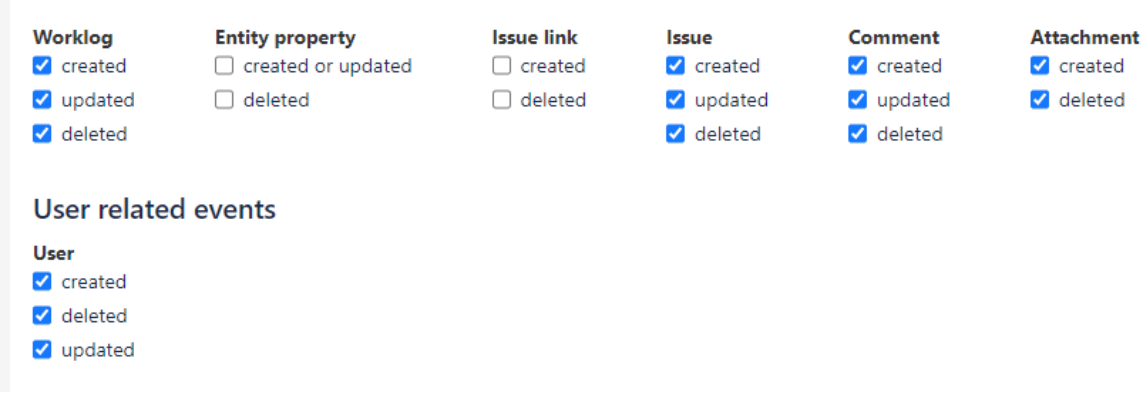
8. In the left menu, scroll down to the bottom of the page and select **Webhooks**.



9. Click **+Create Webhook**.
10. Fill in a **Name** for the Webhook, and select **Enabled** status.

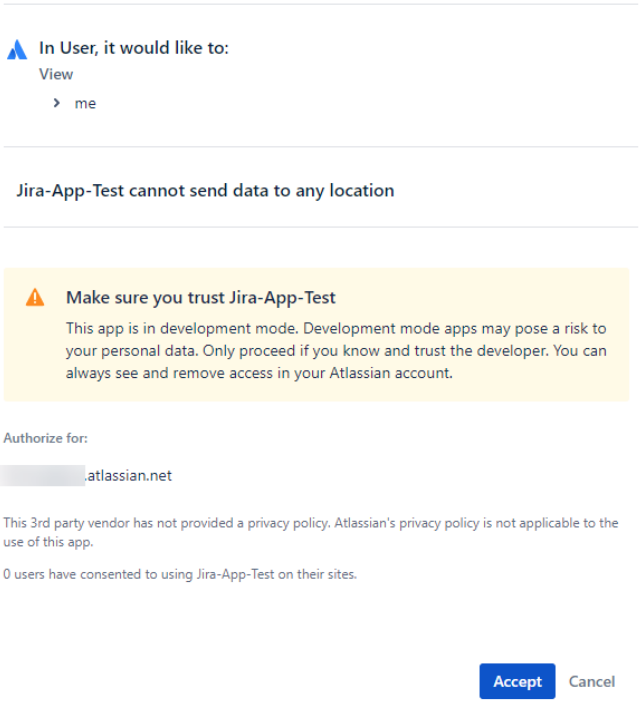


11. Copy the **Webhook URL** from FortiCASB **Jira Jira Account** page and paste it in **URL** field.
12. In **Events**, check the issue related events as below.

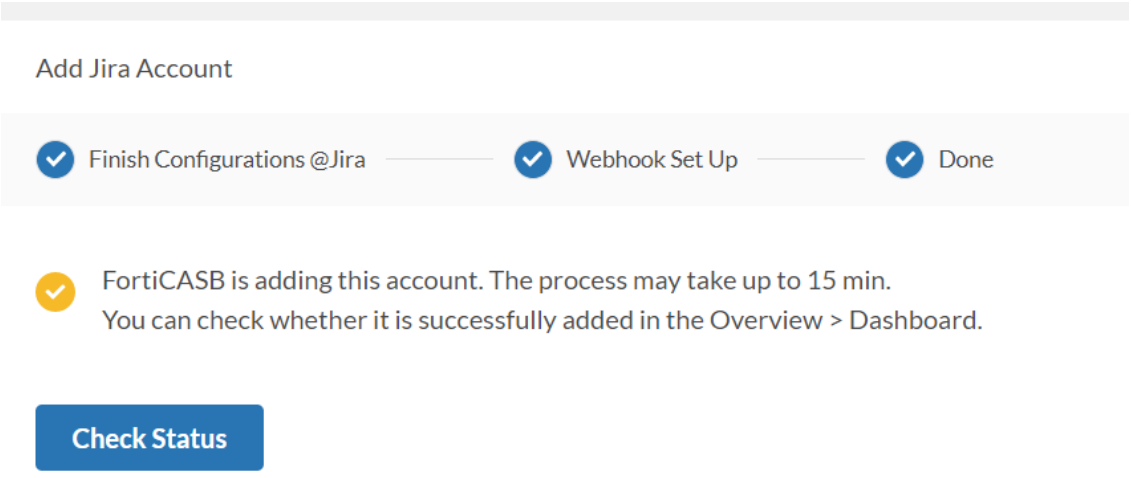


13. Click **Create** to finish.
14. Go back to FortiCASB **Update Jira Account** page, and click **Grant Access @Jira**.

15. You will be re-directed to **Jira OAuth** site, click **Accept** to finish updating the Jira account.



Then you will be re-directed back to FortiCABS. It may take 15 minutes to finish updating the account. You may check the status in **Overview > Dashboard.**



Office 365 (Before 24.2.a Update)

FortiCASB offers an API-based approach, pulling data directly from Office 365 via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Office 365 user activities, provide DLP Data Analysis for files on Office 365.

Microsoft Online Apps Integration

Beginning in 2021, the FortiCASB version **21.2** starts supporting multiple Microsoft online apps under the same Office 365 account.

When you add the Office 365 account on FortiCASB, if you are actively using any of these Microsoft online apps with the same account, they will be under monitoring and protection by FortiCASB.

Supported Microsoft Online Apps and Details:

Microsoft Online Apps	Monitoring Details
Microsoft Yammer	Monitors all **chats** and **shared files**.
Microsoft One Drive	Monitors all **files** shared privately or publicly.
Microsoft Sharepoint	Monitors files in **Document** and "**user-created**" folders.
Microsoft Teams	Monitors all **activities**, **group chats** except personal chats and shared files.
Azure Active Directory	Monitors all **user activities**.

Prerequisites

There are a few prerequisite before adding the Office 365 account on FortiCASB. Please follow the steps below.

1. **Office 365 Account and License on page 176** - Create Office 365 account with Global Administrator role.

2. **Activate Office 365 Account Audit Log on page 178** - Enable Office 365 Audit Log to record user activities of the Office 365 account.
3. **Add Admin to Sharepoint Site on page 180** - Incorporate protection on Office 365 Sharepoint sites by adding the Office 365 account to the site admin.
4. **Add Office 365 Account on page 184**- Activate site collection by adding the Office 365 account to FortiCASB.

New Office 365 Users

After the onboarding process is completed, all the Office 365 users under the account will be protected through Data Scan.

However, when a new Office 365 user is added on the account, the new user's OneDrive data is not proteceted. Please see **New Office 365 User Added After Onboarding on page 191**.

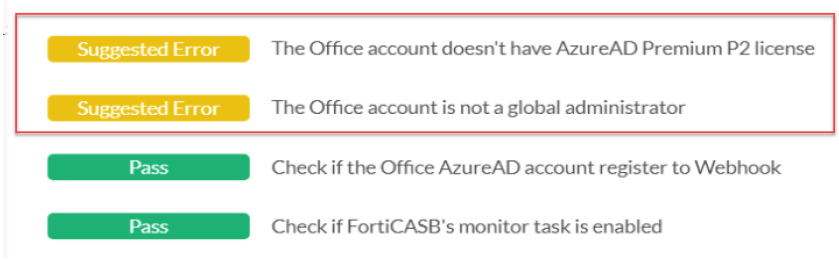
Office 365 Account and License

You may use an existing account or create a new account. If you create a new account, wait for at least 24 hours for the new account to take effect before granting access to FortiCASB. If you already have a Office 365 license, check with Determine the type of Office 365 license on page 178 to determine the type of Office 365 license you have.

License Requirement

1. Make sure your office 365 account license plan includes **Active Directory integration**. FortiCASB requires Active Directory support for most of its features. The following Office 365 licenses support Active Directory integration:
   a. Office 365 Business
   b. Office 365 Business Essentials
   c. Office 365 Business Premium
   d. Office 365 ProPlus
   e. Office 365 Enterprise E1
   f. Office 365 Enterprise E3
   g. Office 365 Enterprise E5
   h. Office 365 Enterprise K1

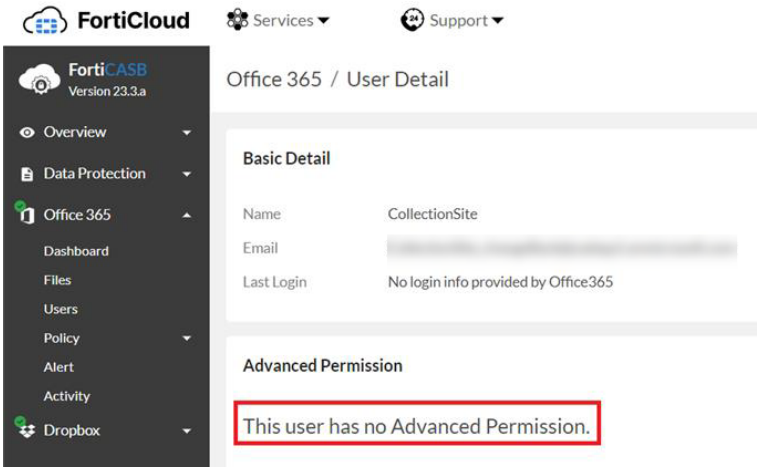
2. The Office 365 account **Global Administrator** role is required to add the Office 365 account to FortiCASB.
3. **Microsoft Entra ID P2 (formerly Azure AD P2) license** is recommended. In the absence of Microsoft Entra ID P2 License, FortiCASB's Discovery feature cannot access user entitlements which leads to the following errors in the onboarding status. All other major functions on FortiCASB will not be affected.



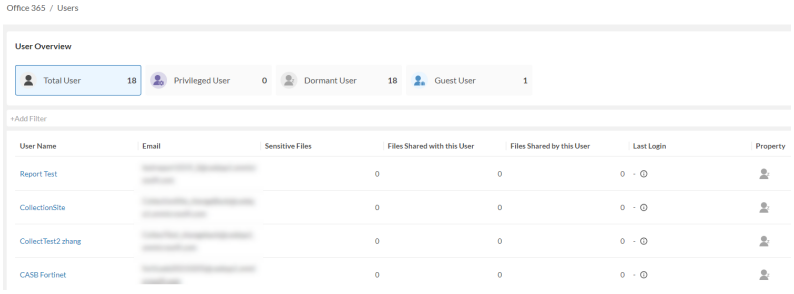
User entitlements is a feature within FortiCASB that enables you to view the roles and permissions that each user is entitled with.

There are some features that are dependent on the user entitlements provided by the Microsoft Entra ID P2 license, for example:

1. In the absence of Microsoft Entra ID P2 license, FortiCASB cannot acquire permissions of the Office 365 users. As a result, in **Office 365 > Users**, the **Advanced Permission** section of the user will show "This users has no Advanced Permission" even the user holds a global administrator role.



2. Without the Microsoft Entra ID P2 license, there is no sufficient data that can be retrieved to show **Privileged User** in **Office 365 > Users**.



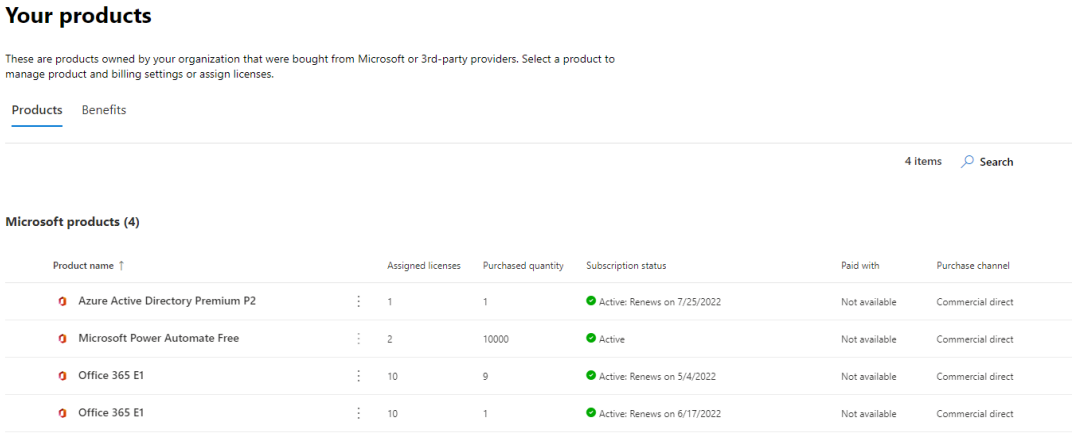
For more information on how to obtain Microsoft Entra ID P2 license, go to: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-get-started-premium

4. **Microsoft Enrtra Privileged Identity Management** also needs to be activated. For more information, go to: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Determine the type of Office 365 license

To determine what Office 365 license you have, follow the steps below:

1. Log into Office 365 account: https://www.office.com/.
2. Click on Apps button , located on the top-left corner of your Office 365 home screen.
3. Select **Admin**, then you will be re-directed to **Microsoft 365 admin center**.
4. On the navigation pane, go to **Billing > Your Products**. It will display your Office 365 license, along with your Microsoft Entra ID P2 license, if you have purchased it.

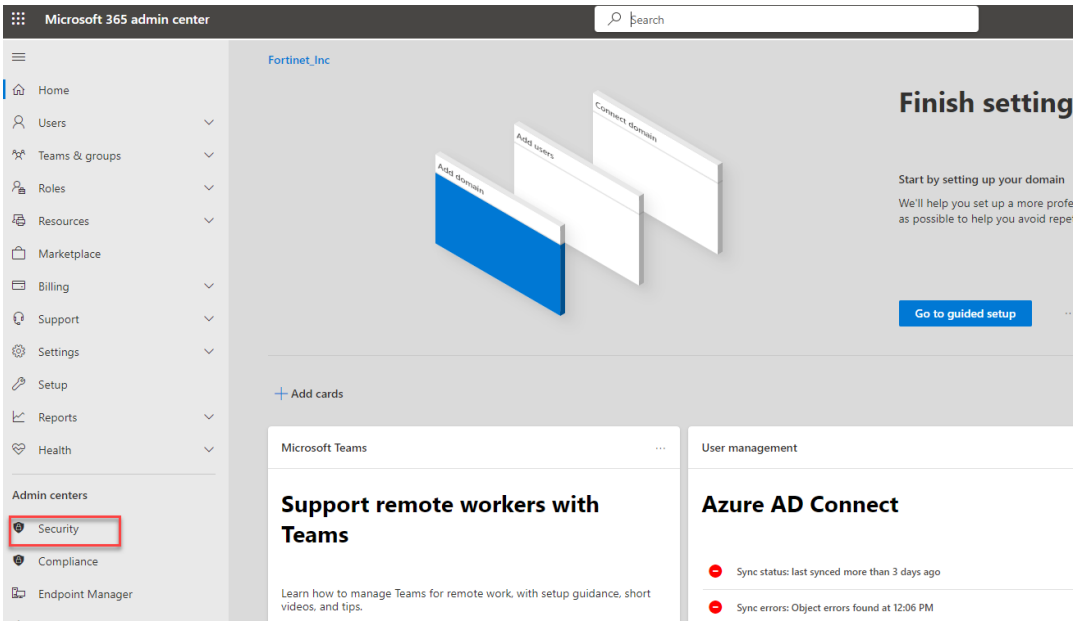


Activate Office 365 Account Audit Log

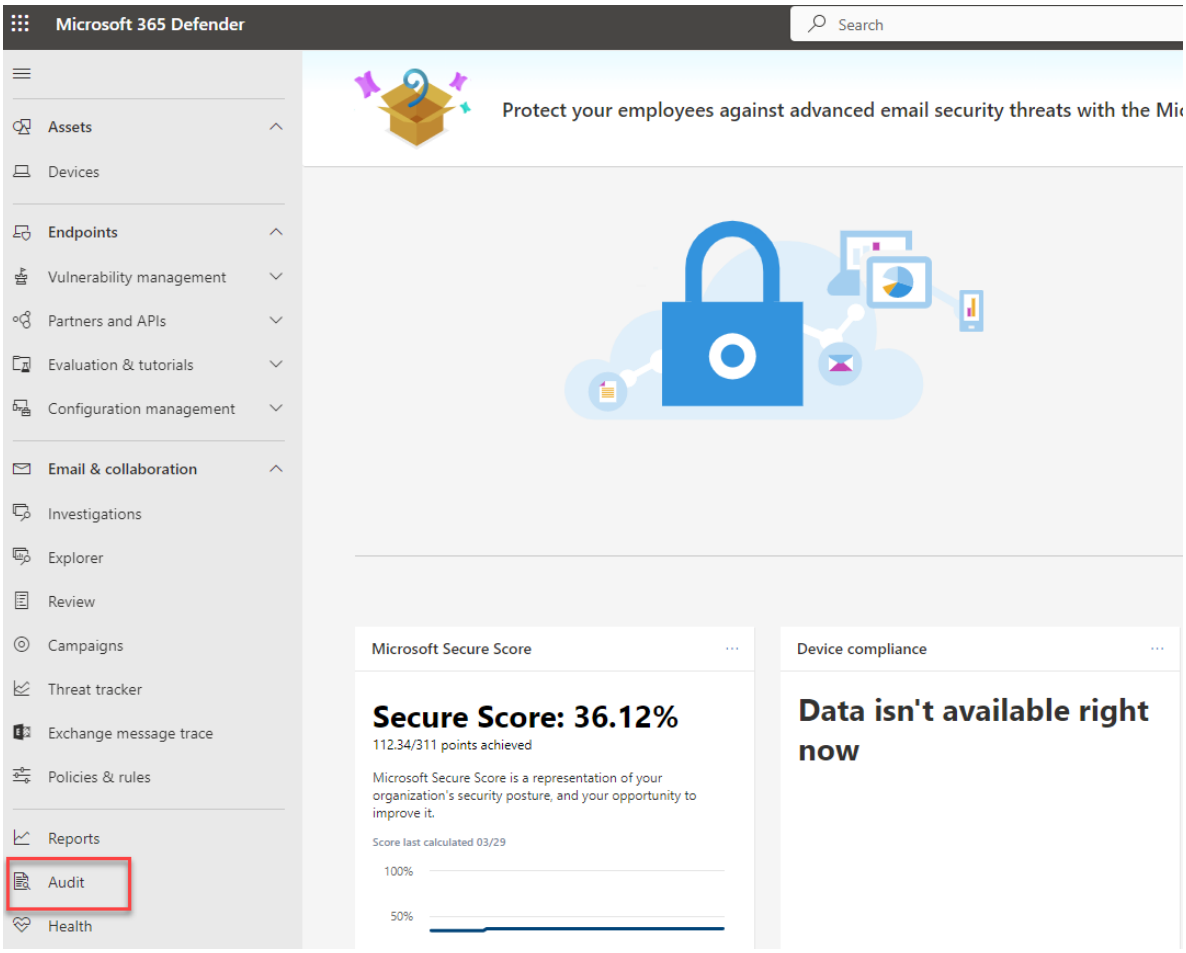
Office 365 audit log needs to be activated to record user and admin activities, this allows FortiCASB to monitor activities of the Office 365 account. It may take several hours after you turn on audit log before FortiCASB receives the audit logs from your Office 365 account.

To enable this feature, follow the steps below:

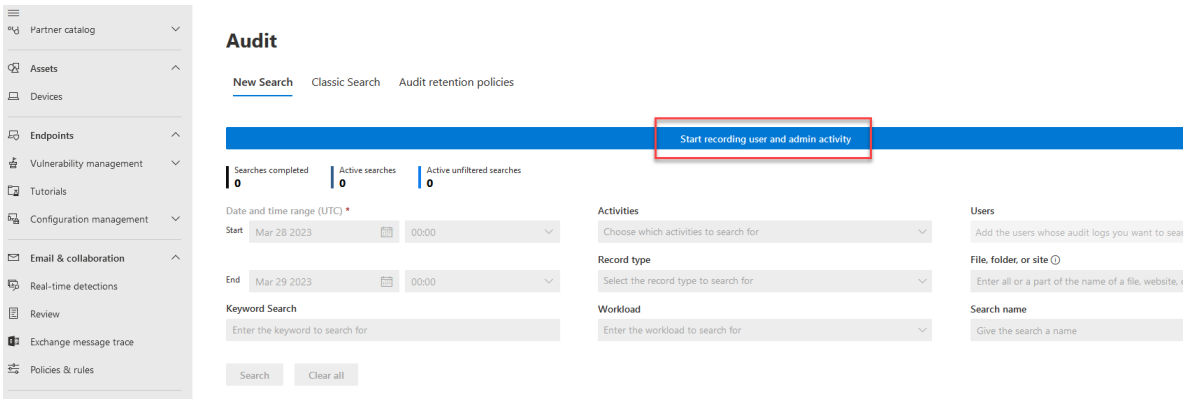
1. Log into Office 365 account as the admin user: https://www.office.com/.
2. Click on Office 365 menu option and select **Admin** portal to be re-directed to **Microsoft 365 admin center**.
3. In **Microsoft 365 admin center**, expand the left menu and click on **Security**, you will be re-directed to **Microsoft 365 Defender** page.



4. In **Microsoft 365 Defender**, scroll down the left menu and click on **Audit**.



5. In **Audit**, click **Start recording and admin activity**.



1. If you do not see this option, that means the organization has already enabled this option.
2. If you are a new tenant, this option can only appear 24 hours after the tenant creation.

6. After turning on auditing, please allow 24 hours for the auditing to become available.

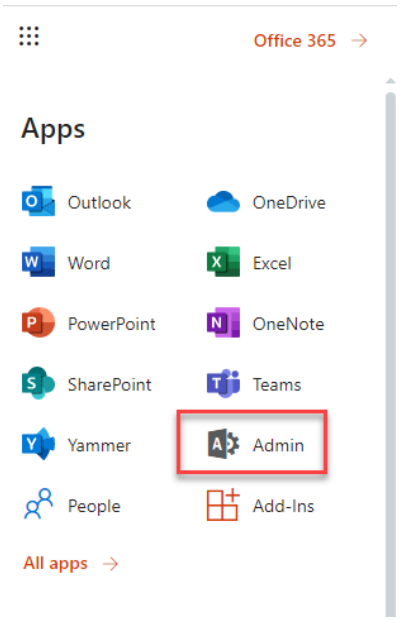
Now you may activate site collection by adding the Office 365 account to FortiCASB.

When you see an error on adding Office 365 to FortiCASB you might need to wait before auditing is enabled on Office 365 portal.

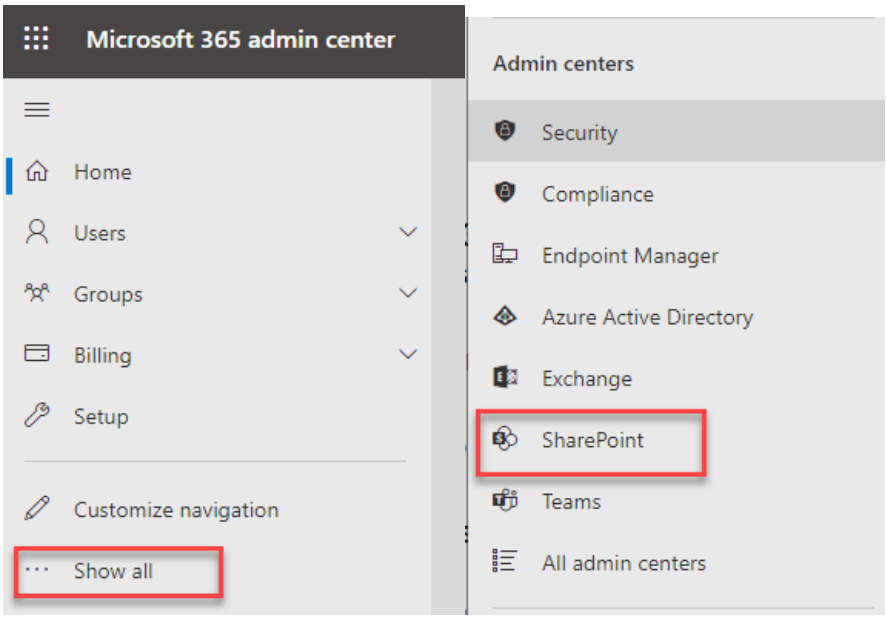
Add Admin to Sharepoint Site

Before adding your Office 365 admin account to FortiCASB, please verify that the account is one of the Company Administrators of the Office 365 Sharepoint Sites. This is to ensure that FortiCASB is able to monitor and protect the account's Sharepoint sites.

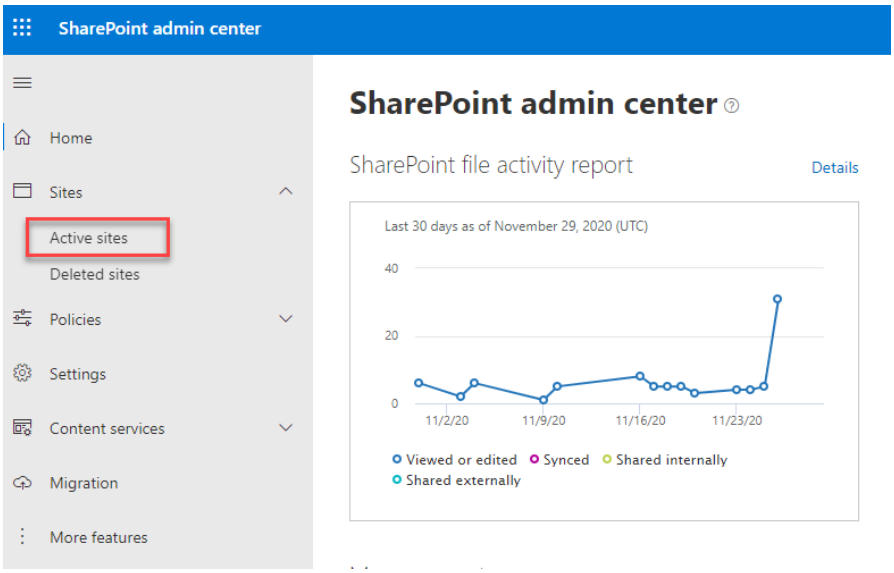
1. Log into Office 365 (https://office.com) with your admin account to be added to FortiCASB.
2. Click on App Launcher button at the top left corner, and select **Admin**.



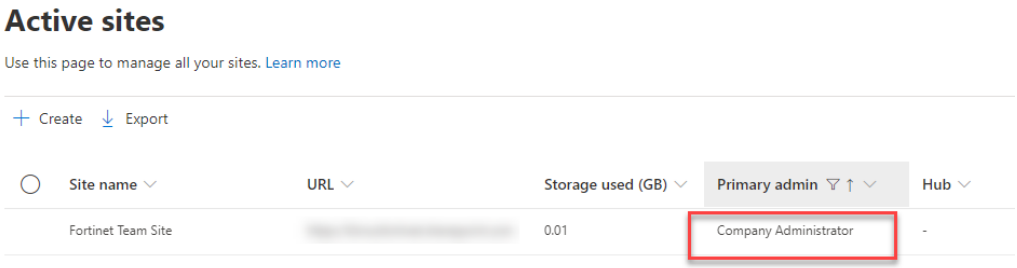
3. In **Microsoft 365 admin center** left navigation menu, click on **Show all** to show other options. Scroll down to **Admin Centers** and click **SharePoint** to enter **SharePoint admin center**.



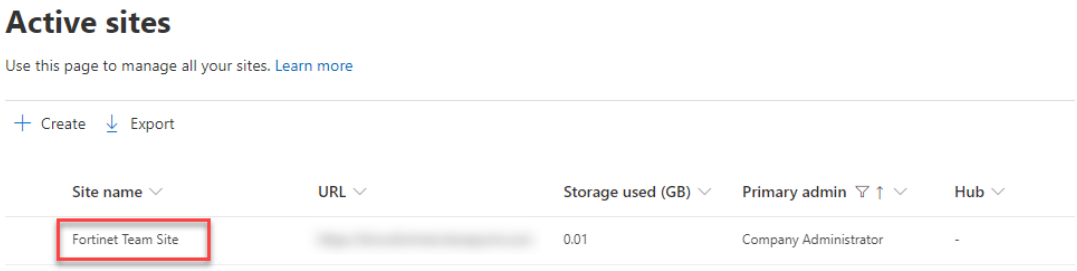
4. In **SharePoint admin center**, click on **Sites** drop down menu, and select **Active Sties**.



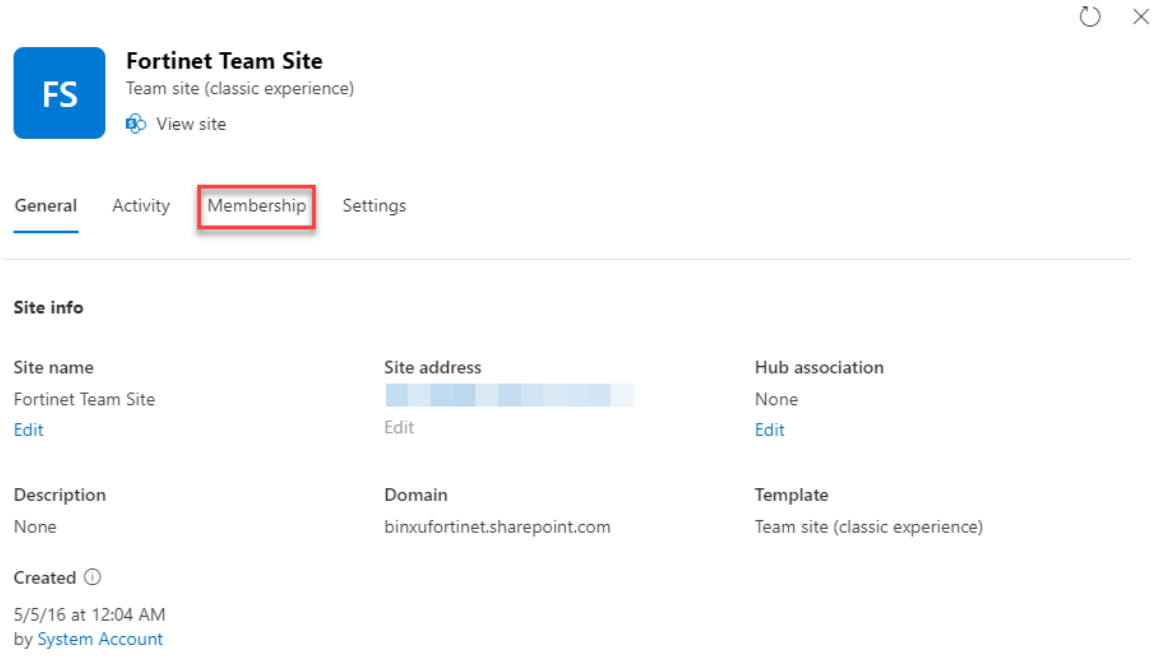
5. In **Active sties**, under **Primary admin** column, scroll down to look for "Company Administrator".



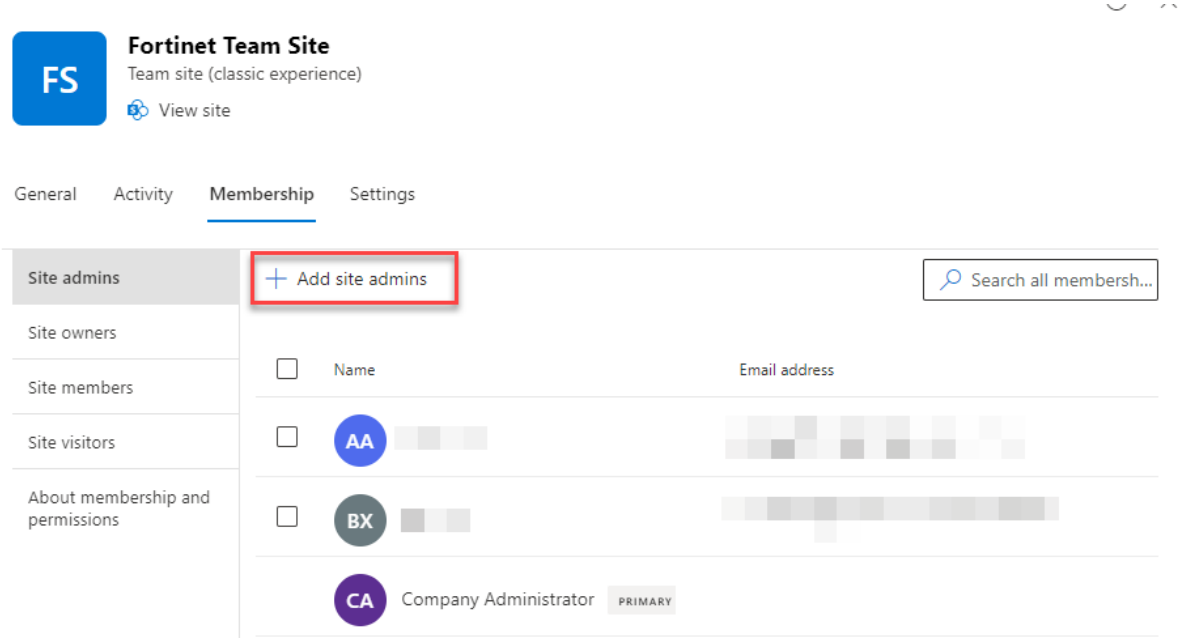
6. Click on the Site name of the user shown as "Company Administrator".



7. The Sharepoint site profile dialog will appear, then click on **Membership** tab.



8. Click **+ Add site admins** to add your account as a new site admin. In this way, FortiCASB will be able to monitor and protect the sharepoint site after your admin account is added to FortiCASB

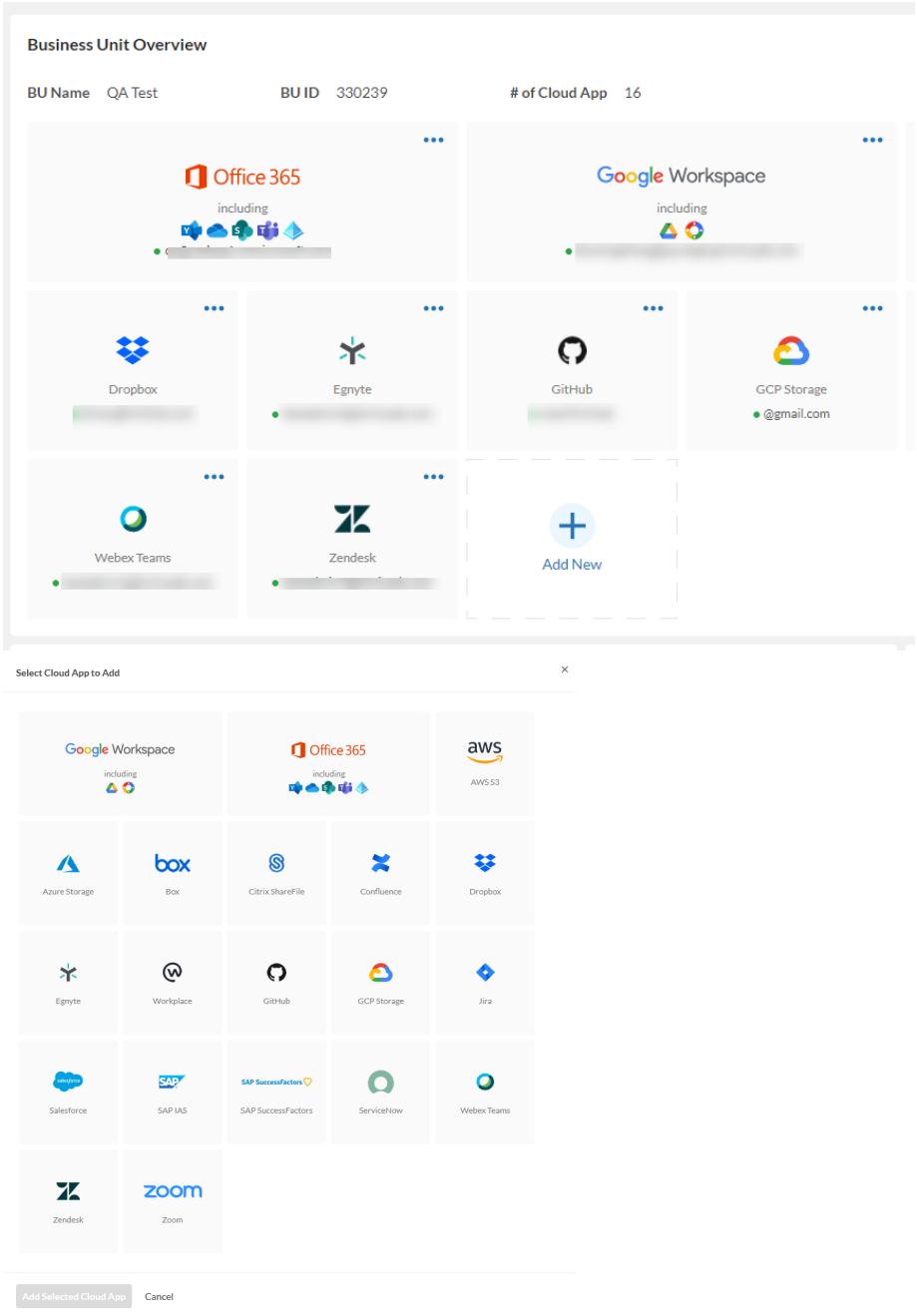


Note: If you want FortiCASB to monitor and protect other Sharepoint sites of the same domain, repeat **step 6-8** with a different Sharepoint site.

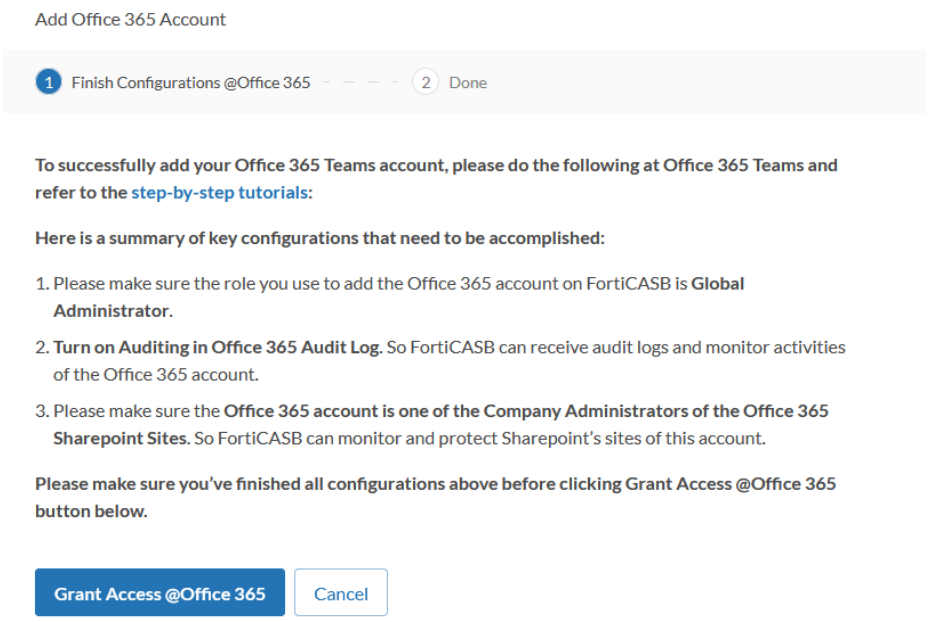
Add Office 365 Account

After all the Office 365 configurations are completed from previous sections, follow these steps to add your Office 365 account on FortiCASB.

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Office 365**, then click **Add Selected Cloud App**.



3. Make sure you have completed all Office 365 configurations, and click **Grant Access @Office 365.**



You will be redirected to the Office 365 login screen, enter your account password and log in.

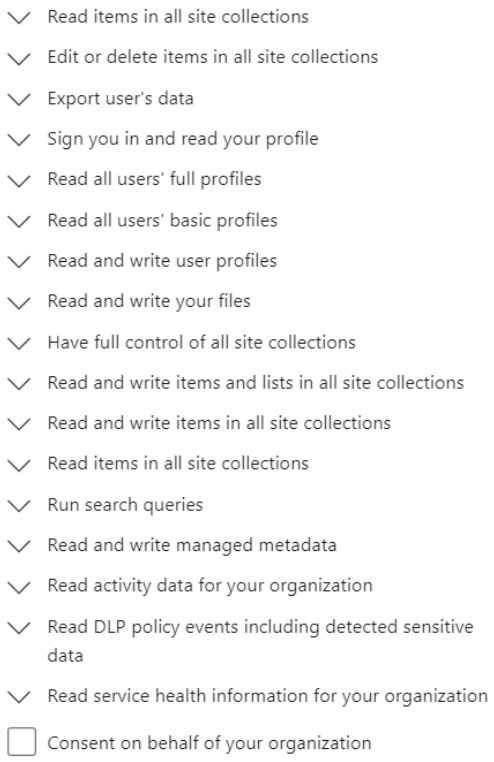
4. After logged in, Office 365 will prompt you to accept FortiCASB access. FortiCASB only request partial permissions from the global administrator user.
Here is the complete list of permissions requested:

Permissions requested by FortiCASB
Manage access reviews that you can access
Read applications
Read audit log data
Read consent requests
Read your contacts
Read delegated permission grants
Access the directory as you
Read directory data
Read domains.
Read all files that you have access to
Have full access to all files you have access to
Read all groups
Read all OneNote notebooks that you

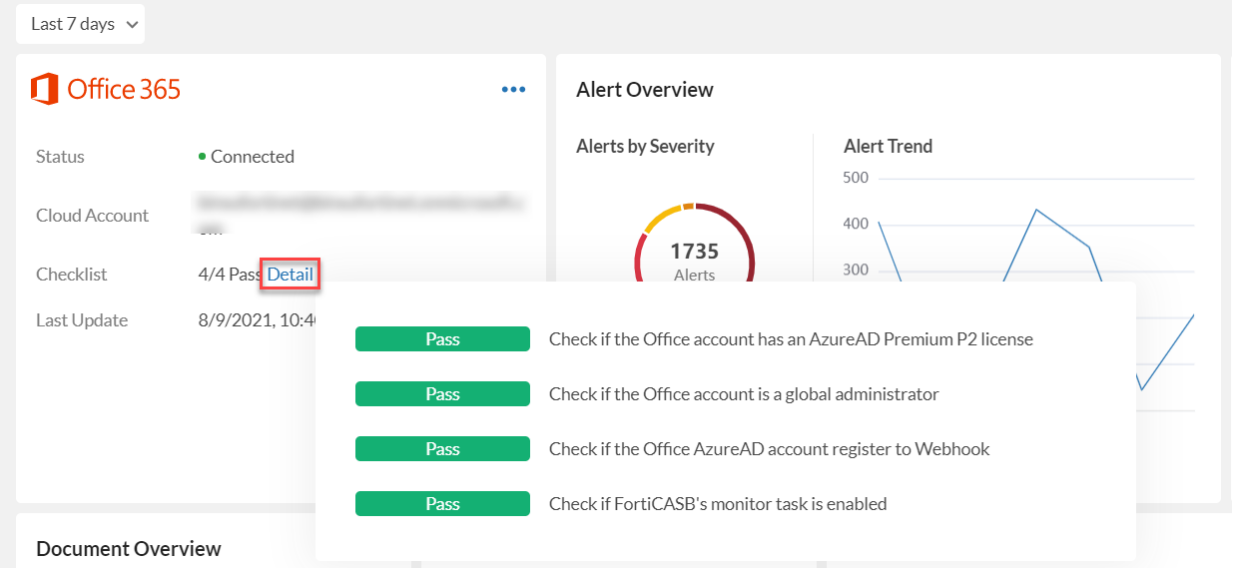
Permissions requested by FortiCASB
can access
Maintain access to data you have given it access to
Read organization information
Read all users' relevant people lists
Read your organization's policies
Read your organization's conditional access policies
Read your organization's identity protection policy
Read consent and permission grant policies
Read privileged access to Azure AD
Read privileged access to Azure AD groups
Read privileged access to your Azure resources
Read directory RBAC settings
Read your organization's security actions
Read your organization's security events
Have full control of all your site collections
Create, edit, and delete items and lists in all your site collections
Read items in all site collections
Edit or delete items in all site collections
Export user's data
Sign you in and read your profile
Read all users' full profiles
Read all users' basic profiles
Read and write user profiles
Read and write your files

Permissions requested by FortiCASB
Have full control of all site collections
Read and write items and lists in all site collections
Read and write items in all site collections
Run search queries
Read and write managed metadata
Read activity data for your organization
Read DLP policy events including detected sensitive data
Read service health information for your organization

5. Click **Accept** to grant permissions to FortiCASB. Office 365 may ask you to grant access to FortiCASB three more times to confirm this process. Afterward, you will be redirected back to FortiCASB.



You can see the installation checklist and status in the Office 365 dashboard. Please allow up to 15 minutes for the account to be fully added.



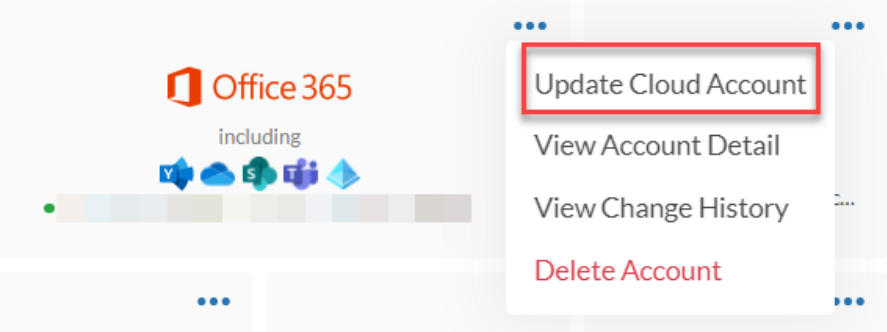
Update Office 365 Account

Before updating the Office 365 account on FortiCASB, complete the same configurations using the same Office 365 account:

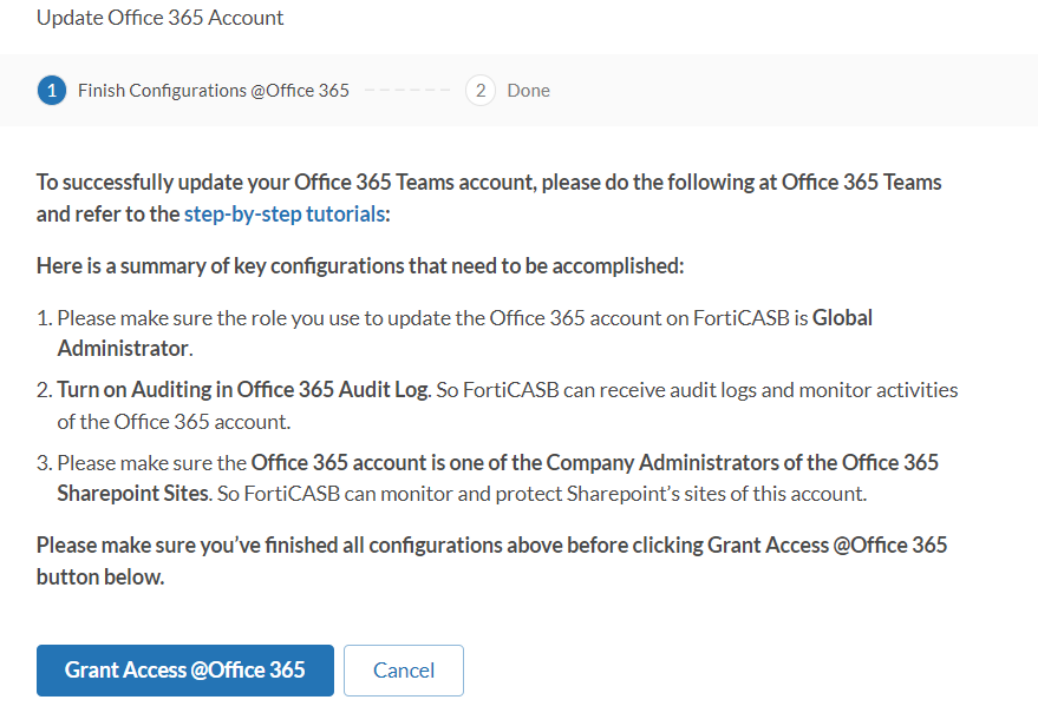
1. **Office 365 Account and License on page 176** - Create Office 365 account with Global Administrator role.
2. **Activate Office 365 Account Audit Log on page 178** - Enable Office 365 Audit Log to record user activities of the Office 365 account.
3. **Add Admin to Sharepoint Site on page 180**- Incorporate protection on Office 365 Sharepoint sites by adding the Office 365 account to the site admin.

After the Office 365 configuration is completed, follow these steps to update your Office 365 account on FortiCASB.

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the Office 365 Account menu and select **Update Cloud Account.**

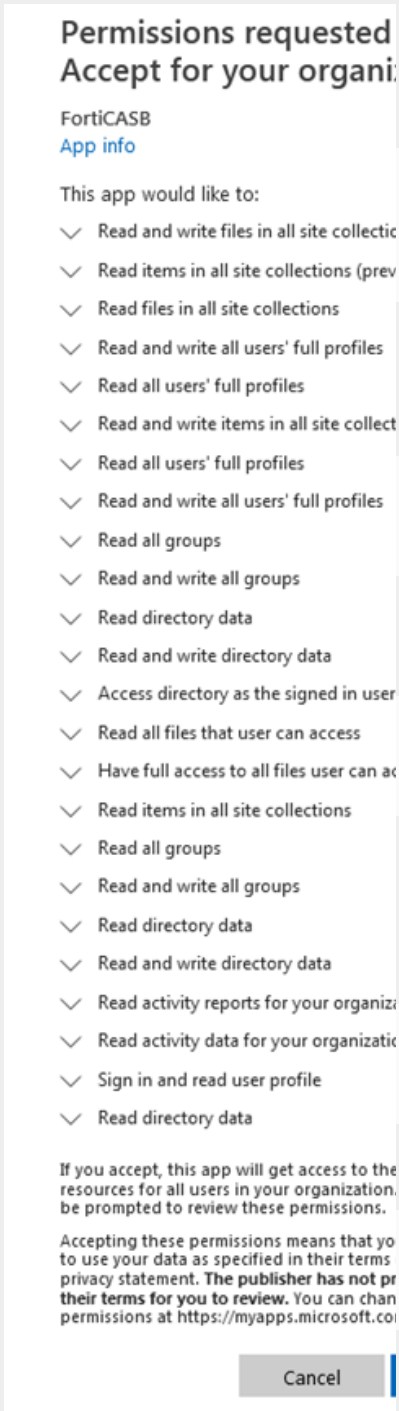


4. Make sure you have completed all Office 365 configurations, and click **Grant Access @Office 365.**



You will be redirected to the Office 365 login screen, enter your account password and log in.

5. After logging in, Office 365 will prompt you to accept FortiCASB access.
Note: FortiCASB does not request all but only partial permissions from the global administrator user. Below is a list of permissions requested by FortiCASB.



Permissions requested by FortiCASB
Read and write files in all site collections
Read items in all site collections (preview)
Read files in all site collections
Read and write all users' full profiles
Read all users' full profiles
Read and write items in all site collections (preview)
Read all users' full profiles
Read all groups
Read and write all groups
Read directory data
Read and write directory data
Access directory as the signed in user

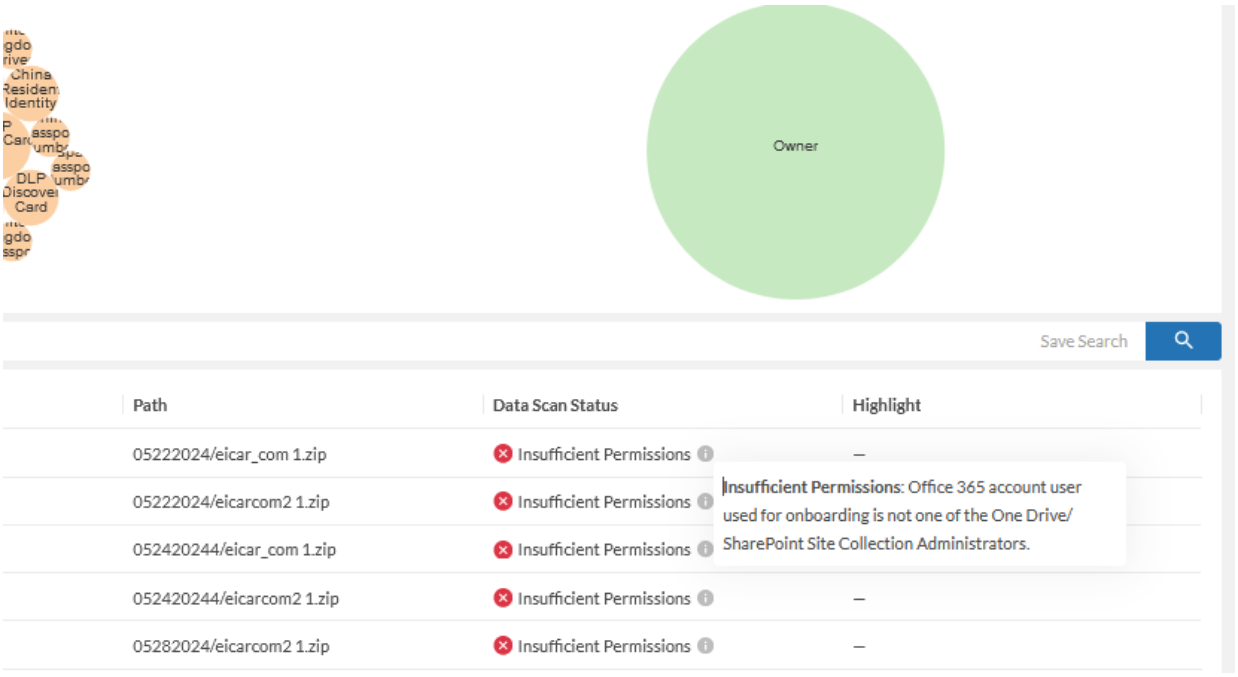
	Read all files that user can access
	Read items in all site collections
	Read all groups
	Read directory data
	Read activity report for your organization
	Read activity data for your organization
	Sign in and read user profile
	Read directory data

6. Office 365 may ask you to grant access to FortiCASB 3 more times then you will be redirected back to FortiCASB.

You can see the installation checklist and status in the Office 365 dashboard. Please allow up to 15 minutes for the account to be fully updated.

New Office 365 User Added After Onboarding

When a new Office 365 user is added to the Office 365 account after the onboarding process. The new user's **OneDrive** data is not accessible, thus the new user's OneDrive data do not have data scan feature. **SharePoint Site** data has similar issue.



OneDrive Solution- The Office 365 service account user (the account that was used in the onboarding process) needs to be added to the new user's OneDrive Site Collection Administrator through the FortiCASB account update process or it needs to be manually updated in the new Office 365 user's OneDrive setting. Please follow the instruction in **Insufficient Permissions(Access Denied) Error (One Drive) on page 525**

SharePoint Site Solution - The Office 365 service account user (the account that was used in the onboarding process) needs to be added to the SharePoint Site admin group through the FortiCASB account update process or it needs to be manually updated in the SharePoint Site Admin Center. Please follow the instruction in **Insufficient Permissions(Access Denied) Error (SharePoint) on page 528**

Office 365 (After 24.2.a Update)

FortiCASB offers an API-based approach, pulling data directly from Office 365 via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Office 365 user activities, provide DLP Data Analysis for files on Office 365.

After **24.2.a update**, Office 365 performance has been improved by supporting higher rates of files scanning by using a dedicated service account instead of a user account. A client application needs to be registered in Microsoft Entra ID on Azure to onboard Office 365.

Microsoft Online Apps Integration

Beginning in 2021, the FortiCASB version **21.2** starts supporting multiple Microsoft online apps under the same Office 365 account.

When you add the Office 365 account on FortiCASB, if you are actively using any of these Microsoft online apps with the same account, they will be under monitoring and protection by FortiCASB.

Supported Microsoft Online Apps and Details:

Microsoft Online Apps	Monitoring Details
Microsoft Yammer	Monitors all **chats** and **shared files**.
Microsoft One Drive	Monitors all **files** shared privately or publicly.
Microsoft Sharepoint	Monitors files in **Document** and "**user-created**" folders.
Microsoft Teams	Monitors all **activities**, **group chats** except personal chats and shared files.
Azure Active Directory	Monitors all **user activities**.

Prerequisites

There are a few prerequisite before adding the Office 365 account on FortiCASB. Please follow the steps below.

1. **Office 365 Account and License on page 194** - The Office 365 account and license requirements in adding the account in FortiCASB.
2. **Activate Office 365 Account Audit Log on page 196** - Enable Office 365 Audit Log to record user activities of the Office 365 account.

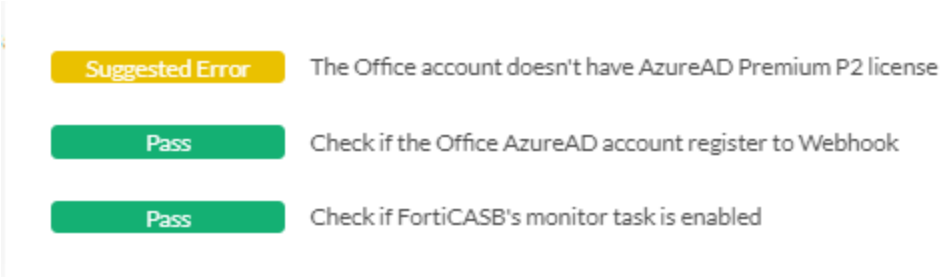
3. **Register FortiCASB with Microsoft Identity Platform on page 198** - Register an application on Microsoft Azure Identity Management platform for Office 365 account onboarding.
4. **Add Office 365 Account on page 202** - Activate site collection by adding the Office 365 account to FortiCASB.

Office 365 Account and License

You may use an existing account or create a new account. If you create a new account, wait for at least 24 hours for the new account to take effect before granting access to FortiCASB. If you already have a Office 365 license, check with **Determine the type of Office 365 license on page 195** to determine the type of Office 365 license you have.

License Requirement

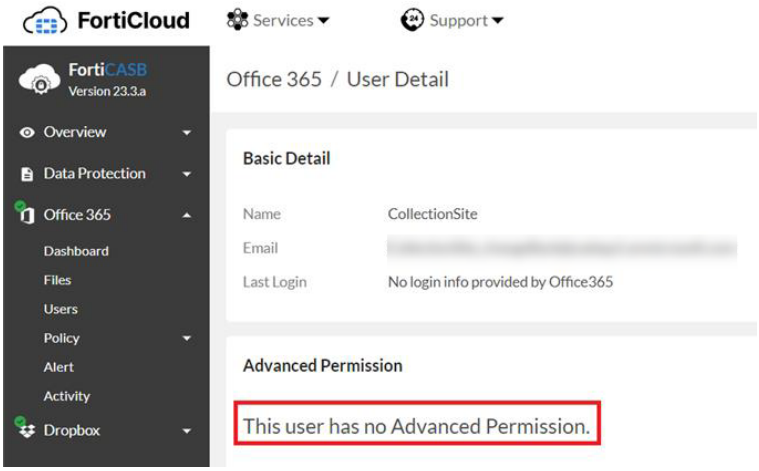
1. Make sure your office 365 account license plan includes **Active Directory integration**. FortiCASB requires Active Directory support for most of its features. The following Office 365 licenses support Active Directory integration:
   a. Office 365 Business
   b. Office 365 Business Essentials
   c. Office 365 Business Premium
   d. Office 365 ProPlus
   e. Office 365 Enterprise E1
   f. Office 365 Enterprise E3
   g. Office 365 Enterprise E5
   h. Office 365 Enterprise K1
2. **Microsoft Entra ID P2 (formerly Azure AD P2) license** is recommended. In the absence of Microsoft Entra ID P2 License, FortiCASB's Discovery feature cannot access user entitlements which leads to the following errors in the onboarding status. All other major functions on FortiCASB will not be affected.



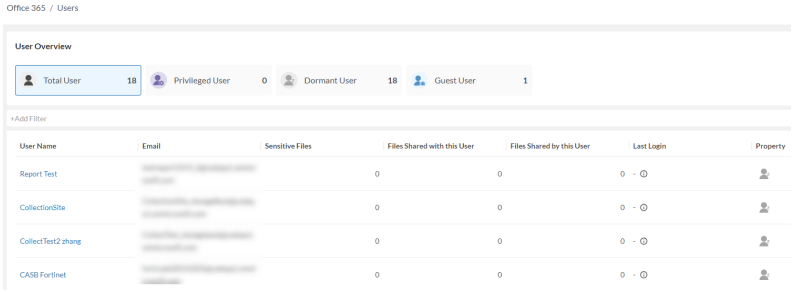
User entitlements is a feature within FortiCASB that enables you to view the roles and permissions that each user is entitled with.

There are some features that are dependent on the user entitlements provided by the Microsoft Entra ID P2 license, for example:

1. In the absence of Microsoft Entra ID P2 license, FortiCASB cannot acquire permissions of the Office 365 users. As a result, in **Office 365 > Users**, the **Advanced Permission** section of the user will show "This users has no Advanced Permission" even the user holds a global administrator role.



2. Without the Microsoft Entra ID P2 license, there is no sufficient data that can be retrieved to show **Privileged User** in **Office 365 > Users**.



3. For more information on how to obtain Microsoft Entra ID P2 license, go to: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-get-started-premium

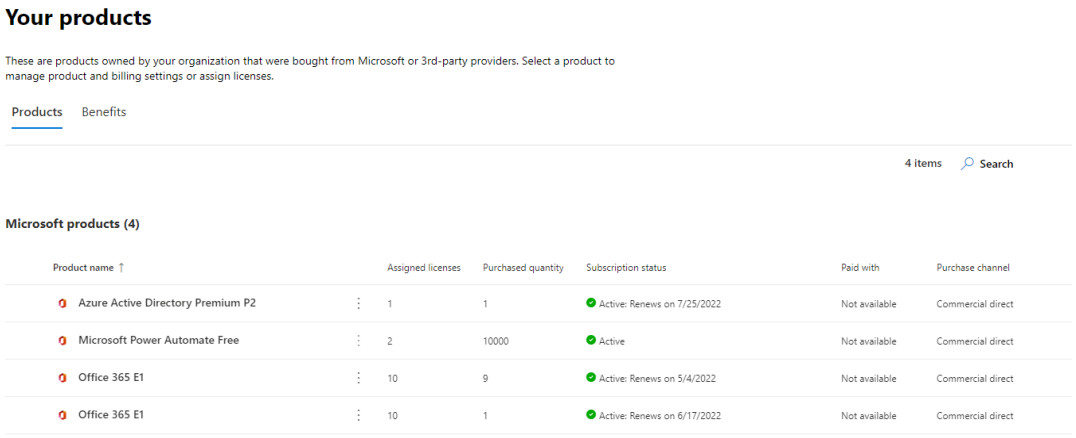
3. **Microsoft Enrtra Privileged Identity Management** also needs to be activated. For more information, go to: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Determine the type of Office 365 license

To determine what Office 365 license you have, follow the steps below:

1. Log into Office 365 account: https://www.office.com/.
2. Click on Apps button , located on the top-left corner of your Office 365 home screen.
3. Select **Admin**, then you will be re-directed to **Microsoft 365 admin center**.
4. On the navigation pane, go to **Billing > Your Products**. It will display your Office 365 license, along with

your Microsoft Entra ID P2 license, if you have purchased it.

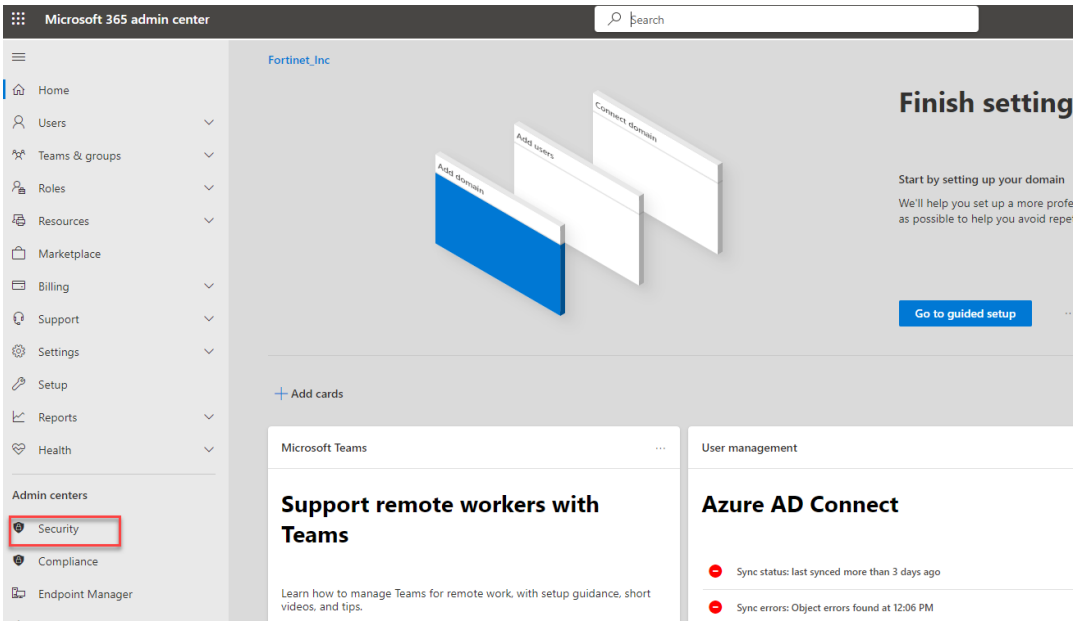


Activate Office 365 Account Audit Log

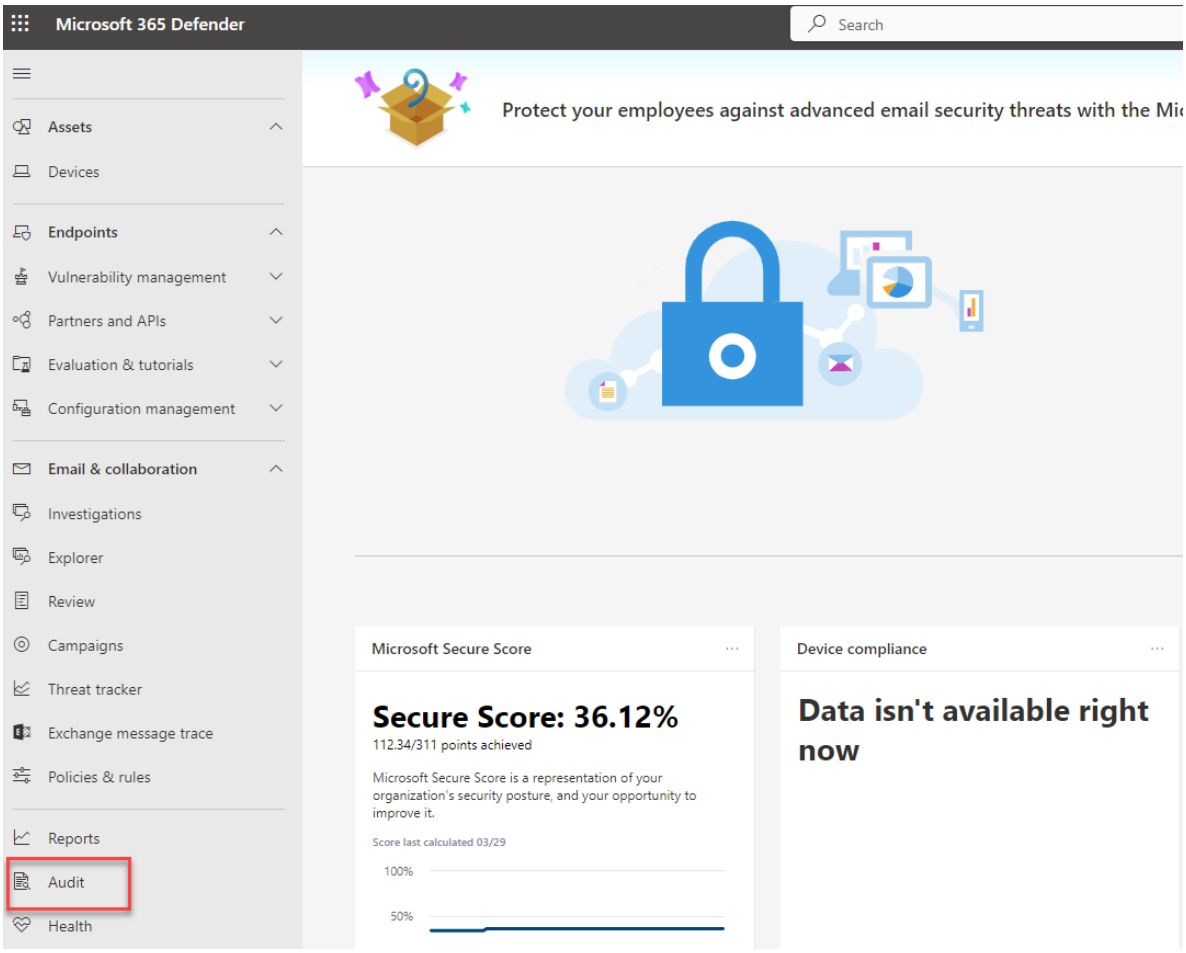
Office 365 audit log needs to be activated to record user and admin activities, this allows FortiCASB to monitor activities of the Office 365 account. It may take several hours after you turn on audit log before FortiCASB receives the audit logs from your Office 365 account.

To enable this feature, follow the steps below:

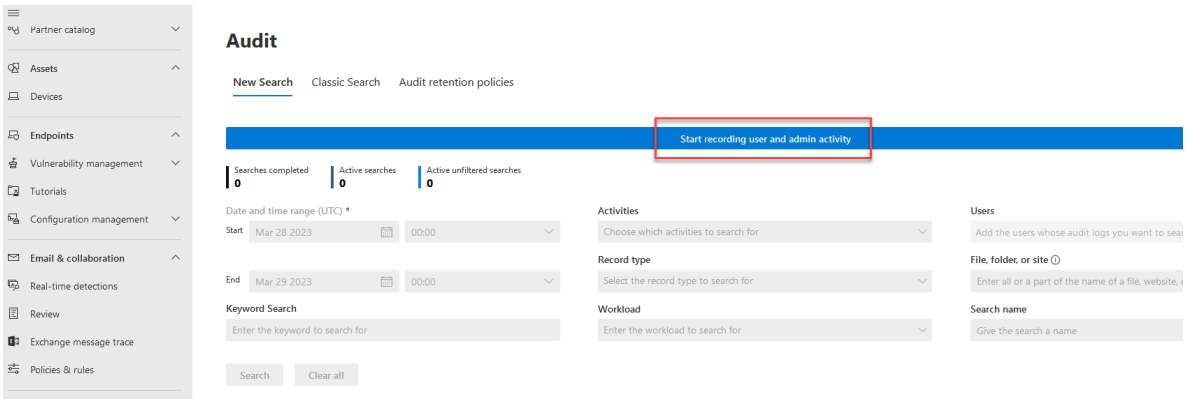
1. Log into Office 365 account as the admin user: https://www.office.com/.
2. Click on Office 365 menu option  and select **Admin** portal to be re-directed to **Microsoft 365 admin center**.
3. In **Microsoft 365 admin center**, expand the left menu and click on **Security**, you will be re-directed to **Microsoft 365 Defender** page.



4. In **Microsoft 365 Defender**, scroll down the left menu and click on **Audit**.



5. In **Audit**, click **Start recording and admin activity**.



1. If you do not see this option, that means the organization has already enabled this option.
2. If you are a new tenant, this option can only appear 24 hours after the tenant creation.

6. After turning on auditing, please allow 24 hours for the auditing to become available.

Now you may activate site collection by adding the Office 365 account to FortiCASB.

When you see an error on adding Office 365 to FortiCASB you might need to wait before auditing is enabled on Office 365 portal.

Register FortiCASB with Microsoft Identity Platform

In order to use identity and access management compatibilities of Microsoft Entra ID in accessing Office 365 resources, a registered FortiCASB application needs to be created first in the Microsoft Entra admin center.

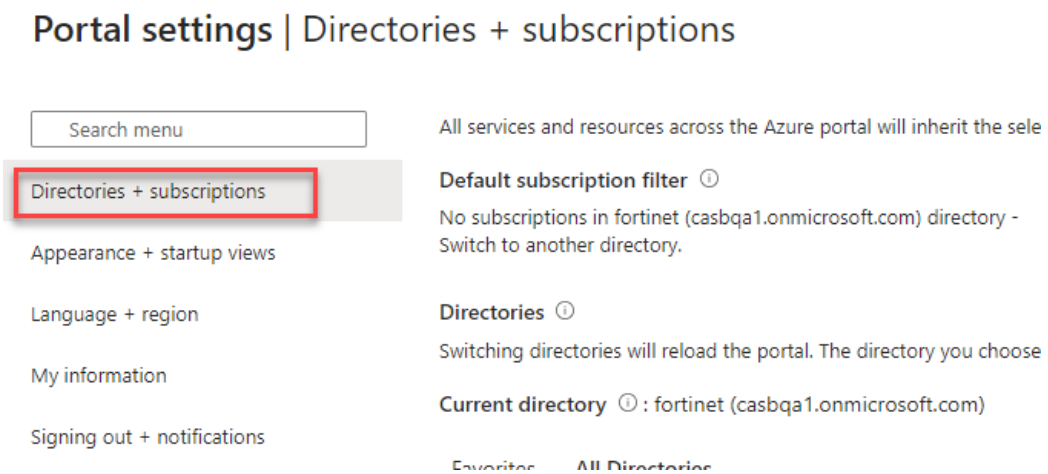
Prerequisite

A Microsoft Entra ID tenant.

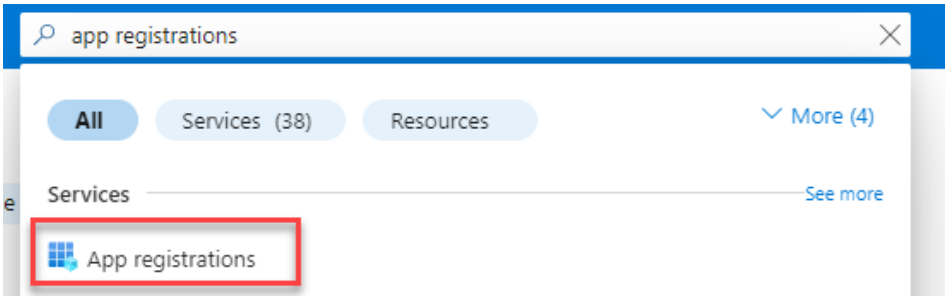
An Office 365 account that has **Global Administrator** role.

FortiCASB Application Registration

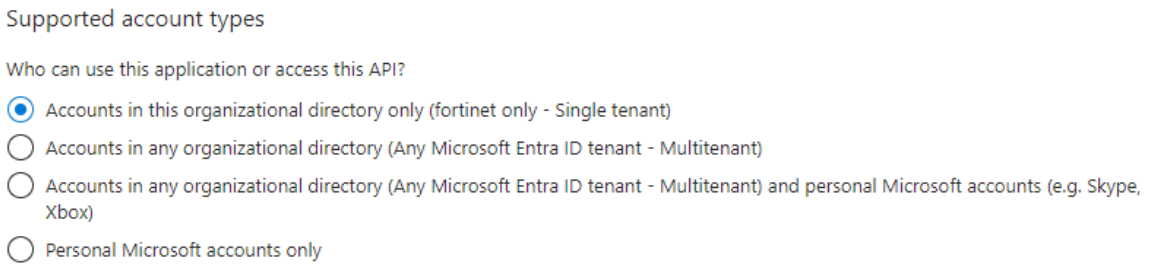
1. Sign in to Microsoft Entra Admin Center with an account that has Global Administrator role.
2. If you have multiple tenants, click on **Settings** icon in the top menu, then go to **Directories + subscriptions** to select the tenant which will register the application with.



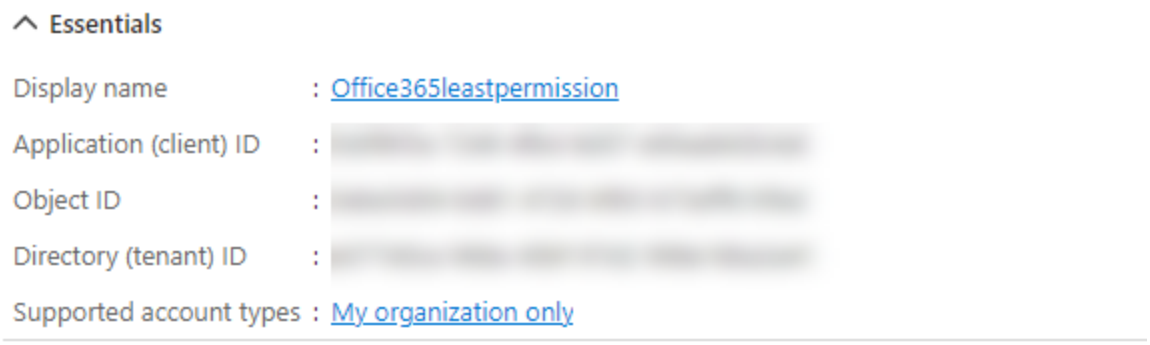
3. In the Azure search field, search and go to **App registrations.**



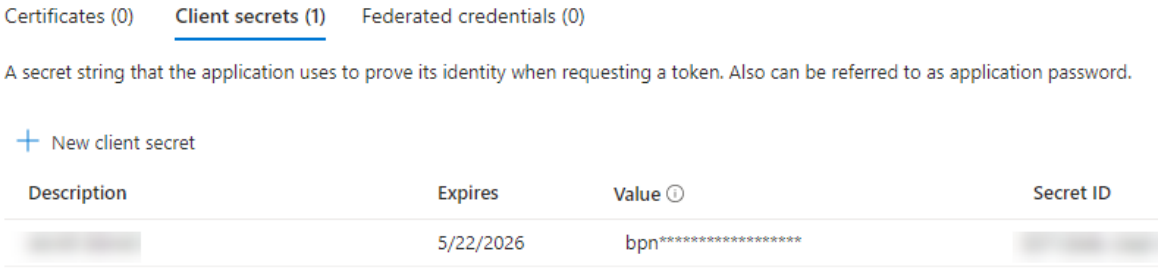
4. Click **New registration** to create a new app registration.
5. Enter a **name** for the application.
6. In **Supported account types**, select "**Accounts in this organizational directory only**" to make the application only available to users under the same tenant.



7. Do not enter anything for **Redirect URI (optional)**.
8. Click **Register** to complete the app registration.
9. After the registration is completed, you will be re-directred to the app registration's **Overview** pane, record down **Application (client) ID** and **Directory (tenant) ID**.



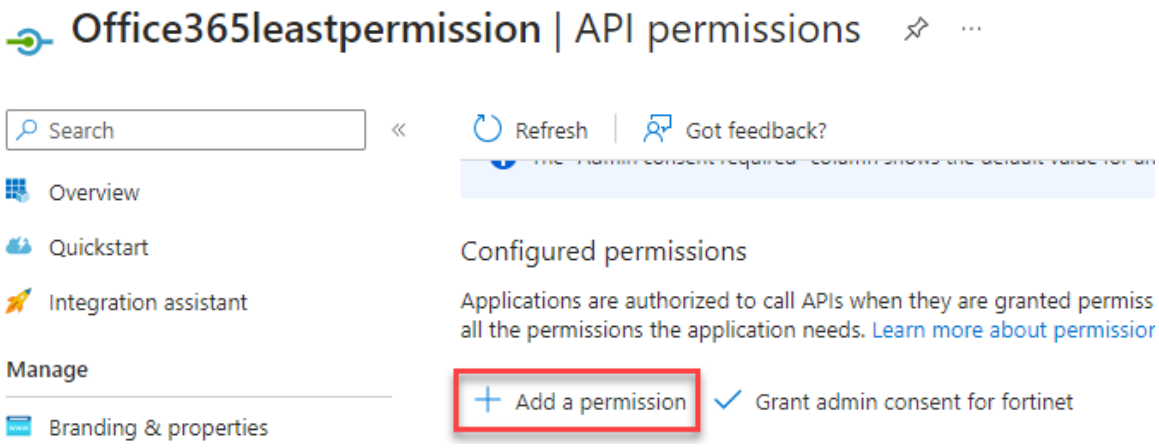
10. From the side panel, click **Certificates & secrets** to see **Client secrets** pane. If you have not setup a client secret yet, create a client secret and record it down.



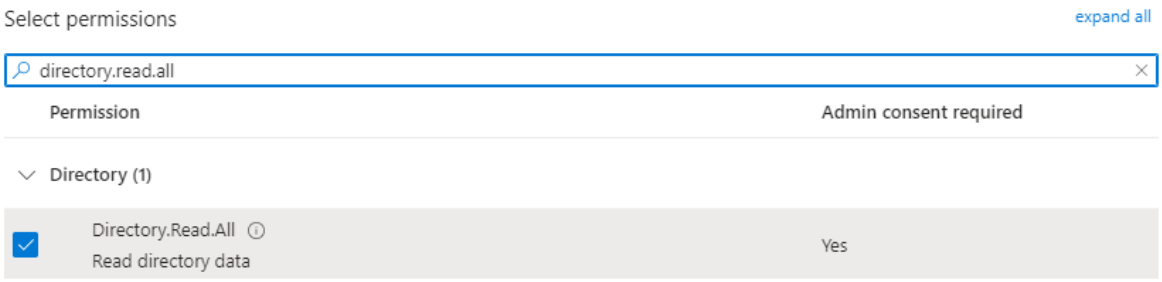
Continue to Add API Permissions on page 200 to finish the rest of the configurations.

Add API Permissions

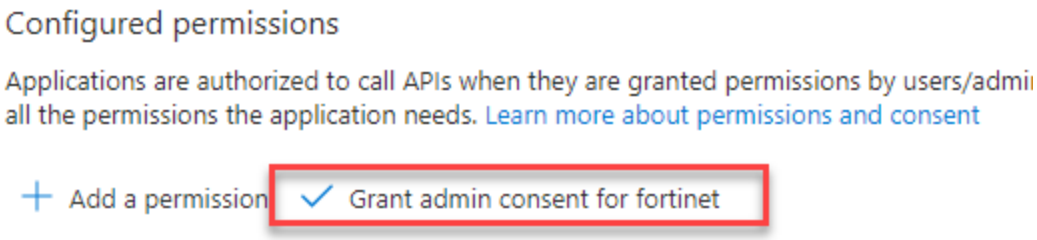
1. Click on **API Permissions** from the side panel to add API permissions.
2. Click **+Add a permission** and select **Microsoft Graph** then select **Application permissions** type.



3. Search for the **Microsoft Graph** permissions from the table below and add them.



4. Click **+Add a permission** again and select **Office 365 Management APIs**, then select **Application permissions** type.
5. Search for the **Office 365 Management APIs** permissions from the table below and add them.
6. Click **Grant admin consent for fortinet** to grant consent for the API permissions for all Office 365 account users under the same tenant.



Microsoft Graph	Office 365 Management APIs
Directory.Read.All	ActivityFeed.Read
Domain.Read.All	ActivityFeed.ReadDlp
Files.ReadWrite.All	ServiceHealth.Read
Group.Read.All	
GroupMember.Read.All	
PrivilegedAccess.Read.AzureAD	
PrivilegedAccess.Read.AzureResources	
Sites.ReadWrite.All	
User.Read	
User.Read.All	

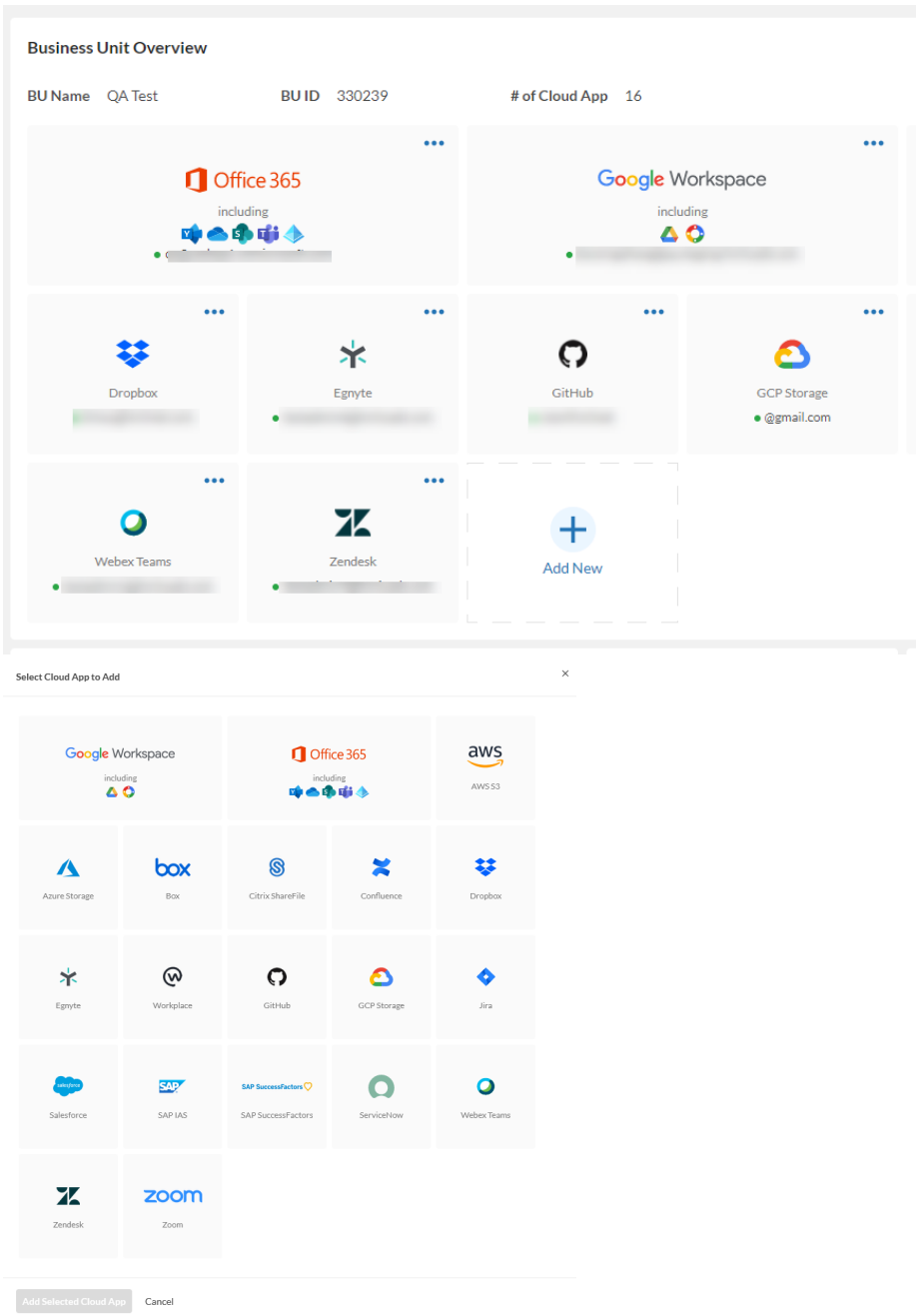
Make sure all the API permissions are in **Granted for fortinet(tenant)** status.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (10)				
Directory.Read.All	Application	Read directory data	Yes	Granted for fortinet
Domain.Read.All	Application	Read domains	Yes	Granted for fortinet
Files.ReadWrite.All	Application	Read and write files in all site collections	Yes	Granted for fortinet
Group.Read.All	Application	Read all groups	Yes	Granted for fortinet
GroupMember.Read.All	Application	Read all group memberships	Yes	Granted for fortinet
PrivilegedAccess.Read.AzureAD	Application	Read privileged access to Azure AD roles	Yes	Granted for fortinet
PrivilegedAccess.Read.AzureRes	Application	Read privileged access to Azure resources	Yes	Granted for fortinet
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	Granted for fortinet
User.Read	Delegated	Sign in and read user profile	No	Granted for fortinet
User.Read.All	Application	Read all users' full profiles	Yes	Granted for fortinet
Office 365 Management APIs (3)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	Granted for fortinet
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes	Granted for fortinet
ServiceHealth.Read	Application	Read service health information for your organization	Yes	Granted for fortinet

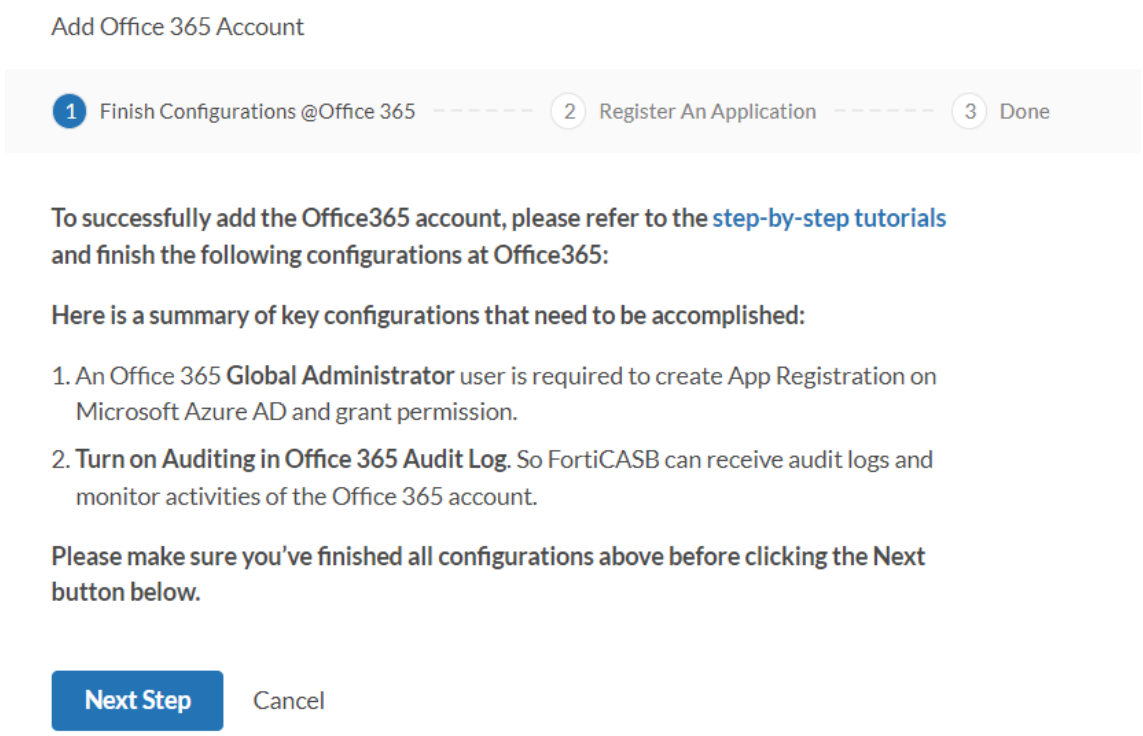
Add Office 365 Account

After all the Office 365 configurations are completed from previous sections, follow these steps to add your Office 365 account on FortiCASB.

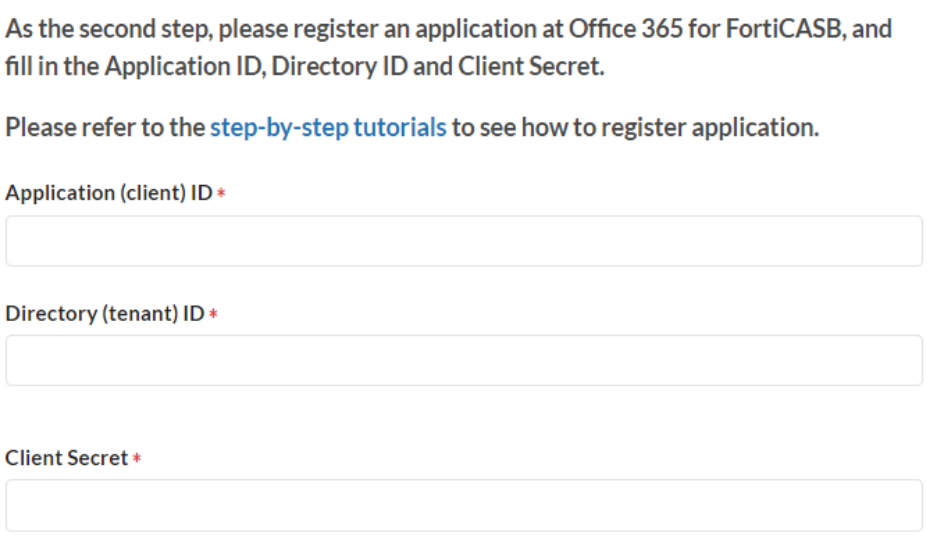
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Office 365**, then click **Add Selected Cloud App**.



3. Click **Next Step** if you have completed the Activate Office 365 Account Audit Log on page 196 and Register FortiCASB with Microsoft Identity Platform on page 198.

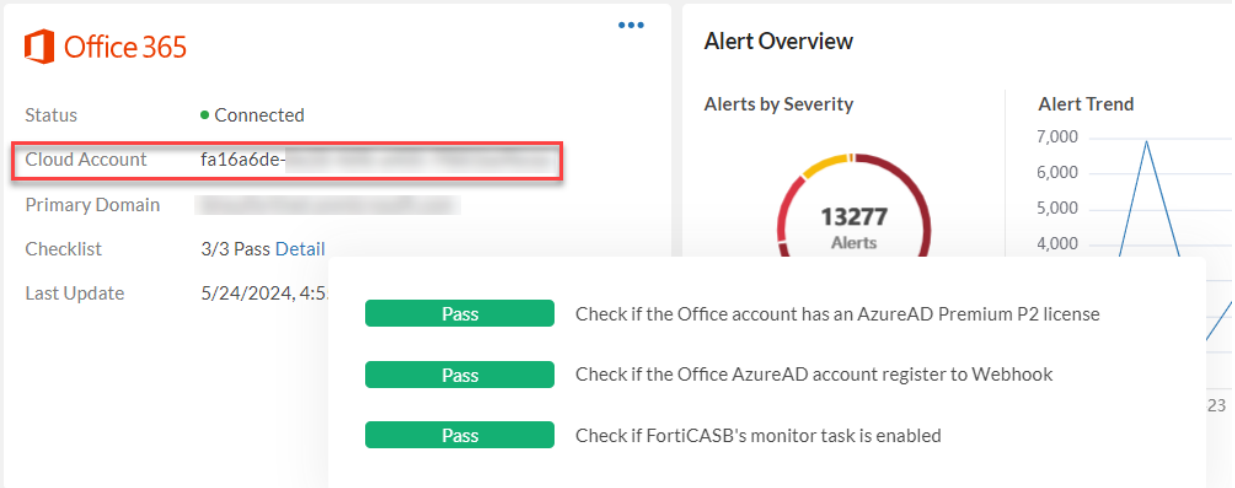


4. Fill in **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** that you have recorded down from App Registration Creation.



5. Click **Grant Access @Microsoft** to complete the add account process.

You will be redirected to Office 365 dashboard with account status. The **Cloud Account** value will be shown as the Office 365 tenant ID. Please allow up to 15 minutes for the account to be fully added.



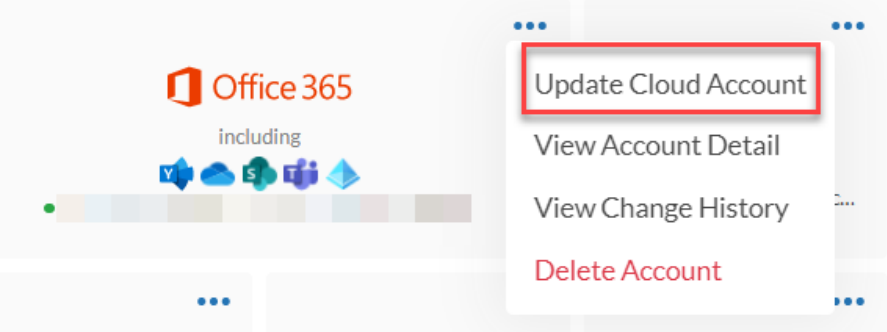
Update Office 365 Account

Before updating the Office 365 account on FortiCASB, complete the same configurations using the same Office 365 account:

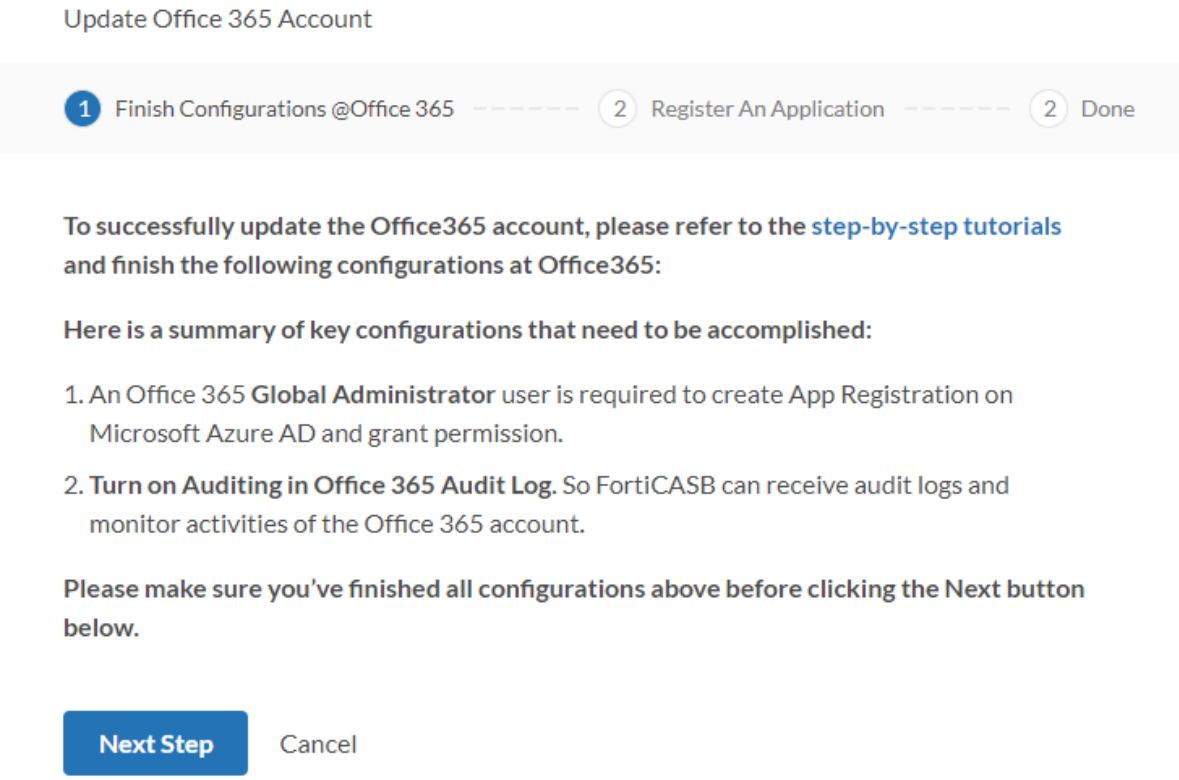
1. **Office 365 Account and License on page 194** - The Office 365 account and license requirements in adding the account in FortiCASB.
2. **Activate Office 365 Account Audit Log on page 196** - Enable Office 365 Audit Log to record user activities of the Office 365 account.
3. **Register FortiCASB with Microsoft Identity Platform on page 198** - Register an application on Microsoft Azure Identity Management platform for Office 365 account onboarding.

After the Office 365 configuration is completed, follow these steps to update your Office 365 account on FortiCASB.

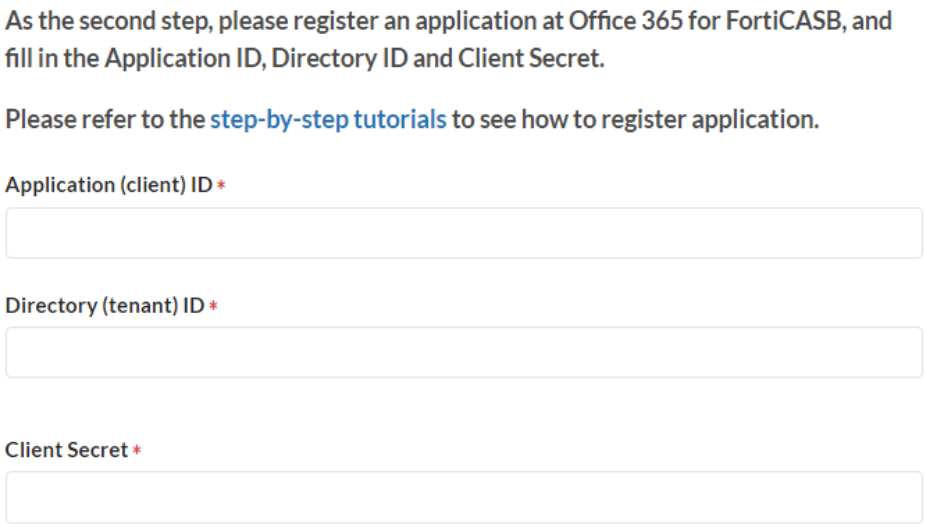
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the Office 365 Account menu and select **Update Cloud Account.**



4. Make sure you have completed all Office 365 configurations, and click **Next Step**.



5. Fill in **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** that you have recorded down from App Registration Creation.



6. Click **Grant Access @Microsoft** to complete the add account process.

You can see the installation checklist and status in the Office 365 dashboard. Please allow up to 15 minutes for the account to be fully updated.

Salesforce

FortiCASB offers an API-based approach, pulling data directly from Salesforce via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Salesforce user activities, provides DLP Data Analysis for files stored on Salesforce.

Prerequisites

FortiCASB supports Salesforce **Small Business Essentials edition** (the API is enabled by default), other editions are not supported.

The user account added on FortiCASB must have the following permissions:

- **View All Data**
- **View All Users**

- **API Enabled**

You may either use an existing account or create a new account. If you create a new account, wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

The following features require "Manage Users" permission as well:

- User login tracking
- User IP address tracking
- Geographical location tracking
- User password change tracking

Without "Manage Users" permissions, FortiCASB cannot obtain user login IPs. Therefore, any user activity will not appear on the Activity map.

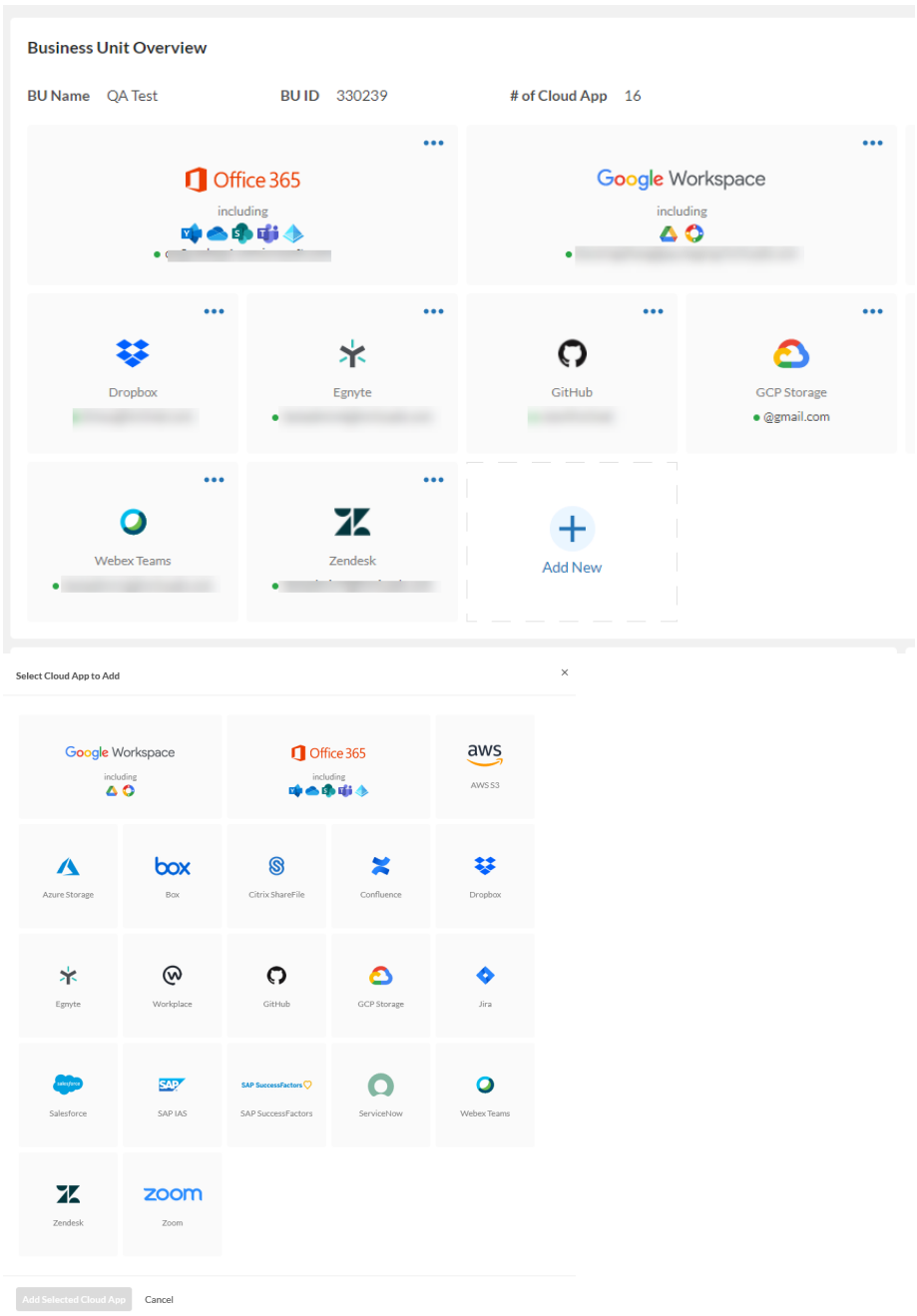
After you have verified the account prerequisite, follow the guides below to **Add** or **Update** the account on FortiCASB:

Add Salesforce Account on page 208

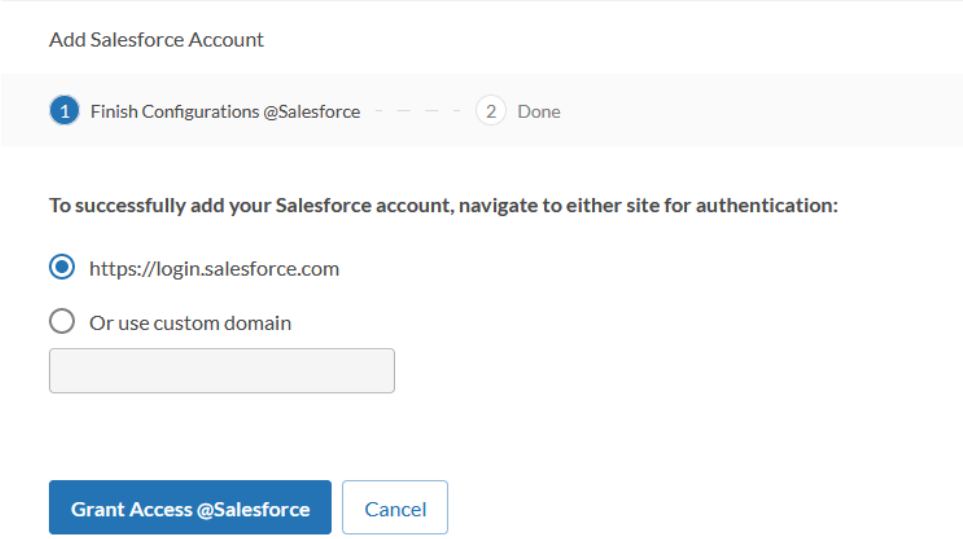
Update Salesforce Account on page 211

Add Salesforce Account

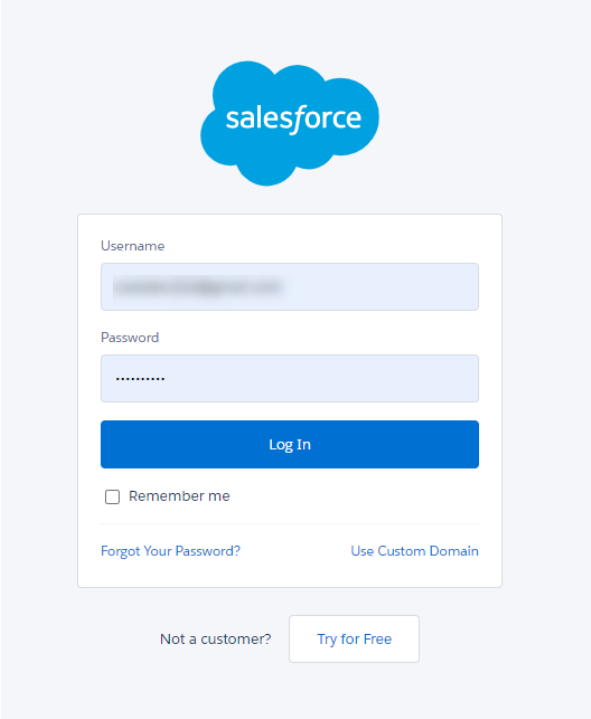
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Salesforce**, then click **Add Selected Cloud App**.



3. Click **Grant Access @Salesforce** to be re-directed to Salesforce for authentication.



4. Log in to authenticate. If you have a custom Salesforce domain, enter it here.



Salesforce will prompt you to **allow** or **deny** access.

5. Click **Allow** to grant FortiCASB permissions to monitor your Salesforce application.

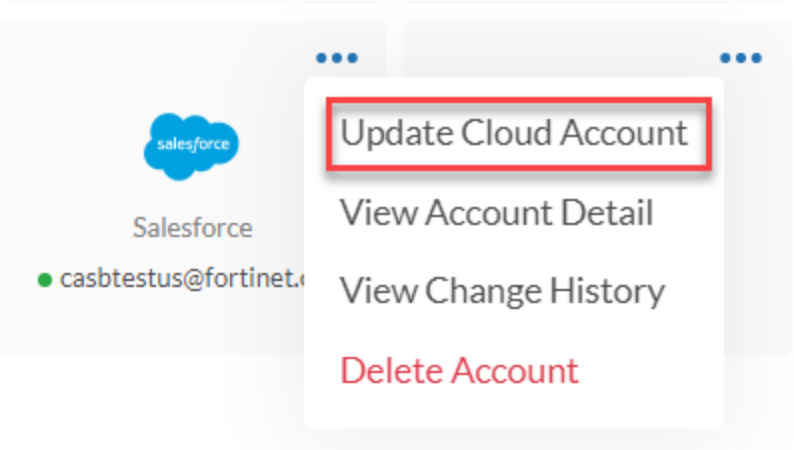
After you click **Allow**, you will be redirected back to the FortiCASB dashboard.

You can check the installation result and SaaS platform monitoring status in the Salesforce dashboard.

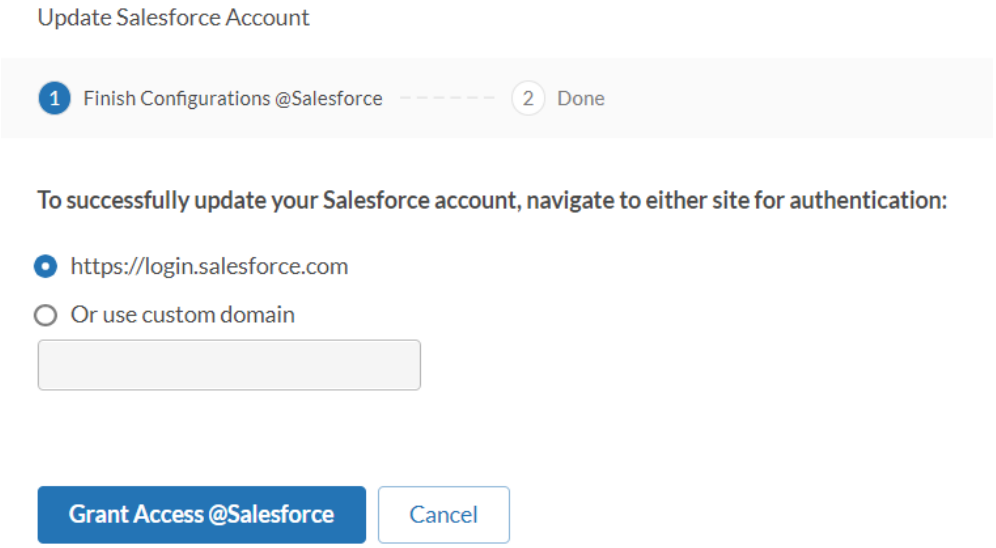
For more information on common installation issues, see "Troubleshooting on page 515".

Update Salesforce Account

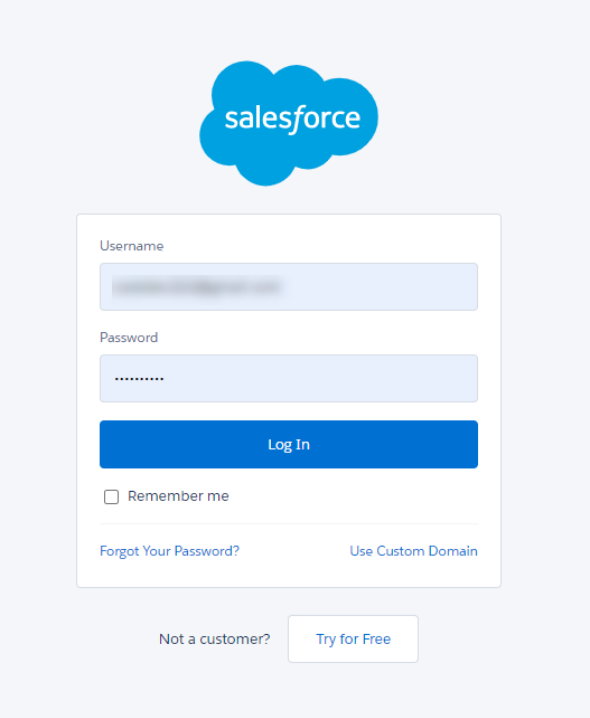
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**
3. Click on the Salesforce account menu, and select **Update Cloud Account**.



4. Click **Grant Access @Salesforce** to be re-directed to Salesforce for authentication.



5. Log in to authenticate. If you have a custom Salesforce domain, enter it here.



Salesforce will prompt you to **allow** or **deny** access.

6. Click **Allow** to grant FortiCASB permissions to monitor your Salesforce application.

   After you click **Allow**, you will be redirected back to the FortiCASB dashboard.

   You can check the installation checklist and platform monitoring status in the Salesforce Dashboard.

For more information on common installation issues, see "Troubleshooting on page 515".

SAP IAS

FortiCASB offers an API-based approach, pulling data directly from SAP IAS via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track SAP IAS user activities such as logins, user assignments, updates and etc.

Prerequisite

The SAP IAS application needs to be hosted in the SAP infrastructure to add the SAP IAS account to FortiCASB. A **System Administrator** needs to be created under the SAP IAS account to provide FortiCASB with access to the account.

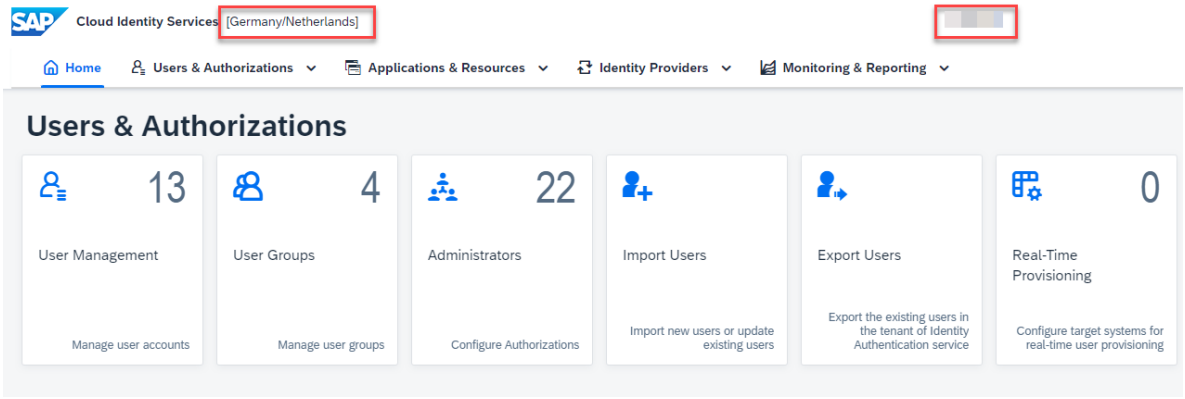
After you have verified the account prerequisite, follow the guides below to **Add** or **Update** the account on FortiCASB:

Add SAP IAS Account on page 213

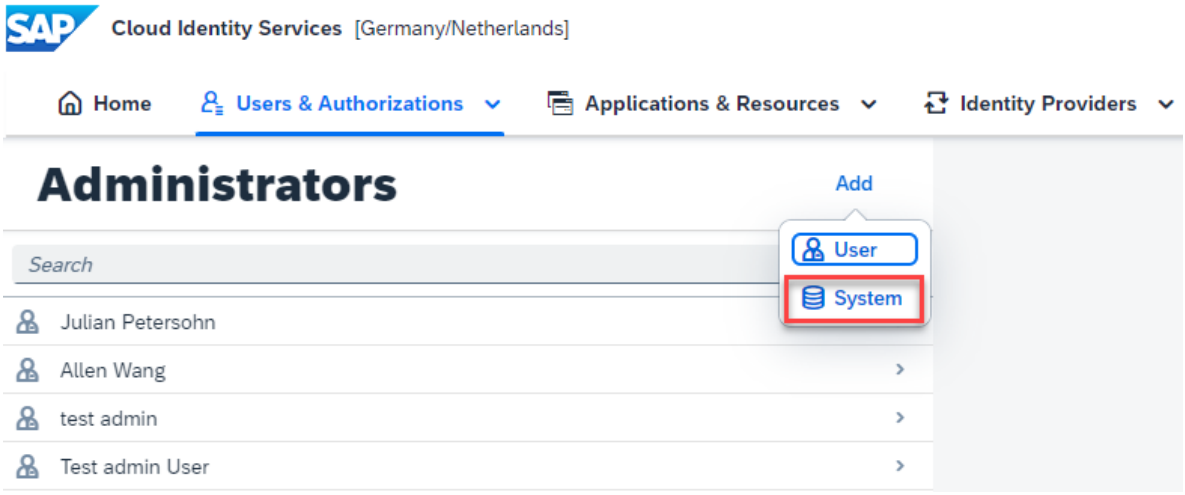
Update SAP IAS Account on page 218

Add SAP IAS Account

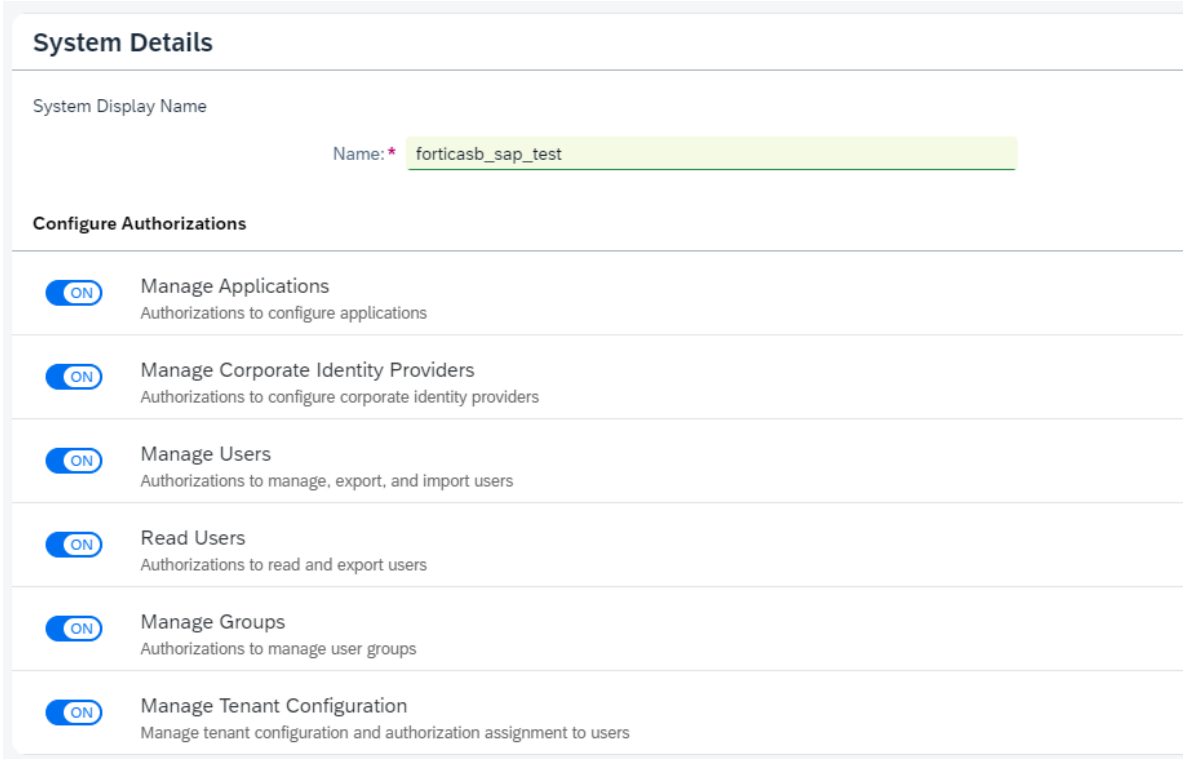
1. Log into SAP IAS Administration Console, keep a record of the **Tenant ID** and the IAS **Region**.



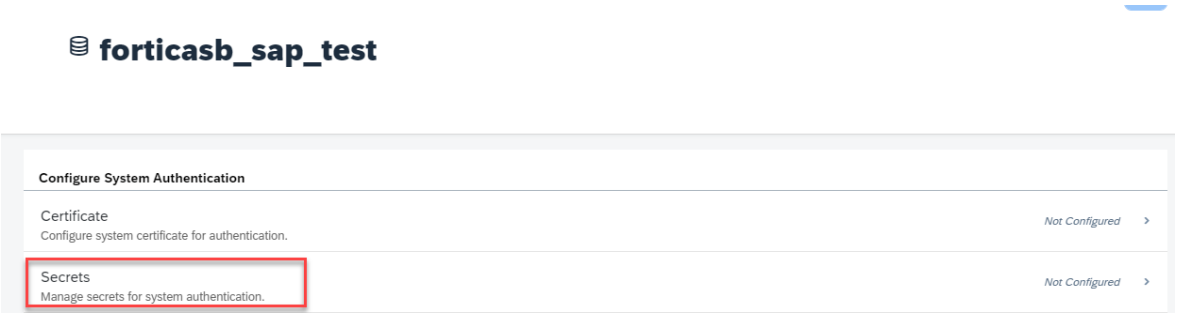
2. In the top menu, go to **Users & Authorization > Administrators**. Click **Add** in the top Administrators section, and select **Systems**.



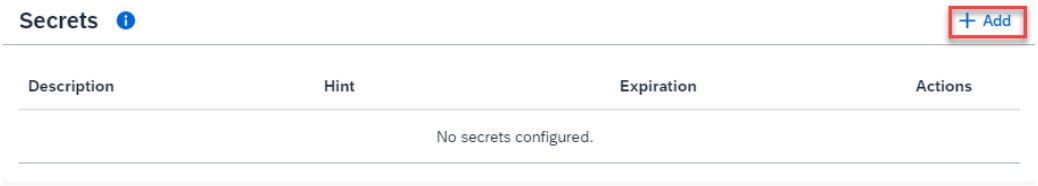
3. In **Add Administrator > System Details**, Give it a System Display name, turn all **Configure Authorizations** to **ON**, and click **Save**.



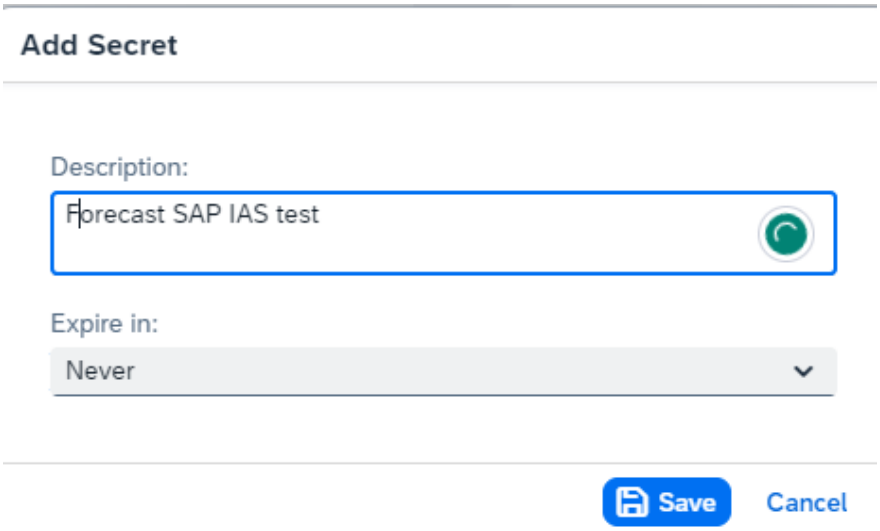
4. Now in **Configure System Authentication**, click **Secrets** to configure new secret for the system authentication.



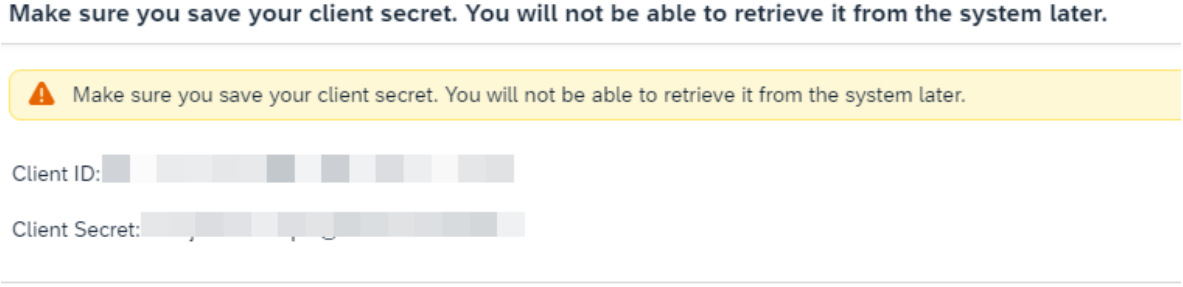
5. Click **+Add** to add a new secret.



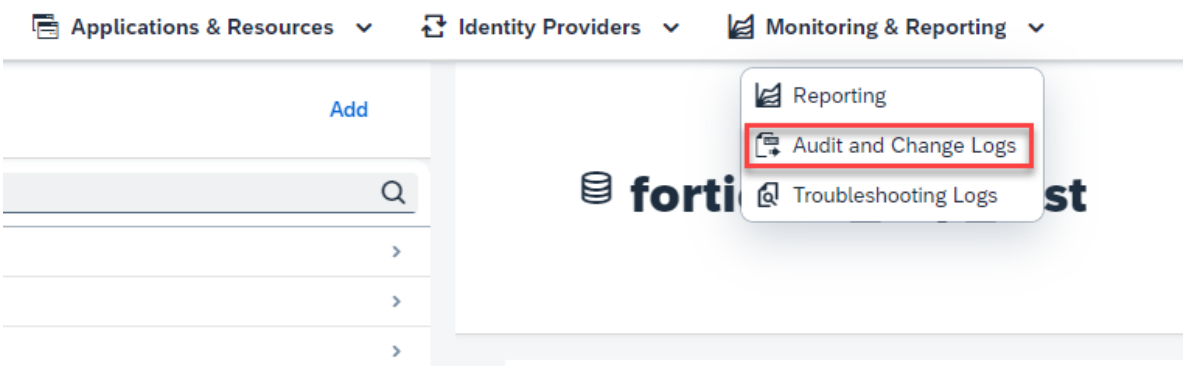
6. In **Add Secret** pop up screen, enter a description and select an expiration duration, and click **Save**.



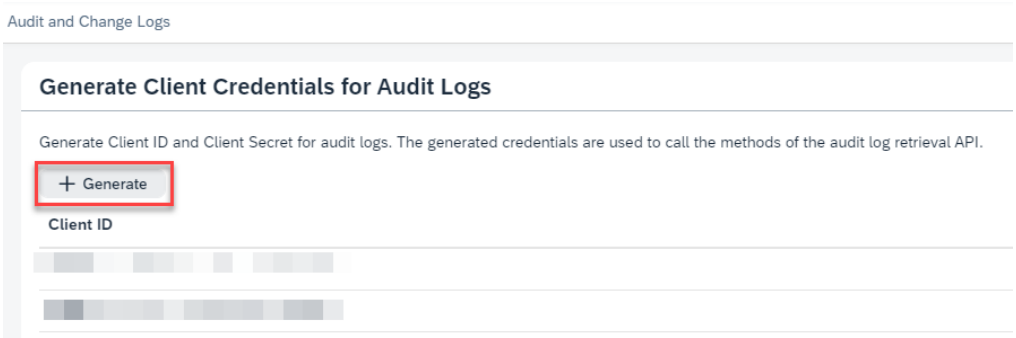
7. The new **Client ID** and **Secret** will be generated. Keep a record of them later for as you will not be able to see them again. They will be used as **System Client ID** and **System Client Secret**.



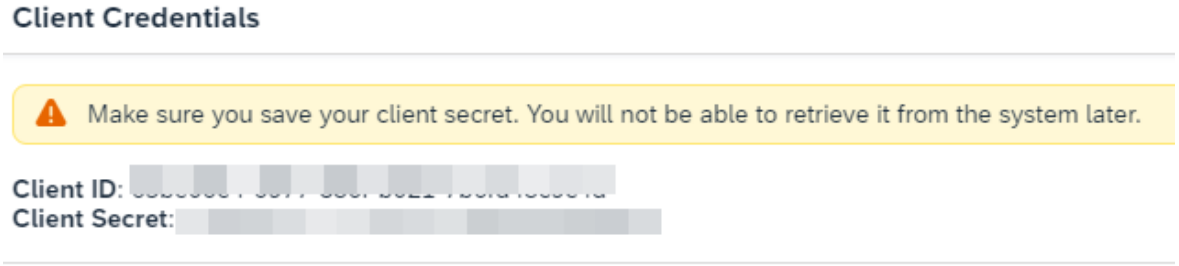
8. Now in the top navigation menu, go to **Monitoring & Reporting > Audit and Change Logs**



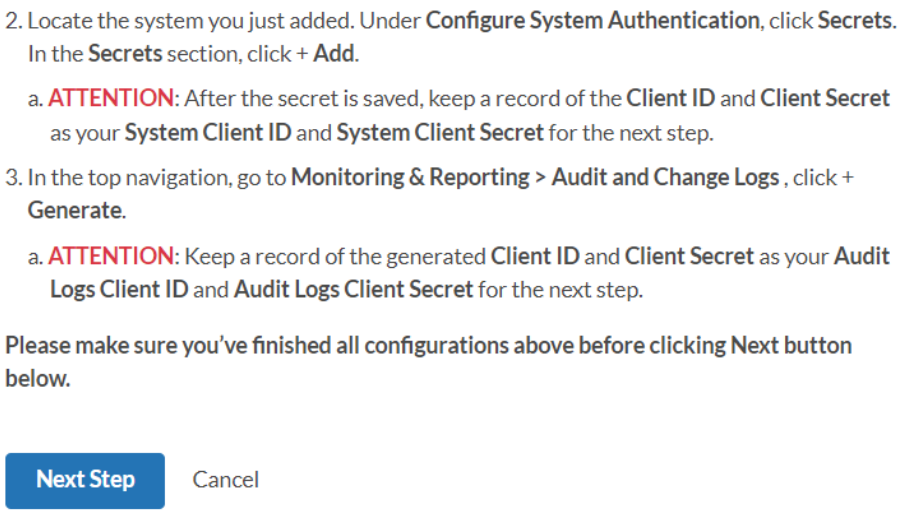
9. Click **+Generate** to generate client credentials for audit logs.



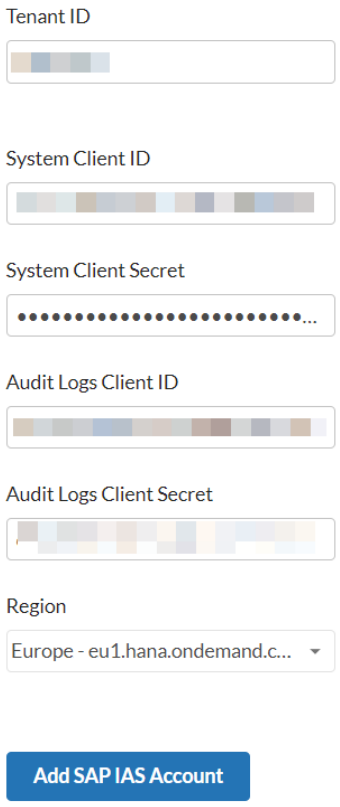
10. The new audit log **Client ID** and **Secret** will be generated. Keep a record of them as you will not be able to see them again. They will be used as **Audit Logs Client ID** and **Audit Logs Client Secret** later to add the account in FortiCABS.



11. Now go back to FortiCASB **Add SAP IAS Account** page.
12. Click **Next Step** on Add SAP IAS Account Page.



13. Enter **System Client ID, System Client Secret, Audit Logs Client ID, Audit Logs Client Secret**, and select the **Region** saved from earlier steps.

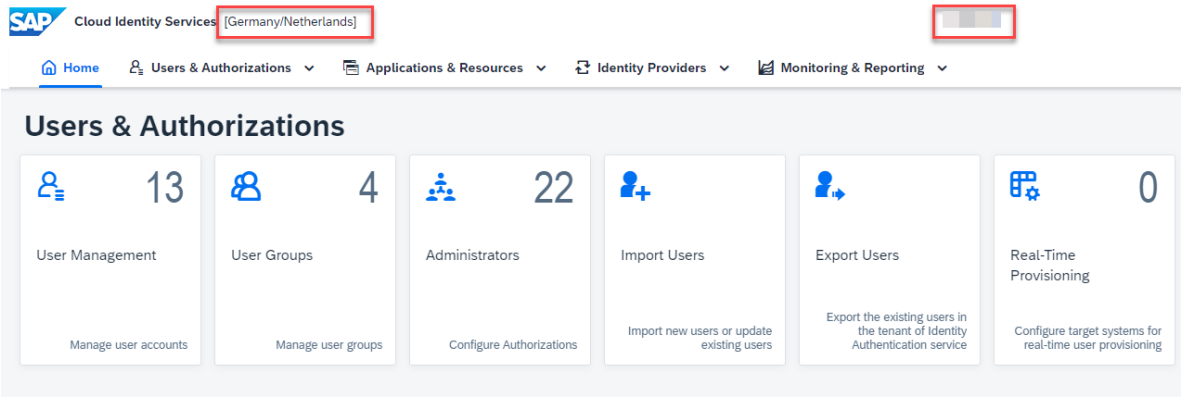


14. Click **Add SAP IAS Account** to finish.

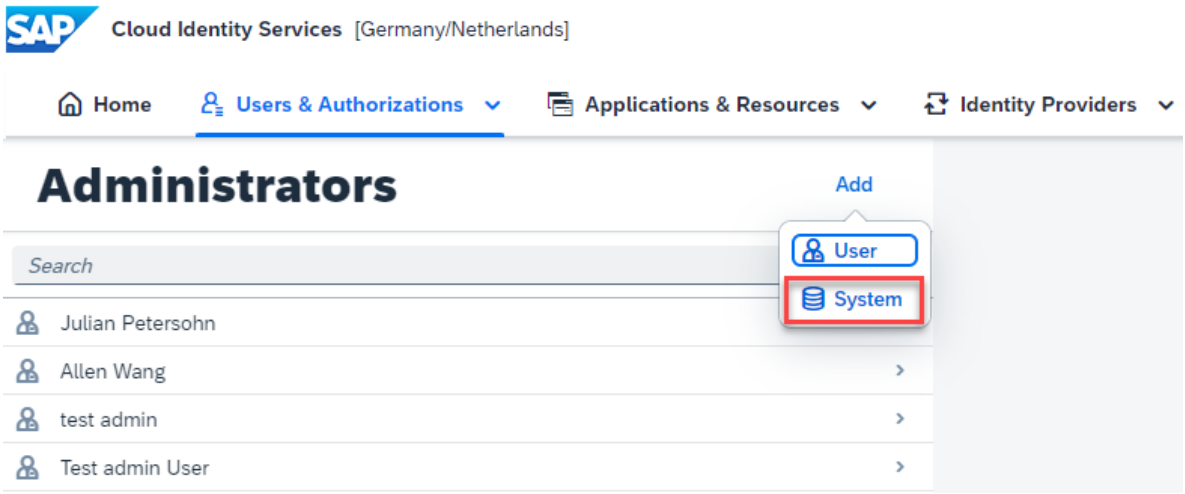
You can check the installation checklist and platform monitoring status in the SAP IAS Dashboard.

Update SAP IAS Account

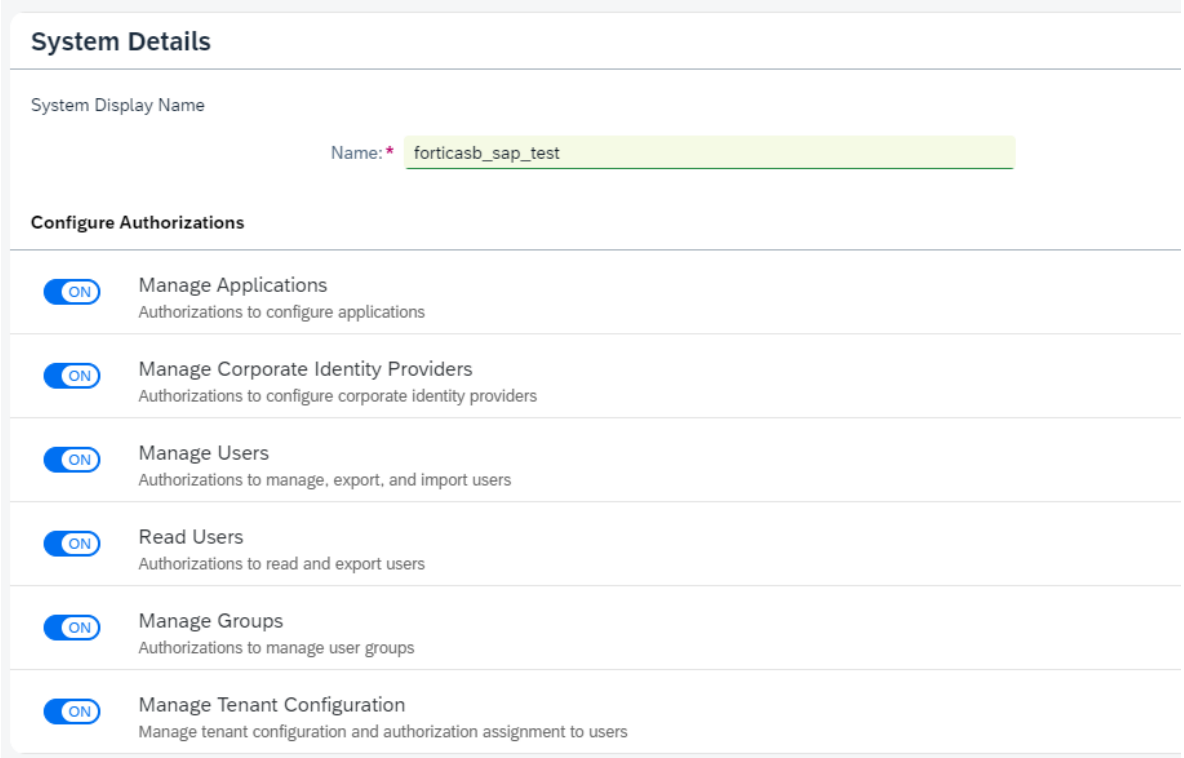
1. Log into SAP IAS Administration Console, keep a record of the **Tenant ID** and the IAS **Region**.



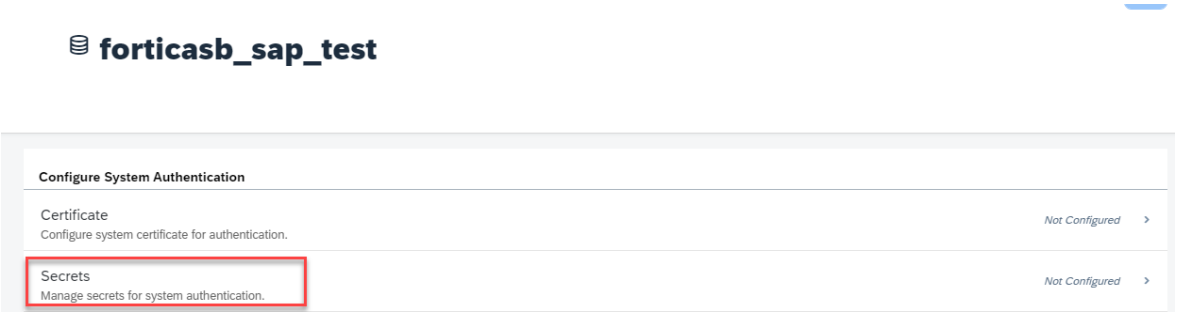
2. In the top menu, go to **Users & Authorization > Administrators**. Click **Add** in the top Administrators section, and select **Systems**.



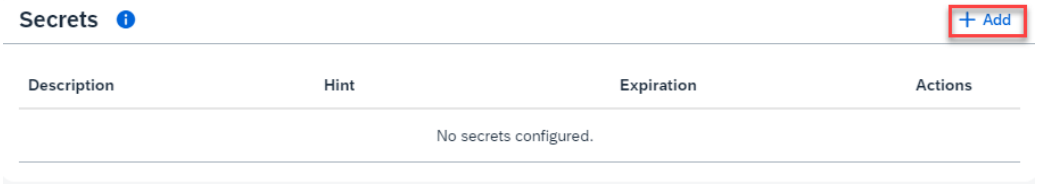
3. In **Add Administrator > System Details**, Give it a System Display name, turn all **Configure Authorizations** to **ON**, and click **Save**.



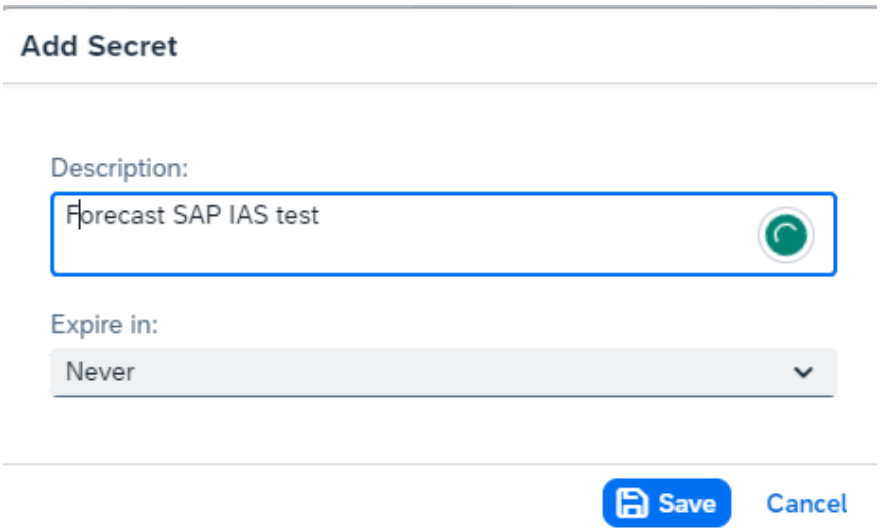
4. Now in **Configure System Authentication**, click **Secrets** to configure new secret for the system authentication.



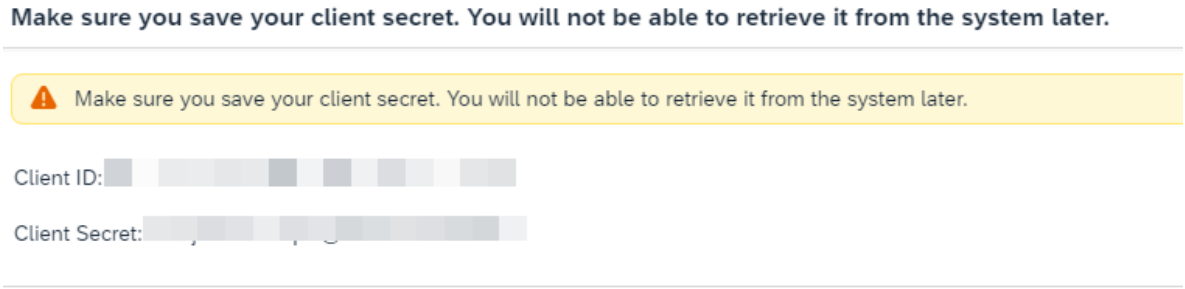
5. Click **+Add** to add a new secret.



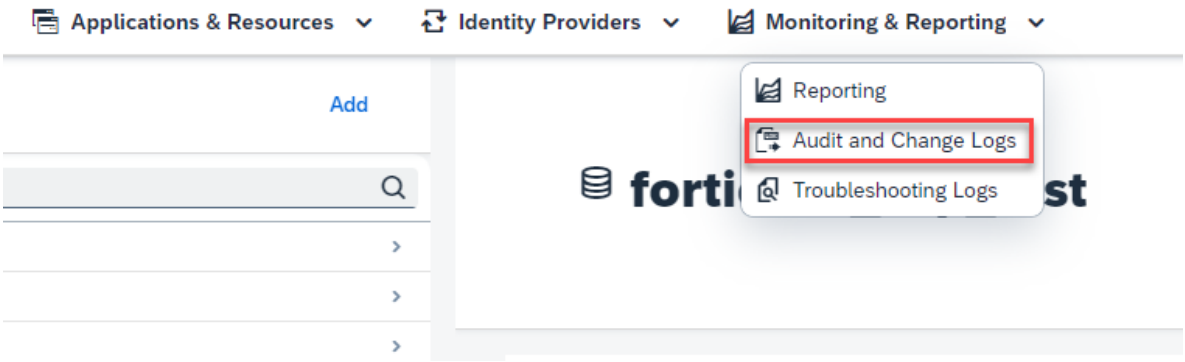
6. In **Add Secret** pop up screen, enter a description and select an expiration duration, and click **Save**.



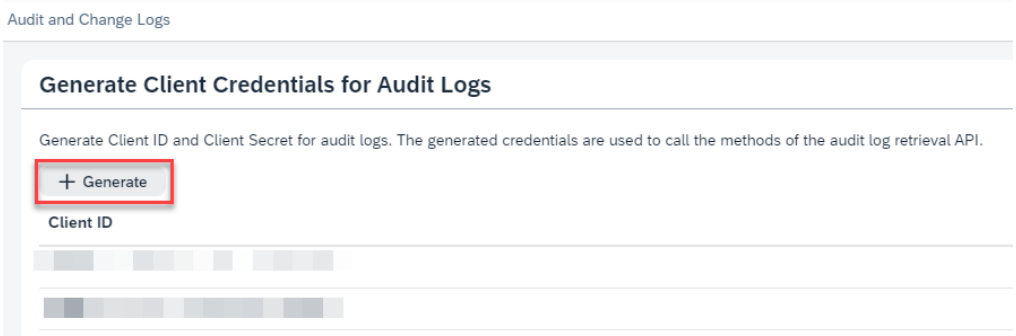
7. The new **Client ID** and **Secret** will be generated. Keep a record of them later for as you will not be able to see them again. They will be used as **System Client ID** and **System Client Secret**.



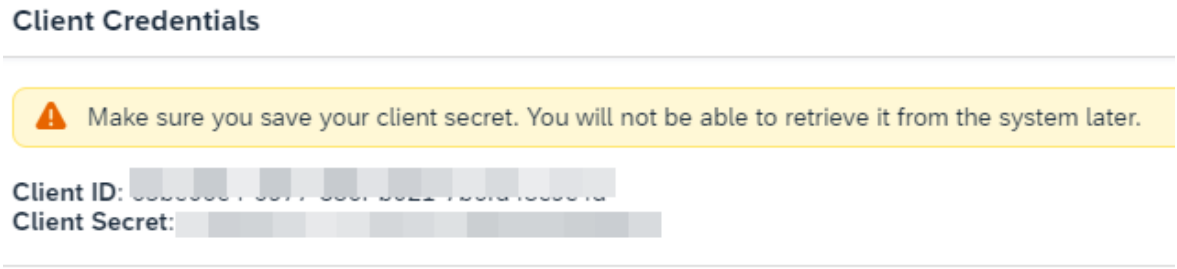
8. Now in the top navigation menu, go to **Monitoring & Reporting > Audit and Change Logs**



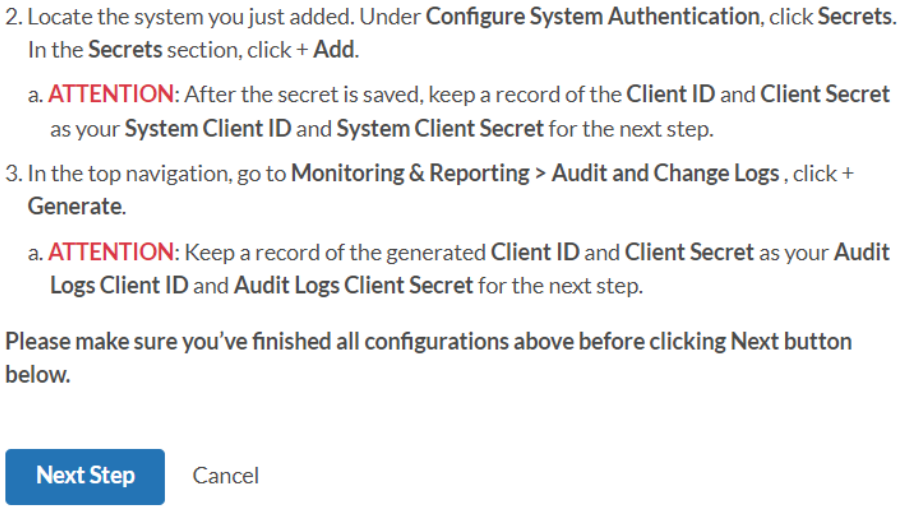
9. Click **+Generate** to generate client credentials for audit logs.



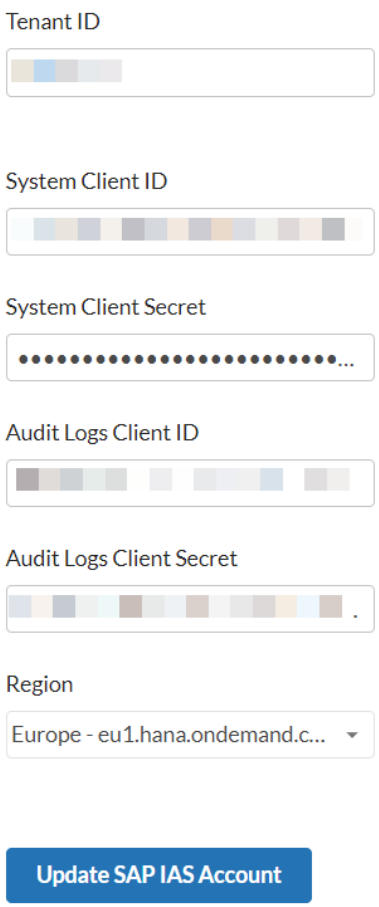
10. The new audit log **Client ID** and **Secret** will be generated. Keep a record of them as you will not be able to see them again. They will be used as **Audit Logs Client ID** and **Audit Logs Client Secret** later to update the account in FortiCABS.



11. Now go back to FortiCASB **Update SAP IAS Account** page.
12. Click **Next Step** on Update SAP IAS Account Page.



13. Enter **System Client ID, System Client Secret, Audit Logs Client ID, Audit Logs Client Secret**, and select the **Region** saved from earlier steps.



14. Click **Update SAP IAS Account** to finish.

You can check the installation checklist and platform monitoring status in the SAP IAS Dashboard.

SAP Success Factors

FortiCASB offers an API-based approach in integrating with SAP Success Factors, pulling data directly from SAP Success Factors via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access

token for API queries. FortiCASB monitors and tracks SAP Success Factors user activities, provides DLP Data Analysis for files shared on the platform.

Follow one of the following guide to **Add** or **Update** the SAP Success Factors Account

Add SAP Success Factors Account on page 223

Update SAP Success Factors Account on page 230

Add SAP Success Factors Account

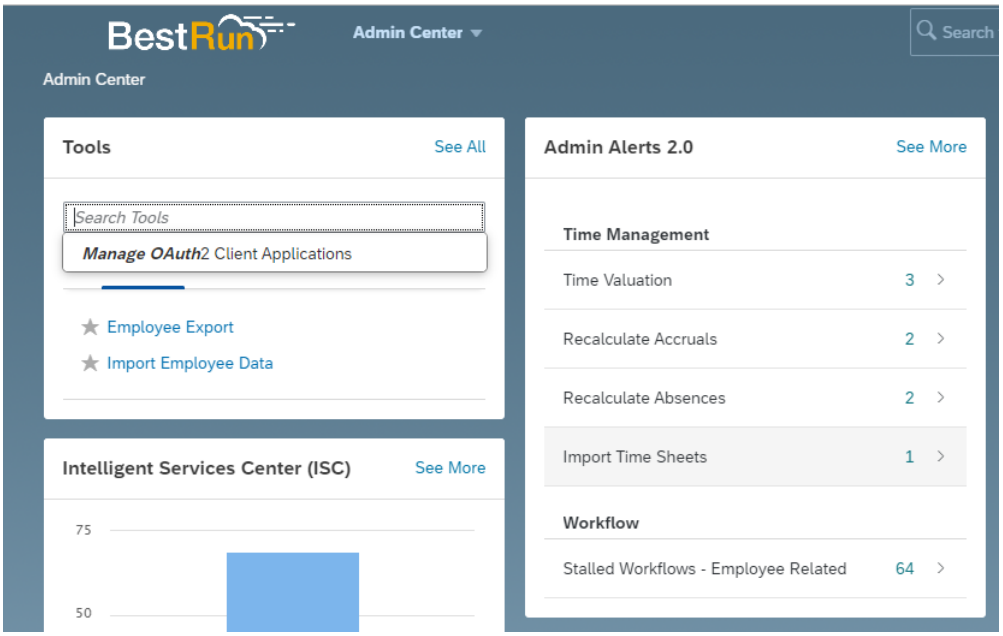
Step 1. Register OAuth Client Applicaiton on page 223

Step 2. Set Permission Scope on page 225

Step 3. Add SAP Success Factors Account on FortiCASB on page 227

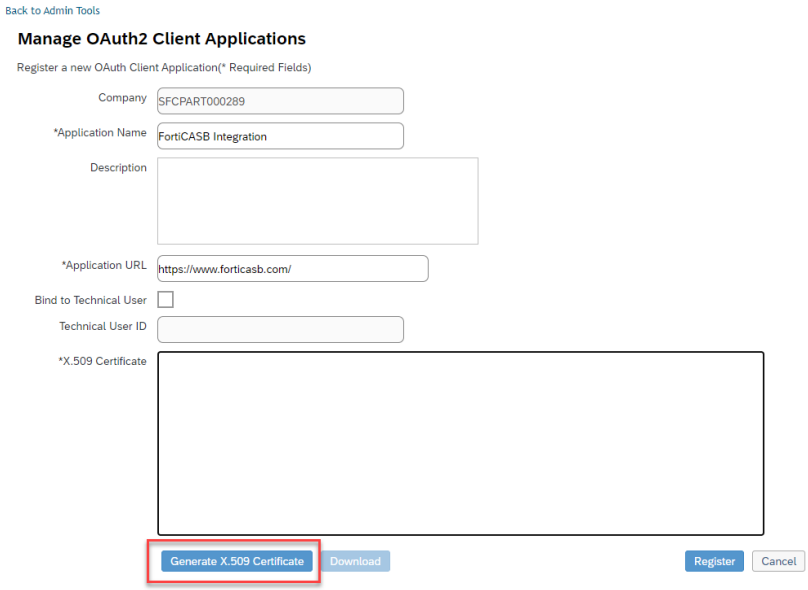
Step 1. Register OAuth Client Applicaiton

1. Log into SAP Success Factors and go to **Admin Center**. In the **Tools** box, search and go to **Manage OAuth2 Client Applications**.

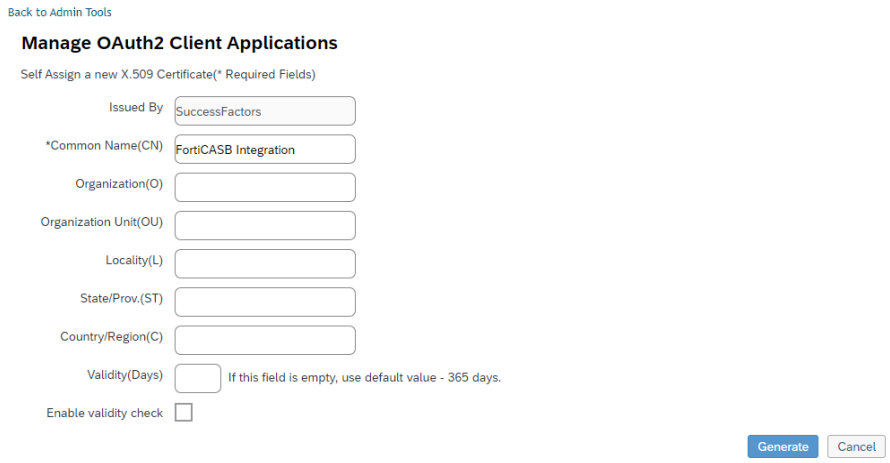


2. In **Manage OAuth2 Client Applications**, click **Register Client Application** to register a new OAuth2 Client Application.
3. Fill in an application name, e.g. FortiCASB Integration, then in **Application URL**, enter a url, e.g. https://www.forticasb.com/.

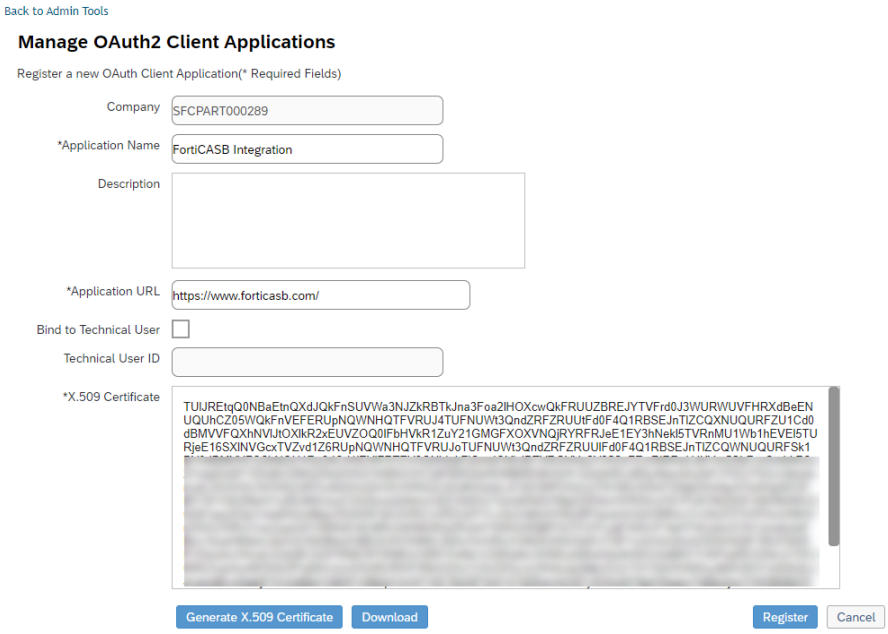
At the bottom of the page, click **Generate X.509 Certificate** to register a certificate.



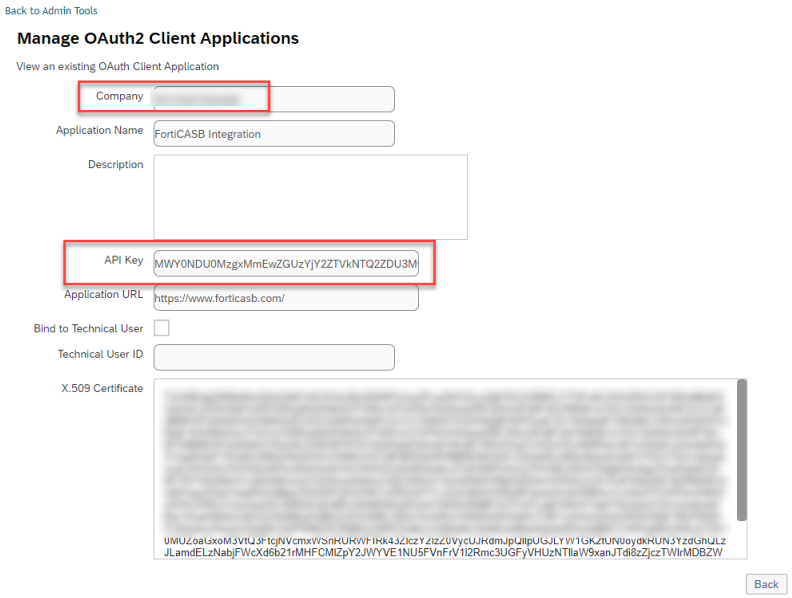
4. In "Self Assign a new X.509 Certificate" page, enter a **Common Name** for the certificate, and click **Generate**.



5. You will be re-directed back to the previous page, and the certificate values will be filled.
Click **Download** to download the certificate pem file as the private key for use later. Then click **Register** to register the client application.

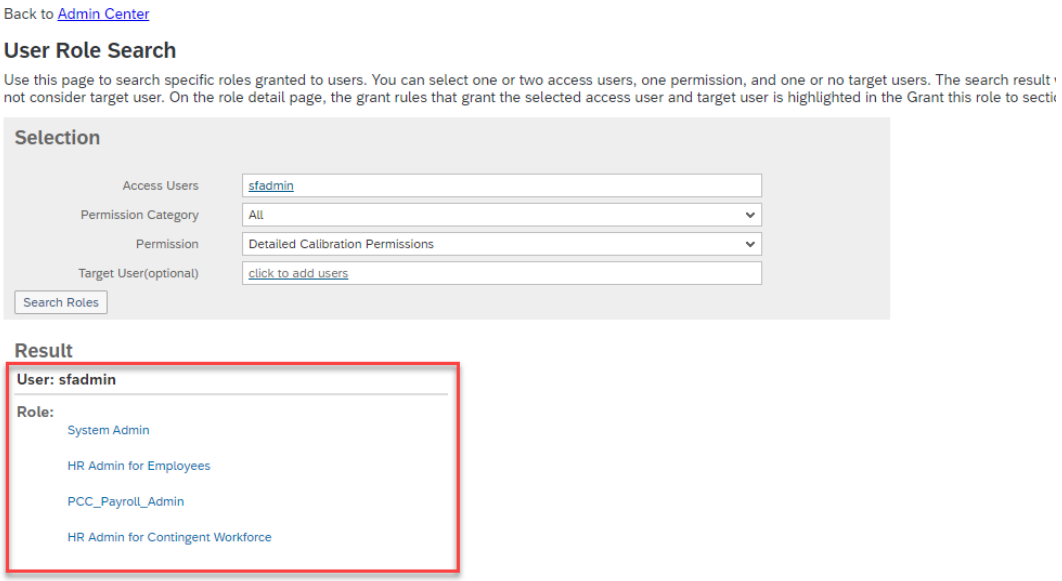


6. Click on the OAuth2 Application that you just created, the **API Key** should be generated automatically, make a record of the **API key** and **Company ID**.

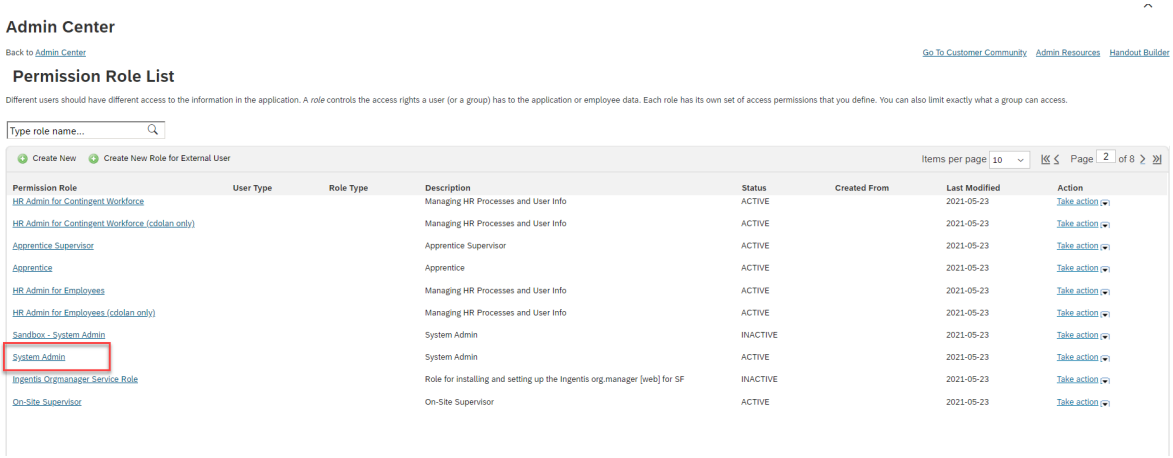


Step 2. Set Permission Scope

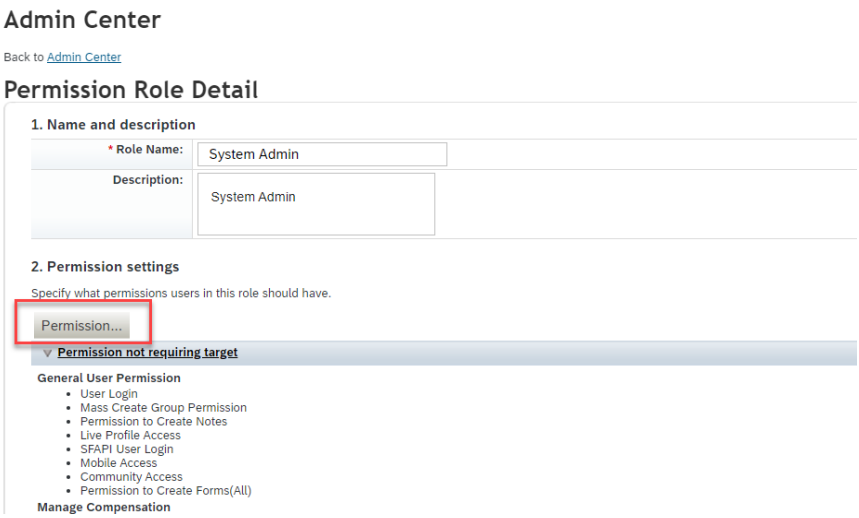
1. In **SAP Success Factors** > **Admin Center**, search and go to **User Role Search**.
2. Look up the User ID to be added on FortiCASB for the Roles under the user.



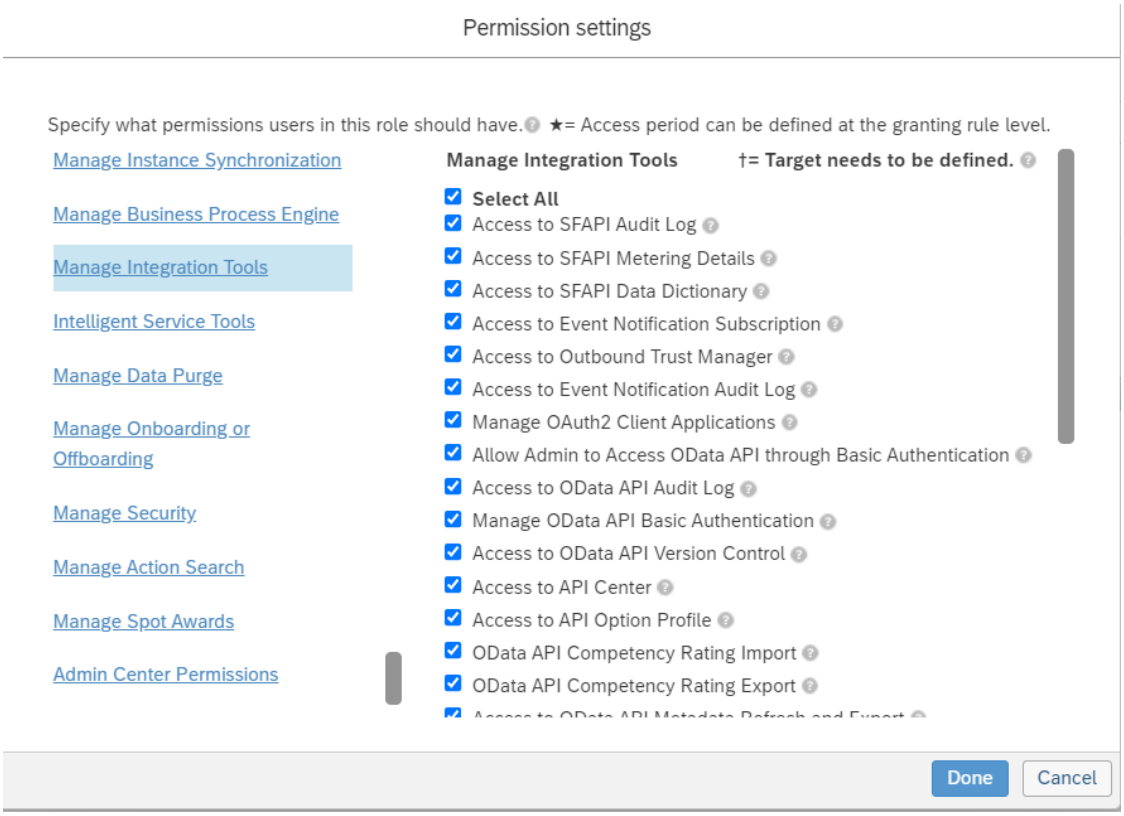
3. Go back to the **Admin Center** again, search and go to **Manage Permission Role**.
4. Look up one of the role that is under the user, e.g. System Admin, and click on it.



5. In **Permission Role Detail**, click on **Permission** button to configure the permission settings.



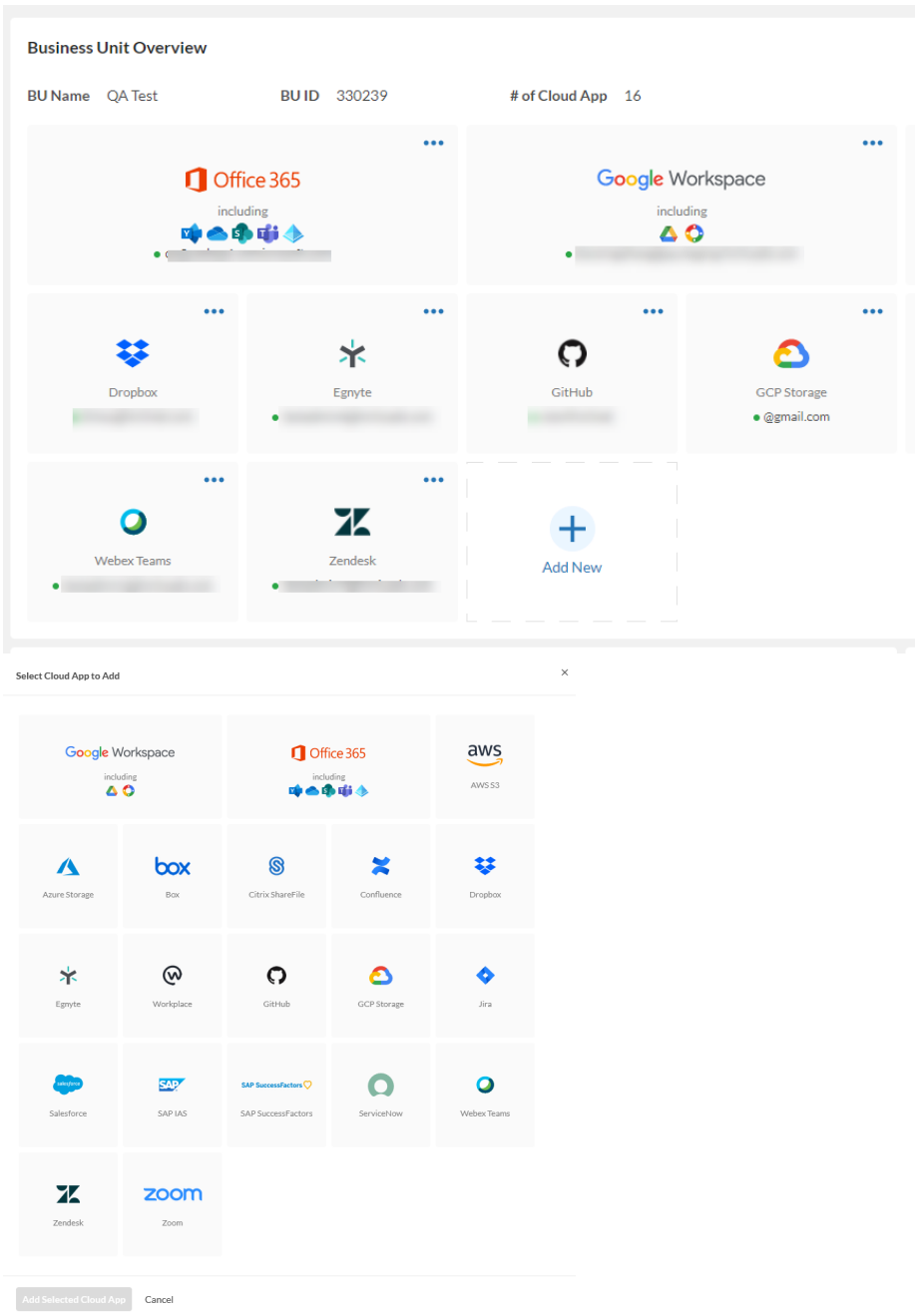
6. Scroll down and select **Manage Integration Tools**, click **Select All** to add all integration permissions, and click **Done**.



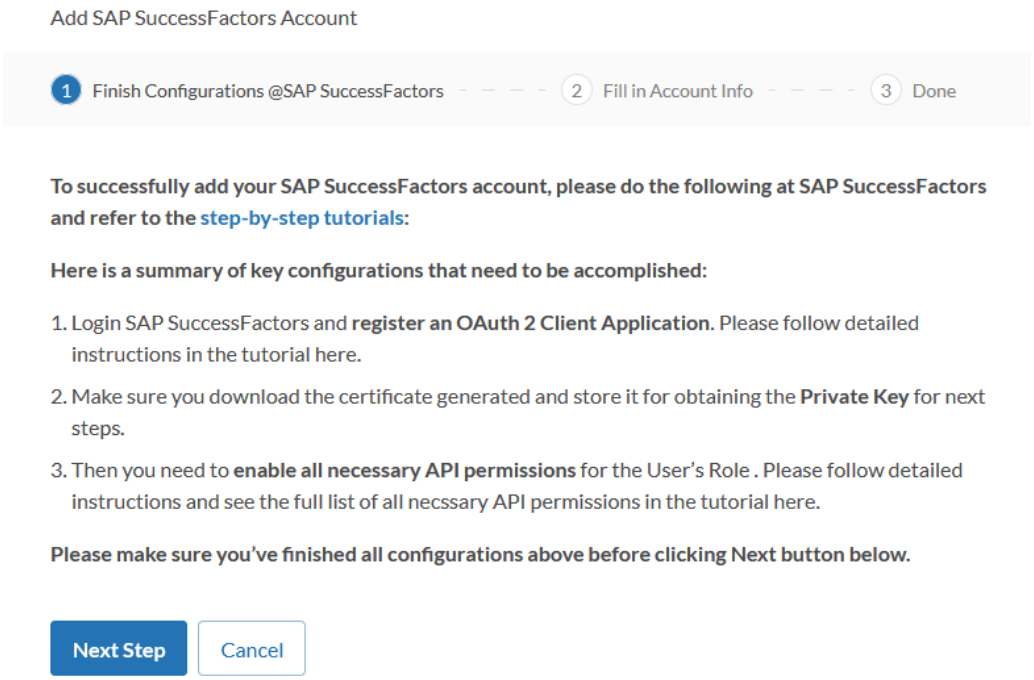
Now go back to FortiCASB to add the SAP Success Factors account.

Step 3. Add SAP Success Factors Account on FortiCASB

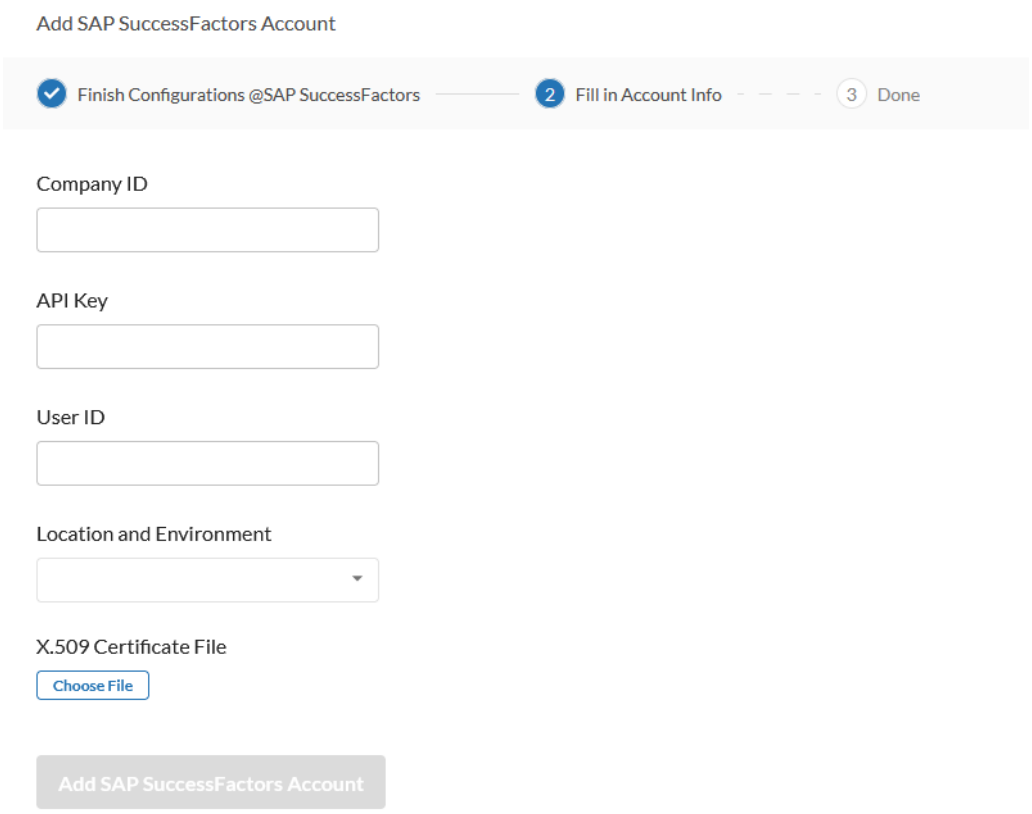
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **SAP SuccessFactors**, then click **Add Selected Cloud App**.



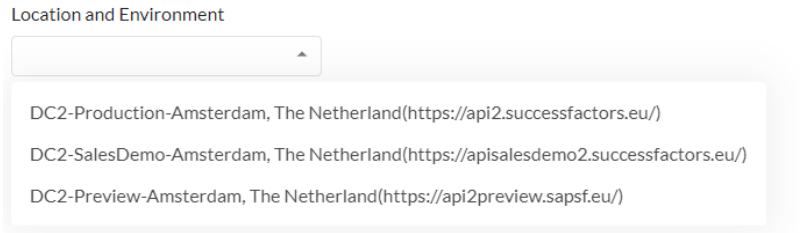
3. Review the configuration list and make sure they are completed, and click **Next Step**.



4. Enter the SAP Success Factors **Company ID**, **API Key** saved earlier, then enter the SAP Success Factors **User ID**.



5. Click **Location and Environment** drop down menu and select one of the **location and environment:**



6. Upload the X.509 Certificate pem file saved from earlier and click **Add SAP Success Factors Account.**
7. Wait for 15 minutes for the account to be fully added to FortiCASB.

Update SAP Success Factors Account

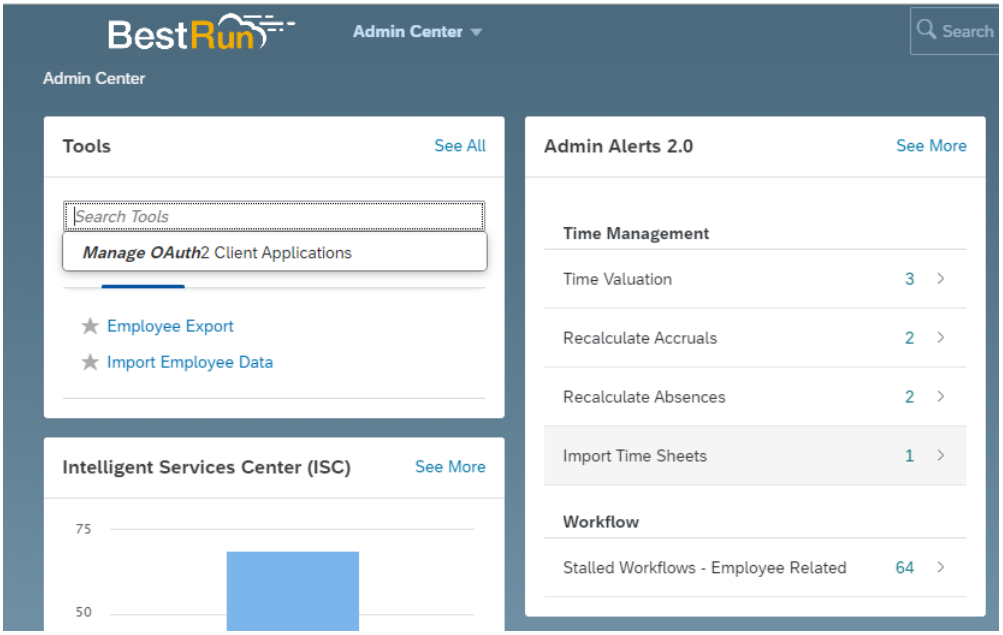
Step 1. Register OAuth Client Applicaiton on page 231

Step 2. Set Permission Scope on page 233

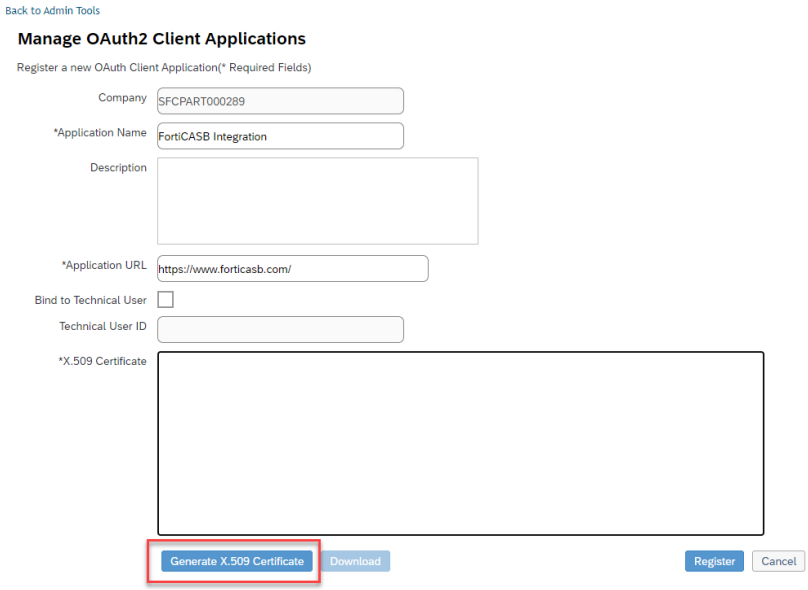
Step 3. Update SAP Success Factors Account on FortiCASB on page 235

Step 1. Register OAuth Client Applicaiton

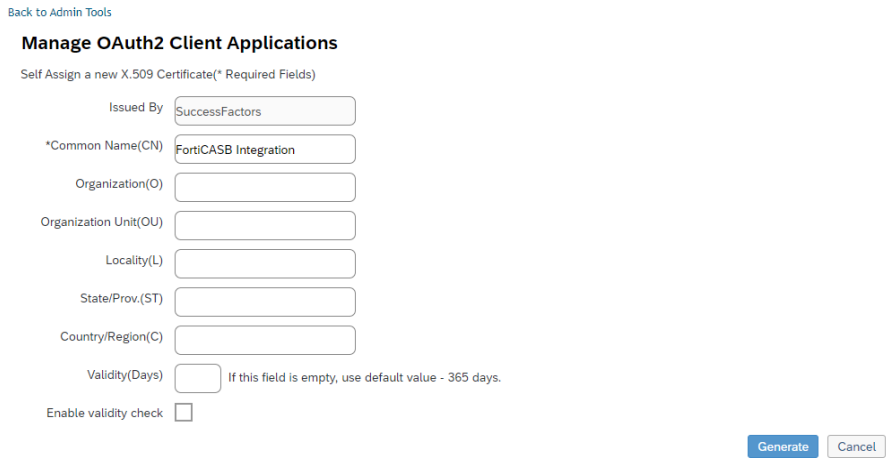
1. Log into SAP Success Factors and go to **Admin Center**. In the **Tools** box, search and go to **Manage OAuth2 Client Applications**.



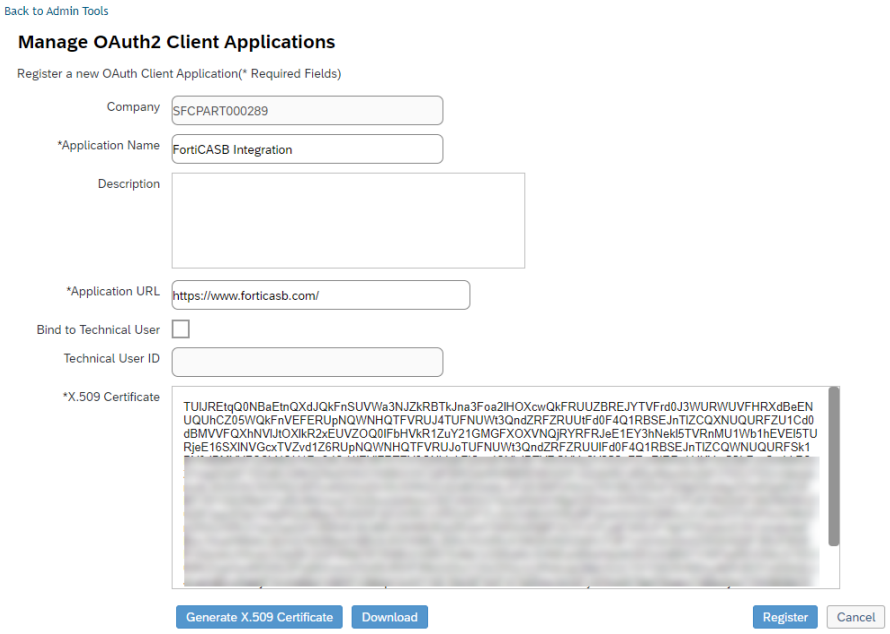
2. In **Manage OAuth2 Client Applications**, click **Register Client Application** to register a new OAuth2 Client Application.
3. Fill in an application name, e.g. FortiCASB Integration, then in **Application URL**, enter a url, e.g. https://www.forticasb.com/.
   At the bottom of the page, click **Generate X.509 Certificate** to register a certificate.



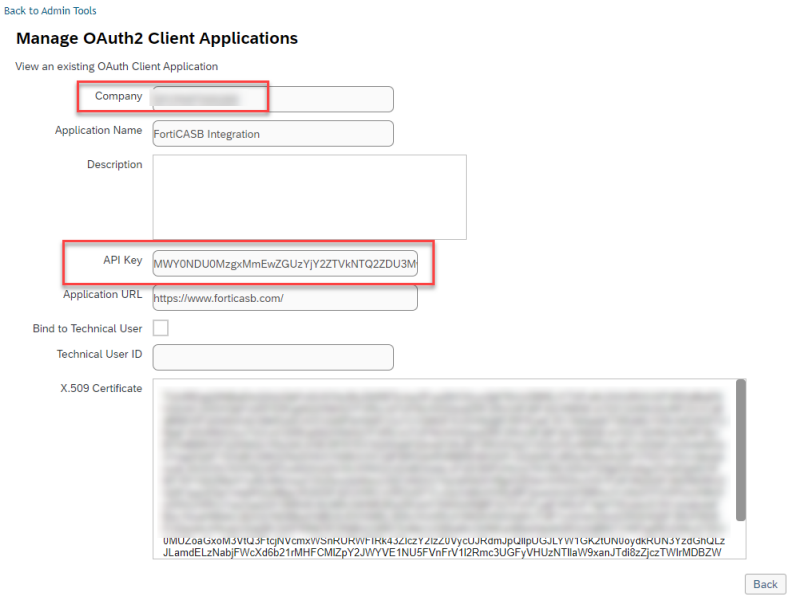
4. In "Self Assign a new X.509 Certificate" page, enter a **Common Name** for the certificate, and click **Generate**.



5. You will be re-directed back to the previous page, and the certificate values will be filled.
   Click **Download** to download the certificate pem file as the private key for use later. Then click **Register** to register the client application.

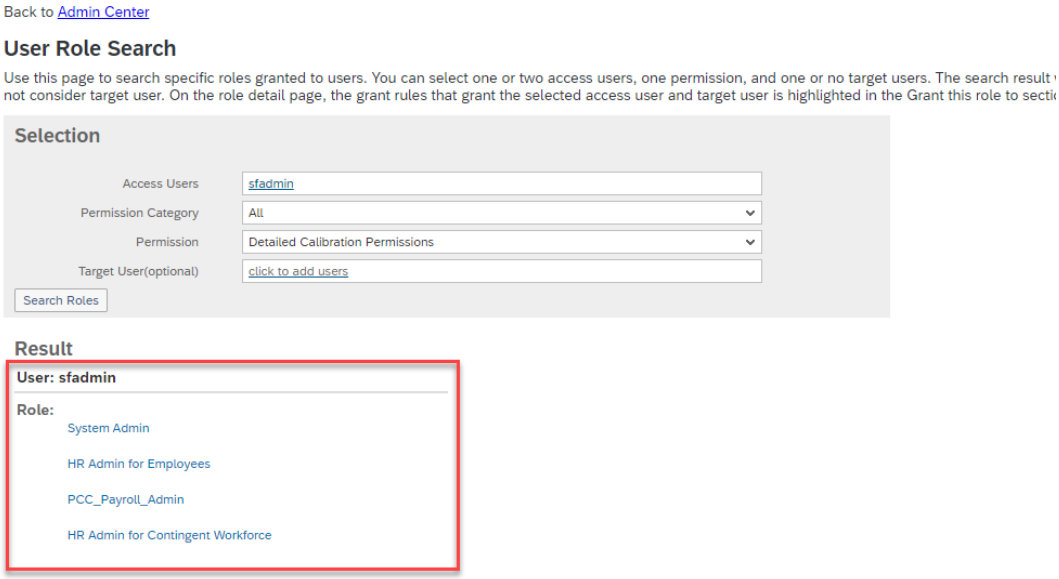


6. Click on the OAuth2 Application that you just created, the **API Key** should be generated automatically, make a record of the **API key** and **Company ID**.

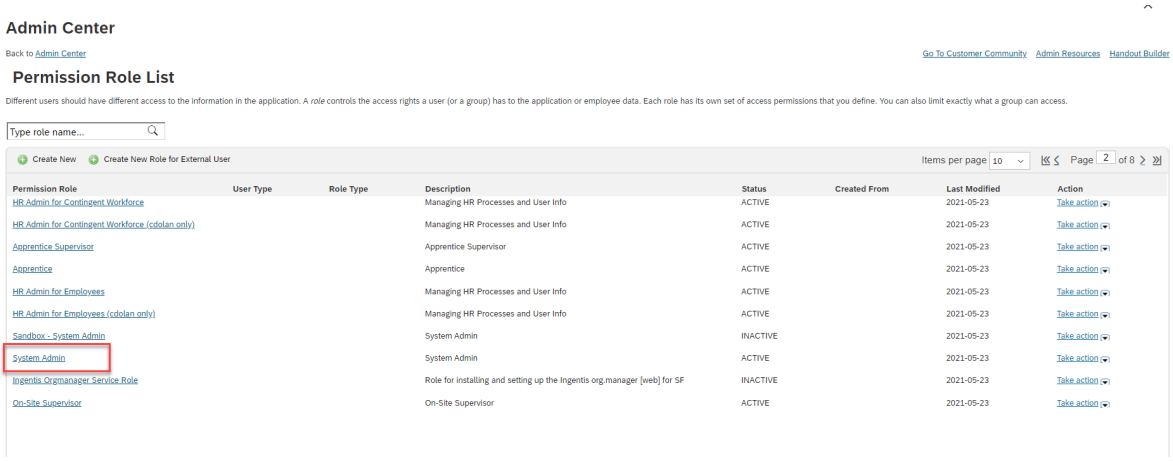


Step 2. Set Permission Scope

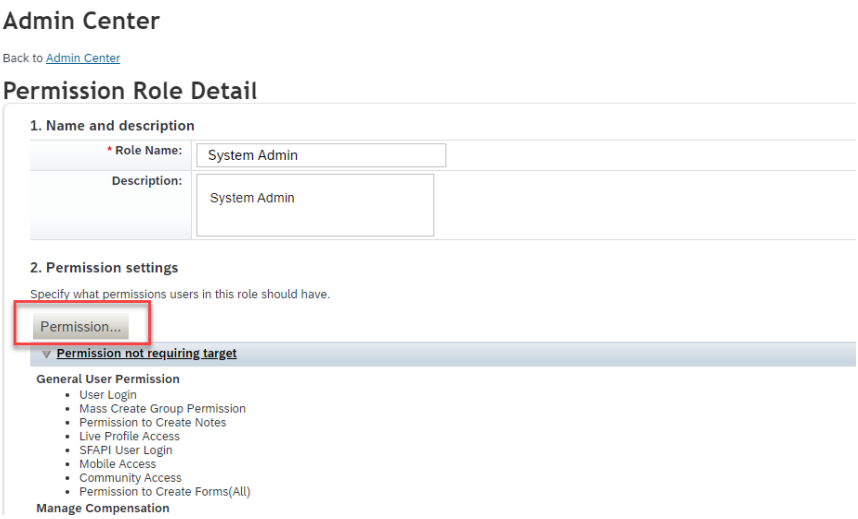
1. In **SAP Success Factors** > **Admin Center**, search and go to **User Role Search**.
2. Look up the User ID to be added on FortiCASB for the Roles under the user.



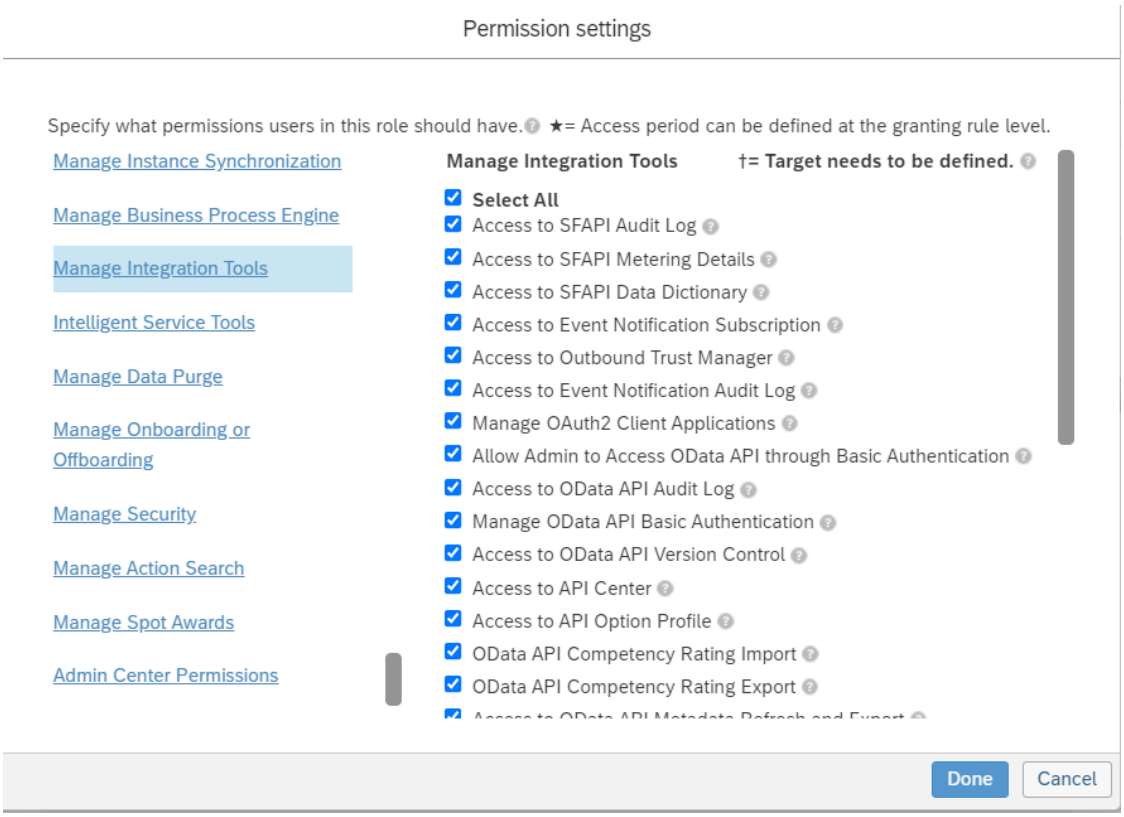
3. Go back to the **Admin Center** again, search and go to **Manage Permission Role**.
4. Look up one of the role that is under the user, e.g. System Admin, and click on it.



5. In **Permission Role Detail**, click on **Permission** button to configure the permission settings.



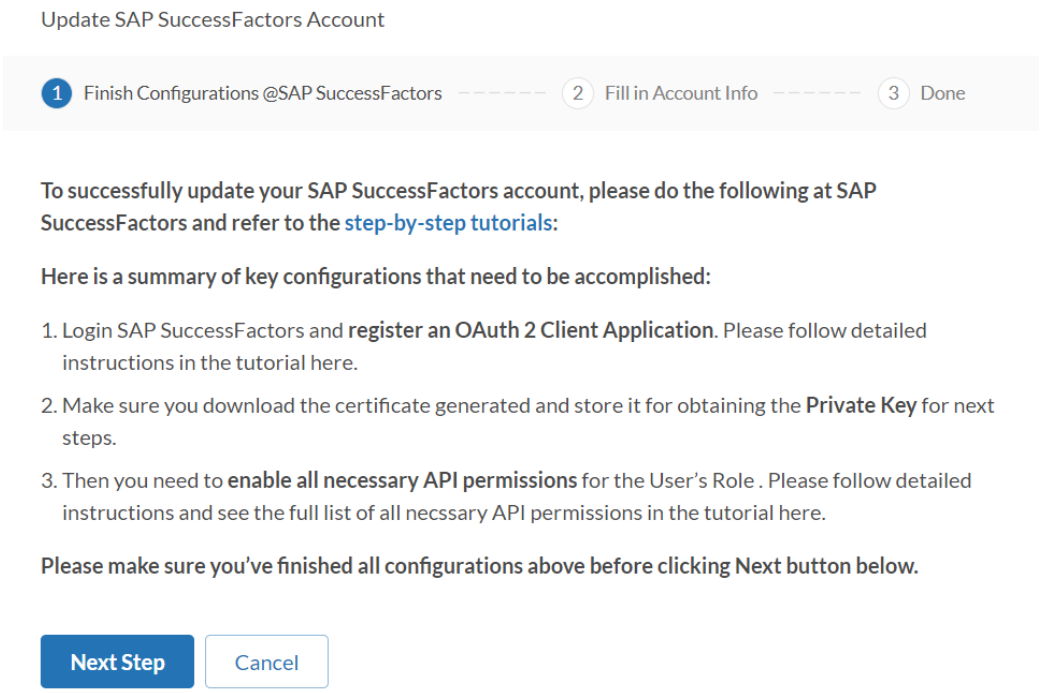
6. Scroll down and select **Manage Integration Tools**, click **Select All** to add all integration permissions, and click **Done**.



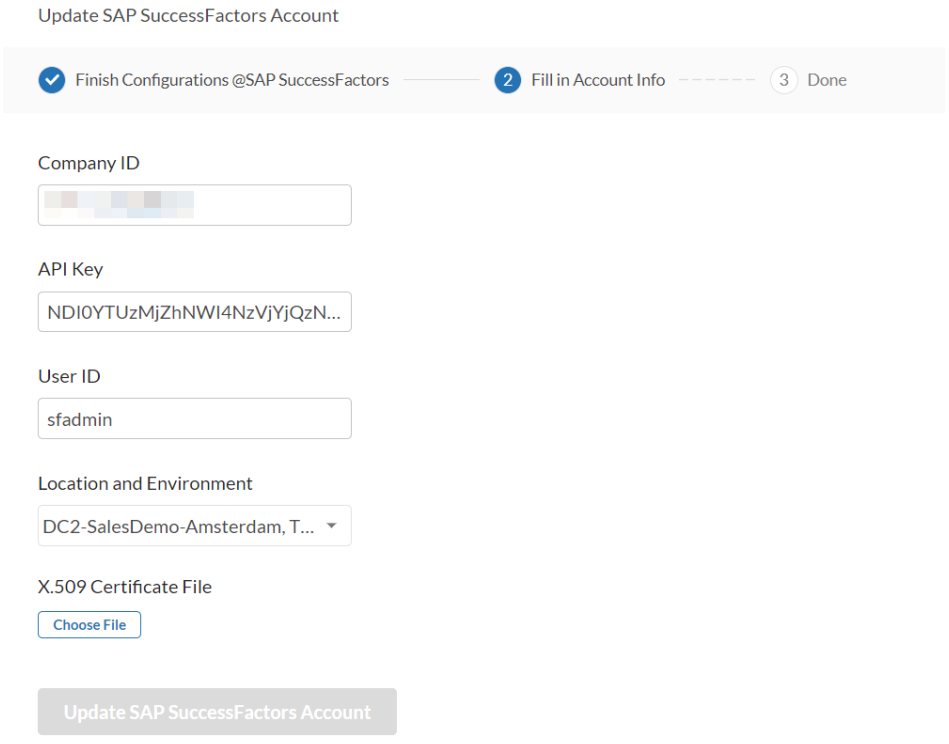
Now go back to FortiCASB to add the SAP Success Factors account.

Step 3. Update SAP Success Factors Account on FortiCASB

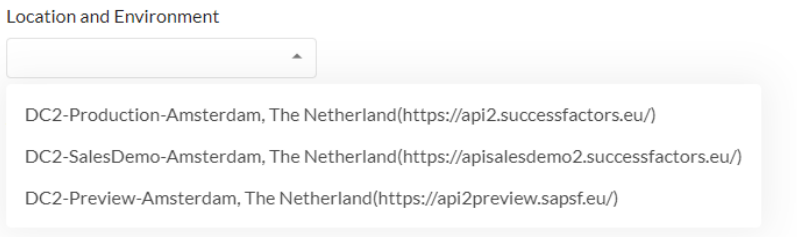
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the SAP Success Factors account menu, and select **Update Cloud Account**.
4. Review the configuration list and make sure they are completed, and click **Next Step**.



5. Enter the SAP Success Factors **Company ID**, **API Key** saved earlier, then enter the SAP Success Factors **User ID**.



6. Click **Location and Environment** drop down menu and select one of the **location and environment:**



7. Upload the X.509 Certificate pem file saved from earlier and click **Update SAP Success Factors Account.**
8. Wait for 15 minutes for the account to be fully added to FortiCASB.

ServiceNow

FortiCASB offers an API-based approach, pulling data directly from ServiceNow via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track ServiceNow user activities, provides DLP Data Analysis for files stored on ServiceNow tickets.

Prerequisite

Before ServiceNow account can be added to FortiCASB, an **OAuth API Endpoint** needs to be created at ServiceNow to establish connection between FortiCASB and ServiceNow.

A **ServiceNow Instance** will be required to create an application registry for OAuth API endpoint.

Note: Only **ServiceNow Istanbul** or higher version is supported.

Follow these steps to configure and add ServiceNow account on FortiCASB:

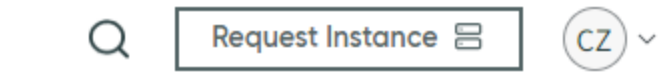
1. **Create ServiceNow Developer Instance on page 238**
2. **Create ServiceNow OAuth API Endpoint on page 239**
3. **Add ServiceNow Account on page 243**

Create ServiceNow Developer Instance

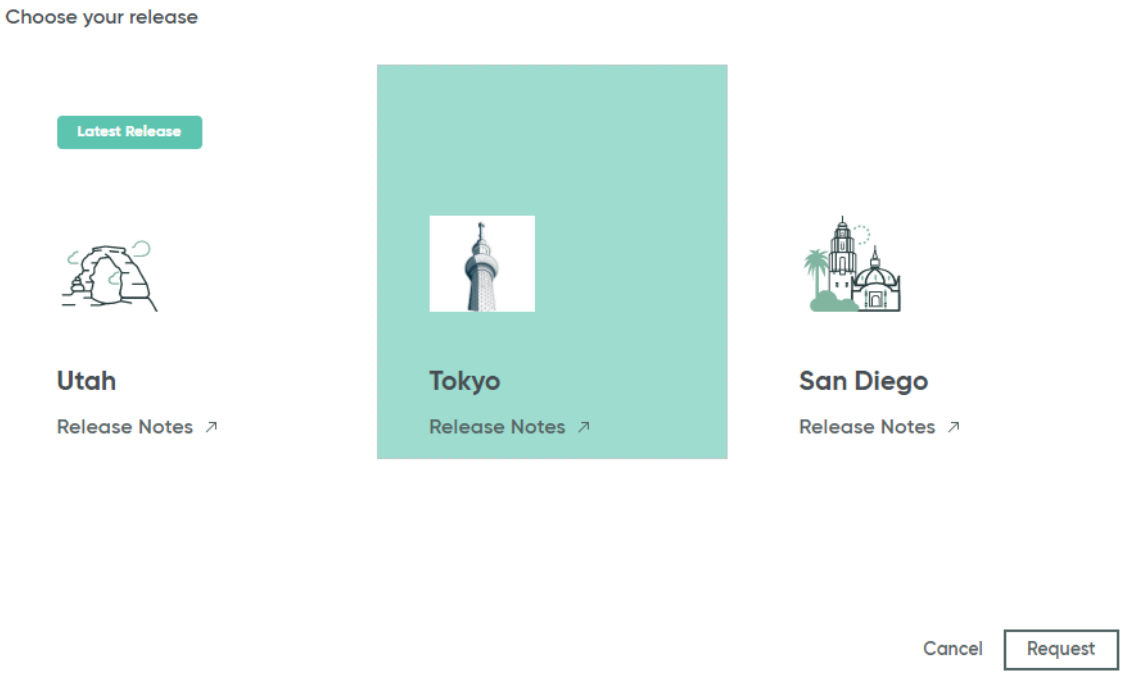
If you have an **existing** ServiceNow developer instance, you may use it to create a ServiceNow application registry to establish connection with FortiCASB.

If not, please create a developer instance following the steps below:

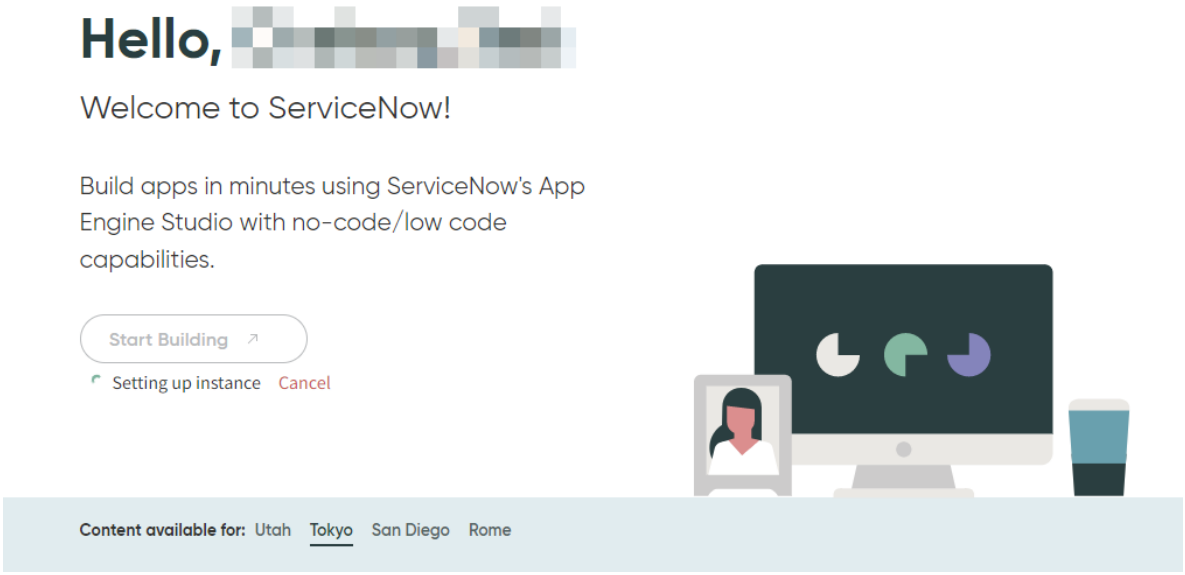
1. Log into ServicewNow Developer Home page.
2. Click **Request Instance** at the right hand corner.



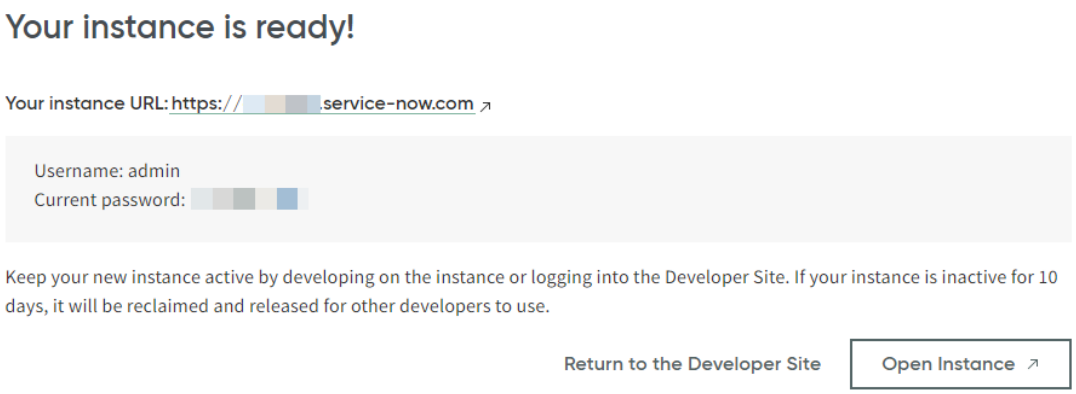
3. Choose an instance type listed and click **Request**.



4. A developer instance will be created, it may take a few minutes.



5. Once the instance is created, it will provide the **instance URL** and **credentials**. Keep a record of them.

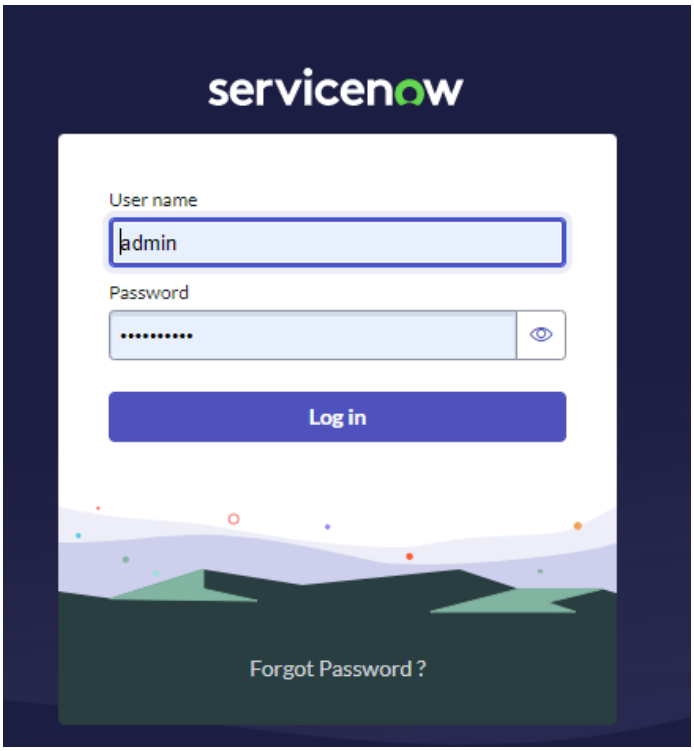


Now proceed to Create ServiceNow OAuth API Endpoint on page 239 to finish the rest of configurations.

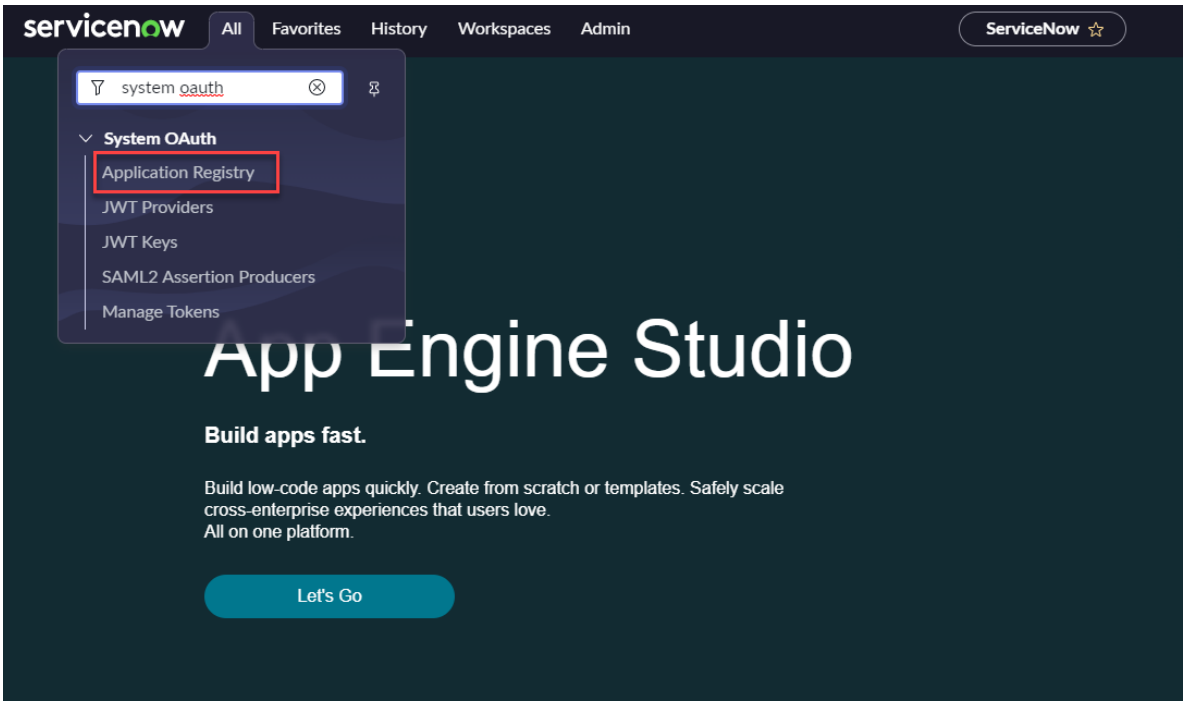
Create ServiceNow OAuth API Endpoint

After a ServicewNow Developer Instance is created, a new application registry along with the OAuth Apl Endpoint can be created under the ServiceNow developer instance.

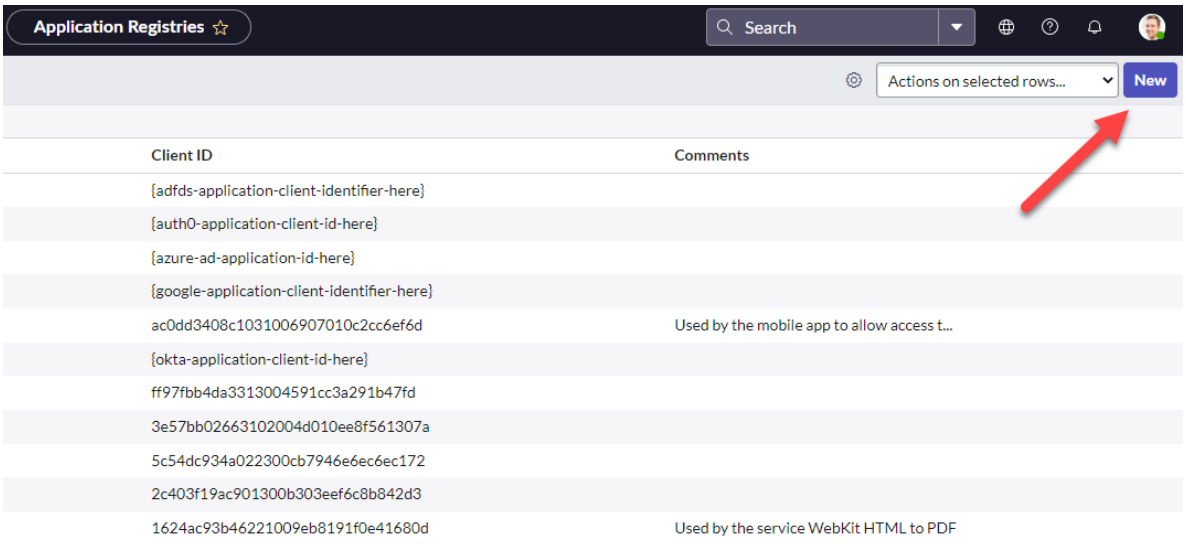
1. Go to the ServicewNow instance created earlier in Create ServiceNow Developer Instance on page 238.
   For example: https://<Instance ID>.service-now.com/
2. Log in with your ServiceNow instance credentials.



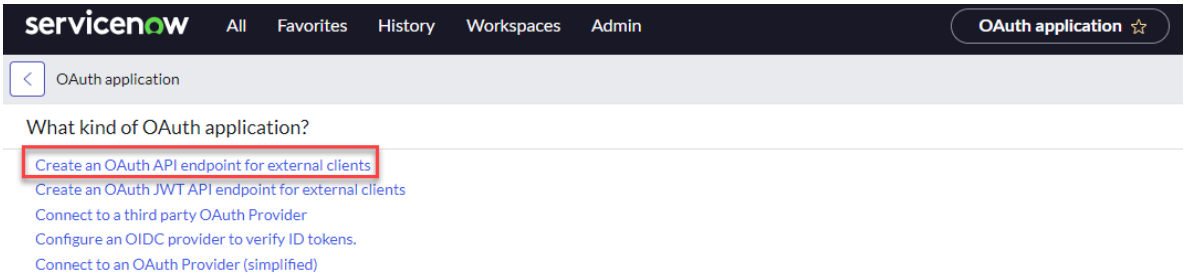
3. Click **All** on the navigation menu, scroll down or search for **System OAuth**, and click on **Application Registry**.



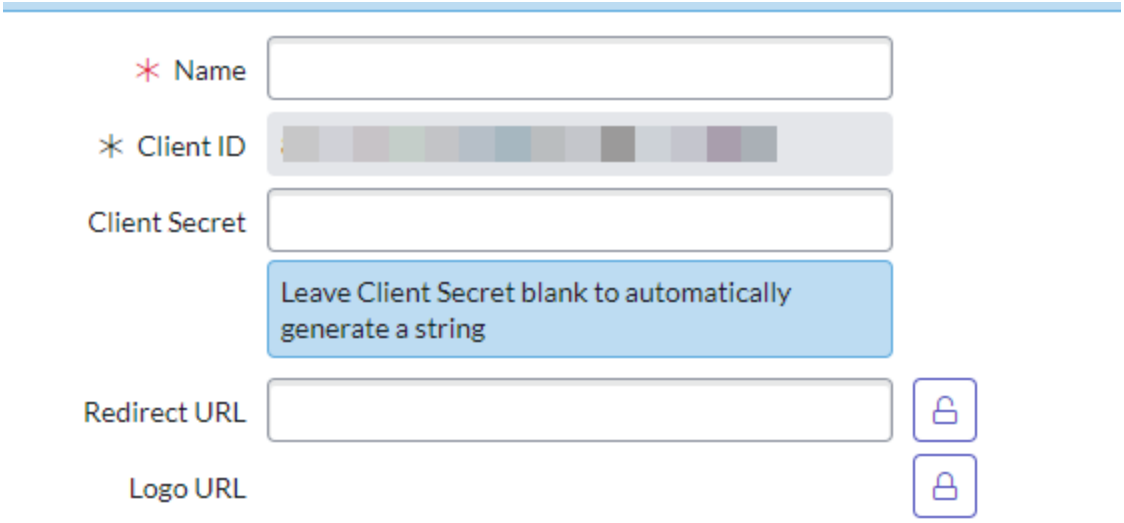
4. Click on **New** in the upper right hand corner to create new application.



5. Select and click **Create an OAuth API endpoint for external clients**.



6. Enter an unique **Name** and **Client Secret** for the OAuth client application.



7. In the **Redirect URL** field, enter the **Redirect URL** provided by FortiCASB **Add ServiceNow Account page** step 4.

4. When you fill in the form, please follow below instructions for certain fields:

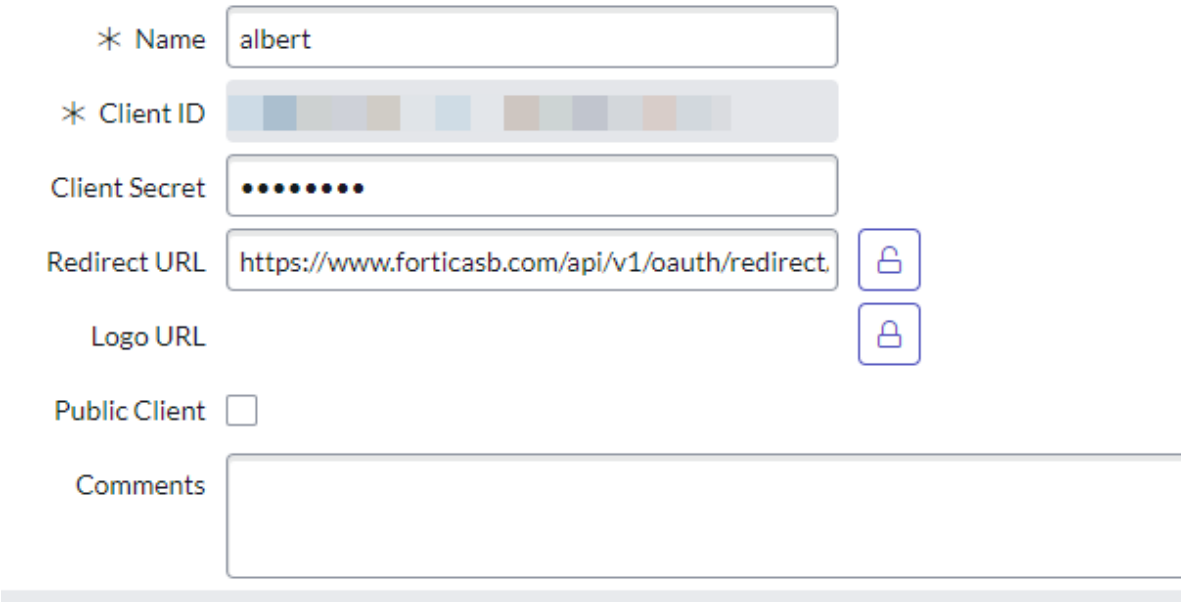
   a. Keep record of **Client ID** and **Client Secret** (these are needed in next step);

   b. In **Redirect URL** field, input **Redirect URL:**

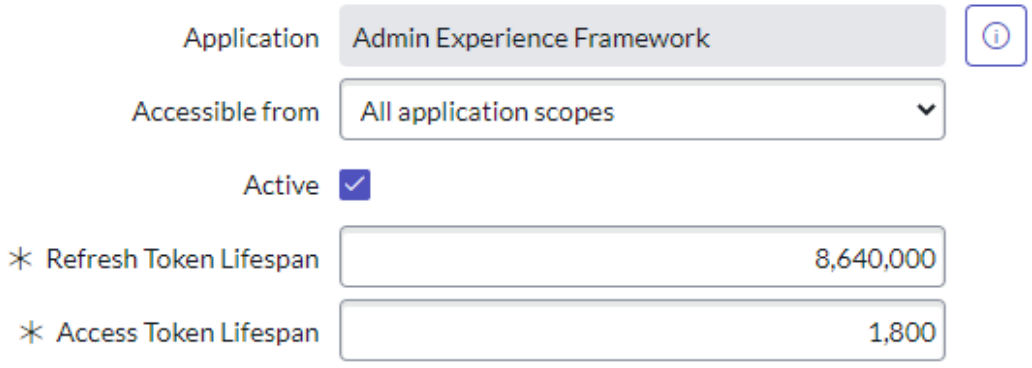
   Redirect URL:

   https://www.forticasb.com/api/v1/oauth/redirect/ServiceNow

8. Keep a record of **Client ID** and **Client Secret** for use later in adding the ServiceNow account to FortiCASB.



9. Leave **Refresh Token Lifespan** and **Access Token Lifespan** fields as default.



10. Click **Submit** and go back to FortiCASB **Add ServiceNow Account** page.

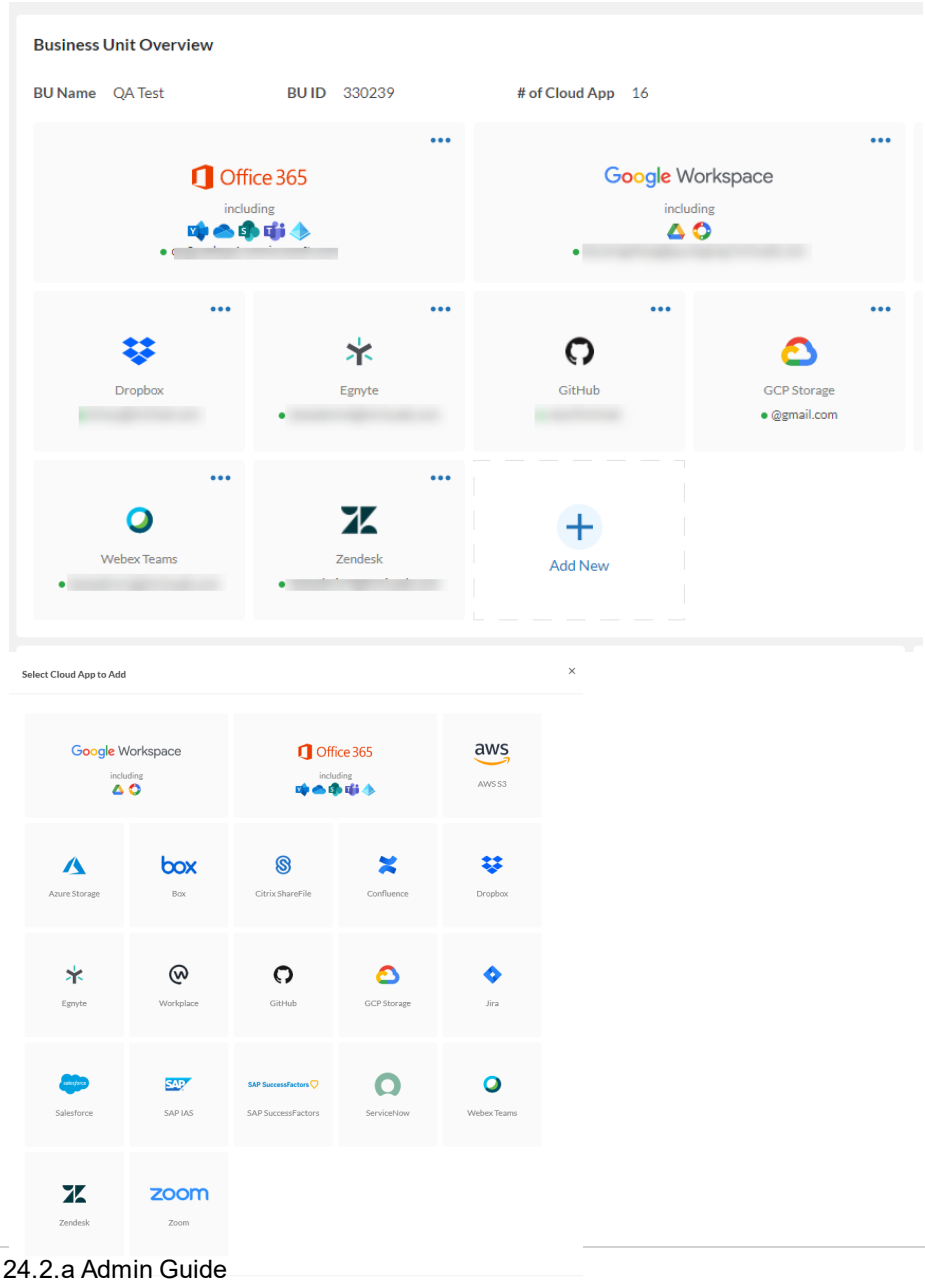
Now the ServiceNow account is ready to be added to FortiCASB. Go to Add ServiceNow Account on page 243.

Add ServiceNow Account

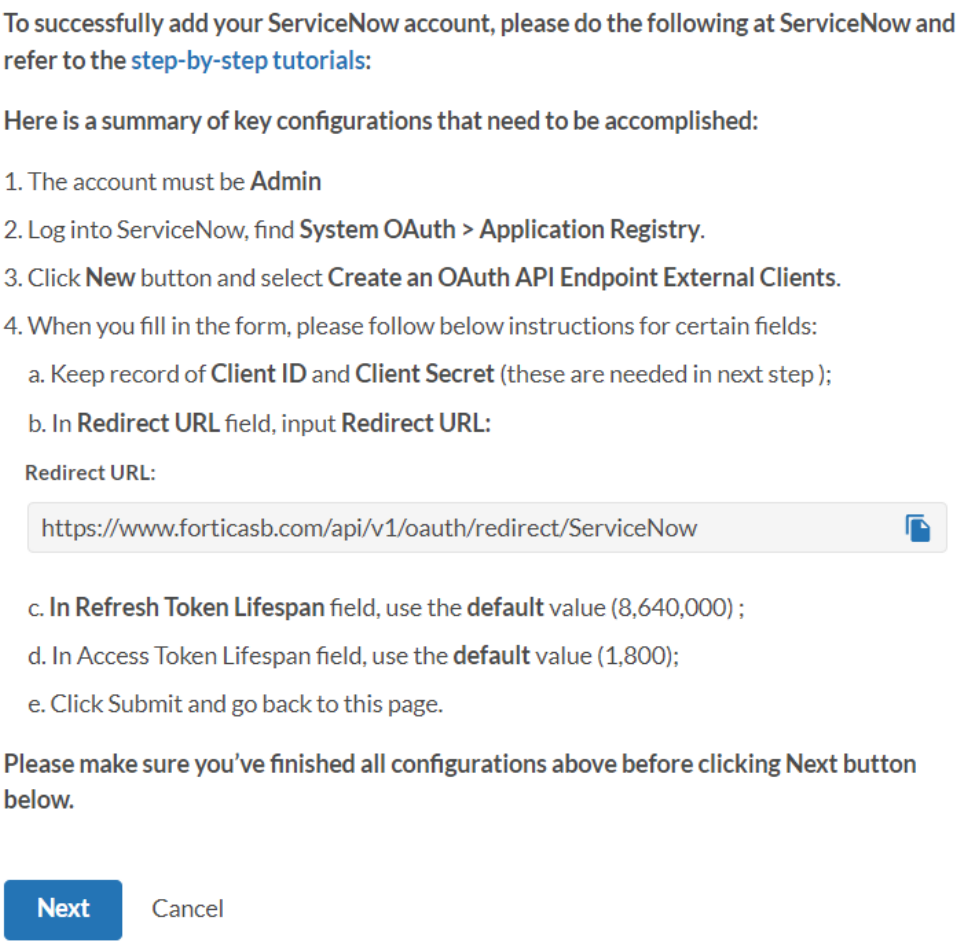
After a ServiceNow OAuth API Endpoint is created, you can now add the ServiceNow account on FortiCASB.

Follow the instructions below to add the ServiceNow account on FortiCASB:

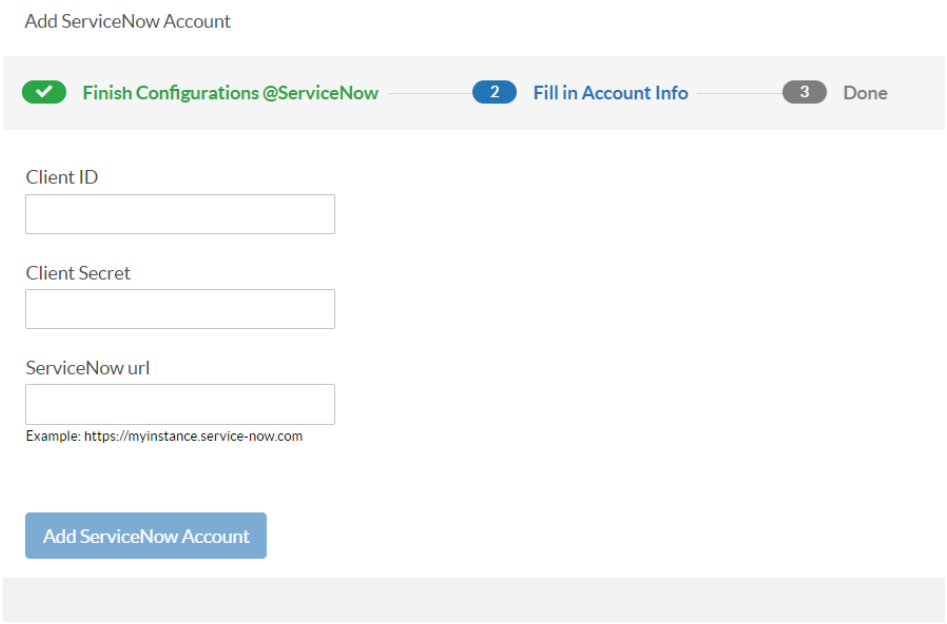
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **ServiceNow**, then click **Add Selected Cloud App**.



3. Review the key configurations list to see if you have finish all the required configurations, and click **Next**.



4. In **Client ID** and **Client Secret** fields, enter the "Client ID" and "Client Secrets" recorded earlier. In **ServiceNow url**, enter your ServiceNow url.



5. Click **Add ServiceNow Account** to add the ServiceNow account. It may take 15 minutes to finish adding the account. You may check the status in **Overview > Dashboard.**

Update ServiceNow Account

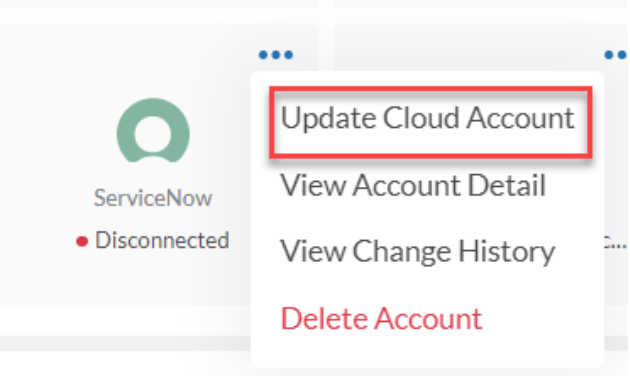
Before updating the ServiceNow account on FortiCASB, complete the same configurations using the same ServiceNow account:

Create ServiceNow Developer Instance on page 238

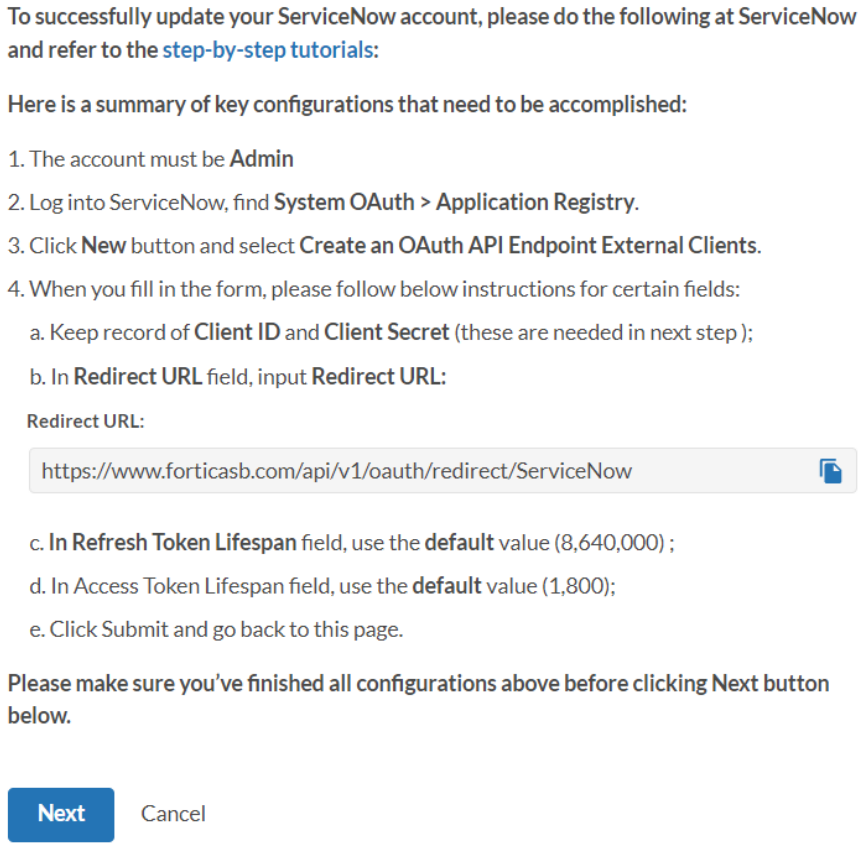
Create ServiceNow OAuth API Endpoint on page 239

After the ServiceNow configuration is completed, follow these steps to update your ServiceNow account on FortiCASB.

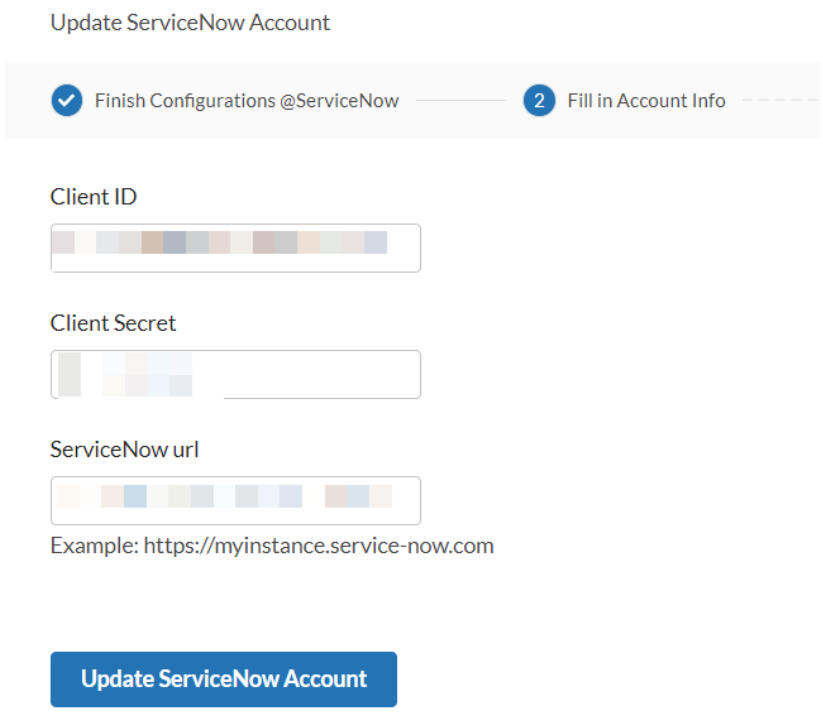
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the ServiceNow menu and select **Update Cloud Account**.



4. Review the key configurations list to see if you have finish all the required configurations, and click **Next**.



5. In **Client ID** and **Client Secret** fields, enter the "Client ID" and "Client Secrets" recorded earlier. In **ServiceNow url**, enter your ServiceNow url.



6. Click **Update ServiceNow Account** to update the ServiceNow account.

It may take 15 minutes to finish updating the account. You may check the status in **Overview > Dashboard.**

Webex Teams

FortiCASB offers an API-based approach, pulling data directly from Webex Teams via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication.

Subsequently FortiCASB combines these data to offer protection on Webex Teams file sharing and events monitoring. All the files shared on Webex Teams space chats are protected against virus and monitored for compliance violation. Events monitoring monitors for suspicious user activities or unauthorized events.

Types of Webex account activities monitored by FortiCASB:

Admin Event (With IP)	Regular Event (Without IP)
File Activities	Upload File
	Delete File
Create User	Create Memberships
Delete User	Delete Memberships
	Update Memberships
	Participant Join Meeting
	Participant Left Meeting

Prerequisites

The Webex user account should be under a **Basic, Business, or Enterprise** subscription plan.

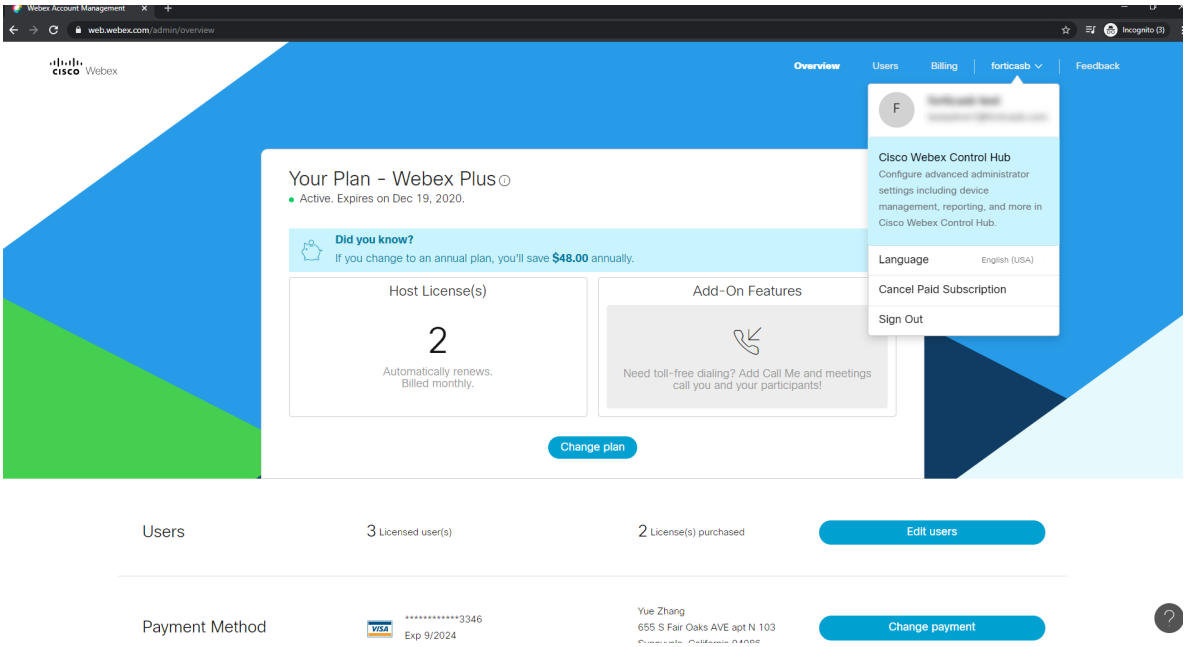
Add Webex Teams

Follow the steps below to add Webex team to FortiCASB:

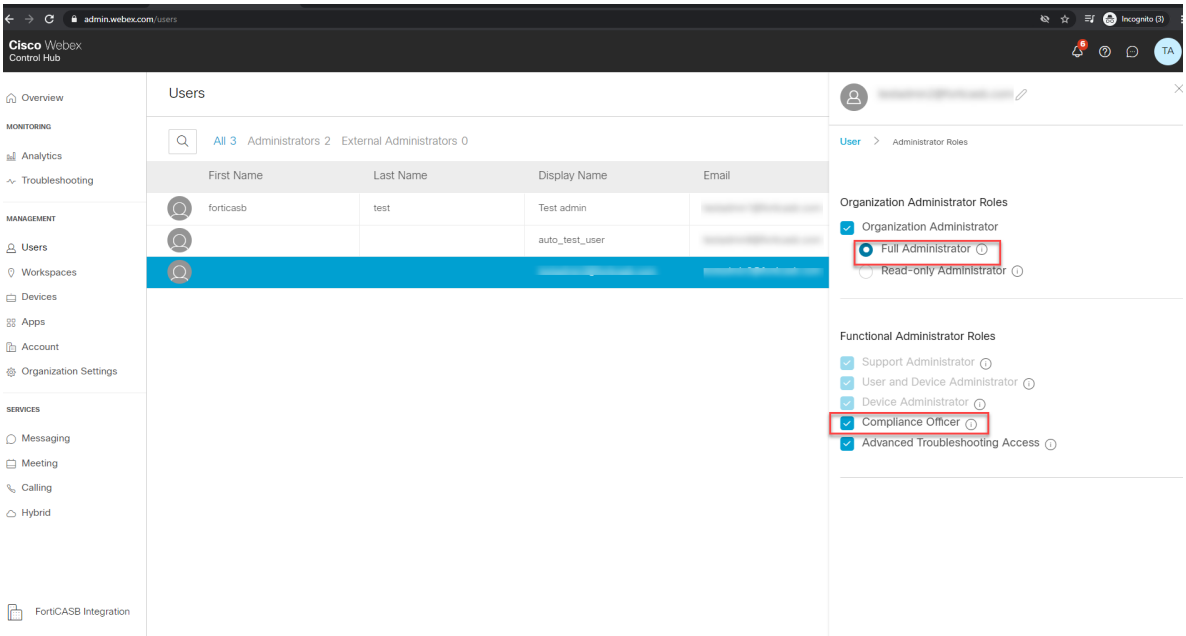
1. **Configure WebEx admin account on page 248**
2. **Add Webex Teams account on page 250**

Configure WebEx admin account

1. Log into Cisco WebEx Admin with your Webex **admin** account
2. Click on your user profile icon drop down menu, and click **Cisco Webex Control Hub**.



3. In **Cisco Webex Control Hub** navigation menu, click on **Management > Users**.
4. Click on the user that will the added to FortiCASB. In **Roles and Security**, click on **Administrator Roles**, make sure the user is a **Full Administrator**.
   (Ask another admin to assign the role if needed.)

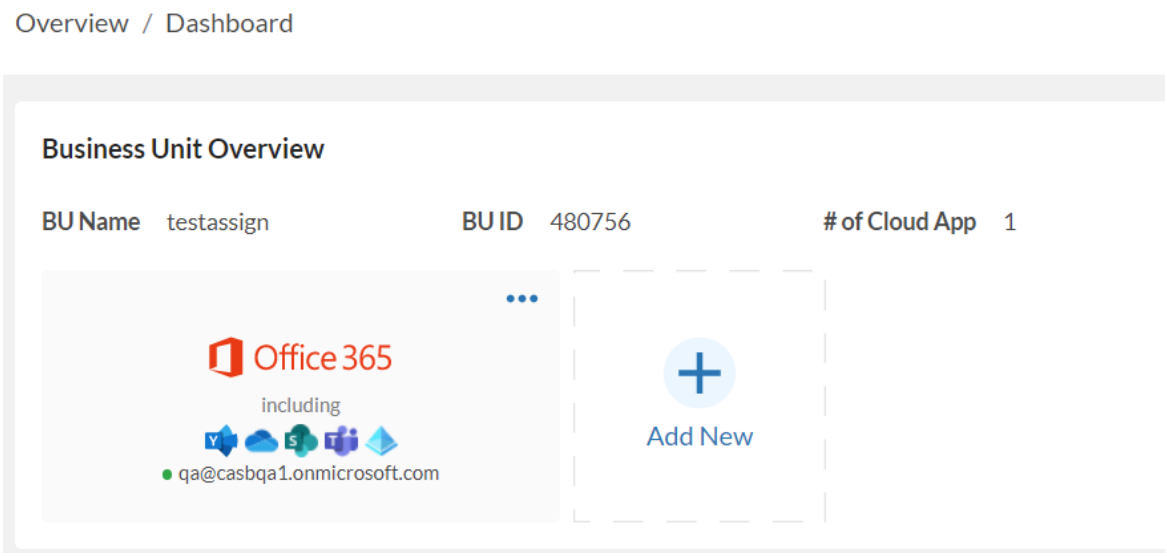


Follow the rest of the steps in Add Webex Teams account on page 250 to complete adding the Webex account on FortiCASB.

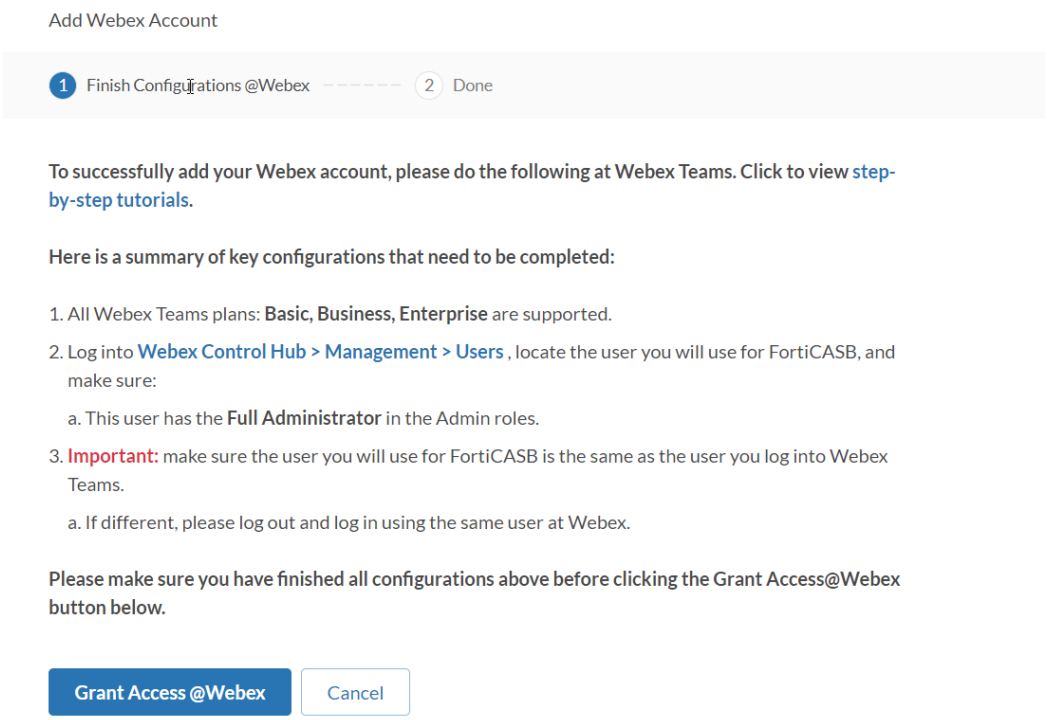
Add Webex Teams account

After the Webex Team configurations are completed from the previous section, follow these steps to add your Webex Team account on FortiCASB.

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Webex Teams**, then click **Add Selected Cloud App**.



3. Review the key configurations list to see if you have finish all the required configurations, click **Grant Access@Webex**. Then you will be re-directed to Webex OAuth verification page.
Note: Before clicking on **Grant Access@Webex**, make sure you log out of Webex if you have another account that is log in on another web page.



4. Enter your Webex credentials and press **Submit**. Then go back to the FortiCASB page.

It may take 15 minutes to finish adding the account. You may check the status in **Overview > Dashboard.**

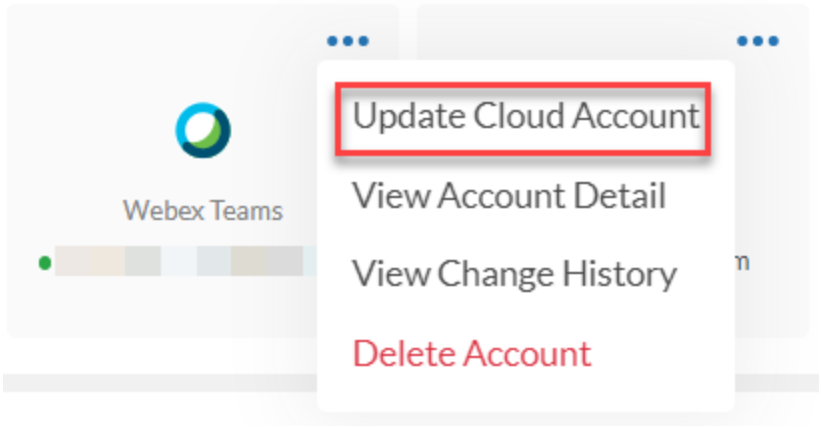
Update Webex Teams Account

Before updating the Webex Teams account on FortiCASB, complete the same configurations using the same Webex Teams account:

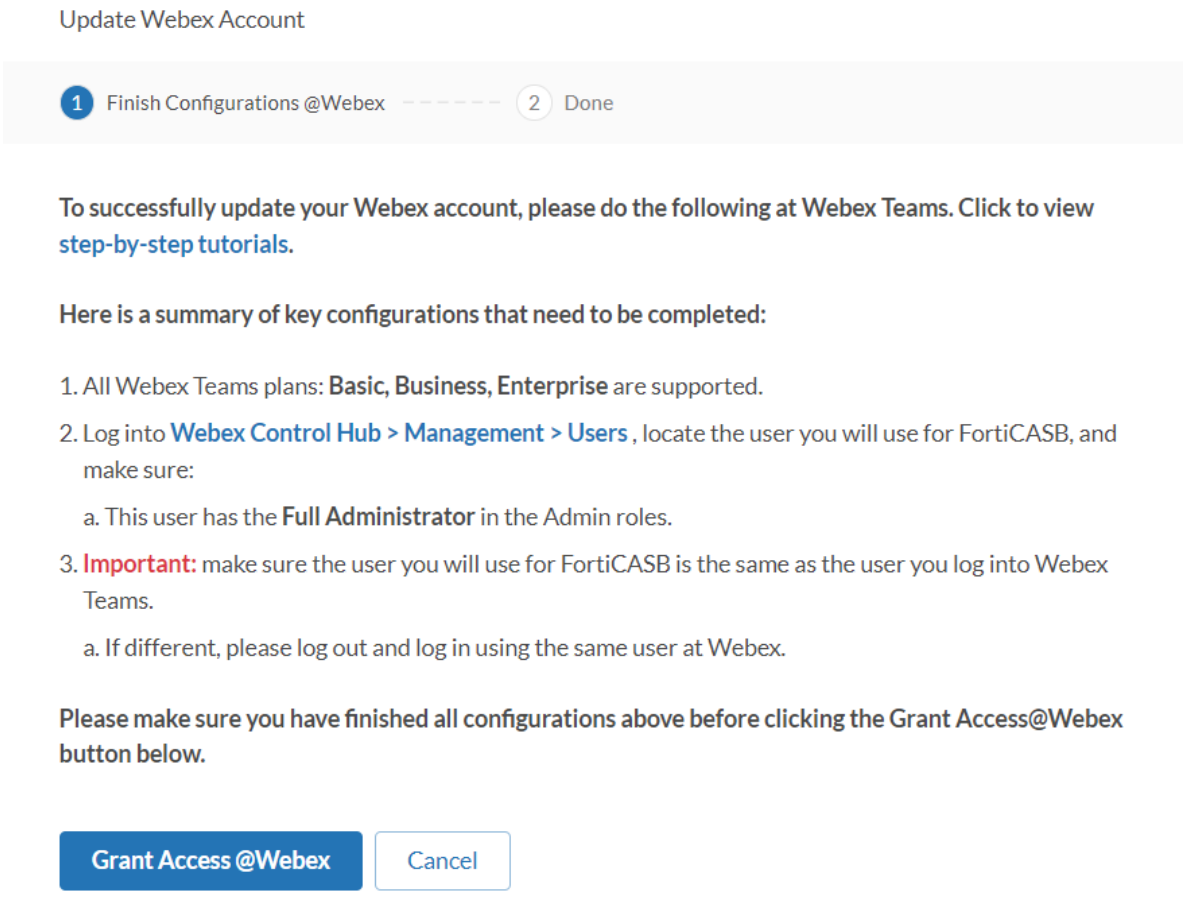
Configure WebEx admin account on page 248

After the Webex Teams configuration is completed, follow these steps to update your Webex Teams account on FortiCASB.

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the Webex Teams menu and select **Update Cloud Account**.



4. Review the key configurations list to see if you have finish all the required configurations, click **Grant Access@Webex**. Then you will be re-directed to Webex OAuth verification page.
Note: Before clicking on **Grant Access@Webex**, make sure you log out of Webex if you have another account that is log in on another web page.



5. Enter your Webex credentials and press **Submit**. Then go back to the FortiCASB page.

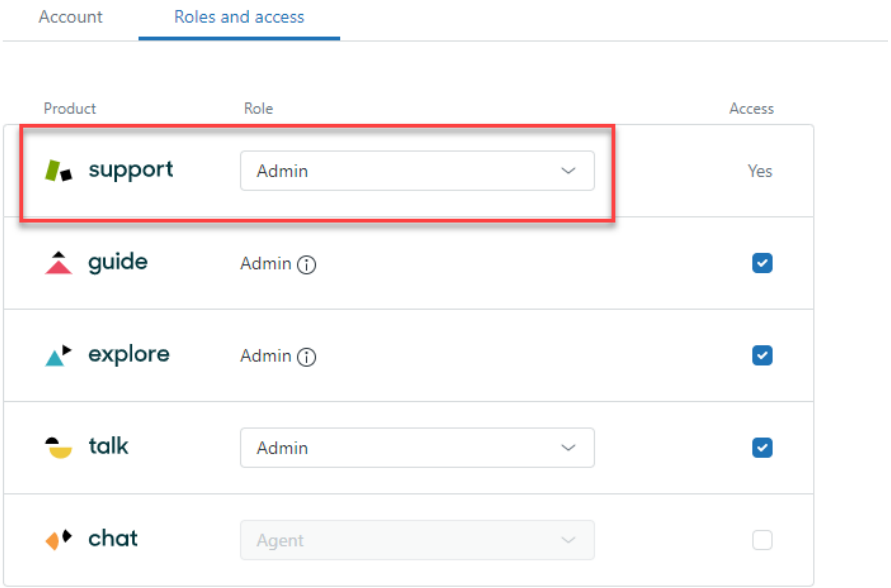
It may take 15 minutes to finish updating the account. You may check the status in **Overview > Dashboard.**

Zendesk

FortiCASB offers an API-based approach, pulling data directly from Zendesk via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Zendesk user activities and ticketing system, provides DLP Data Analysis for files on tickets.

Prerequisite

1. FortiCASB requires the Zendesk account to be under an **Enterprise** plan.
2. The Zendesk account to be added to FortiCASB must have **Admin Role** in Support.



3. A **Zendesk OAuth Client** needs to be created to authorize access for FortiCASB REST API.

After you have verified the account prerequisite, follow the guides below to **Add** or **Update** the account on FortiCASB:

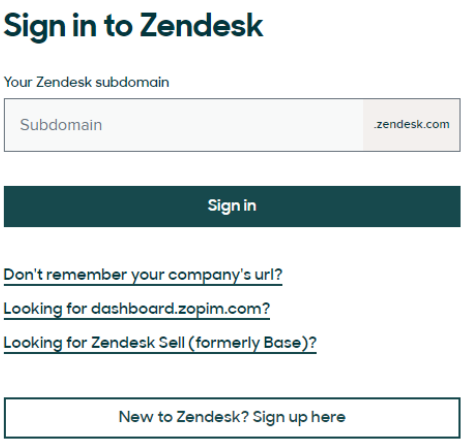
Add Zendesk Account on page 254

Update Zendesk Account on page 258

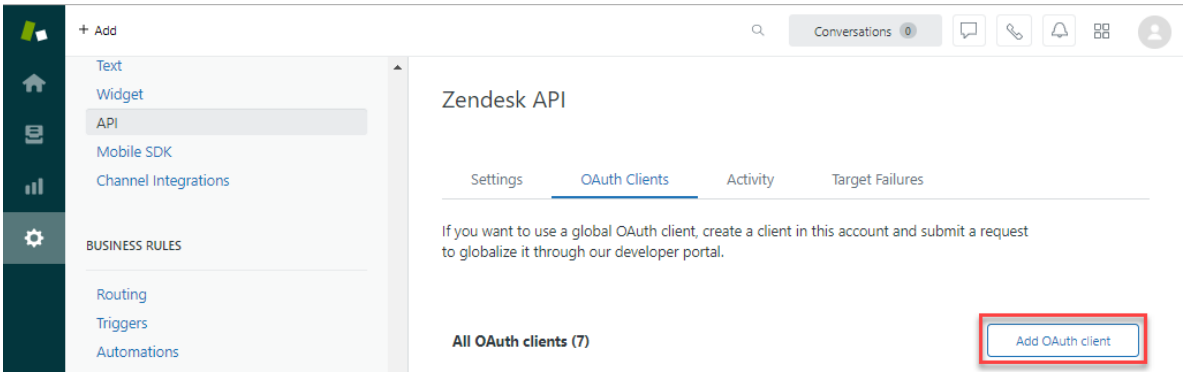
Add Zendesk Account

Step 1: Create Zendesk OAuth Client

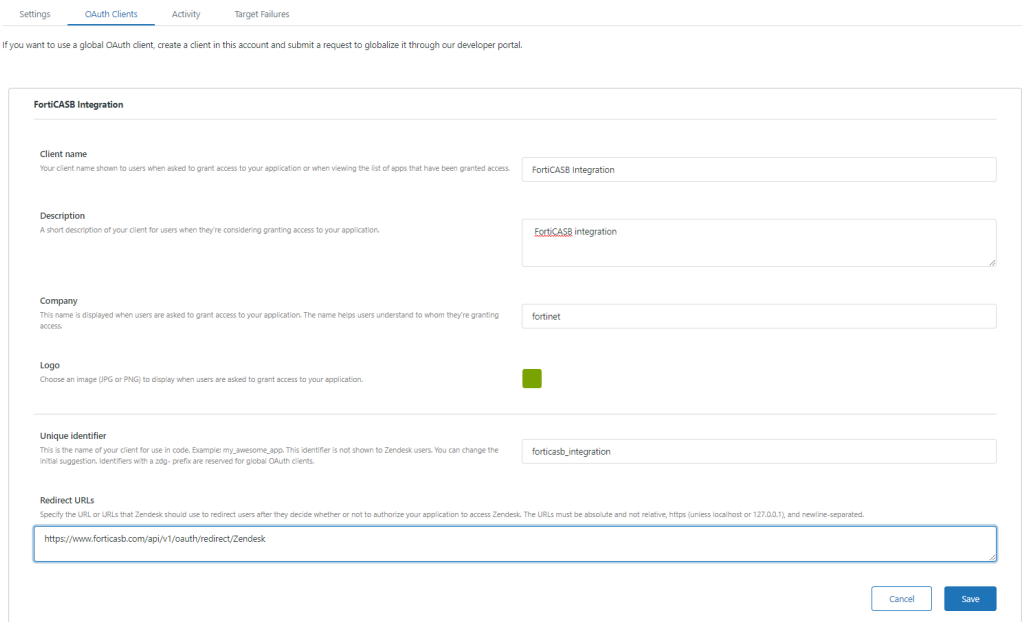
1. Log into Zendesk with your sub-domain, and then with your admin account.



2. In the left navigation pane, click **Admin**  , scroll down to **Channels**, and click on **API**.
3. In **Zendesk API** page, select **OAuth Clients** tab, then click **Add OAuth client**.



4. Fill in a **Client Name** of your choice, **Short Description**, and an **Unique Identifier** which should be populated automatically. Keep a record of the unique identifier for use later.



5. In **Redirect URLs**, use one of the corresponding redirect url provided by FortiCASB:

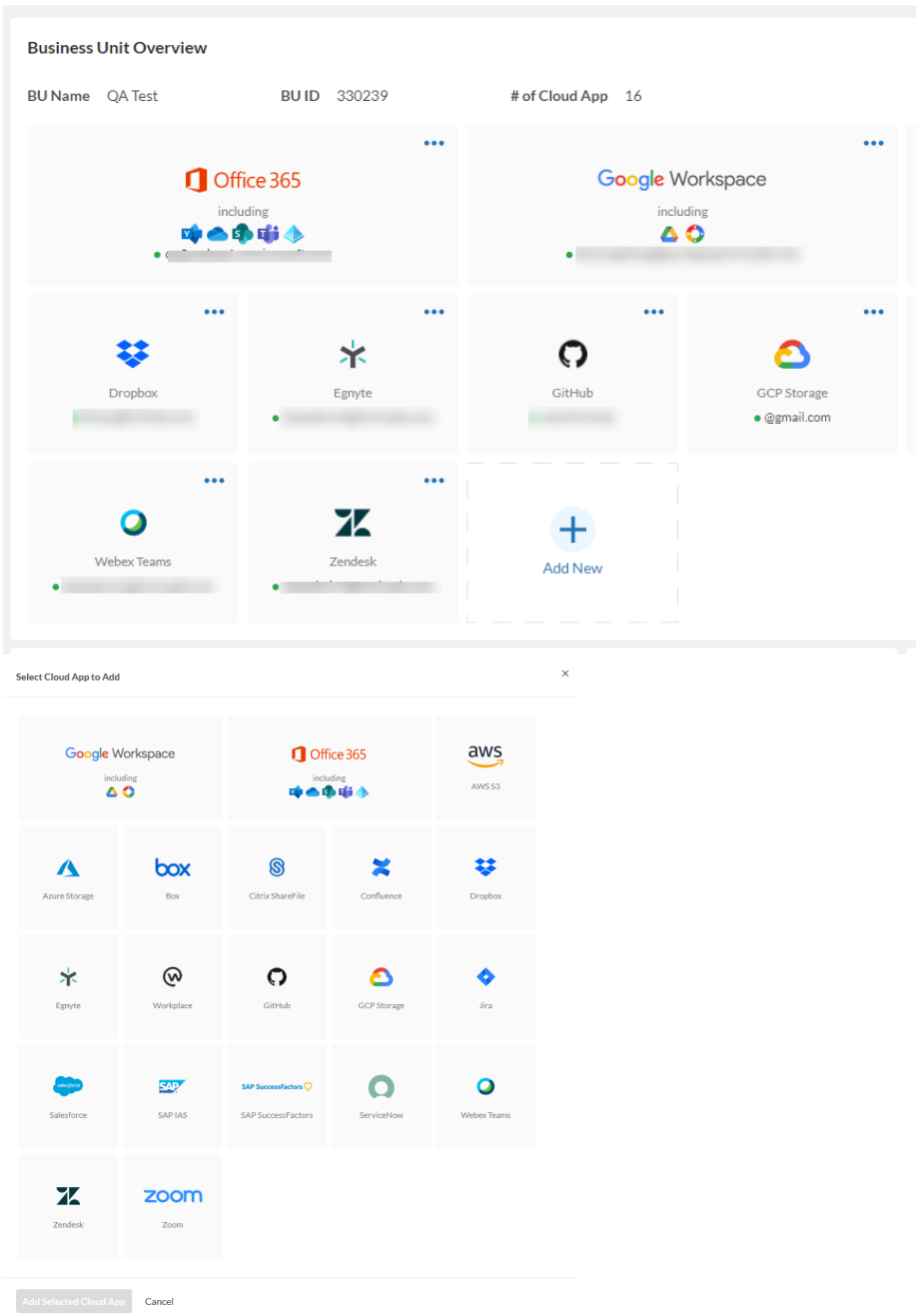
Region	Redirect URL
Global Region	https://www.forticasb.com/api/v1/oauth/redirect/Zendesk
European Union Region	https://eu.forticasb.com/api/v1/oauth/redirect/Zendesk

6. Click **Save**, and then in **Secret** field, click **Generate** to generate the secret token.
   Note:Make sure to copy down the secret token as it will only appear once.

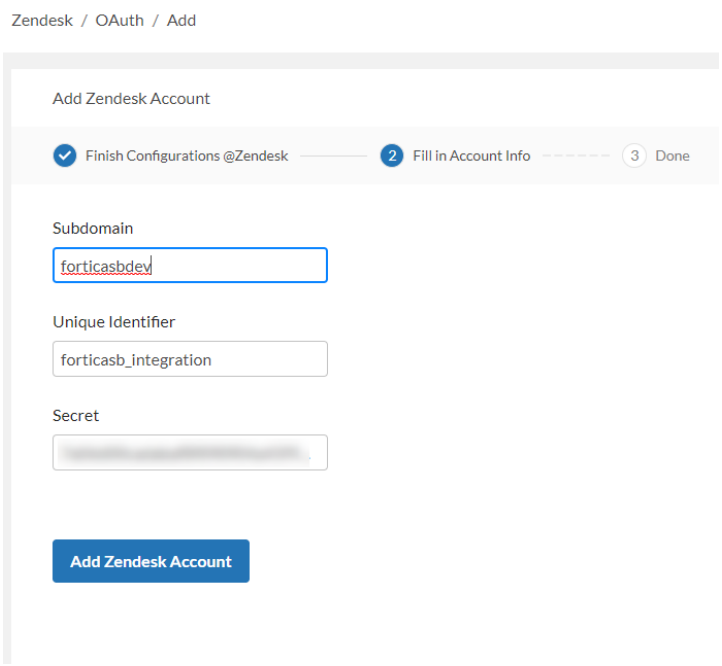
Now go back to **FortiCASB** to add the Zendesk account.

Step 2: Add Zendesk Account

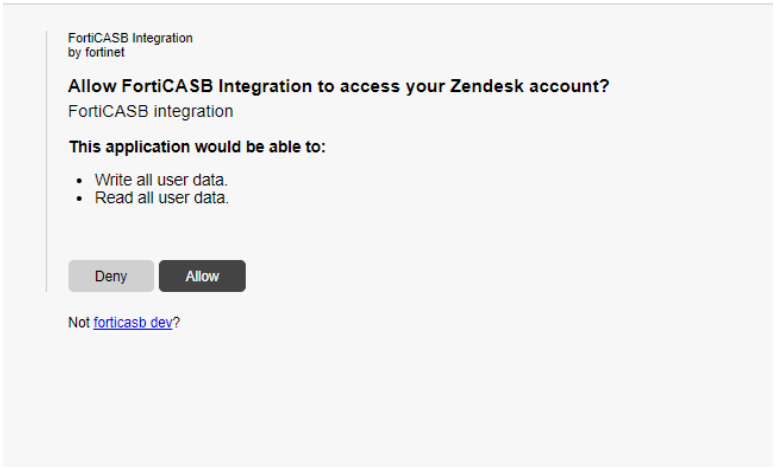
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Zendesk**, then click **Add Selected Cloud App**.



3. Fill in the Zendesk **Sub-Domain**, **Unique Identifier**, and the **Secret Token** saved from earlier, and click **Add Zendesk Account**.



4. You will be prompt to authorize FortiCASB to access to your Zendesk account, click **Allow** to complete adding the Zendesk account.

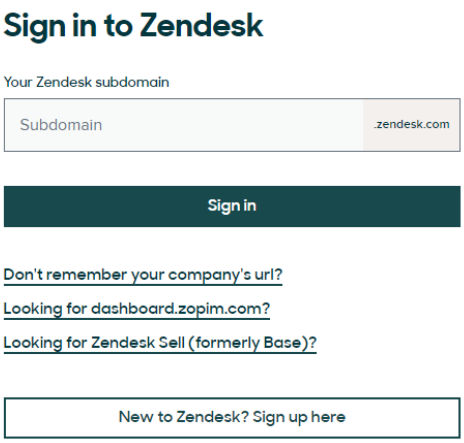


5. Wait 15 minutes to complete adding the Zendesk account to FortiCASB.

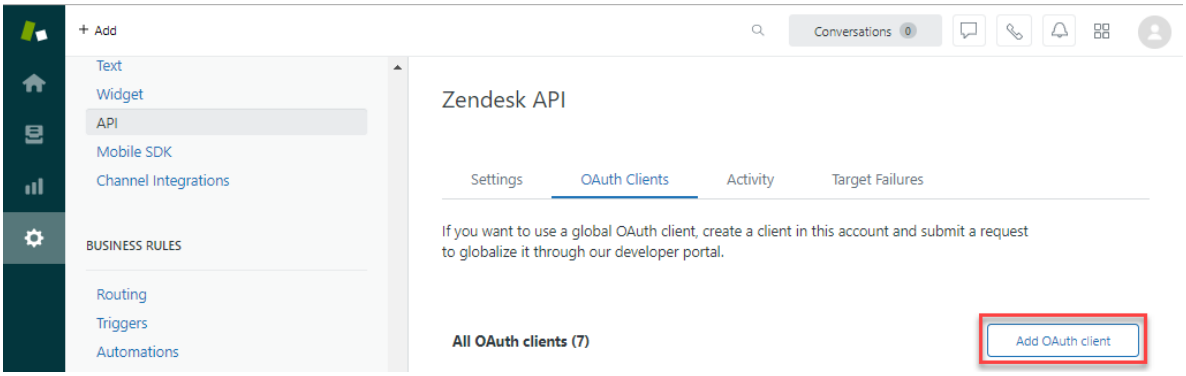
Update Zendesk Account

Step 1: Create Zendesk OAuth Client

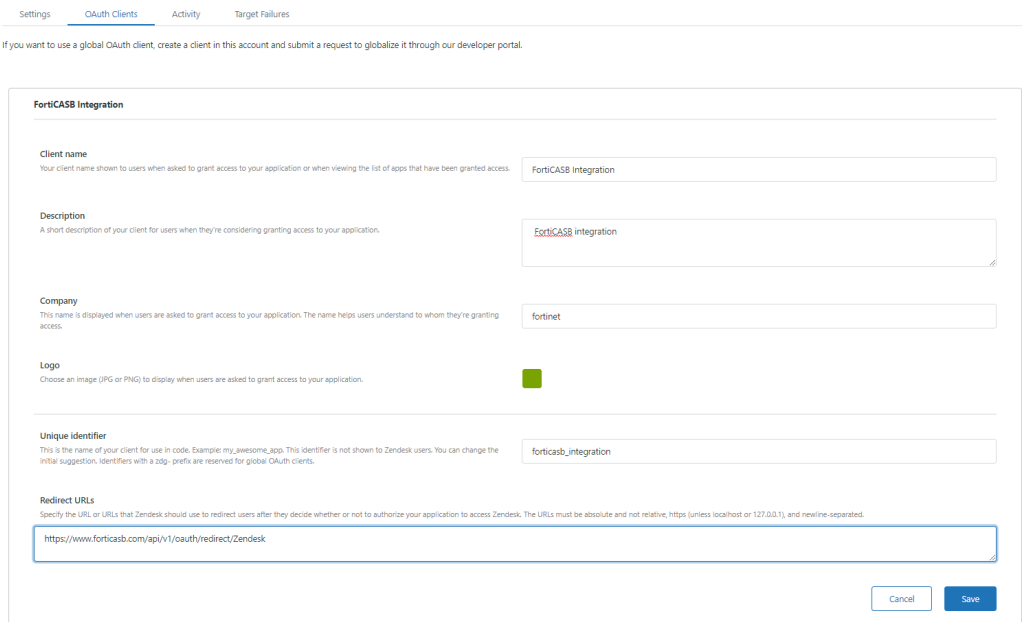
1. Log into Zendesk with your sub-domain, and then with your admin account.



2. In the left navigation pane, click **Admin**  , scroll down to **Channels**, and click on **API**.
3. In **Zendesk API** page, select **OAuth Clients** tab, then click **Add OAuth client**.



4. Fill in a **Client Name** of your choice, **Short Description**, and an **Unique Identifier** which should be populated automatically. Keep a record of the unique identifier for use later.



5. In **Redirect URLs**, use one of the corresponding redirect url provided by FortiCASB:

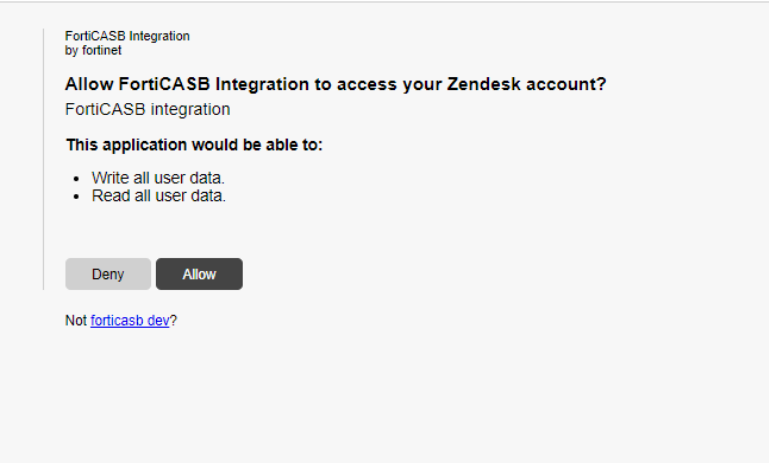
Region	Redirect URL
Global Region	https://www.forticasb.com/api/v1/oauth/redirect/Zendesk
European Union Region	https://eu.forticasb.com/api/v1/oauth/redirect/Zendesk

6. Click **Save**, and then in **Secret** field, click **Generate** to generate the secret token.
   Note:Make sure to copy down the secret token as it will only appear once.

Now go back to **FortiCASB** to add the Zendesk account.

Step 2: Update Zendesk Account

1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**.
3. Click on the Zendesk account menu, and select **Update Cloud Account**.
4. Fill in the Zendesk **Sub-Domain**, **Unique Identifier**, and the **Secret Token** saved from earlier, and click **Update Zendesk Account**.
5. You will be prompt to authorize FortiCASB to access to your Zendesk account, click **Allow** to complete adding the Zendesk account.



6. Wait 15 minutes to complete updating the Zendesk account to FortiCASB.

Zoom

FortiCASB offers an API-based approach, pulling data directly from Zoom via RESTful API. Then FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. Subsequently, FortiCASB combines these data to monitor and track Zoom user activities, provides DLP Data Analysis for files shared through Zoom.

Prerequisites

Make sure the Zoom account plan that will be used on FortiCASB is **Pro**, **Business**, **Business Plus**, or **Enterprise** Zoom plans. Free plan is NOT supported.

The Zoom account user to be added on FortiCASB must be the **Account Owner** or **Admin** of the Zoom account.

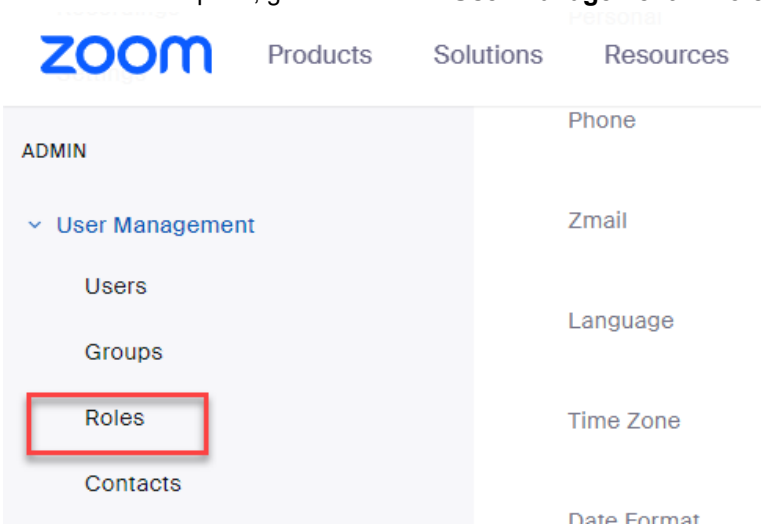
Add Zoom Account Steps

Configure Zoom Account Configuration on page 261

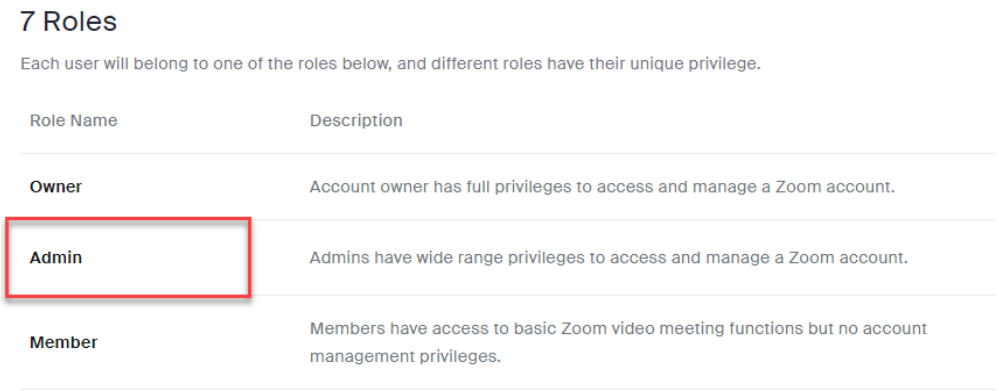
Create OAuth App on Zoom Account on page 262

Configure Zoom Account Configuration

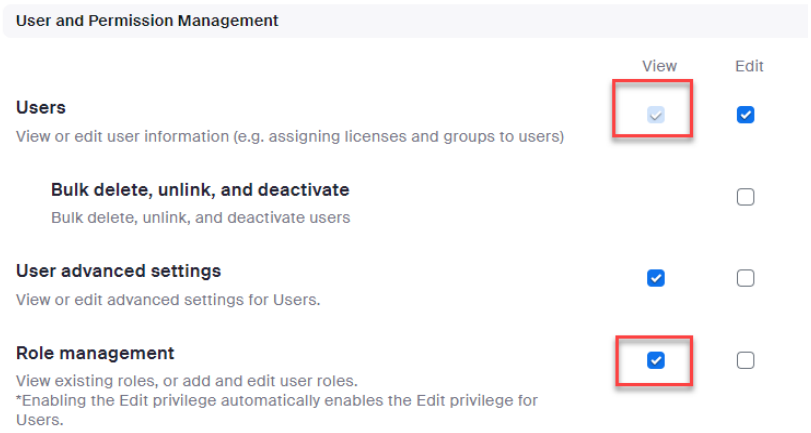
1. Log into Zoom as the **Account Owner** or **Admin**.
2. In the left control pane, go to **ADMIN > User Management > Roles**



3. In **Admin** Role section, click on the icon for Admin Role Settings.

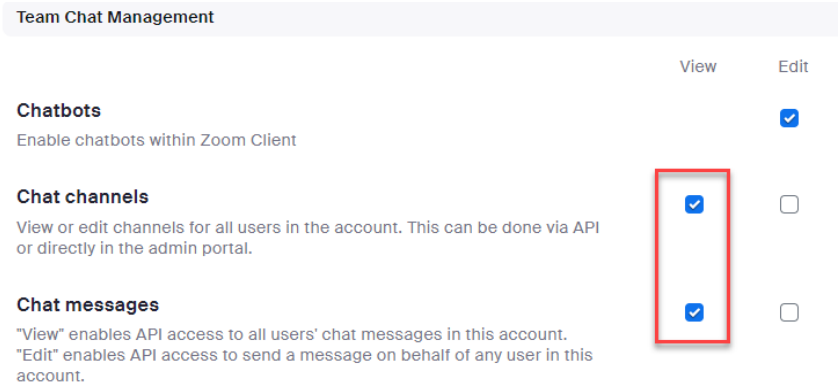


4. In **Role Settings** tab, make sure the settings below are checked:
   User and Permission Management
   - **Users**: View
   - **Role management**: View



Team Chat Management

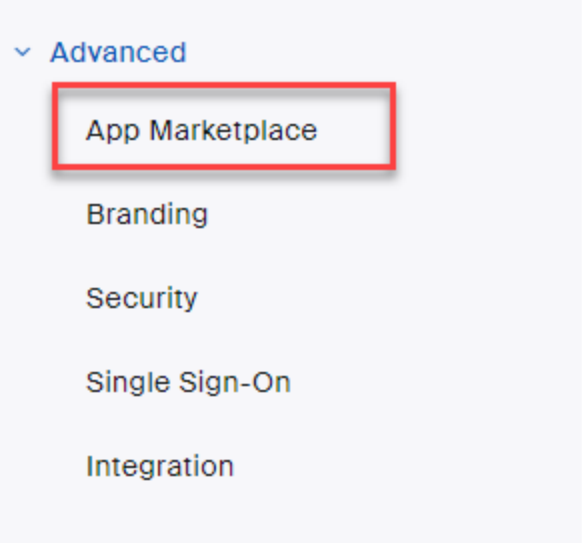
- **Chat Channels**: View
- **Chat messages**: View



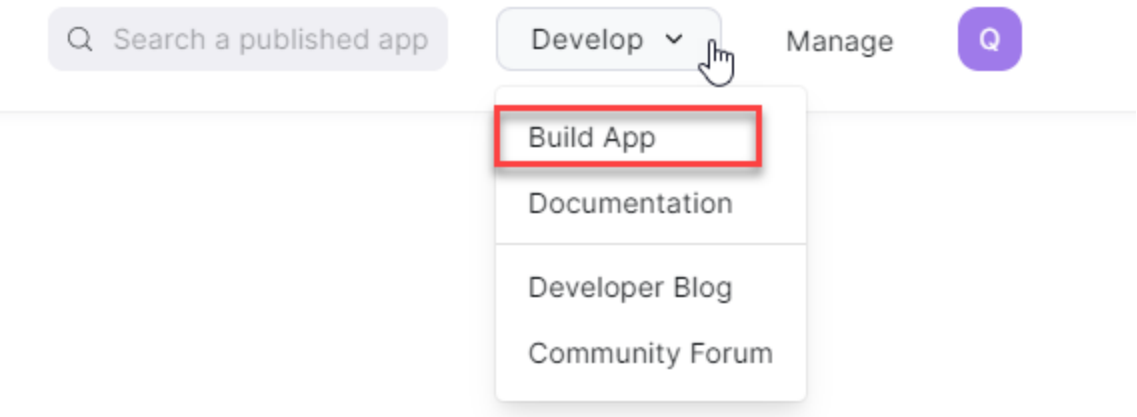
Continue to Create OAuth App on Zoom Account on page 262

Create OAuth App on Zoom Account

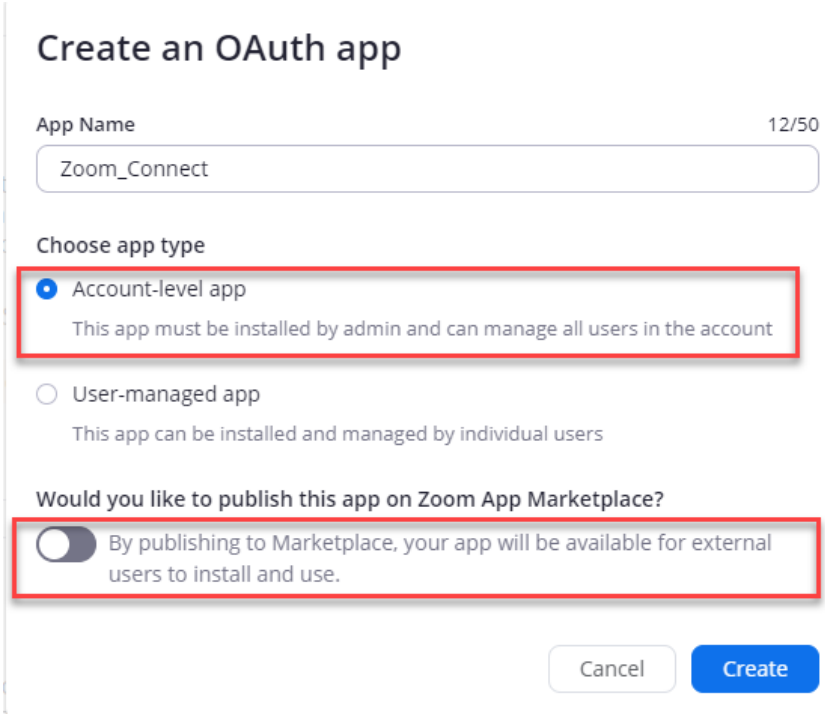
1. Log into Zoom as the **Account Owner** or **Admin**. (Same account as from Part 1)
2. In the left control pane, go to **ADMIN > Advanced > App Marketplace**, you will be re-directed to App Marketplace.



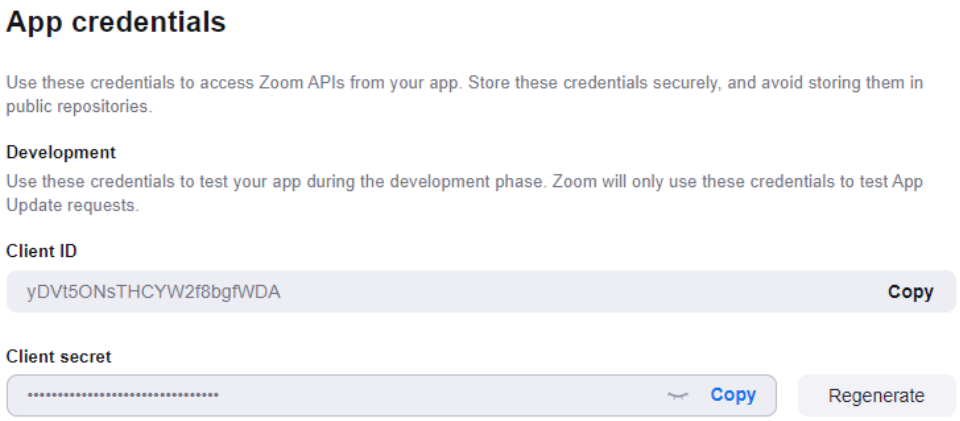
3. In App Marketplace, on the top right hand corner, click **Develop** drop down menu, and select **Build App**.



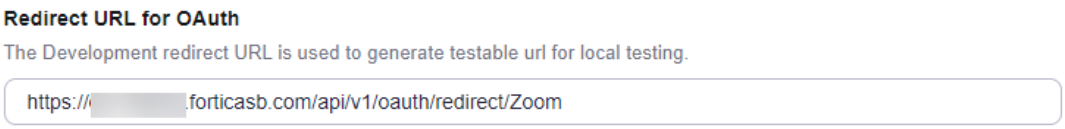
4. Select **OAuth** app type and click **Create**.
5. Enter an App name of your preference,
   a. Select **Account-level** app, and
   b. Uncheck the option to publish the app on Zoom App Marketplace, and click **Create**.



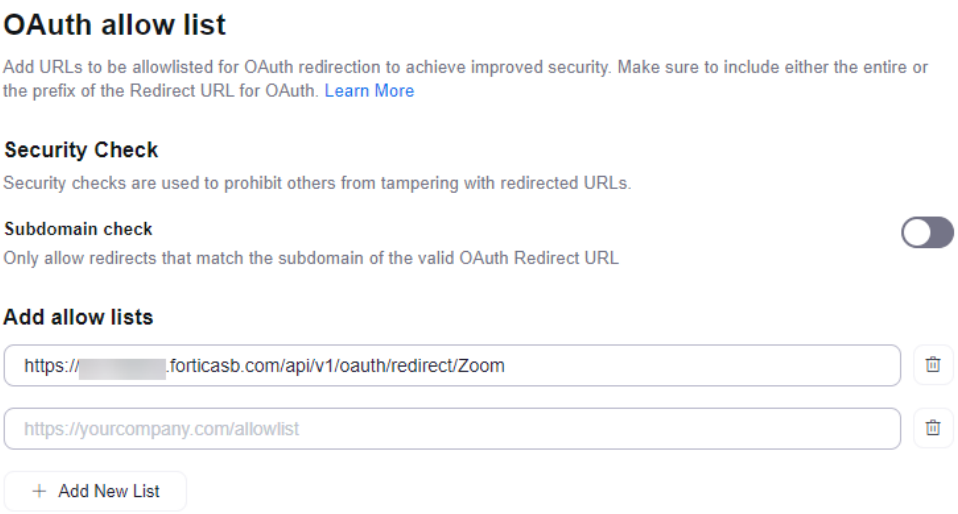
6. In **App Credentials**, keep a record of the **Client ID** and **Client Secret**.



7. Copy the **Redirect URL for OAuth** from FortiCASB **Add Zoom Account page** and paste it to **Redirect URL for OAuth** field.

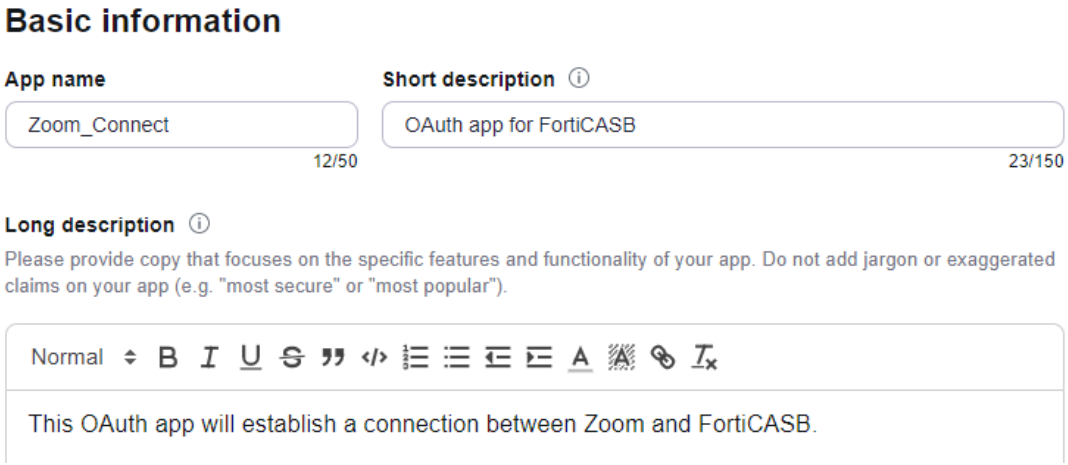


8. Scroll down to **OAuth allow list**, add the same redirect URL to the **Add allow list**, then click **Continue**.

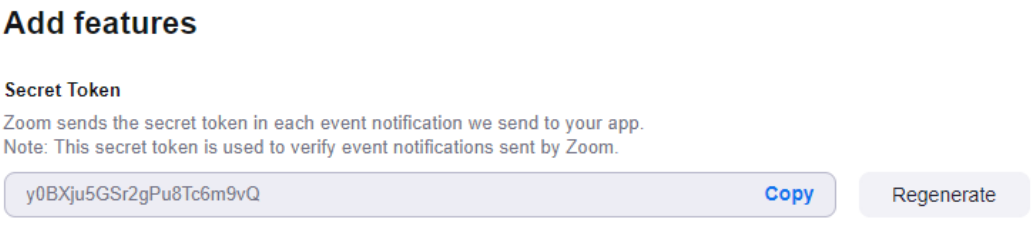


9. Fill in the following information:
   a. In **Basic Information**, fill in **Short Description**, **Long Description**, and **Company Name**.
   b. In **Developer Contact Information**, fill in **Name** and **E-Mail Address**.
   c. Click **Continue**

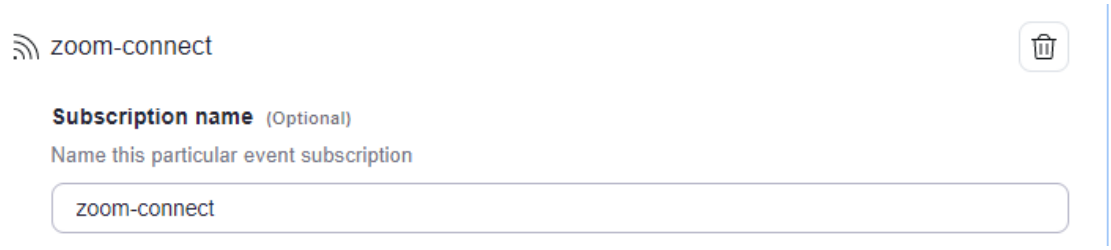
   (Note: the app cannot be created without filling out these information)



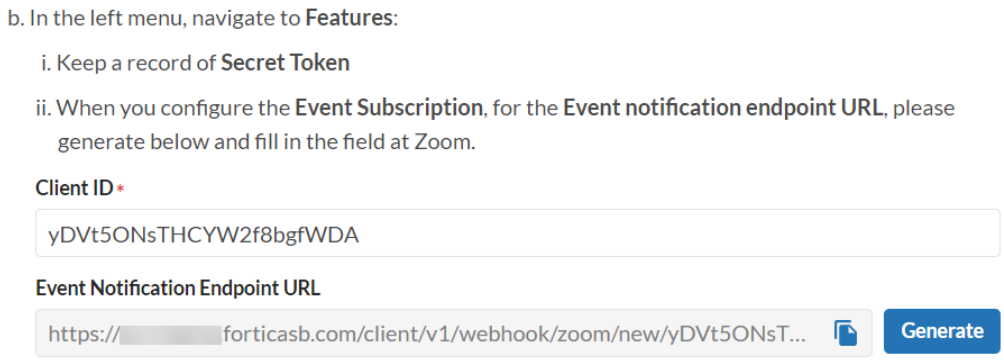
10. In **Add Feature**, keep a record of the **Secret Token**.



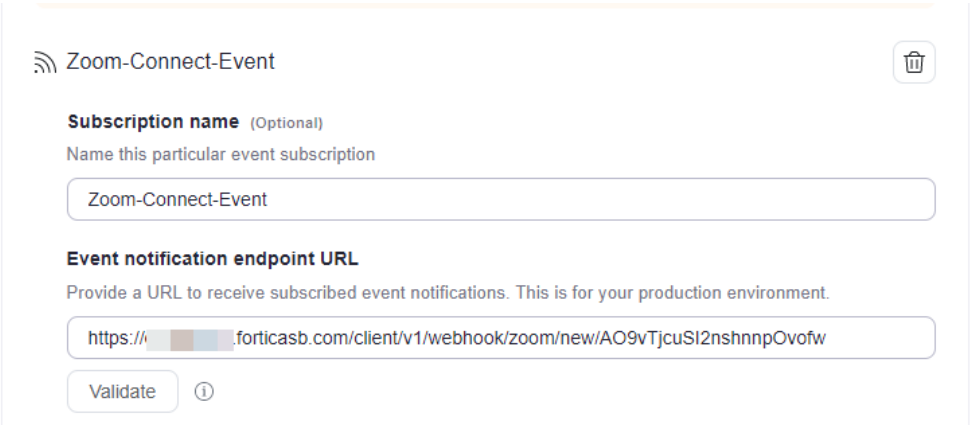
11. Turn on **Event Subscription**, then click
    a. **+Add new subscription**, fill in a **Subscription Name**.



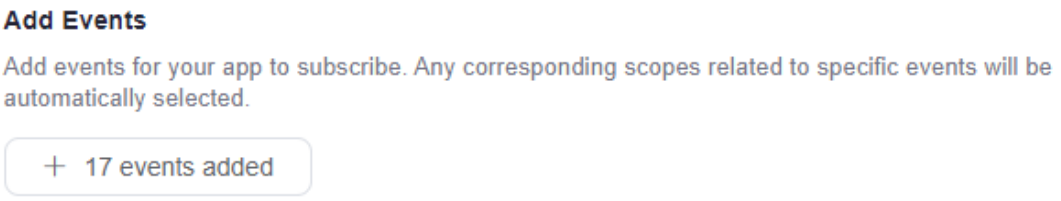
    b. Go back to **FortiCASB Add Zoom Account** page, paste the client ID recorded earlier in the **Client ID** field, and click **Generate** to generate **Event Notification Endpoint URL**.



    c. Copy the endpoint URL and paste it in **Zoom Event notification endpoint URL** and click **Validate**.

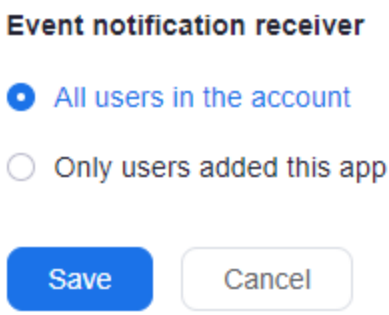


12. In **Add Events**, click on **+Add Events** on Zoom and add the event types below, and click **Done**.



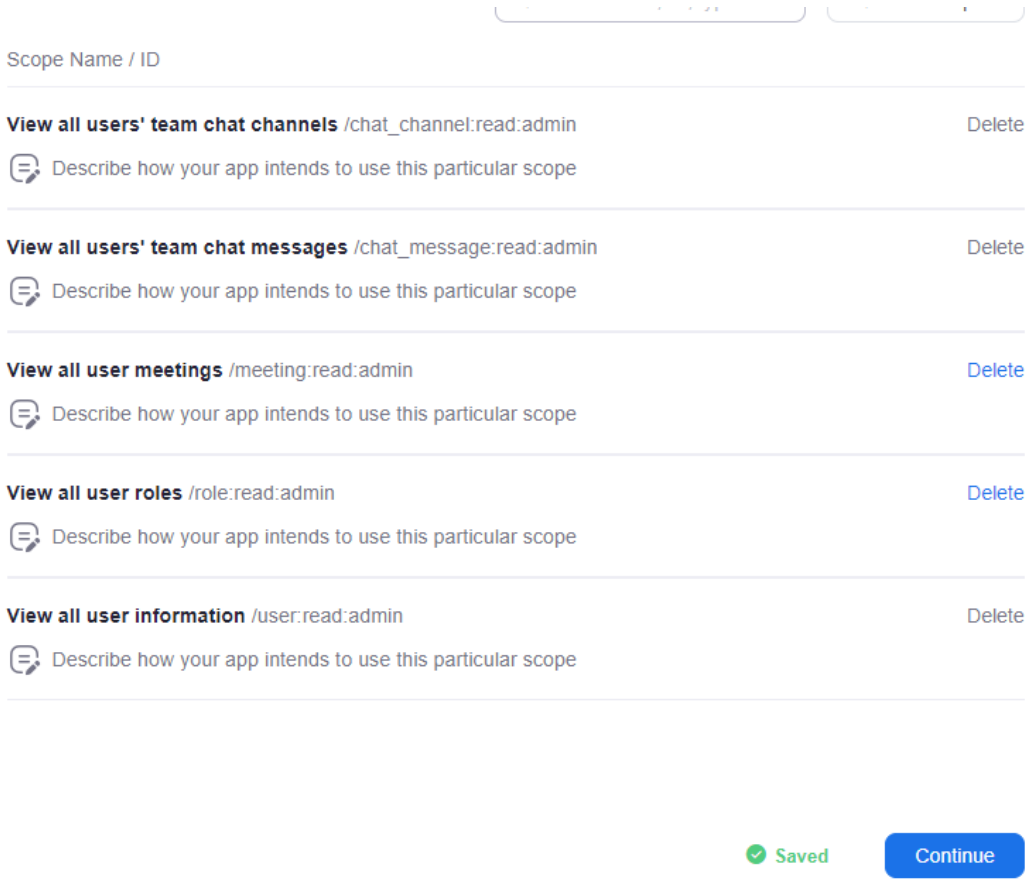
User	User Activity	Chat Channel	Chat Message
User has been created	User has signed in	Chat Channel Created	Chat Message Sent
User has been disassociated	User has signed out	Chat Channel Deleted	Chat Message Updated
User has been deleted		Member Removed	Chat Message Deleted
User has been activated		Member Left	Chat Message Replied
User has been deactivated			
User has accepted the account invitation			
User's profile info has been updated			

13. In **Event notification receiver**, make sure **All users in the account** is selected. Then click **Save** to save the Event Subscription.

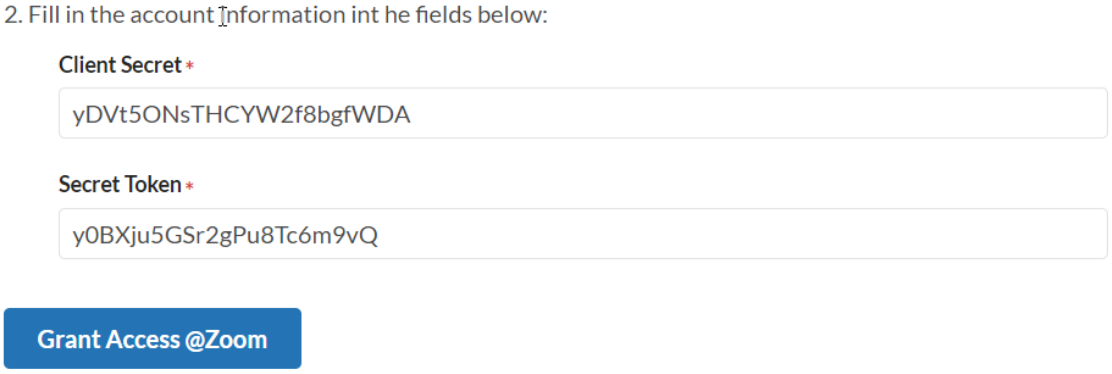


14. Click **Continue** to go to the **Scopes** page.
15. In **Add Scopes** page, click **+Add Scopes**, then add the following scopes and click **Continue**.

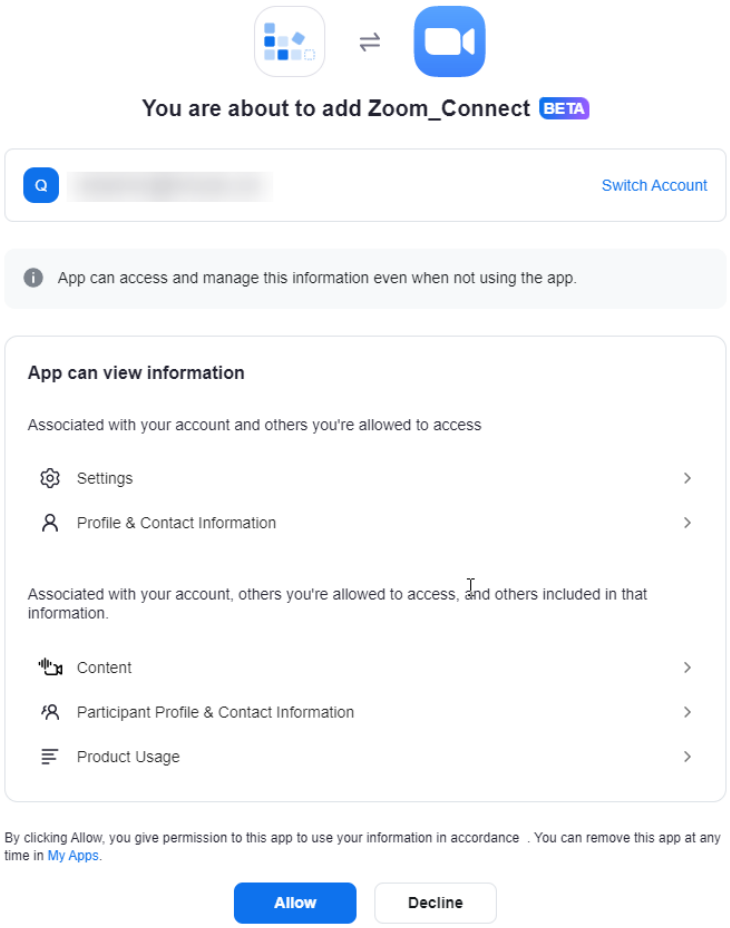
Scope Type	Scope
User	View all user information/user:read:admin
Team Chat	View all users' team chat channels/chat_channel:read:admin View all users' team chat messages/chat_message:read:admin
Role	View all user roles/role:read:admin



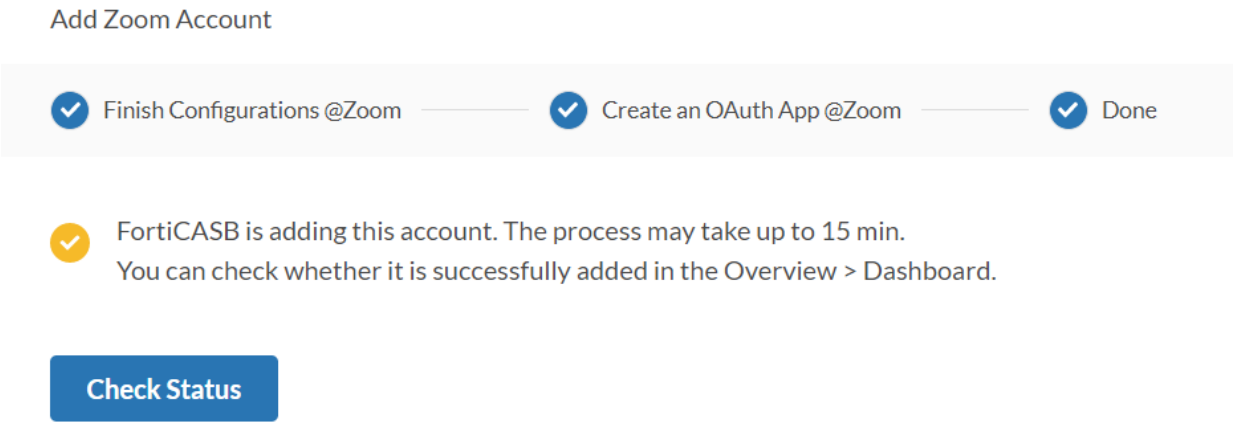
16. Now Go back to FortiCASB **Add Zoom Account** Page, fill in the Zoom **Client Secret** and the **Secret Token** from earlier, then click **Grant Access @Zoom**.



17. You will be re-directed to Zoom OAuth authorization page to authorize sharing user information with FortiCASB. Click **Allow** to authorize the sharing of information and be re-directed back to FortiCASB.



The add account process is completed, please wait 15 minutes and check on the status of the account.



Update Zoom Account

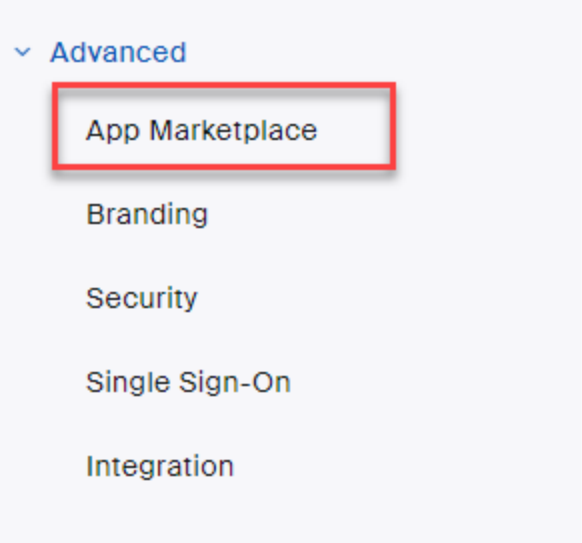
Before updating the Zoom account on FortiCASB, complete the same configurations using the same Zoom account:

Configure Zoom Account Configuration on page 261

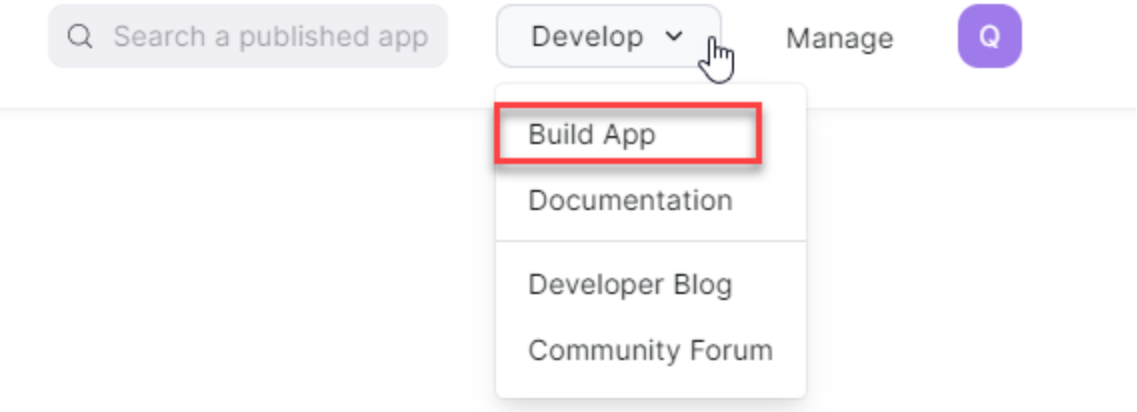
After the Zoom configuration is completed, follow these steps to update your Zoom account on FortiCASB

Create OAuth App on Zoom Account

1. Log into Zoom as the **Account Owner** or **Admin**. (Same account as from Part 1)
2. In the left control pane, go to **ADMIN > Advanced > App Marketplace**, you will be re-directed to App Marketplace.

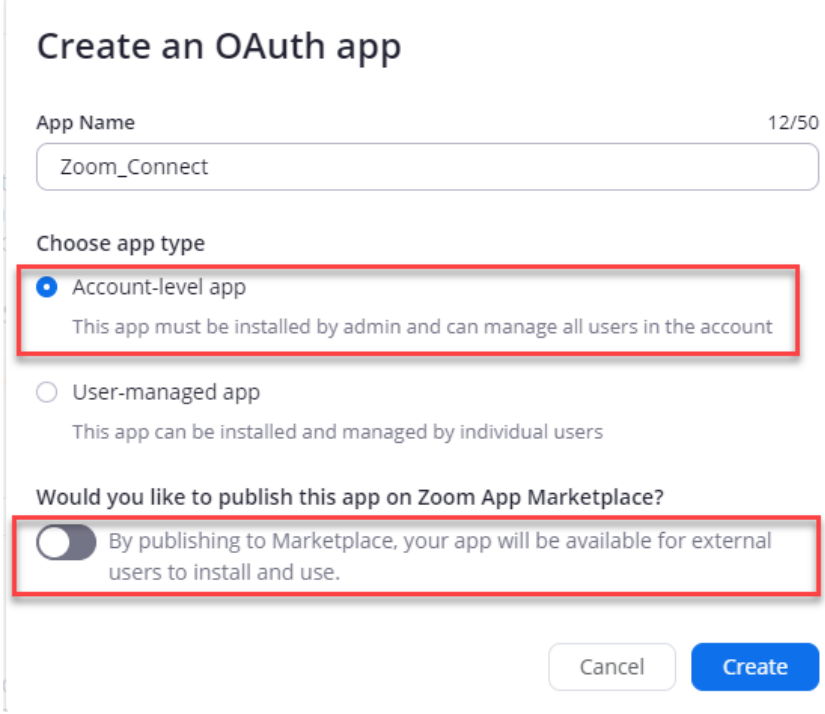


3. In App Marketplace, on the top right hand corner, click **Develop** drop down menu, and select **Build App**.

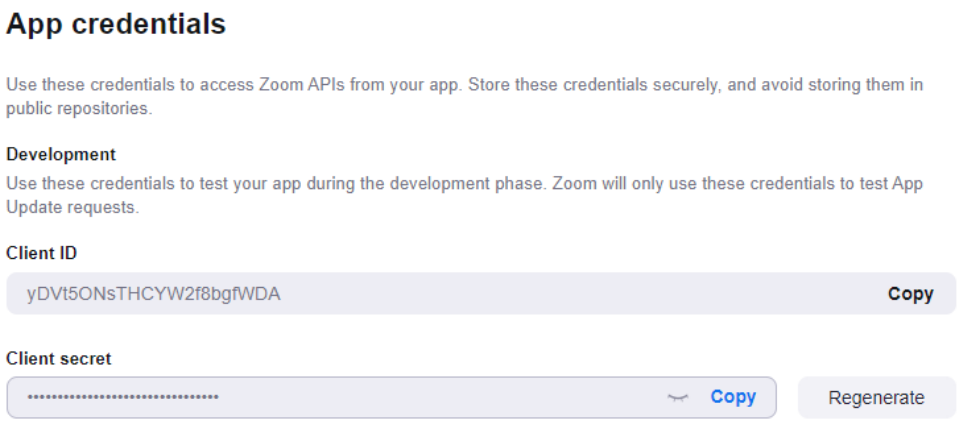


4. Select **OAuth** app type and click **Create**.

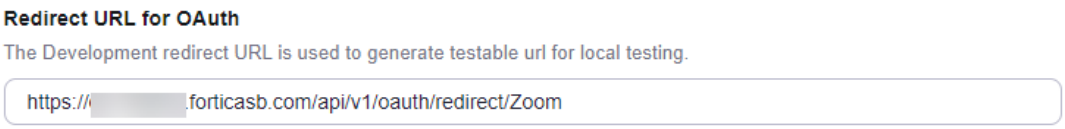
5. Enter an App name of your preference,
   a. Select **Account-level** app, and
   b. Uncheck the option to publish the app on Zoom App Marketplace, and click **Create**.



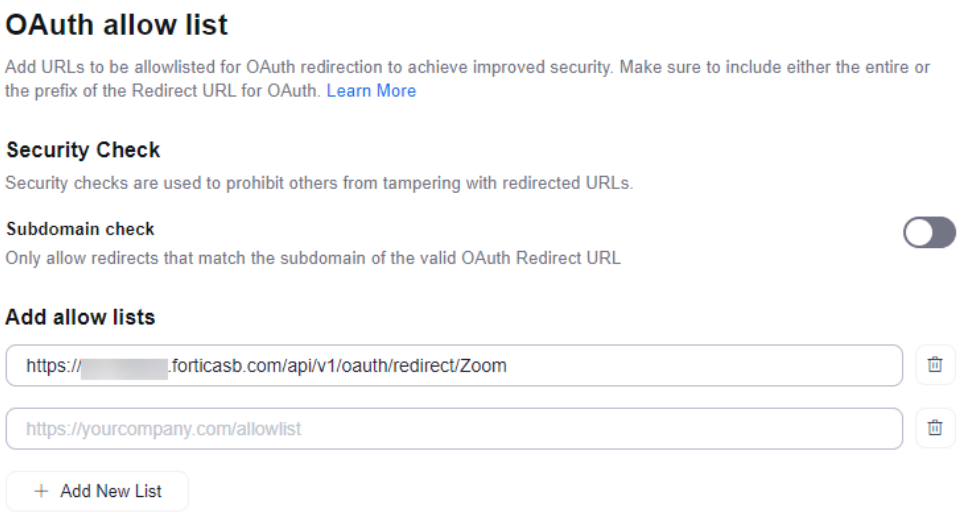
6. In **App Credentials**, keep a record of the **Client ID** and **Client Secret**.



7. Copy the **Redirect URL for OAuth** from FortiCASB **Update Zoom Account page** and paste it to **Redirect URL for OAuth** field.

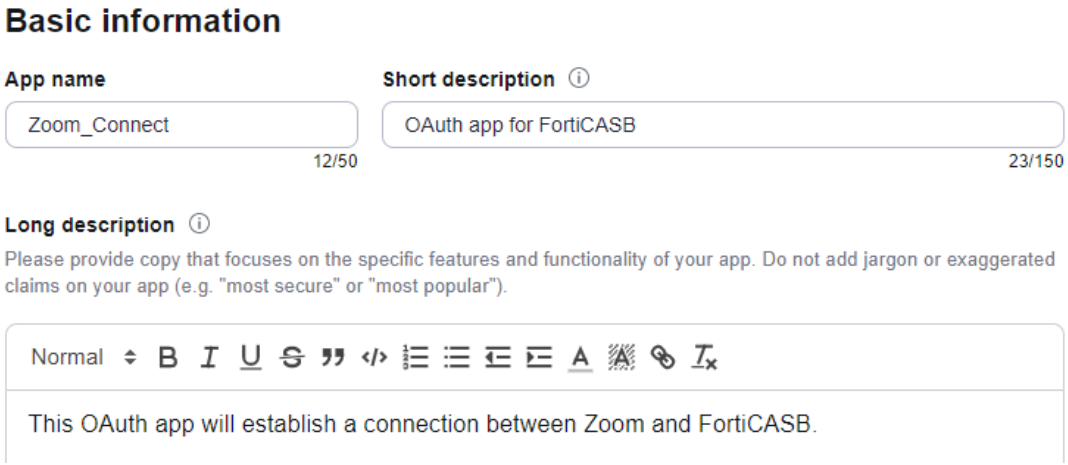


8. Scroll down to **OAuth allow list**, add the same redirect URL to the **Add allow list**, then click **Continue**.

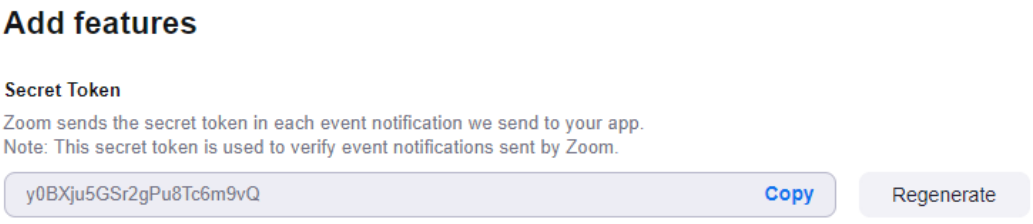


9. Fill in the following information:
   a. In **Basic Information**, fill in **Short Description**, **Long Description**, and **Company Name**.
   b. In **Developer Contact Information**, fill in **Name** and **E-Mail Address**.
   c. Click **Continue**

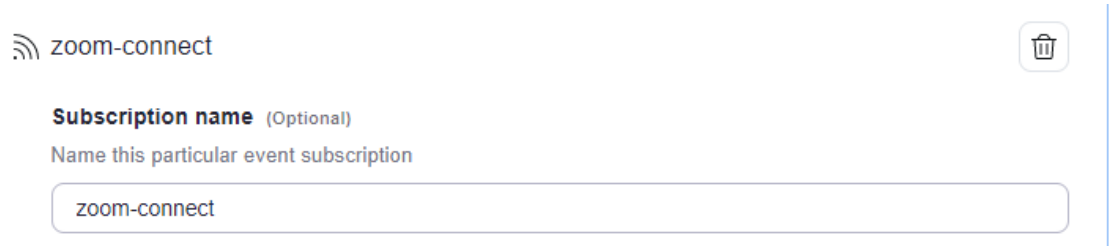
   (Note: the app cannot be created without filling out these information)



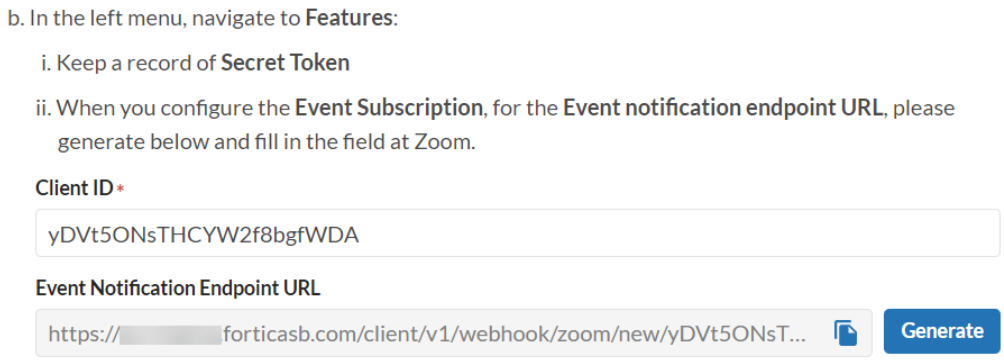
10. In **Add Feature**, keep a record of the **Secret Token**.



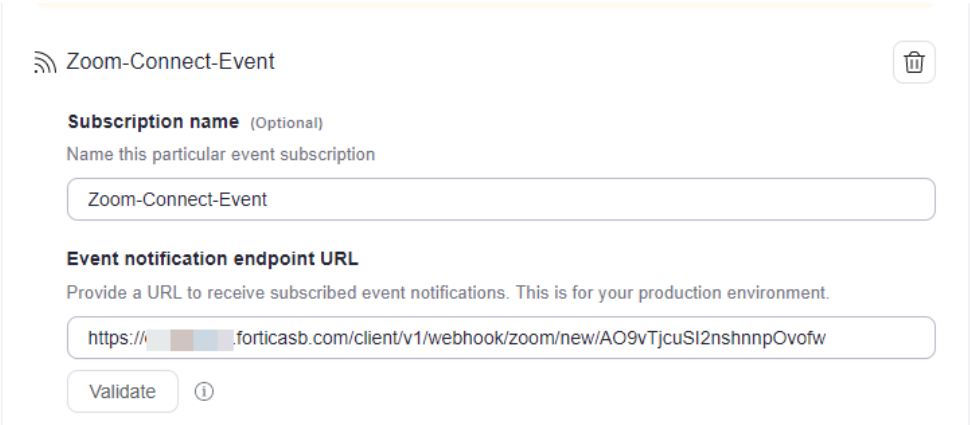
11. Turn on **Event Subscription**, then click
    a. **+Add new subscription**, fill in a **Subscription Name**.



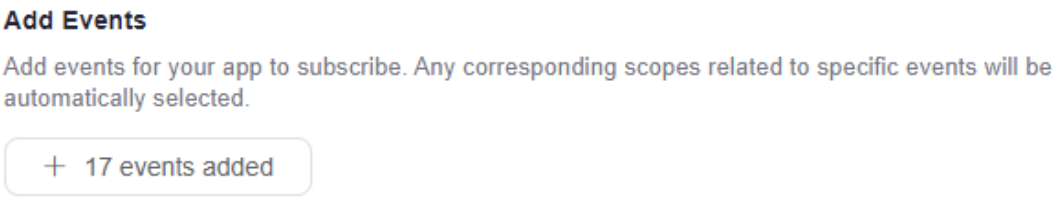
    b. Go back to **FortiCASBUpdate Zoom Account** page, paste the client ID recorded earlier in the **Client ID** field, and click **Generate** to generate **Event Notification Endpoint URL**.



    c. Copy the endpoint URL and paste it in **Zoom Event notification endpoint URL** and click **Validate**.

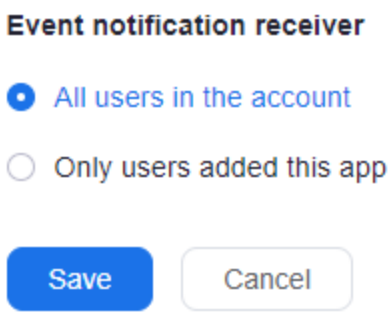


12. In **Add Events**, click on **+Add Events** on Zoom and add the event types below, and click **Done**.



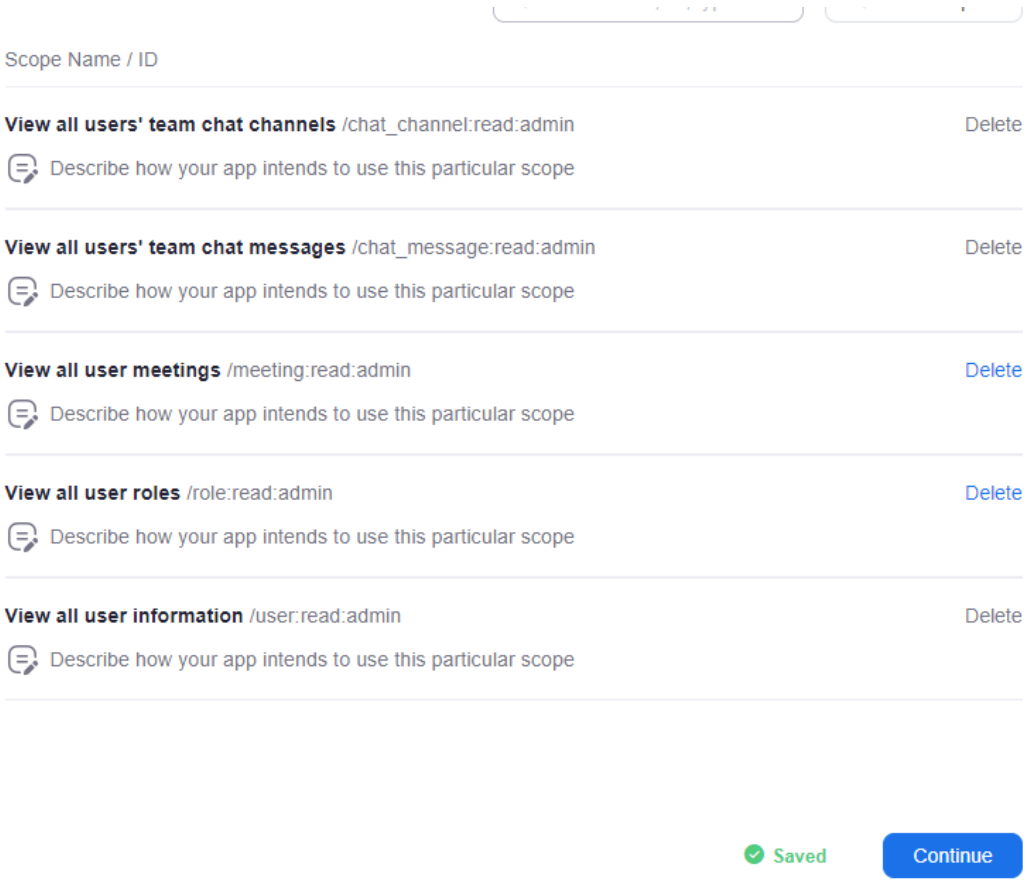
User	User Activity	Chat Channel	Chat Message
User has been created	User has signed in	Chat Channel Created	Chat Message Sent
User has been disassociated	User has signed out	Chat Channel Deleted	Chat Message Updated
User has been deleted		Member Removed	Chat Message Deleted
User has been activated		Member Left	Chat Message Replied
User has been deactivated			
User has accepted the account invitation			
User's profile info has been updated			

13. In **Event notification receiver**, make sure **All users in the account** is selected. Then click **Save** to save the Event Subscription.

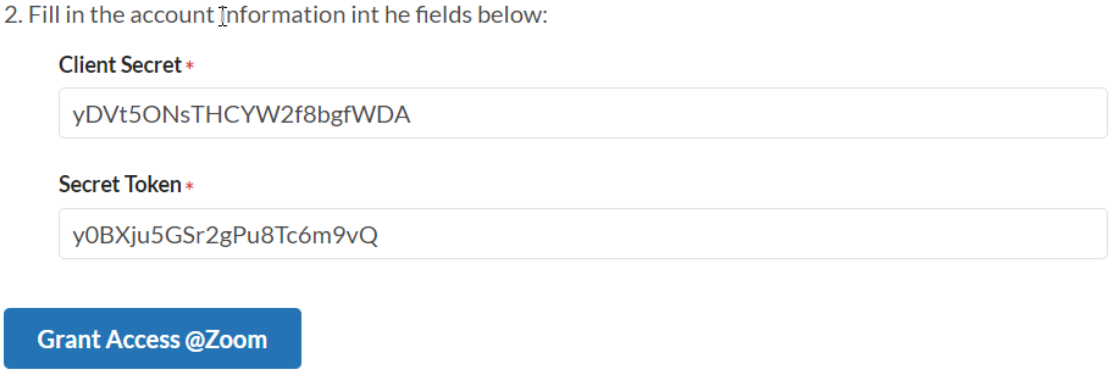


14. Click **Continue** to go to the **Scopes** page.
15. In **Add Scopes** page, click **+Add Scopes**, then add the following scopes and click **Continue**.

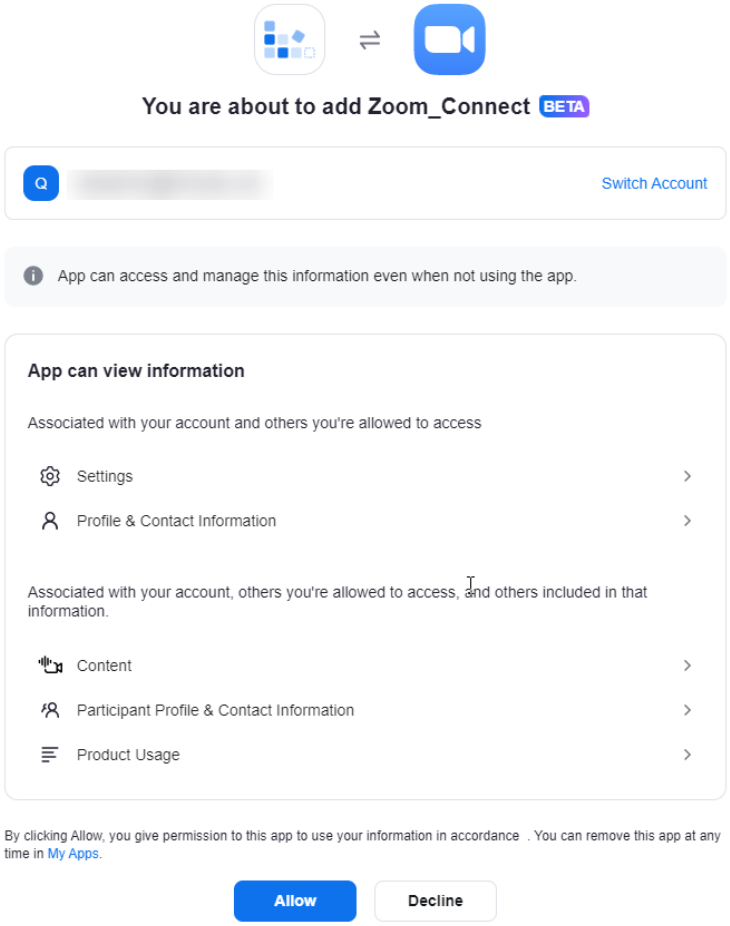
Scope Type	Scope
User	View all user information/user:read:admin
Team Chat	View all users' team chat channels/chat_channel:read:admin View all users' team chat messages/chat_message:read:admin
Role	View all user roles/role:read:admin



16. Now Go back to FortiCASB **Update Zoom Account** Page, fill in the Zoom **Client Secret** and the **Secret Token** from earlier, then click **Grant Access @Zoom**.



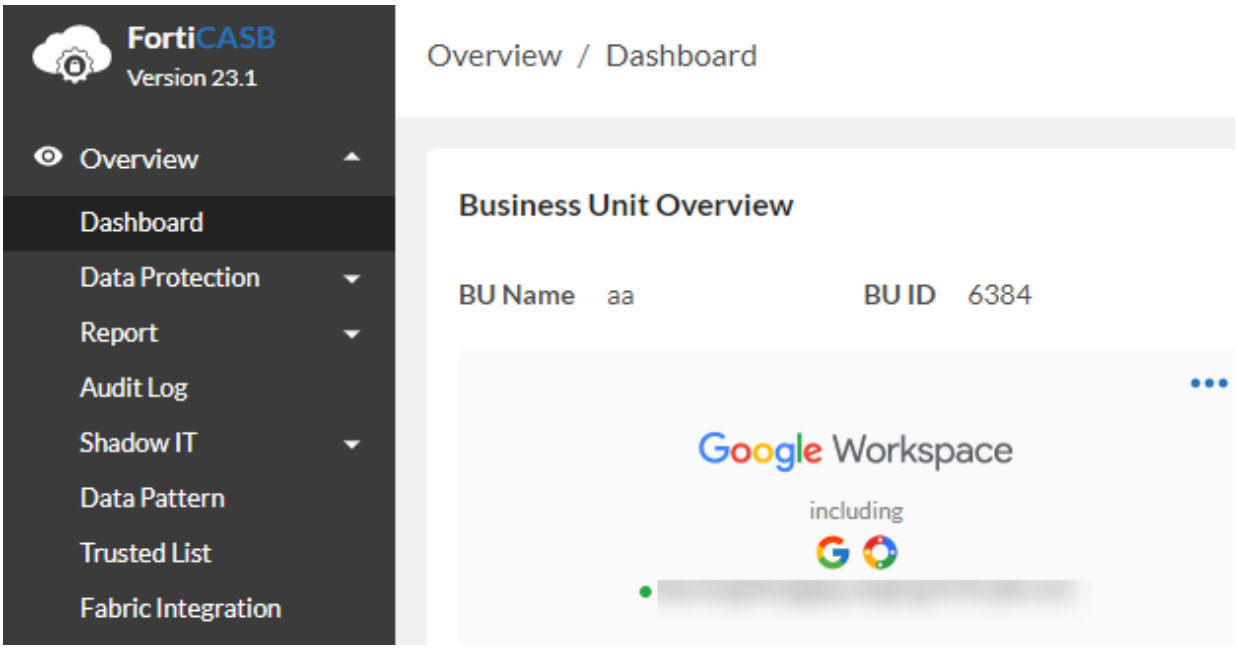
17. You will be re-directed to Zoom OAuth authorization page to authorize sharing user information with FortiCASB. Click **Allow** to authorize the sharing of information and be re-directed back to FortiCASB.



The update account process is completed, please wait 15 minutes and check on the status of the account.

Overview Features

This section covers general operations and **Overview** features in FortiCASB.



Overview features are features not specific to cloud accounts. They are features that incorporate data collected from cloud accounts onboard in FortiCASB.

Overview Topics

Activate and Generate Reports on page 280

View FortiCASB Audit logs on page 290

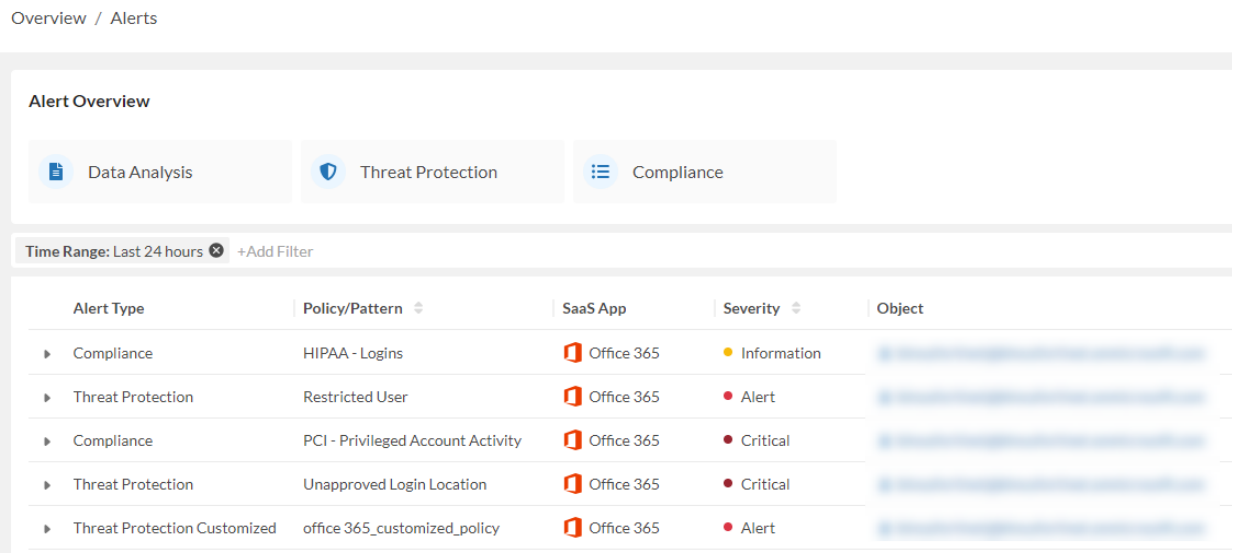
Shadow IT Discovery Configurations

App Events Supported by FortiCASB on page 307

Fabric Integration Configuration on page 325

Global Alert

Global Alert is located in **Overview > Alert** page. Global Alert combines all alerts from all supported cloud applications onboard in one single view.



Alert Types

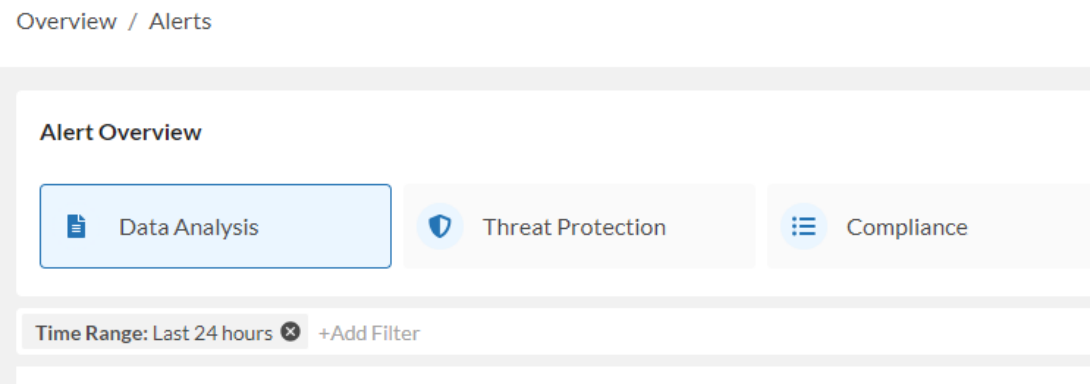
Alert Types - There are 3 types of alerts, **Data Analysis**, **Threat Protection**, and **Compliance**

Data Analysis alerts are alerts generated by Data Security Policies created in **Data Protection > Policies > Data Policies**.

Threat Protection alerts are alerts generated by Threat Protection policies. For Threat Protection policy configuration, click on the cloud application account and go to **Policy > Threat Protection**. For more details see Threat Protection on page 403

Compliance alerts are alerts generated by Compliance policies. For Compliance policy configuration, click on the cloud application account and go to **Policy > Compliance**. For more details see Compliance Policy on page 404.

Click on any of the three types of alerts to filter the alert type.

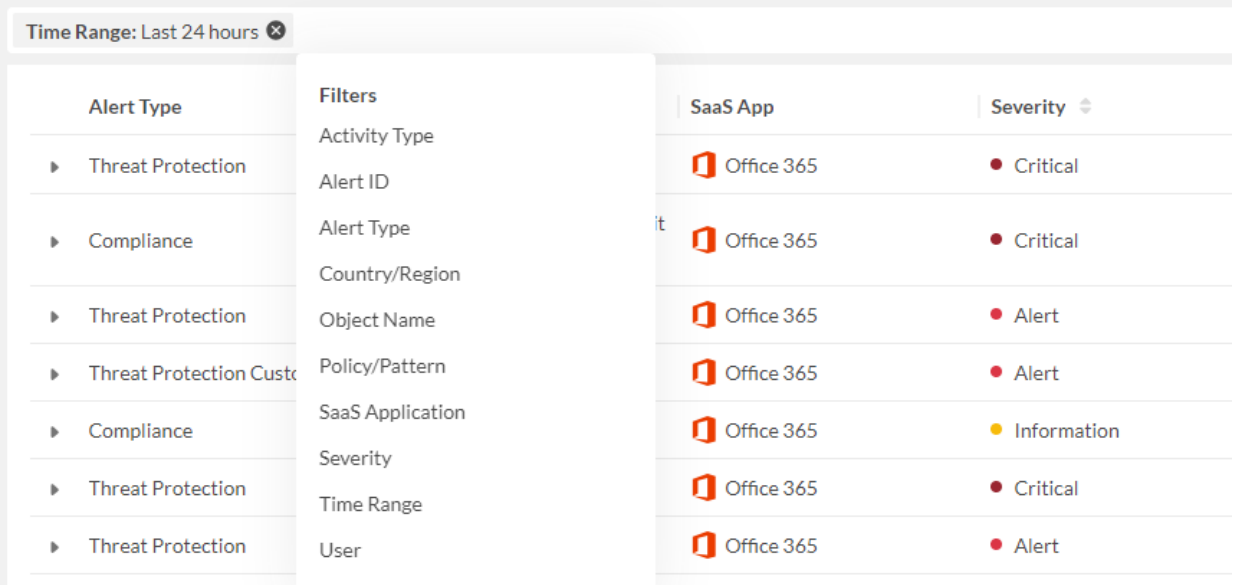


Threat Protection and **Compliance** policies only support the following cloud applications:

Cloud Applications
Salesforce
Office 365
Box
Dropbox
Confluence
Egnyte
GitHub
Jira
SAP IAS
ServiceNow
Webex Teams
Zoom

Alert Filters

Click on **+Add Filter** to filter the alerts by different types of alert attributes, then click search button to filter.



Activity Type - filter alerts by the specific cloud application account activity.

Policy/Patterns - filter alerts by the specific policy of the cloud application account.

Alert ID - each alert has its own specific alert ID.

SaaS application - filter alerts by the cloud application account. For example, when Office 365 is selected, only Office 365 alerts are shown.

Activate and Generate Reports

FortiCASB allows you to generate **C-level**, **Compliance**, and **Shadow IT reports**.

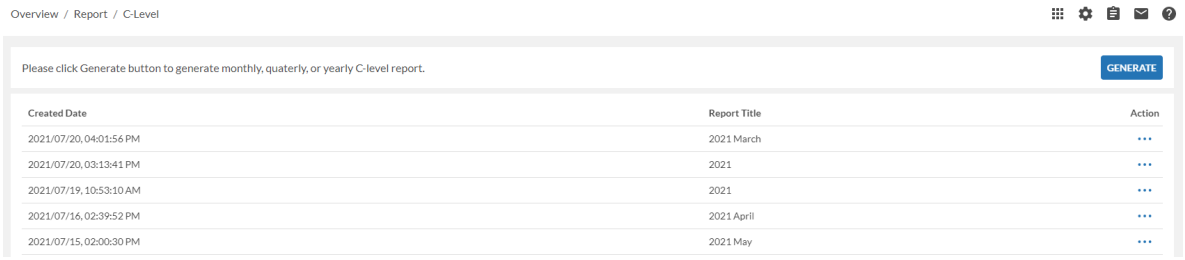
C-Level reports are quarterly, monthly, or annual reports.

Compliance reports give an overview of overall compliance with policies such as HIPAA, SOX/COBIT, and PCI.

Shadow IT reports highlight unsanctioned application usage.

Generate C-Level Report

1. Go to **Overview > Report > C-Level** from FortiCASB left navigation pane.
2. Click **Generate** to generate C-Level Report
3. Choose a **Type** (Yearly, Quarterly, or Monthly Report), select the **Year**, then click **Generate C-Level Report**.
4. After the report is generated, it will be available under the **Action** column, click ••• to download the report.



Generate Compliance Report

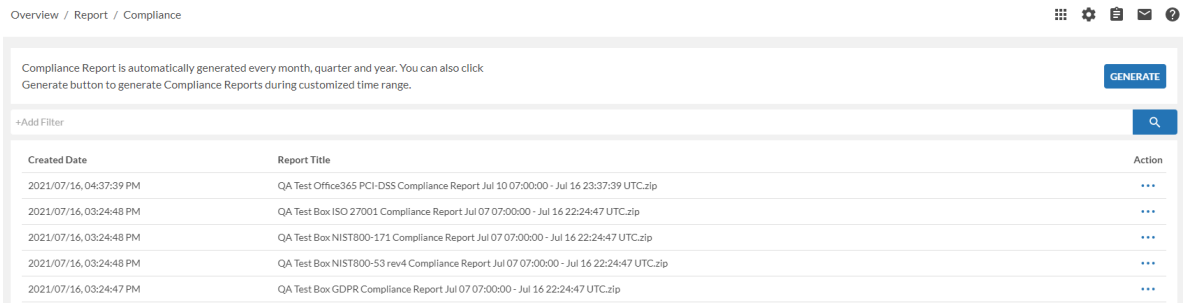
Compliance report are automatically generated monthly, quarterly, and yearly. You may also customized a time frame to generate compliance reports. HIPAA, GDPR, SOX-COBIT, and PCI-DSS are generated in zip format while ISO 27001 and NIST800 reports are in PDF. Click on the action icon ••• to download the report.

The prerequisite to generate Compliance report is to enable and configure Compliance Policies required by your organization. For more details on configuring Compliance policies, please refer to **Policy Configuration on page 405**.

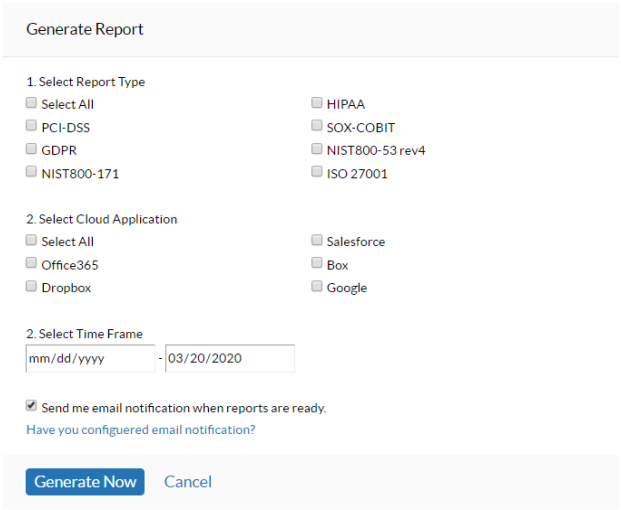
Customized Compliance Report

After you have enabled Compliance Policies, follow the steps below to generate Compliance report.

1. Go to **Overview > Report > Compliance** from FortiCASB navigation pane, Click on **Generate** to generate Compliance Report.



2. Select a **Report Type**, then select a **Cloud Application** (Office 365, Google Workspace etc.)



3. Select a **Time Frame** that is within 90 days from today.
4. Click **Generate Now** to generate the report.
5. The report will be generated with your user name, cloud application, report type, and date range as the file title.
   For example, an Office 365 PCI compliance report with a date range of 3/1/2020 to 3/14/2020 will be " 'User Name' Office 365 PCI Compliance Report Mar 14 00:00:00 - Mar 14 23:59:59 UTC.zip".

Activate Alert Report

Alert Report keeps track of all daily security alerts and lets you download daily security report. At the end of each month, all daily Alert report will be consolidated into one monthly report for download.

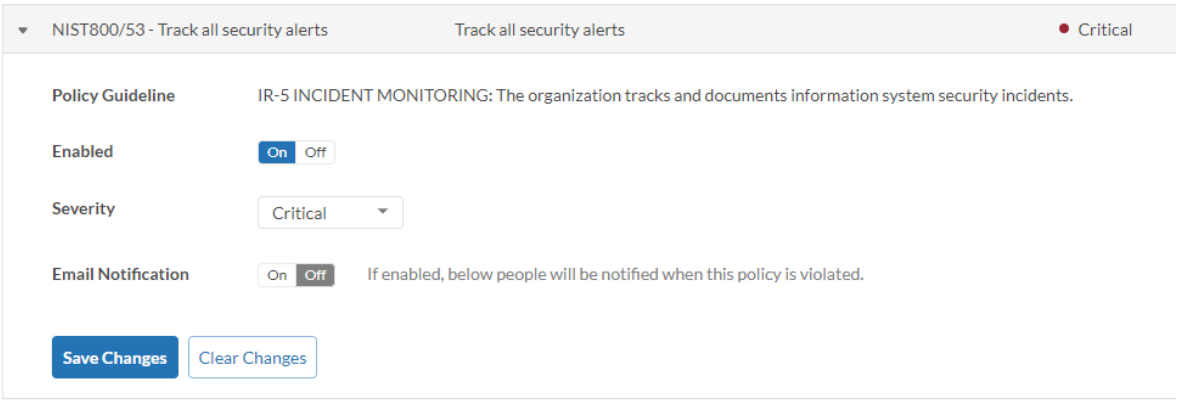
To enable Alert Report to export all daily security alerts, please enable any of the Compliance policies below to activate the feature:

- **NIST800/53** - Track all security alerts
- **NIST800/171** - Track all security alerts
- **ISO27001** - Track all security alerts

Note: only one policy from above needs to be enabled to activate Alert Report.

Activate Alert Report through NIST800/53

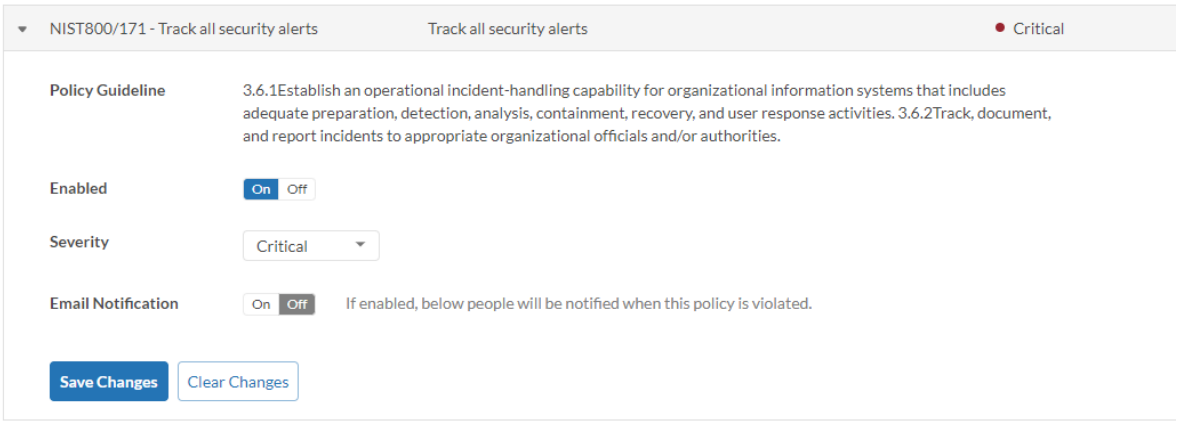
1. Click on the targeted cloud account. (**Salesforce**, **Office 365**, etc.) from FortiCASB navigation menu.
2. Go to **Policy > Compliance**, and click **NIST800-53 rev4** tab.
3. Locate the policy **NIST800/53 - Track all security alerts**.



4. Enable the policy by clicking the **On** button.

Activate Alert Report through NIST800/171

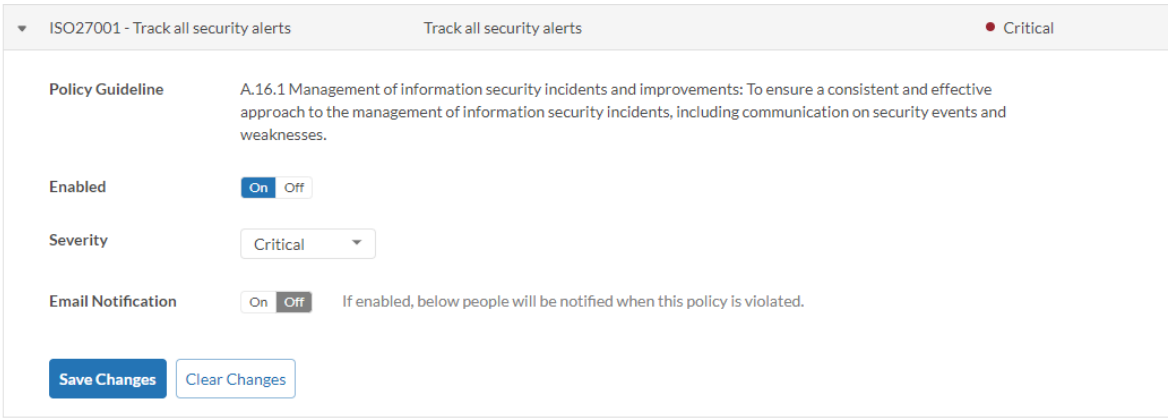
1. Click on the targeted cloud account. (**Salesforce**, **Office 365**, etc.) from FortiCASB navigation menu.
2. Go to **Policy > Compliance**, and click **NIST SP800-171** tab.
3. Locate the policy **NIST800/171 - Track all security alerts**.



4. Enable the policy by clicking the **On** button.

Activate Alert Report through ISO27001

1. Click on the targeted cloud account. (**Salesforce**, **Office 365**, etc.) from FortiCASB navigation menu.
2. Go to **Policy > Compliance**, and click **ISO 27001** tab.
3. Locate the policy **ISO27001 - Track all security alerts**.



4. Enable the policy by clicking the **On** button.

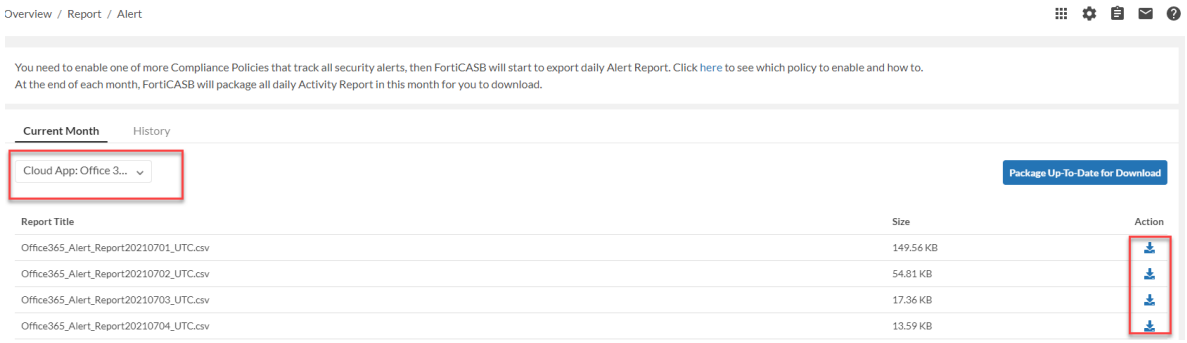
Generate Alert Report

Daily alert report is compiled into a CSV file and made available for export. At the end of each month, all daily reports of the that month are combined and packaged into a ZIP file and made available for download.

An alternative option of exporting daily reports is to consolidate up-to-date daily reports of the current month into one ZIP file.

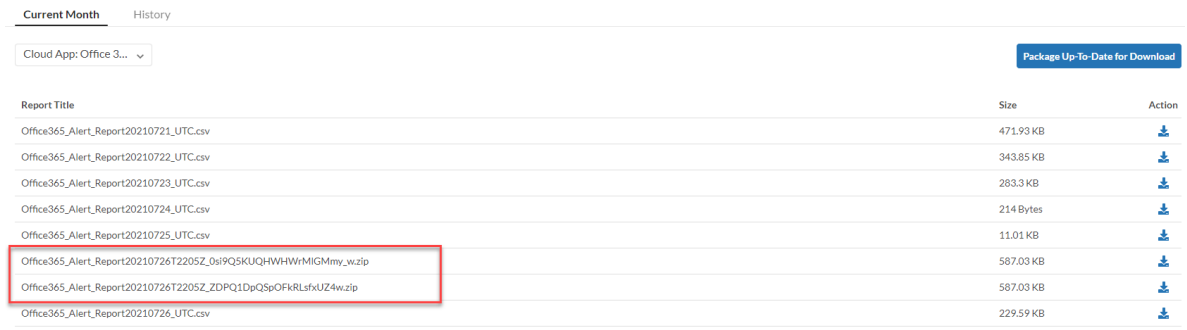
Export Reports

1. From FortiCASB navigation menu, go to **Overview > Report > Alert**.
2. In the **Current Month** tab, click the **Cloud App** drop down menu and select a cloud application (**Salesforce**, **Office 365**, etc.).



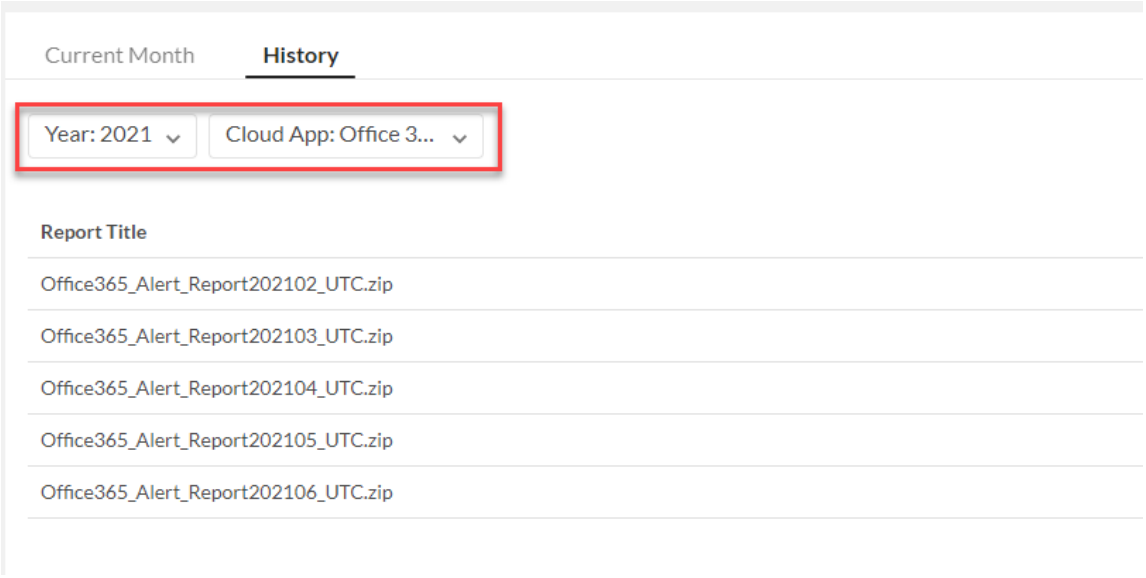
Option 1 - Select any of the daily report and click download button to download the daily report.

Option 2 - Click **Package Up-To-Date for Download** button to combine all up to date daily reports of the current month into one zip file. The combined ZIP file will be made available for download with .zip extension.



3. Click **History** tab to export monthly security alert reports. Click the **year** drop down menu to select year, and **Cloud App** drop down menu to select a cloud account, and all monthly security alert reports available

of that year will be available for export.



Activate Activity Report

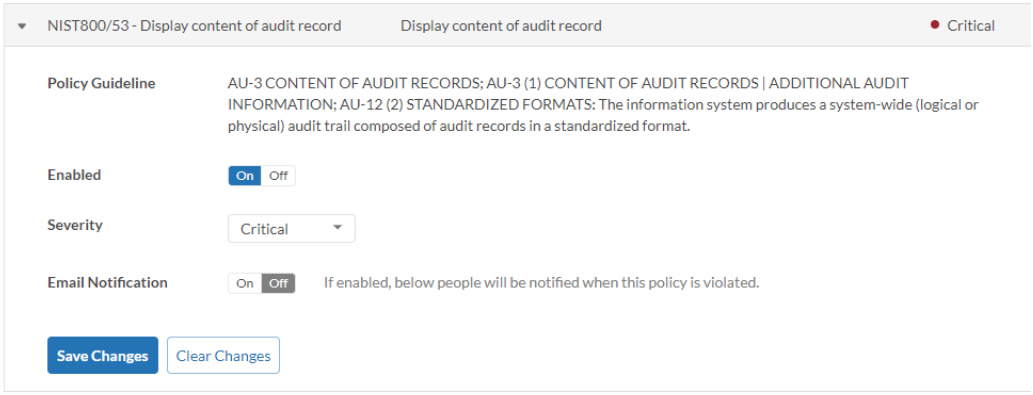
Activity Report keeps track of all daily cloud account activities and lets you download daily activity report. At the end of each month, all daily activity reports will be consolidated into one monthly report for download.

To enable Activity Report to export all daily activities, please enable the following Compliance policy below to activate the feature:

- **NIST800/53 - Display content of audit record**

Enable NIST800/53 - Display content of audit record:

1. Click on the targeted cloud account (**Salesforce**, **Office 365**, etc.) from FortiCASB navigation menu.
2. Go to **Policy > Compliance**, and click **NIST800-53 rev4** tab.
3. Locate the policy **NIST800/53 - Display content of audit record**.



4. Enable the policy by clicking the **On** button.

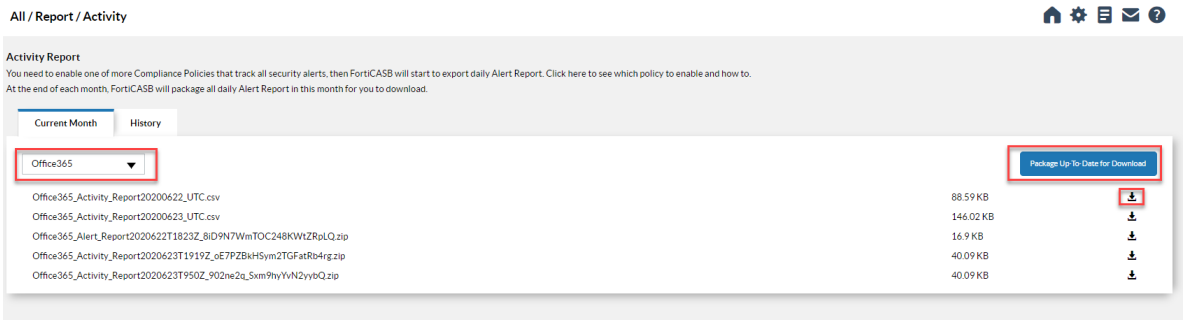
Generate Activity Report

Daily activity report is compiled into a CSV file and made available for export. At the end of each month, all daily reports of the that month are combined and packaged into a ZIP file and made available for download.

An alternative option of exporting daily reports is to consolidate up-to-date daily reports of the current month into one ZIP file.

Export Report

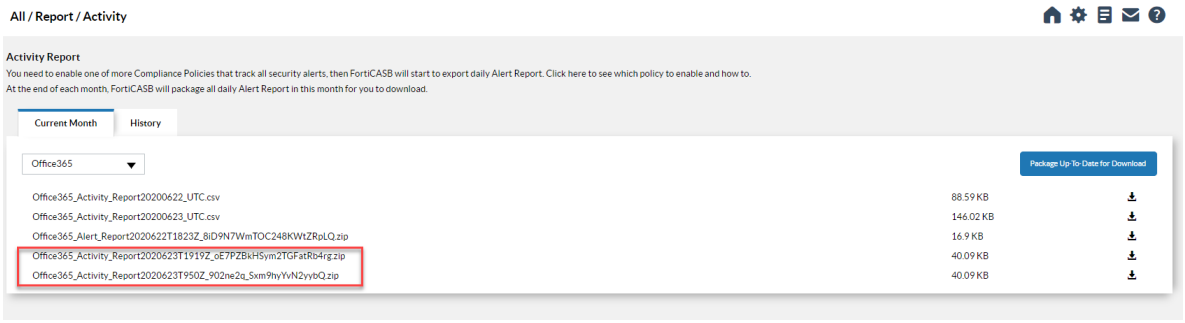
1. From FortiCASB navigation menu, go to **Overview > Report > Activity**.
2. In the **Current Month** tab, click the cloud account drop down menu and select a cloud application (**Salesforce**, **Office 365**, etc.).



Option 1 - Select any of the daily report and click download button to download the daily report.

Option 2 - Click **Package Up-To-Date for Download** button to combine all up to date daily reports of the current month into one zip file. The combined ZIP file will be made available for download with .zip

extension.

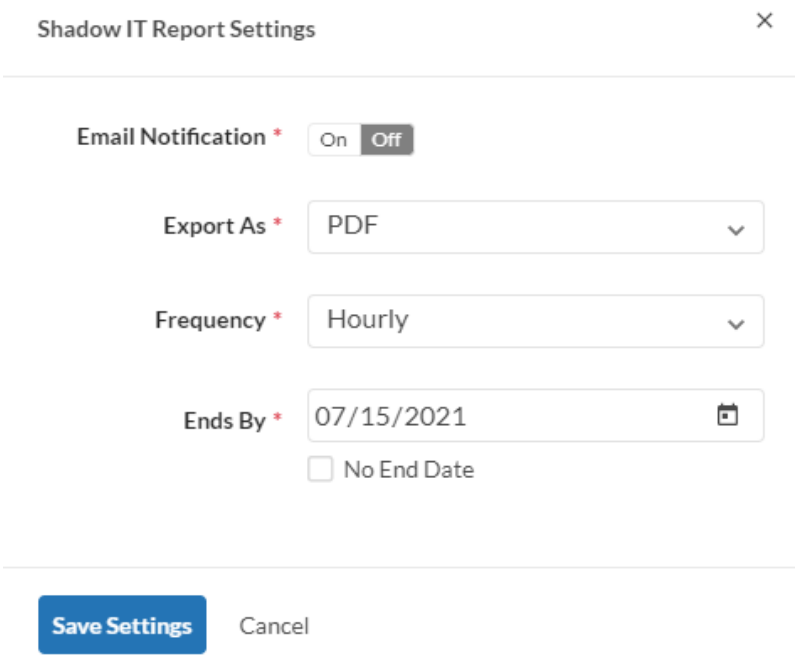


3. Click **History** tab to export monthly activity reports. Click the **year** drop down menu to select year, and **Cloud Applicationt** drop down menu to select a cloud account, and all monthly activity reports available of that year will be available for export.

Generate Shadow IT Report

Go to **Overview > Report > Shadow IT** page to download Shadow IT reports, Shadow IT reports are generated automatically.

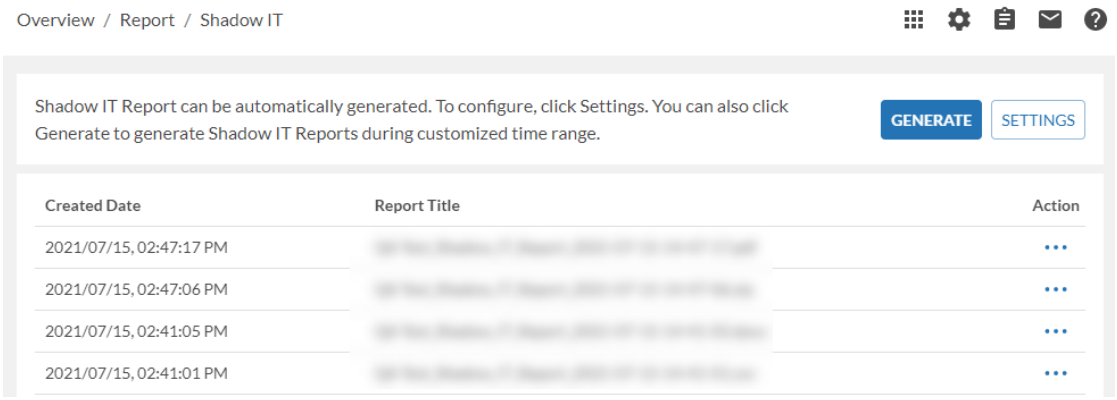
Click on **Settings** to configure notification, report format, and report generation frequency.



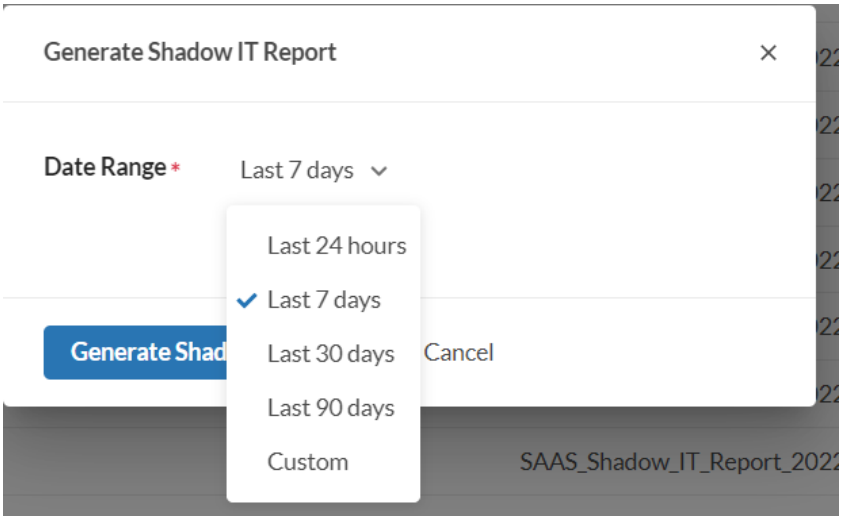
Customized Shadow IT Reports

Shadow IT reports with customized date range can be generated for a fixed time frame.

1. In **Shadow IT** page, click on **Generate**.



2. Click on **Date Range** to select a time frame of the report.



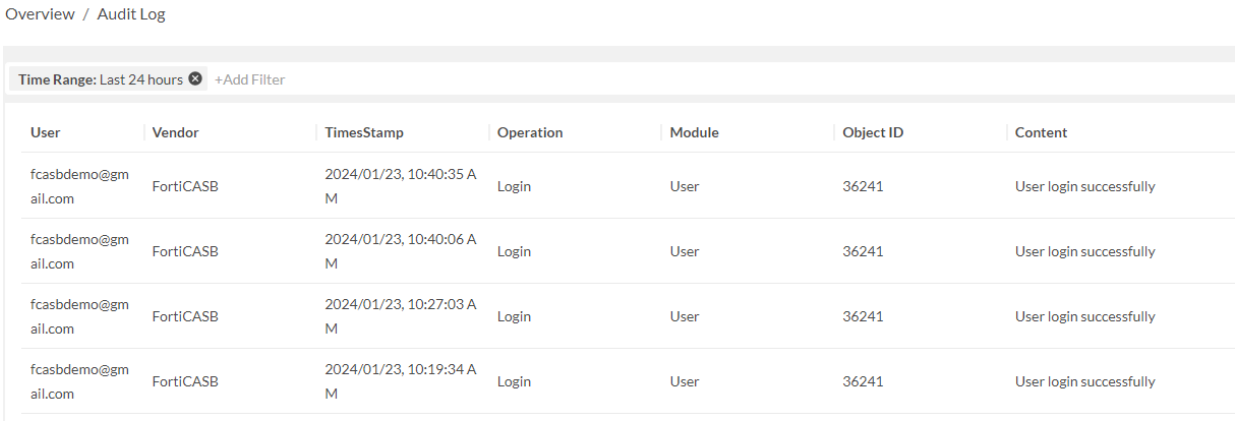
3. Click **Generate Shadow IT Report** to generate the report.
4. After the report is generated, it will be available to download under **Action** column.

View FortiCASB Audit logs

Audit logs records all administrative and user activities in FortiCASB.

To access the Audit log page, go to **Overview > Audit log.**

You can filter searches by using the **+Add Filter** option.



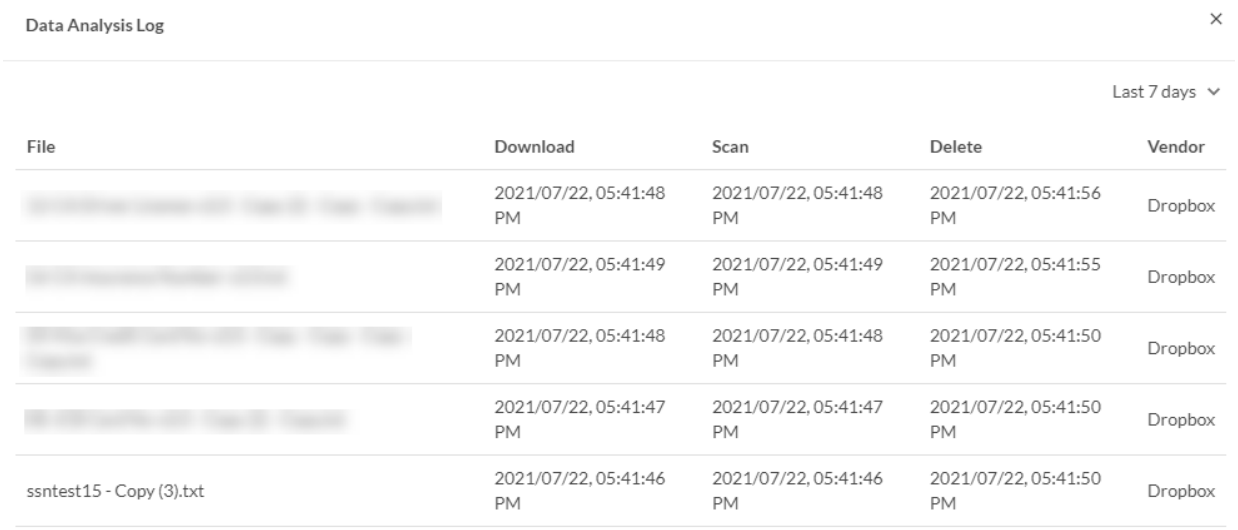
For detailed description of each operation or event, please refer to App Events Supported by FortiCASB on page 307.

Data Analysis Logs

FortiCASB accesses your information by downloading files, scanning the downloads, then subsequently deleting the downloads at regular intervals.

NOTE: For your privacy, FortiCASB does not retain your files. You may check to see when and which files FortiCASB has downloaded, scanned, and deleted by clicking the **Data Analysis Logs** button, located at the top-right corner.

Click on the icon below in the top right corner to access Data Analysis Logs.


Data Analysis Log

Last 7 days

File	Download	Scan	Delete	Vendor
[redacted]	2021/07/22, 05:41:48 PM	2021/07/22, 05:41:48 PM	2021/07/22, 05:41:56 PM	Dropbox
[redacted]	2021/07/22, 05:41:49 PM	2021/07/22, 05:41:49 PM	2021/07/22, 05:41:55 PM	Dropbox
[redacted]	2021/07/22, 05:41:48 PM	2021/07/22, 05:41:48 PM	2021/07/22, 05:41:50 PM	Dropbox
[redacted]	2021/07/22, 05:41:47 PM	2021/07/22, 05:41:47 PM	2021/07/22, 05:41:50 PM	Dropbox
ssntest15 - Copy (3).txt	2021/07/22, 05:41:46 PM	2021/07/22, 05:41:46 PM	2021/07/22, 05:41:50 PM	Dropbox

Shadow IT Discovery

FortiCASB provides features for shadow IT discovery. By integrating with FortiGate and FortiAnalyzer, FortiCASB gives users a concrete overview of all sanctioned and unsanctioned cloud applications within the organization. Furthermore, FortiCASB calculates a risk score for each application and gives users the ability to control application usage.

FortiCASB's Shadow IT discovery helps users enhance the security of their cloud application environment with the following features:

- **Unsanctioned Application Discovery**— FortiCASB uses logs from FortiGate and FortiAnalyzer as well as its own discovery process to deliver a comprehensive view of risk and usage of cloud applications.
- **Cloud Risk Score**—FortiCASB generates a cloud risk score for each cloud application. This score is calculated using many factors, such as but not limited to: user numbers, size of the company, multi-factor authentication support, and service hosting location. These factors are used to generate scores in multiple criteria, which are then aggregated into one final score.
- **Access Control**—Users can block or monitor certain applications using FortiCASB and FortiGate.
- **Data Correlation**—FortiCASB uses data from FortiGate and FortiAnalyzer, as well as its own data to define and identify riskier activities.

Configurations and Requirements

Shadow IT discovery requires a **FortiGate** or **FortiAnalyzer** policy.

Configuration details depend on your specific setup requirements. See the scenarios below, and find the one which best suits your needs.

Scenario 1: Receive logs from FortiGate.

Complete the FortiGate and FortiCASB configurations in the following order:

1. **FortiGate Configuration on page 292** (Complete all 3 parts)
2. **Log Configuration Using FortiGate GUI on page 295**
3. **FortiCASB Configuration on page 301**

Scenario 2: Receive logs from FortiAnalyzer.

Complete the FortiGate, FortiAnalyzer and FortiCASB configurations in the following order:

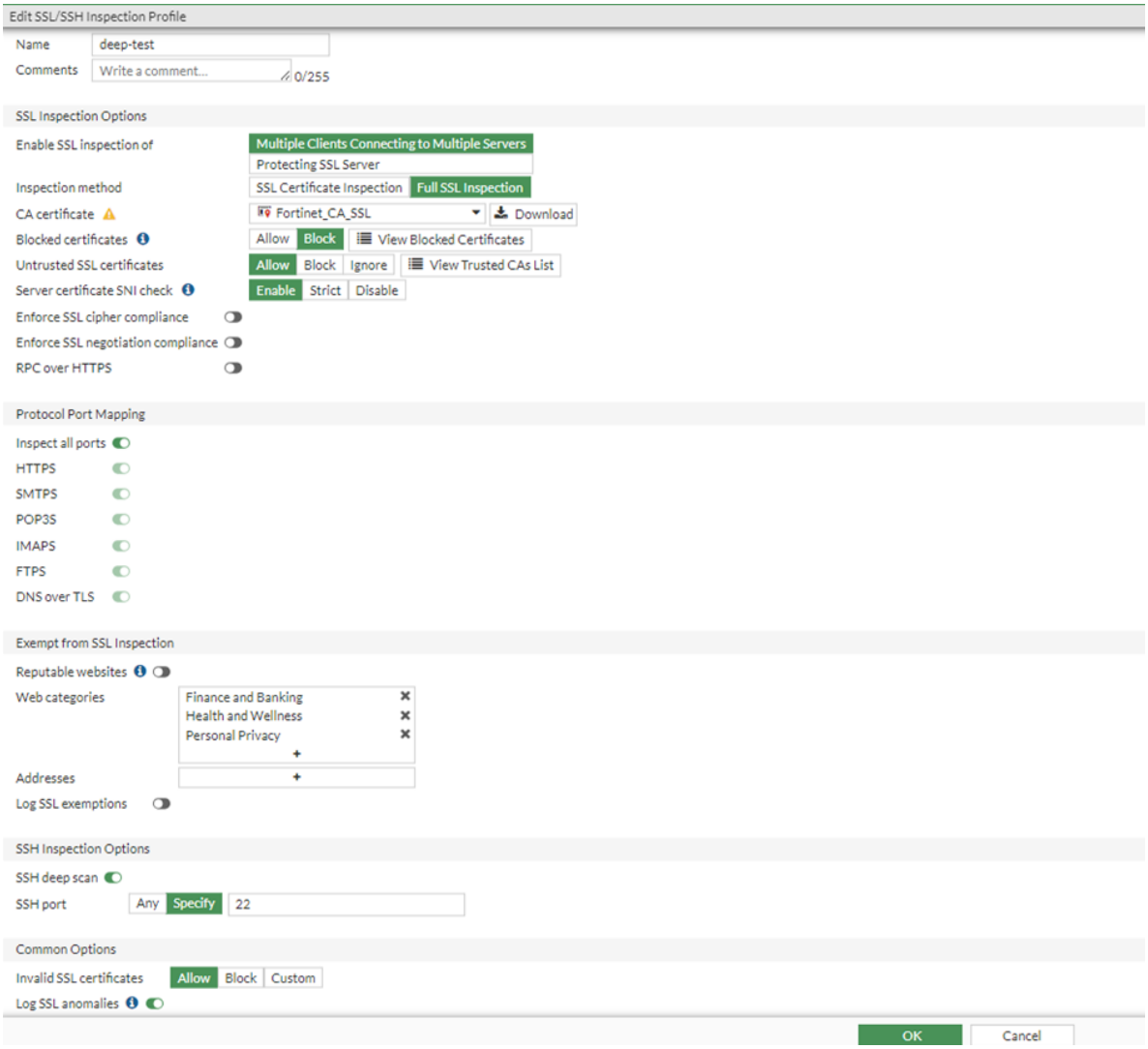
1. **FortiGate Configuration on page 292** (Complete all 3 parts)
2. **FortiAnalyzer Configurations on page 298**
3. **FortiCASB Configuration on page 301**

FortiGate Configuration

Part 1 - Create SSL/SSH Inspection Profile

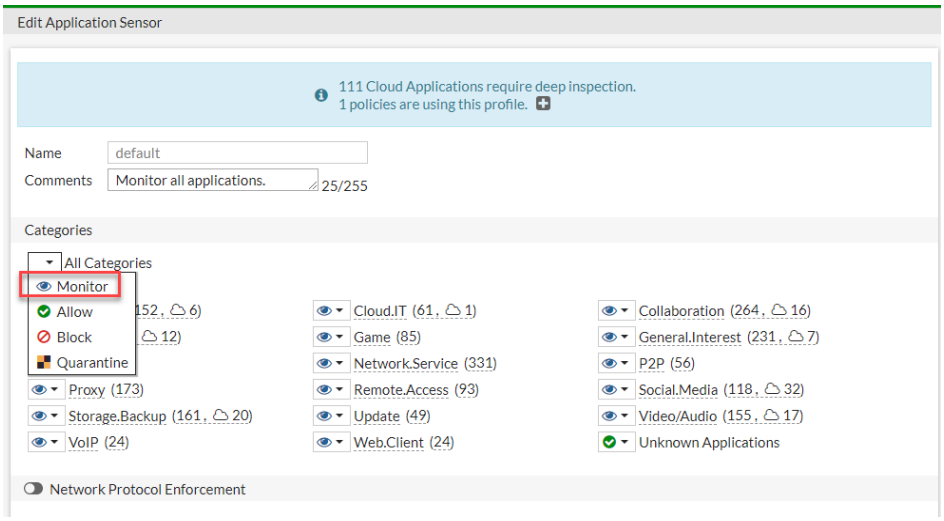
1. Log into FortiGate, go to **Security Profiles > SSL/SSH Inspection.**
2. Create a new SSL/SSH inspection profile called "deep-test".
3. In **Protocol Port Mapping**, enable **Inspect all ports**.
4. Scroll down to **SSH Inspection Options**, enable **SSH deep scan**, click **Specify** and enter ssh port: 22.
5. Scroll down to **Common Options**, select **Allow** for **Invalid SSL certificates**
6. In **Common Options**, **enable Log SSL anomalies**.

The completed configuration should be as the following:

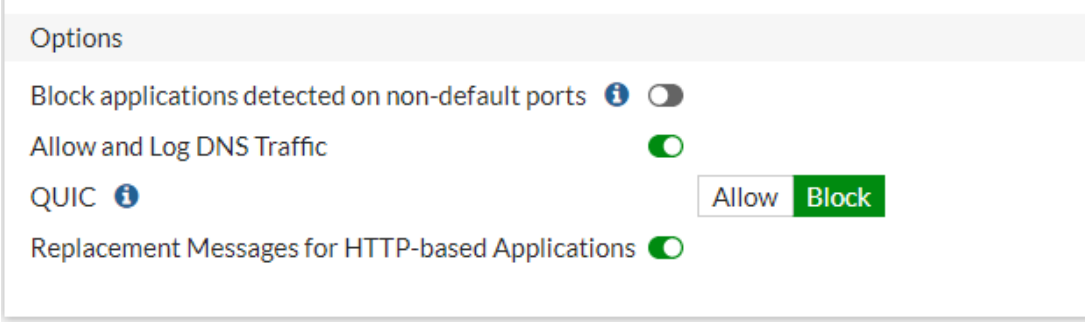


Part 2 - Application Control Configuration

1. Go to **Security Profiles > Application Control.**
2. Select **default** or create a new profile
3. Click **All Categories** drop down menu and select **Monitor**.



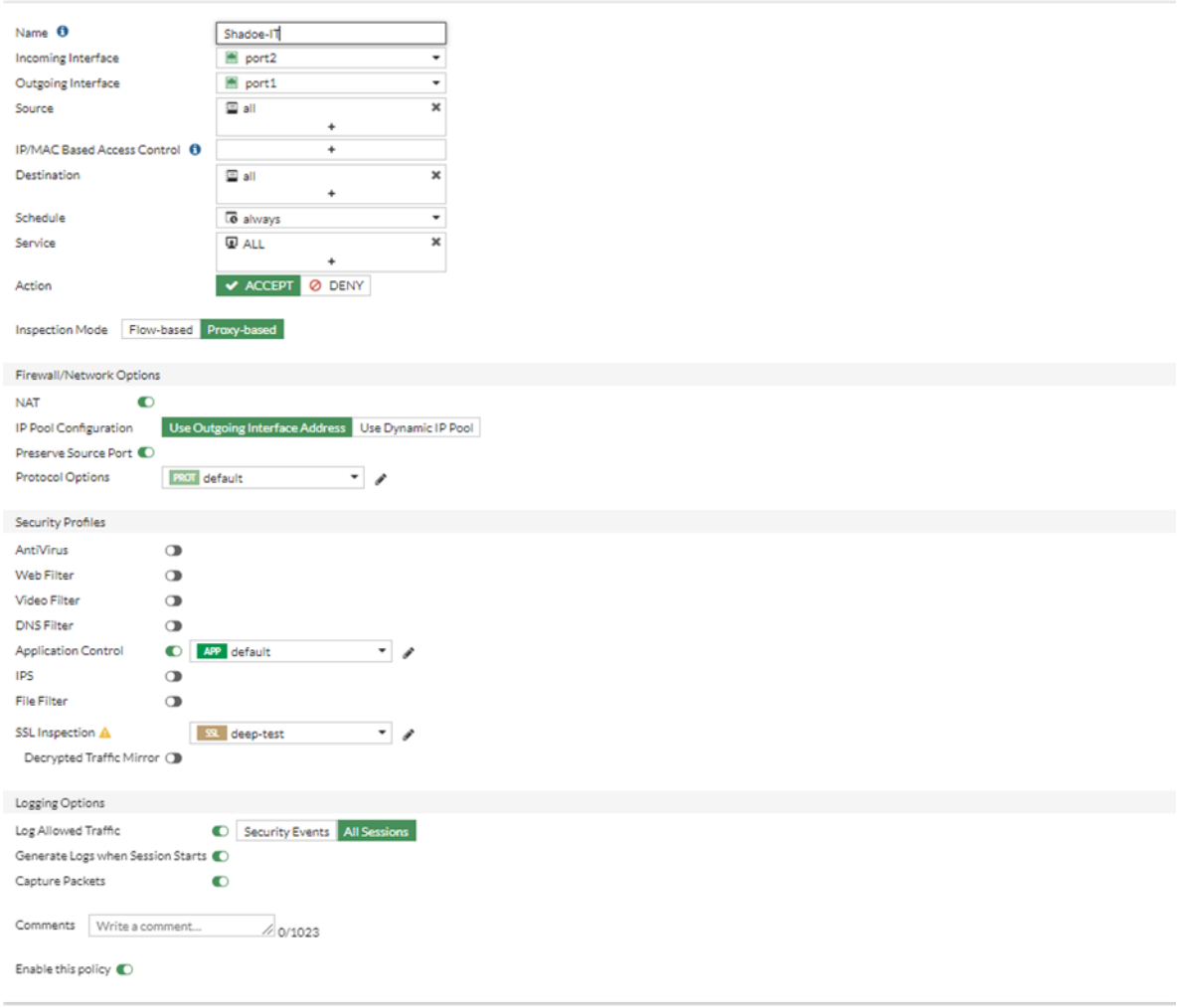
4. Under **Options**, enable **Allow and Log DNS Traffic** and **Replacement Messages for HTTP-based Applications**.



Part 3 - Firewall Policy Configuration

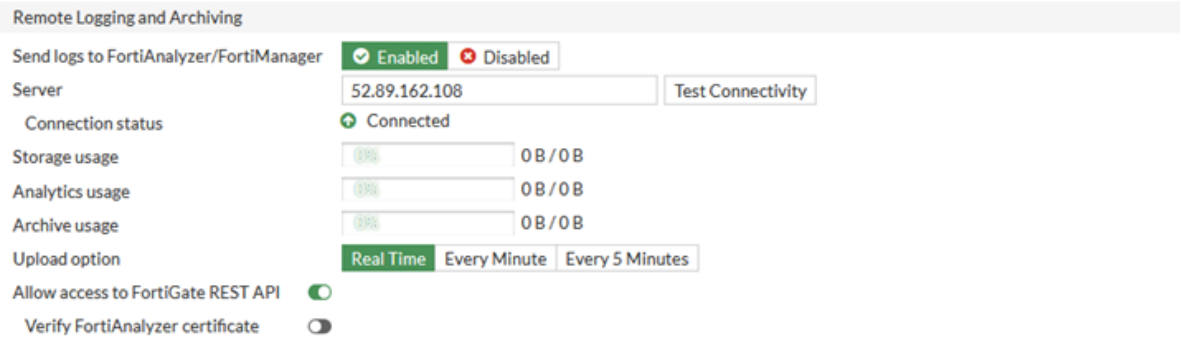
1. Go to **Policy & Objects > Firewall Policy**.
2. Create a new policy named "Shadow-IT".
3. Configure **Security Profiles**:
   a. To use access control, enable the **Web Filter** created with the URL filter set. (If you have setup web filter profile)
   b. Enable **Application Control** to allow FortiCASB to track how many cloud applications are visited.
   c. To correlate log data with FortiCASB data, make sure **Application Control** is enabled, and click **SSL/SSH Inspection** drop down menu to select **deep-test**.
4. In Logging Options, enable **Log Allowed Traffic**, and select either **Security Events** or **All Sessions**.

The completed configuration should be as the following:



Log Configuration Using FortiGate GUI

1. In FortiGate, go to **Log & Report > Log Settings.**
2. Enable **Send Logs to FortiAnalyzer/FortiManager**.



3. In **Server**, enter the FortiCASB receiver's IP address.
   The FortiCASB receiver IP address can be found by pressing the **Device** button from the FortiCASB Shadow IT dashboard. It will be one of the following addresses:

Global and US Users	52.89.162.108 or 52.24.189.163
EU Users	54.155.112.218 or 34.240.128.139

4. Test the connectivity by clicking **Test Connectivity**.

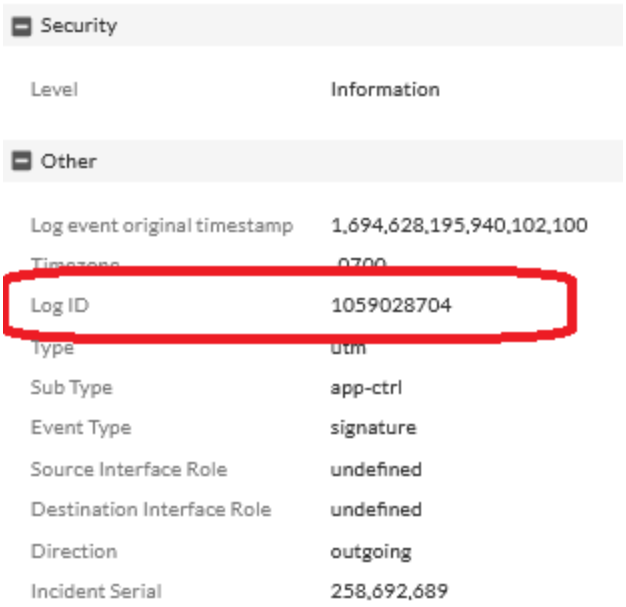
You can also configure and check the connection by using the following CLI.

Please only choose one method(**CLI or GUI**) to configure FortiCASB connection. If you have already done it through GUI, do not configure it again through CLI.

Log configuration using FortiGate CLI

Obtain the **Application Control ID** from FortiGate:

Go to **FortiGate > Security Events > Application Control > Other**



Then continue with the log configuration using FortiGate CLI mode.

1. Login to the FortiGate's CLI mode.
2. Configure log settings for the FortiCASB device on the FortiGate.

```
#config log fortianalyzer setting
   #set status enable
   #set server <FortiCASB server IP>
   #set enc-algorithm high-medium
   #set upload-option realtime
   #set reliable enable
#end
```

3. (Optional) Configure the log filter to only forward application-ctrl logs using the application control ID obtained earlier:

```
#config log fortianalyzer filter
   #config free-style
   #edit 1
   #set filter-type include
   #set filter "logid <Application Control ID>"
#end
```

4. Test the connection using the following CLI command:

```
#execute log fortianalyzer test-connectivity
```

If the connection is successful, the FortiGate will return the following:

```
Registration: registered
Connection: allow
```

Otherwise, the FortiGate will return an error code

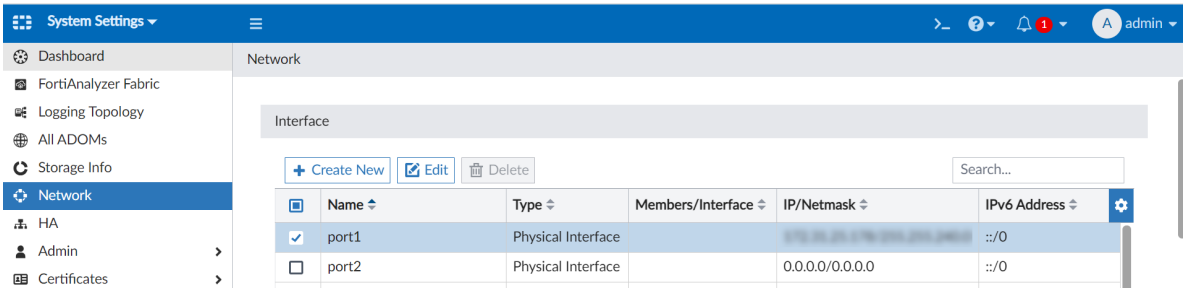
FortiAnalyzer Configurations

Part 1: FortiAnalyzer Port Configuration

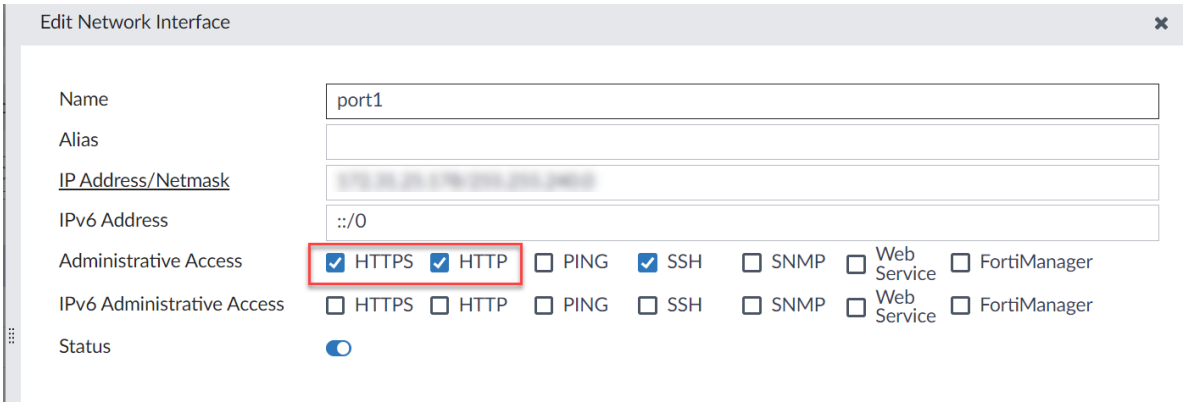
This section is to provide a public IPv4 address for FortiAnalyzer and make sure the IP address with the following ports can be accessed from the external network.

Protocols	TCP Port
HTTP	80
HTTPS	443

1. In FortiAnalyzer, go to **System Settings > Network**, select the interface.

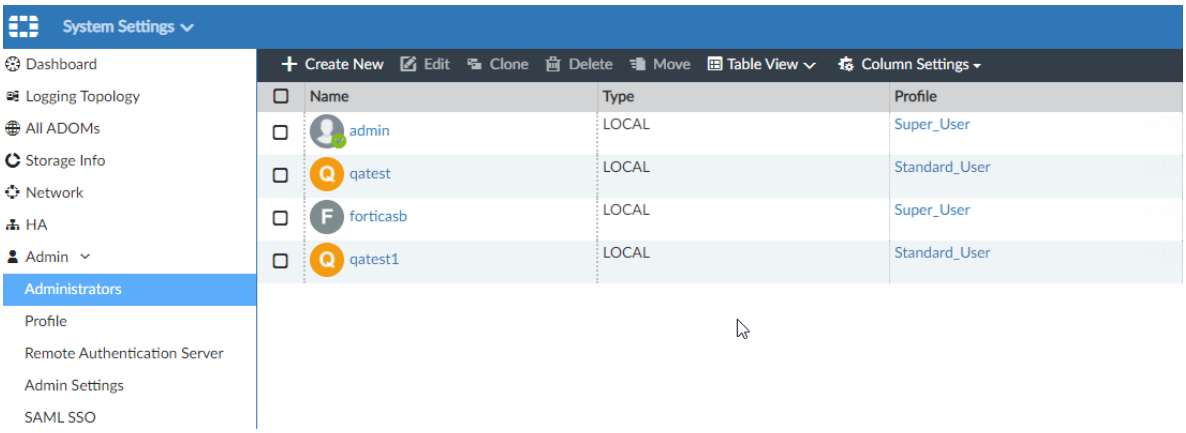


2. Then click **Edit** to edit the network interface.
3. Enable **HTTPS** or **HTTP** in **Administrative Access**. (The network connection will be tested in FortiCASB Configuration on page 301)

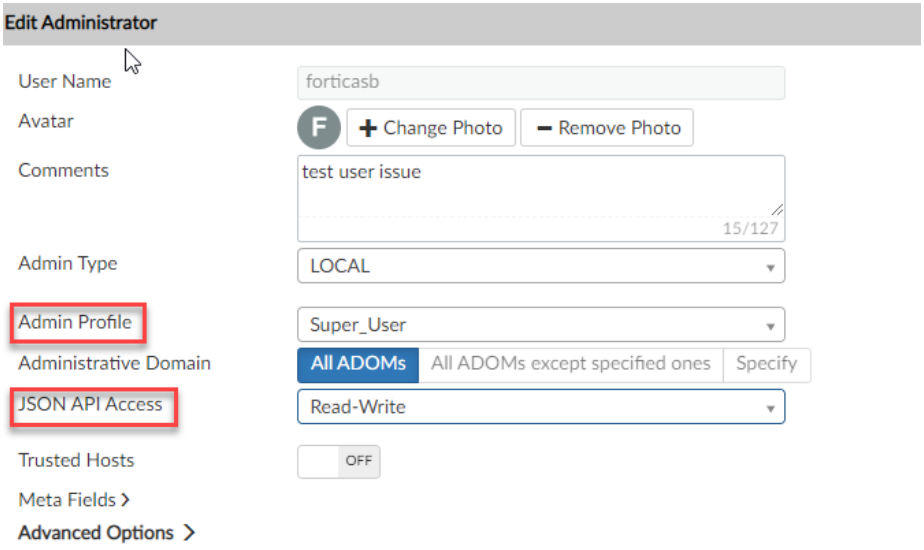


Part 2: FortiAnalyzer System Configuration

1. Finish all parts 1-3 in the FortiGate Configuration on page 292.
2. Go to **FortiAnalyzer > System Settings**, click on **Administrators**, select the user to be connected to FortiCASB and press **Edit**.

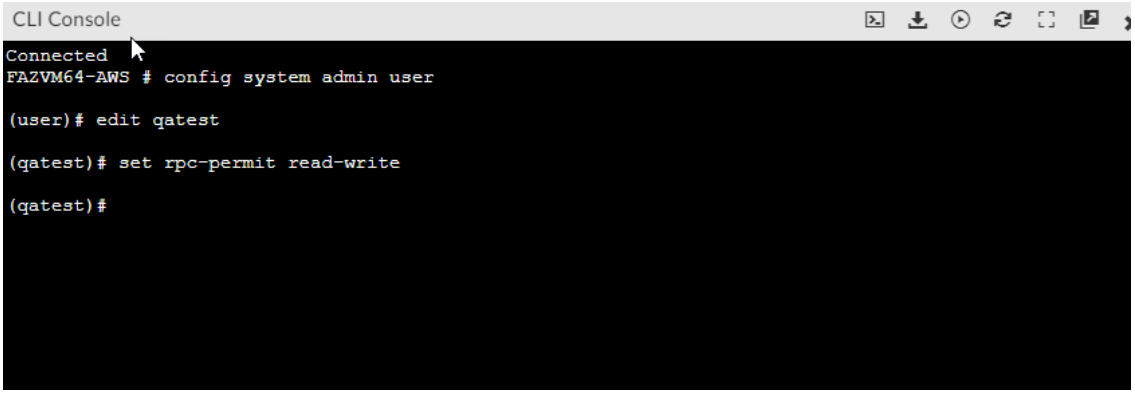


3. Click **Admin Profile** drop down menu and select "Standard_User" or "Super_User".



4. Click **JSON API Access** drop down menu and select "Read-Write".
5. Use the following CLI commands to add RPC-permit's read and write permissions to the user:

```
config system admin user
edit "user" (The FortiAnalyzer user that will be used to connect to FortiCASB.)
 set rpc-permit read-write
```

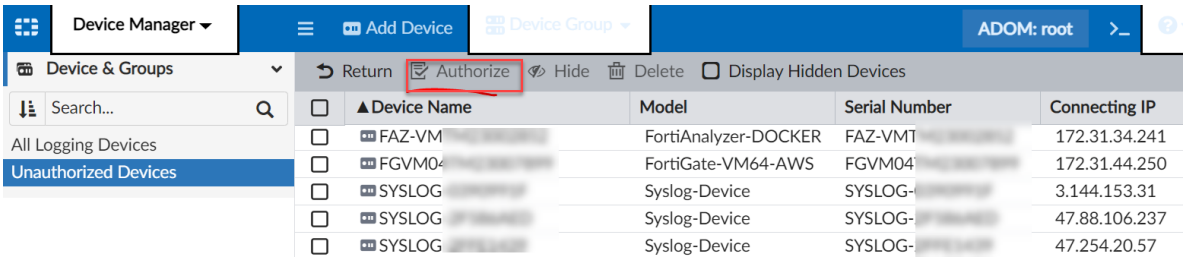


Part 3: Configure FortiAnalyzer on FortiGate

1. Go to FortiGate and open CLI, then enter the following command:

```
#config log fortianalyzer2 setting
   #set status enable
   #set server <FortiAnalyzor server IP>
   #set enc-algorithm high-medium
   #set upload-option realtime
   #set reliable enable
#end
```

2. Go to **FortiAnalyzer > Device & Groups**.
3. Look for the unauthorized FortiGate device and authorize it.



4. Go to back to FortiGate then execute the following command to test the connection.

```
#execute log fortianalyzer test-connectivity 2
```

5. If the connection is successful, FortiGate will return the following:

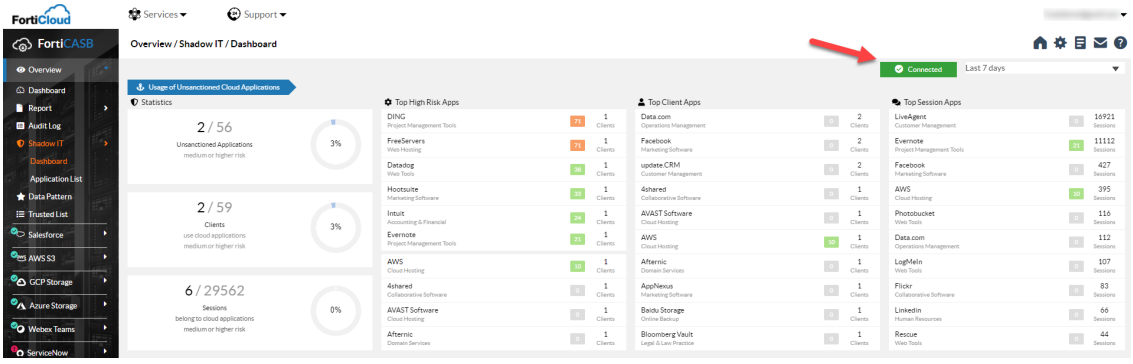
```
Registration: registered
Connection: allow
```

The entire CLI output should look like below:

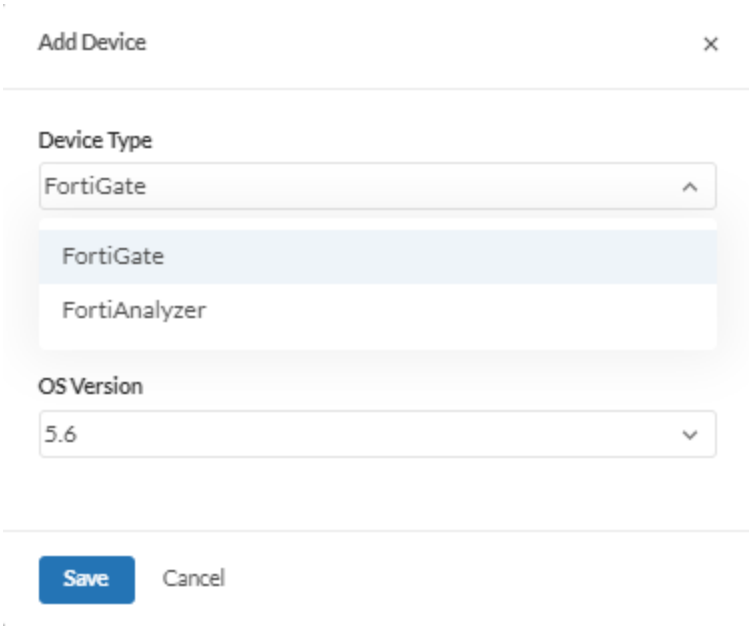
```
FGVM04TMXXXXXX # execute log fortianalyzer test-connectivity 2
FortiAnalyzer Host Name: FAZAWS
FortiAnalyzer Adom Name: root
FortiGate Device ID: FGVM04TMXXXXXX
Registration: registered
Connection: allow
Adom Disk Space (Used/Allocated): 3921305424B/53687091200B
Analytics Usage (Used/Allocated): 790079985B/37580963840B
Analytics Usage (Data Policy Days Actual/Configured): 32/60 Days
Archive Usage (Used/Allocated): 3131225439B/16106127360B
Archive Usage (Data Policy Days Actual/Configured): 55/365 Days
Log: Tx & Rx (6 logs received since 15:21:34 08/29/23)
IPS Packet Log: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
Certificate of Fortianalyzer valid and serial number is: FAZ-VMTMXXXXXX
```

FortiCASB Configuration

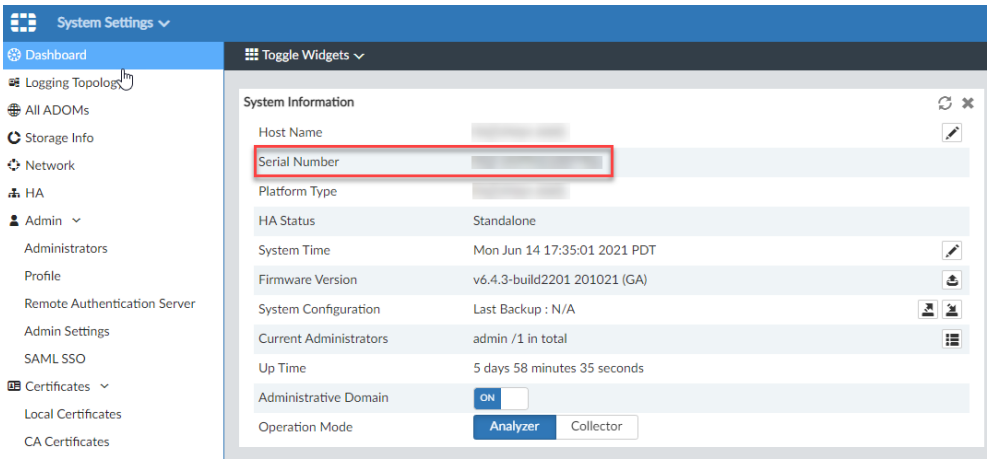
1. Go to **Overview > Shadow IT > Dashboard**.
   a. Click the **Connect** button, located on the top right, from the **Shadow IT** dashboard, then click **Add Device**.



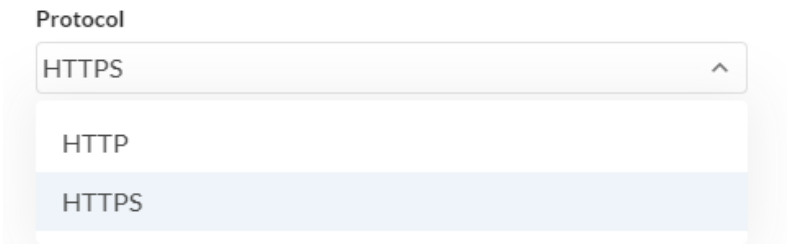
   b. In **Device Setting**, click **Device Type** drop down menu to select either **FortiGate** or **FortiAnalyzer**.



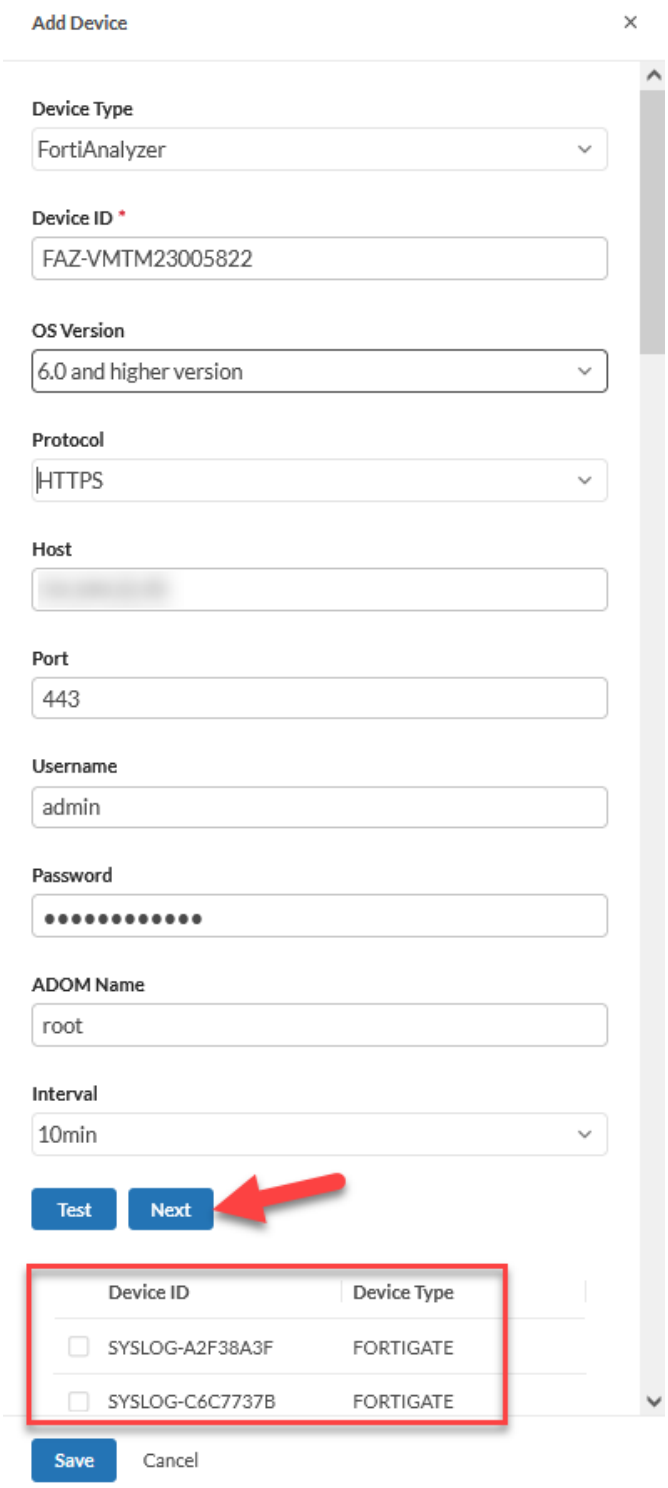
2. Enter the **Device ID**. The Device ID is the **Serial Number** of the FortiAnalyzer or FortiGate.
   For Example, on FortiAnalyzer, the Serial Number is shown in **System Setting** Dashboard.



3. In **OS Version**, if the FortiGate or FortiAnalyzer version is 6.0 or above, select **6.0 and higher version**.
4. In **Protocol**, select **HTTP** or **HTTPS** depending on which one is enabled in FortiAnalyzer Setting. The port will update automatically with the HTTP/HTTPS selection.



5. Click **Test** to test the HTTP/HTTPS connection.
6. **a.** For **FortiGate**, click **Save** to finish the device setting.
   b. For **FortiAnalyzer**, fill in the rest of the fields, press **Next**, then you will be prompt to select the FortiGate device(s) (The FortiGate device you authorized in FortiAnalyzer) to add.



c. Click **Save** to finish add device, then a summary page will be shown as below.

Status	Device ID	Type	Host	Parent Device	Action
✓	FAZ-VMTM21007706	FORTIANALYZER	18.237.184.156	–	•••
✓	FGVM04TM22002360	FORTIGATE	–	–	•••
✓	54.156.122.76	FORTIGATE	–	–	•••
✓	11272403	FORTIGATE	–	–	•••
✓	FGVM04TM22002361	FORTIGATE	–	–	•••
✓	FGVM04TM21010966	FORTIGATE	–	FAZVCLTM21000881	🗑

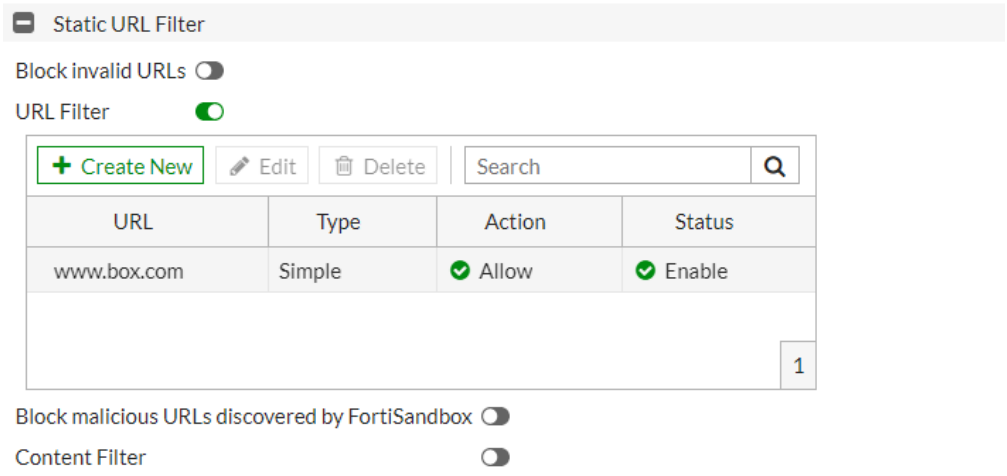
Note: Please make sure the FAZ is shown under the **Parent Device** column.

Using Shadow IT Discovery

Access control

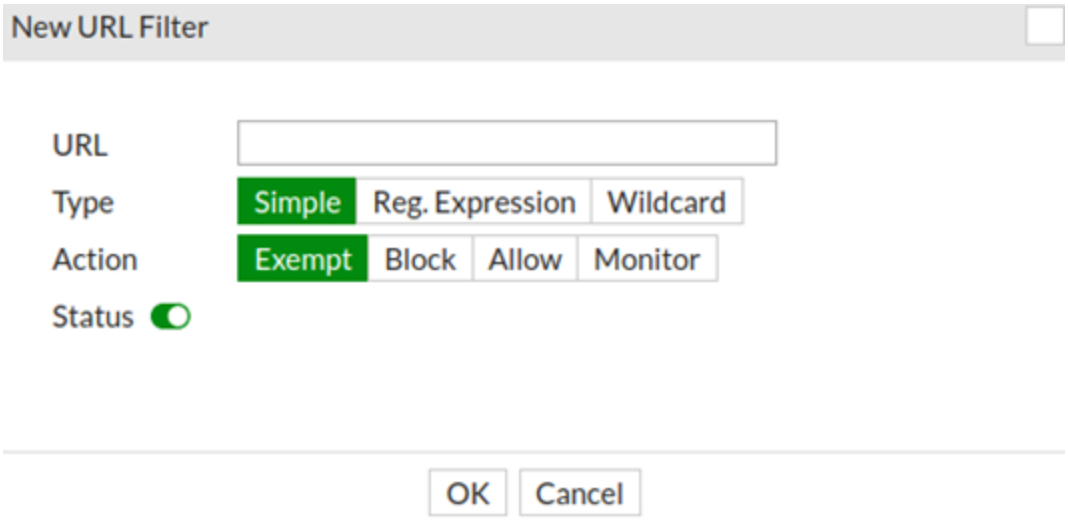
After analyzing an application using FortiCASB, users can use FortiGate's Web Filter to block or monitor the application.

1. Use FortiCASB to get the host name of the traffic to be controlled.
2. On the FortiGate device, go to **Security Profile > Web Filter.**
3. Under **Static URL Filter**, choose the URL filter.



4. Click **Create New** to add a new URL filter.
5. Choose a **Type**.

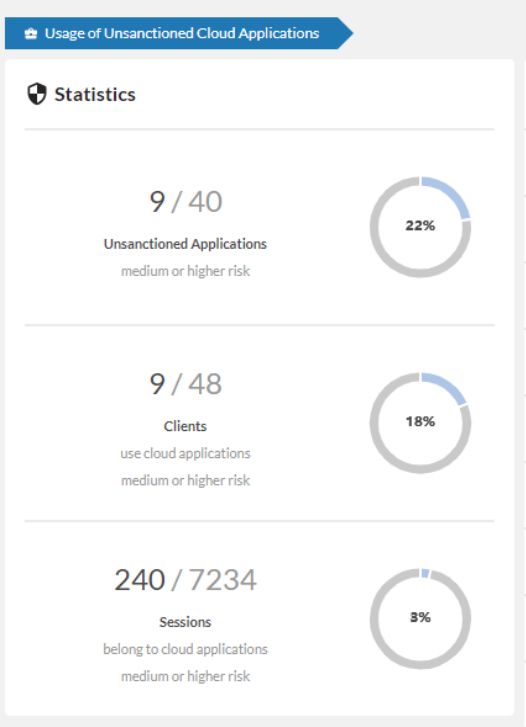
6. Choose an **Action**.
7. Set Status to **Open**.
8. Click **OK**.



Shadow IT Dashboard

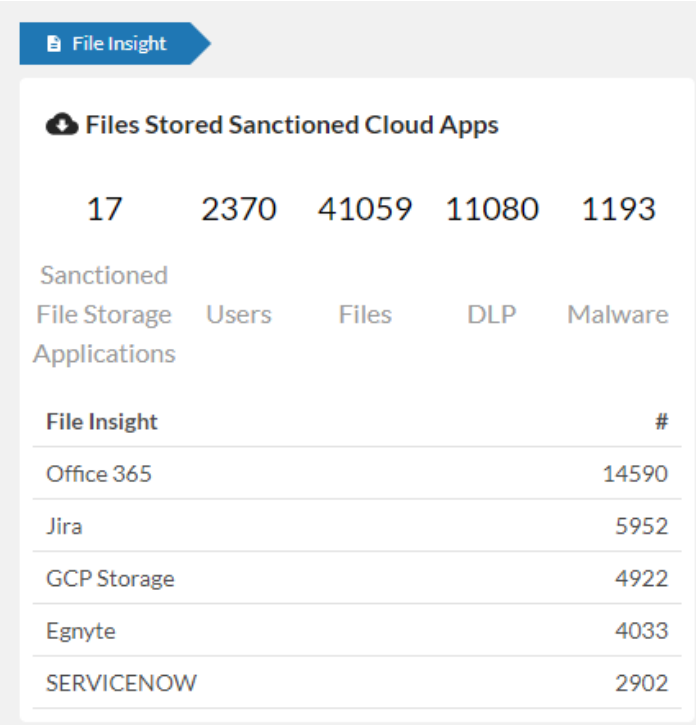
Usage of unsanctioned cloud applications

All unsanctioned cloud applications are given a ranking based on the risk score, the number of users, and use volume. FortiCASB uses that data to pinpoint and display the applications, clients, and sessions that are most at risk. FortiCASB also displays the statistics and percentage of risky applications, clients, and sessions using pie charts.



File insight

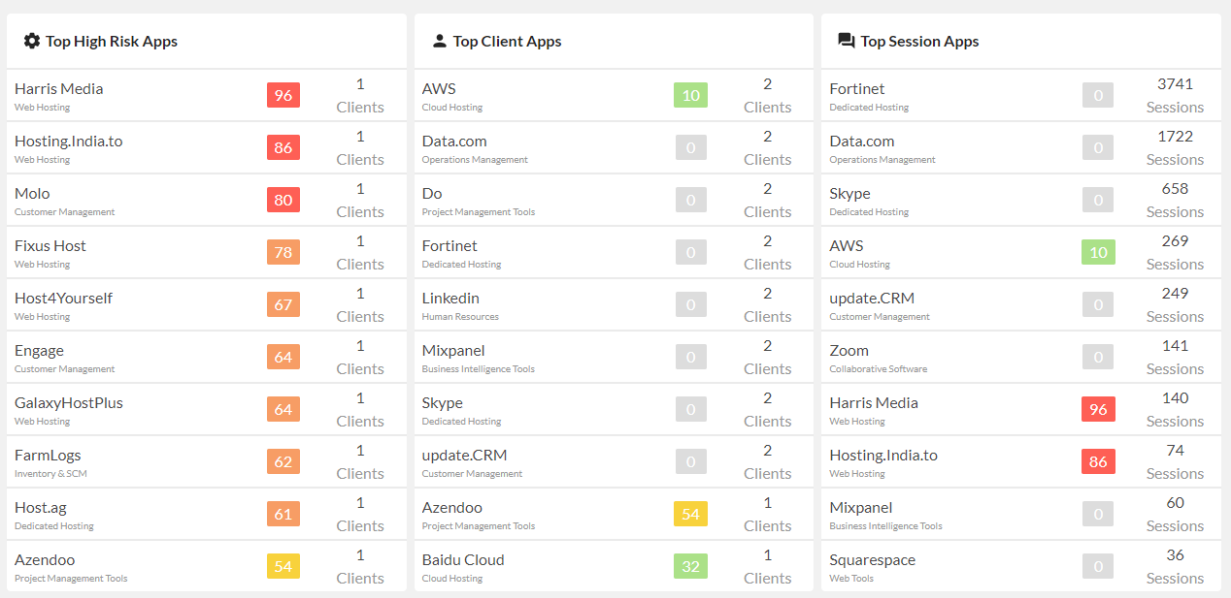
File insight shows the total number of sanctioned cloud applications the organization is using, the total number of users, and the total number of files stored in each cloud application.



Top Unsanctioned Apps

The **Top High Risk**, **Client**, and **Session Apps** displays all applications monitored by FortiCASB. Filter the list using the time range box on the top right.

Click on an app to display detailed information regarding the application.



Top High Risk Apps			Top Client Apps			Top Session Apps		
Harris Media Web Hosting	96	1 Clients	AWS Cloud Hosting	10	2 Clients	Fortinet Dedicated Hosting	0	3741 Sessions
Hosting.India.to Web Hosting	86	1 Clients	Data.com Operations Management	0	2 Clients	Data.com Operations Management	0	1722 Sessions
Molo Customer Management	80	1 Clients	Do Project Management Tools	0	2 Clients	Skype Dedicated Hosting	0	658 Sessions
Fixus Host Web Hosting	78	1 Clients	Fortinet Dedicated Hosting	0	2 Clients	AWS Cloud Hosting	10	269 Sessions
Host4Yourself Web Hosting	67	1 Clients	Linkedin Human Resources	0	2 Clients	update.CRM Customer Management	0	249 Sessions
Engage Customer Management	64	1 Clients	Mixpanel Business Intelligence Tools	0	2 Clients	Zoom Collaborative Software	0	141 Sessions
GalaxyHostPlus Web Hosting	64	1 Clients	Skype Dedicated Hosting	0	2 Clients	Harris Media Web Hosting	96	140 Sessions
FarmLogs Inventory & SCM	62	1 Clients	update.CRM Customer Management	0	2 Clients	Hosting.India.to Web Hosting	86	74 Sessions
Host.ag Dedicated Hosting	61	1 Clients	Azendoo Project Management Tools	54	1 Clients	Mixpanel Business Intelligence Tools	0	60 Sessions
Azendoo Project Management Tools	54	1 Clients	Baidu Cloud Cloud Hosting	32	1 Clients	Squarespace Web Tools	0	36 Sessions

App Events Supported by FortiCASB

This section shows the types of cloud account events FortiCASB supports. These types of events will be traced at the **Activity** page of each cloud application, and they can also be used as criteria when configuring policy and applying filters.

The **File Download** events are monitored within the FortiCASB Audit log, go to **Overview > Audit Log** from the navigation menu.

Box Events

Event Type	Event
File/Folder	Upload File
	Copy File
	Download File
	Edit File
	Move File
	Preview File
	Rename File
	Open File
	Modify File
	Create Lock
	Comment
Login	Login Success
	Login Failed
User	Create User
	Modify User
	Delete User
Group	Add Group
	Update Group
	Group Add Membership
Metadata	Create Metadata Template
	Update Metadata Template
	Create Metadata Instance
	Update Metadata Instance
Collaboration	Collaboration Invite
	Collaboration

Event Type	Event
	Accept
	Collaboration Role Change
	Update Collaboration Expiration
	Collaboration Expiration
Share	Share File
	Update Shared File
	Update Shared Expiration
	Share Expiration

Confluence Events

Type	Event	Description
User	Create User	New user created in the account.
	Delete User	A user is deleted from the account.
	Deactivate User	A user is deactivated from the account.
	Reactivate User	A user is reactivated on the account.
Group	Create Group	Creates a new user group.
	Remove Group	Delete user group.
	Add user to Group	Adds a user as a member in a group.
	Remove user from Group	Remove user as a member from a group.
File (Attachment in Webhook Events)	File View	File view activity via Webhook Event.
	Create/Upload	Create File/Upload File activity via Webhook

Type	Event	Description
	File	Event.
	Edit/Update File	File update activity via Webhook Event.
	Trash/Delete File	Trash/Delete File activity via Webhook Event.
	Restore File	File restore activity via Webhook Event.
	Remove File	File removed activity via Webhook Event.
Label	Label Add/Create	Label create activity via Webhook Event.
	Label Remove/Delete	Label removed activity via Webhook Event.
Space	Create Space	Space create activity via Webhook Event.
	Update Space	Space update activity via Webhook Event.
	Logo Update Space	Space logo activity via Webhook Event.
	Delete Space	Delete space activity via Webhook Event
Page	Page View	Page view activity via Webhook Event.
	Page Create	Page create activity via Webhook Event.
	Page Update	Page update activity via Webhook Event.
	Page Move	Page move activity via Webhook Event.
	Page Removed	Page removed activity via Webhook Event.
	Page Archived	Page archived activity via Webhook Event.
	Page Restored	Page restored activity via Webhook Event.
	Page Deleted	Page deleted activity via Webhook Event.
Comment	Create Comment	Create comment under this page.
	Edit Comment	Edit comment under this page.
	Delete Comment	Delete comment under this page.

Dropbox Business Events

Event Type	Event
Login	Login Success
	Login Failed
	Logout
	Login As User Session Start
	Login As User Session End
User (Member)	Create User
	User Change Name
	User Change Status
	User Change Admin Role
	User Change Email
	Change Password
	Password Restore
	Password Restore All
Group	Add Group
	Delete Group
	Add Group Member
	Remove Group Member
	Group Rename
File	File Add
	File Download
	File Preview
	File Edit

Event Type	Event
	File Delete
	File Add Comment
	File Move
	File Copy
	File Rename
	File Restore
	File Revert
File Share	Share Link Create
	Share Link Create Password
	Share Link Public
	Share Link Disable
	Share Link Team Only
	Share Link Set Expiration
	Share Link Remove Expiration
	Share Link View
	Share Link Download
	Share Link Team Copy

Egnyte Events

Event Type	Event	Description
File	Upload File	Upload a new file
	Delete File	Delete an existing file
	Move File	Move a file to different path
	Copy File	Copy file to different path
	Add Version	Modification in the existing file, create a new version of the file

Event Type	Event	Description
	Delete Version	Delete version of the file by user
	Delete Version (VPC)	Delete version (Version Policy Control) of the file by Egnyte System
	Restore File	Restore the file from trash
	Rename File	Change the name of the existing file
	Upload File Via Link	Create shared link for sharing to upload file
Folder	Add Folder	Upload a new folder
	Delete Folder	Delete an existing folder
	Move Folder	Move folder to different path
	Copy Folder	Copy folder to different path
	Restore Folder	Restore folder from the trash
	Rename Folder	Change name of the folder
Permission	Change share permission	Any change in user permissions on sharing the folder
Feed	Create comment	Any note/comment posted by user regarding the file

Google Workspace Events

Event Type	Event
Login	Login Success
	Login Failure
	Login Challenge

Event Type	Event
	Logout
File	Create File
	Upload File
	Edit File
	View File
	Rename File
	Move File
	Delete File
	Download File
	Preview File
	Trash File
	Untrash File
User	Create User
	Suspend User
	Unsuspend User
	Modify User
	Change Password
	Create Data Transfer Request
	Delete User
	Assign Role

Event Type	Event
	Unassign Role

GitHub Events

Event Type	Event	Description
User	Add Member	Add a member to the organization
	Add Outside Collaborator	Add a person to the repository. (This person is not an existing organization member and does not exist in outside collaborator)
	Remove Member	Remove a member from the organization
	Remove Outside Collaborator	Remove a person from all of the repositories where this person belongs to. (This person is not an organization member but an outside collaborator)
	Change Role	Change an organization member's role between owner and member
	Convert To Outside Collaborator	Convert an organization member to outside collaborator
Team	Add Team	Add team in organization
	Add Team Member	Add member in existing team
	Remove Team Member	Remove member from team
	Delete Team	Delete the team from organization
	Change Parent Team	This event contains three cases: • Add a parent team to team • Change the parent team of team • Remove the parent team of team
Repository Privilege	Change Repository Visibility	Repository Visibility can be change between public and private.

Event Type	Event	Description
	Change Base Permission	Change repository access base permission for organization members.
	Update Team's Role In Repository	Update team's role in the repository.
	Update People's Role In Repository	This event contains two cases: Update an organization member's role in the repository and Update an outside collaborator's role in the repository
Collaborators And Teams In Repository	Add People To Repository	This event contains three cases: • Add an existing organization member to the repository. • Add the person that doesn't belong to this organization in the repository. (This person become an outside collaborator) • Add an existing outside collaborator to the repository.
	Remove People From Repository	This event contains two cases: • Remove an existing organization member from the repository • Remove an outside collaborator from the repository
	Add Team To Repository	Add an existing organization team into the repository
	Remove Team From Repository	Remove team from the repository
File	Upload File	Upload new file
	Delete File	Delete a file
	Modify File	Make changes of a file
	Create Branch	Create a branch in the repository
	Delete Branch	Delete a branch from repository

Event Type	Event	Description
	Create Repository	Create a repository of the organization
	Delete Repository	Delete a repository of the organization
	Rename Repository	Change name of the repository
	Add Folder	Add a new folder in the branch
	Delete Folder	Delete a folder from the branch

Jira Events

Event Type	Event	Description
User Activity	User login	A user has logged in.
	User login failure	A user log in has failed.
	User logout	A user has logged out.
	Create user	A user has been created.
	Update user	A user profile has been updated.
	Delete user	A user is deleted.
File Activity	File created	A file attachment is created on the project or issue.
	File deleted	A file attachment is deleted from the project or issue.
Issue Activity	Issue created	An issue is created.
	Issue updated	An issue is updated.
	Issue	An issue has been deleted.

Event Type	Event	Description
	deleted	
Comment Activity	Comment created	A comment is created.
	Comment updated	A comment is updated.
	Comment deleted	A comment is deleted.

Office 365 Events

Event Type	Event
Login	Login Success
	Login Failed
User	Create User
	Delete User
	Modify User
	Restore User
	Change Password
	Modify Role
Group	Add Group
	Delete Group
	Add Group Member
	Update

Event Type	Event
	Group
	Add Group Owner
	Delete Group Owner
	Set Group Managed By
	Create Group Settings
	Update Group Settings
	Delete Group Settings
	Set Group License
File	Upload File
	Delete File
	Download File
	Modify File
	Access File
	Move File
	Copy File
	Rename File
	Edit File
Share	Share File
	Create Anonymous Link

Event Type	Event
	Delete Anonymous Link
	Create Company Link
	Delete Company Link
	Company Link Used
Other	Modify License
	Delete Folder
	Create Sharing Invitation
	Edit Company Info

Salesforce Events

Event Type	Event
Login	Login Success
	Login Failed
User	Create User
	Modify User
	Change Password
	Activate User
	Deactivate User
	Change User Profile
	Change User Role

Event Type	Event
	Change User Email
	Change User Permission Set
Group	Add Group
	Add Group Member
	Update Group
	Change Group Access
	Add External Group Member (Customer)
	Invite People
Profile	Create Profile
	Modify Profile
Permission Set	Add Permission Set
	Modify Permission Set
Feed	Post
	Modify Post
	Comment
	Modify Comment
File	Upload File
	Upload New Version
	Download File
	Edit File
Share	Share File
	Share File with People
	Share File with Group

Event Type	Event
	Share File via Link
	Download File via Link
Business	Account Modification
	Account Owner Change
	Contact Modification
	Contact Owner Change
	Account Create
	Contact Create

SAP IAS Events

Type	Event	Description
User	Login Success	User log in success activity.
	Login Failed	User log in failed activity.
	Log out success	User log out success activity.
	Create User	Create user activity.
	Delete User	Delete user activity.
	Activate user	Activate user activity.
	Deactivate user	Deactivate user activity.
	Update user	Update user activity.
	Assign user group	Assign group activity.
	Unassign user group	Unassign group activity.

ServiceNow Events

Event Type	Event list	Description
Login	Login Success	A user has logged in successfully
	Login Failed	A user login failed
	Logout	A user has logged out
User	Create User	A user has been created
	Delete User	A user has been deleted
	Modify User	Modify user's attribution
	Restore user	Recover a deleted user
	Change Password	Change user's login password
	Add User Role	Add user's role
	Delete User Role	Delete user's role
Group	Add User to Group	Add a user to selected group
	Remove User from Group	Remove user from the selected group
	Add Group Role	Add group's role
	Delete Group Role	Delete group's role
File	Upload File	Upload a file in the table
	Rename File	Rename a file
	Download File	Download a file
	Delete File	Delete a file

Webex Teams Events

Event Type	Event	Description
User Activity	User login	A user log into to Webex.
	Create user	A user is created.
	Delete user	A user is deleted.
	Create memberships	Add someone to a room by Person ID or email address.
	Delete memberships	Deletes a membership by ID.
	Update memberships	Update a membership by ID.
	Participant joined a meeting	A participant join the meeting.
	Participant left a meeting	A participant left the meeting.
File activity	Upload file	A file is uploaded in chat.
	Delete file	A file is deleted from chat.

Zoom Events

Event Type	Event	Description
User	Create User	A user has been created.
	Update User	A user profile has been updated.
	Delete User	A user has been deleted.
	Activate User	A user has been activated on Zoom.
	Deactivate	A user has been deactivated on Zoom.

Event Type	Event	Description
	User	
	Disassociate User	A user has been disassociated.
User Activity	Login Success	A user has log in successfully.
	Logout	A user has log out successfully.
	Change Password	The user password has been changed.
	Change User Role	The user role has been changed.
Channel	Create Channel	A chat channel is created.
	Delete Channel	A chat channel is deleted.
Message	Message Send	A chat message is sent in the chat room.
	Message Reply	A chat message is replied in the chat room.
	Message Update	A chat message is updated in the chat room.
	Message Delete	A chat message is deleted in from the chat room.

FortiCASB only monitors messages in **Team Chat Channel**, but not private messages between Zoom users

Fabric Integration Configuration

Overview

As part of the Fortinet Security Fabric, FortiCASB security alerts and logs can be shared with **FortiAnalyzer** to leverage SaaS security context.

FortiAnalyzer is a centralized security analytics that can view all Fortinet Security Fabric products in a bird's-eye view.

The purpose of Fabric Integration is so that other Fortinet security Fabrics such as **FortiGate** and **FortiClient** can access FortiCASB's SaaS security alerts and provide more oversight.

Fabric Integration Procedures

FortiAnalyzer will be configured and added on FortiCASB to initiate fabric integration.

Follow these configuration guide to add and configure FortiAnalyzer on FortiCASB:

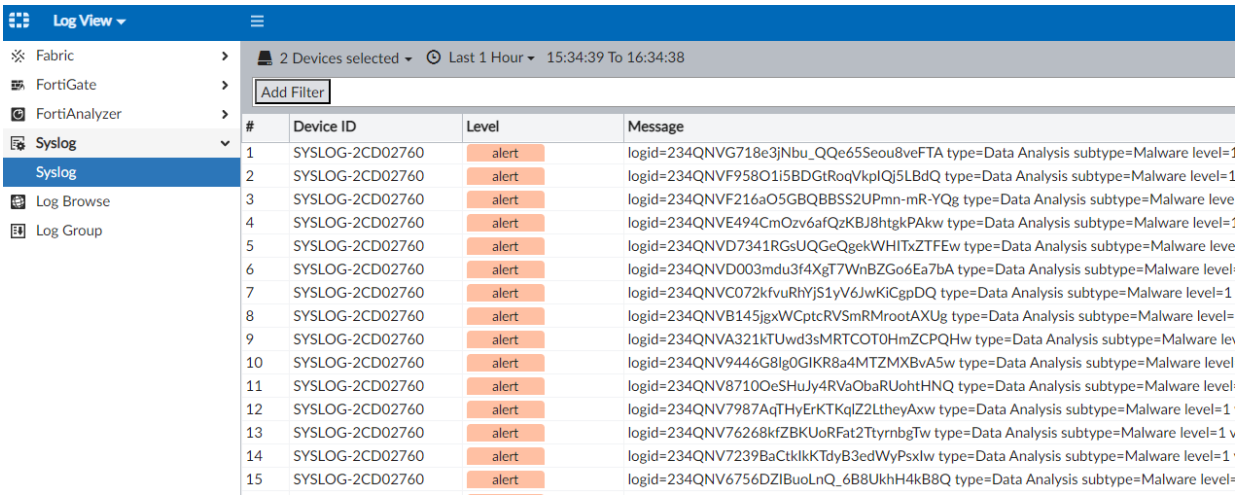
1. **Add FortiAnalyzer on FortiCASB on page 328**
2. **Authorize FortiCASB on FortiAnalyzer on page 330**

View FortiCASB Security Alerts on FortiAnalyzer

After FortiAnalyzer is configured and added on FortiCASB, FortiCASB will be recognized as a **Syslog** device

When Data Analysis alerts are sent to FortiAnalyzer, they will be displayed as **Syslog messages**.

In FortiAnalyzer, Syslog messages can be viewed in **Log View > Syslog**.



The Syslog details contain alert details sent from FortiCASB.

FortiCASB Syslog Message Variables Specifications:

Variable Name	Description
type	The type of alert sent from FortiCASB: **Data Analysis**, **Threat Protection**, or **Compliance**.
subtype (optional)	Subtype is the Data Analysis policy's Data Pattern Category: **Personal Identity Information**, **Financial Information**, or **Malware**.
devid	The FortiCASB product serial number of which the alert is originated.
sessionid	The alert ID of the FortiCASB security alert sent.
eventtype	Event type is a static variable and will always show "FORTICASB-FINDING".
tz	Time Zone of the alert sent.
docsource	The cloud application where the security alert is triggered, e.g. **Salesforce, Office 365, Box, Dropbox, Google Workspace**, etc.

FortiAnalyzer Version Requirement

Fabric Integration requires FortiAnalyzer version **5.4 or later**.

Fabric Integration Port Requirement

There are two FortiAnalyzer ports that are required in Fabric Integration.

1. FortiCASB utilizes FortiAnalyzer TCP port for connection testing. A ping request is sent from FortiCASB to FortiAnalyzer TCP port 514 when FortiAnalyzer is first added to FortiCASB.
2. FortiAnalyzer UDP port 514 is used for sending Syslog messages from FortiCASB to FortiAnalyzer.

Please make sure FortiAnalyzer **UDP port 514** and **TCP port 514** are open to the following FortiCASB IPs depending on your region:

FortiCASB Global(US) IP - **52.41.24.220**

FortiCASB European Union IP - **34.247.192.72**

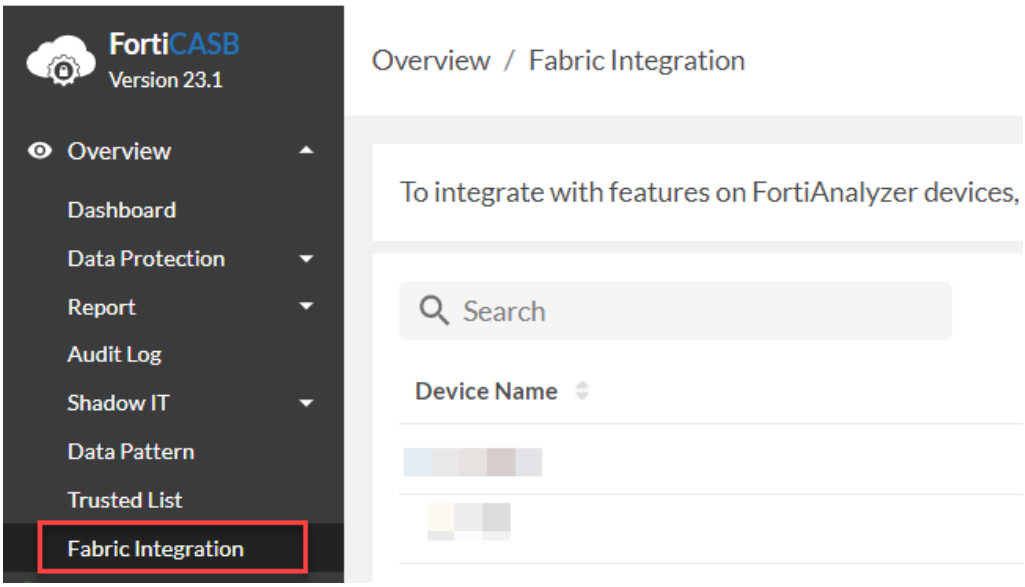
Add FortiAnalyzer on FortiCASB

Collect the following FortiAnalyzer information first before configure and add FortiAnalyzer on FortiCASB.

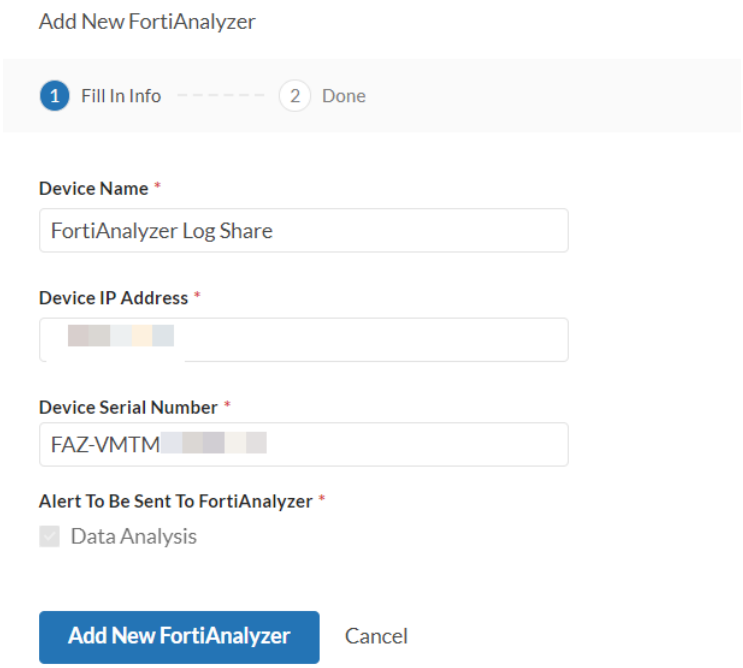
- IP Address of the FortiAnalyzer
- FortiAnalyzer Serial Number

Steps to add FortiAnalyzer on FortiCASB

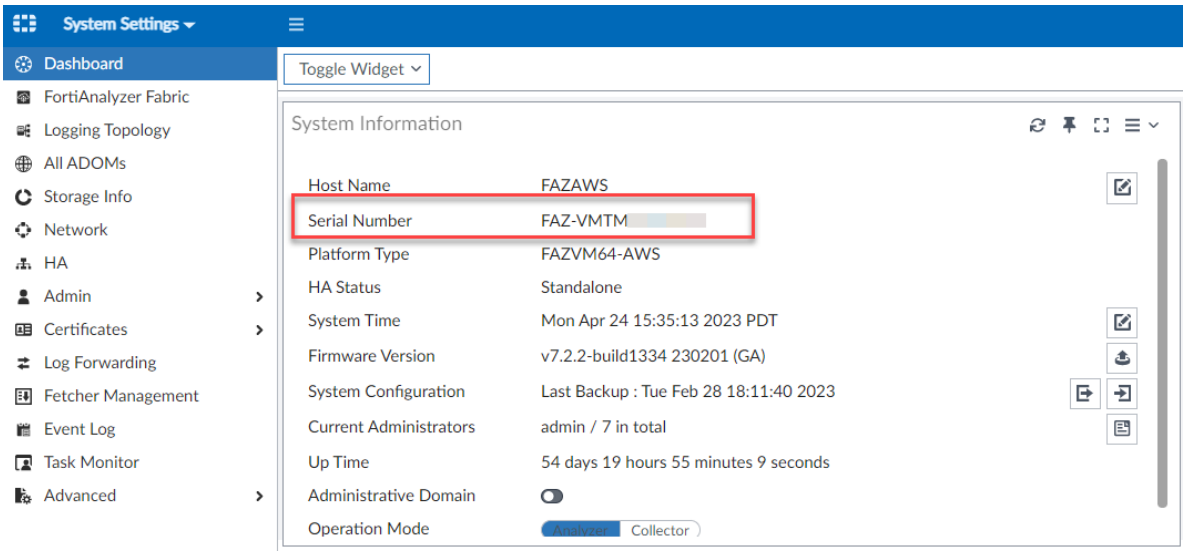
1. Go to **Overview > Fabric Integration**



2. Click **+Add New** to add new device.
   For **Device IP Address**, it is the IP address of the FortiAnalyzer, e.g.,254.254.254.254



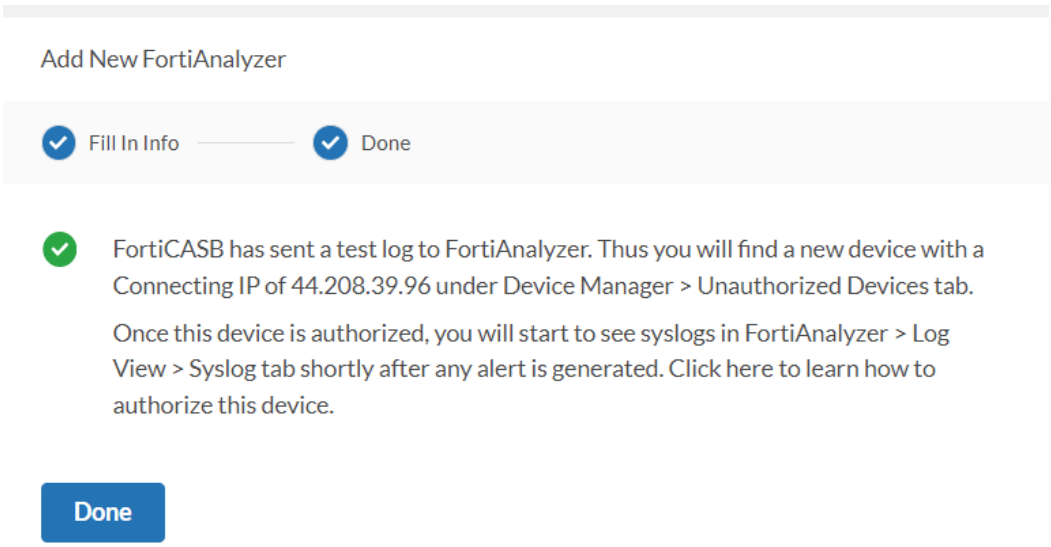
For **Device Serial Number**, in FortiAnalyzer, go to **System Settings**. Serial Number is located in **System Information**



3. Click **Add New FortiAnalyzer** to finish.

FortiCASB will send a test log to FortiAnalyzer and awaiting to be authorized.

See Authorize FortiCASB on FortiAnalyzer on page 330 to authorize FortiCASB on FortiAnalyzer.



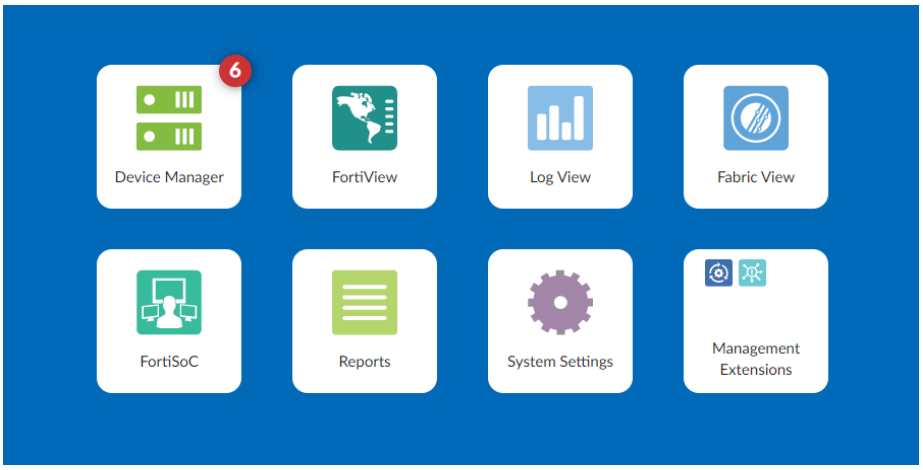
Authorize FortiCASB on FortiAnalyzer

After FortiAnalyzer is added and configured on FortiCASB, the last step is to authorize FortiCASB on FortiAnalyzer.

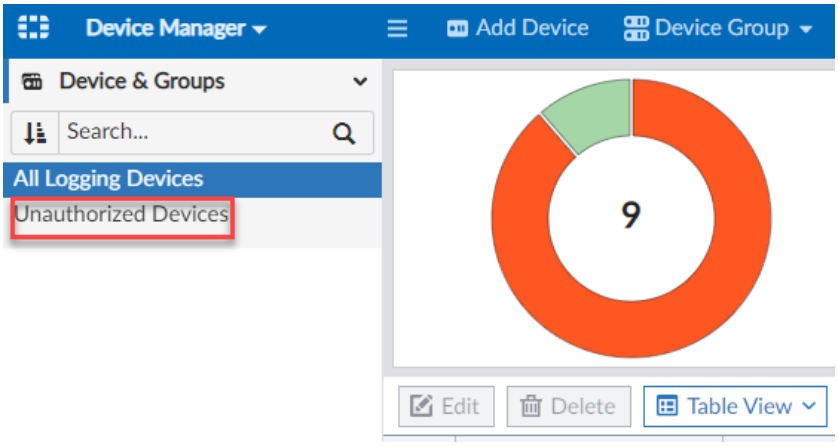
Please wait **5-10 minutes** for FortiCASB device to show up in FortiAnalyzer's list of unauthorized devices.

Once FortiCASB is authorized on FortiAnalyzer, FortiCASB security logs and alerts can be shared with FortiAnalyzer.

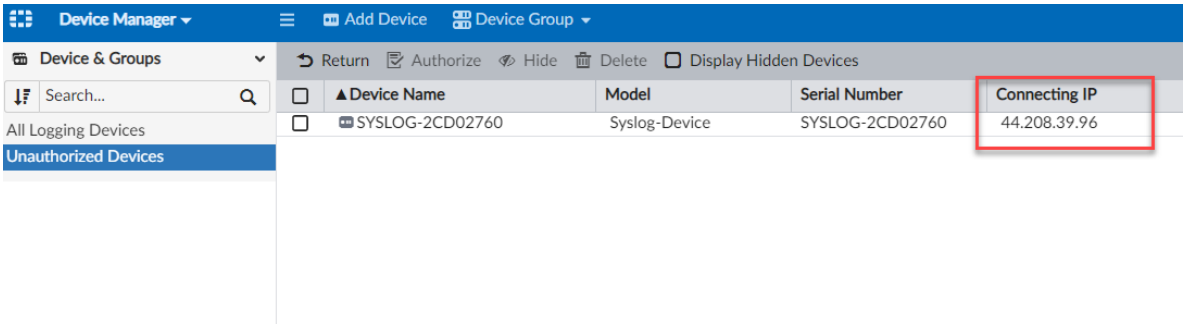
1. Log into FortiAnalyzer with your credentials.
2. Go to **Device Manager** from the main page.



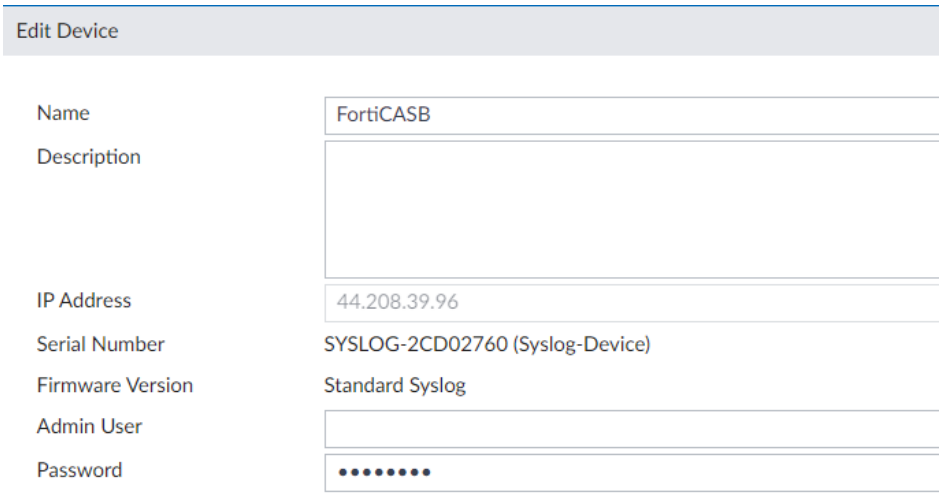
3. In **Device & Groups**, select **Unauthorized Devices**.



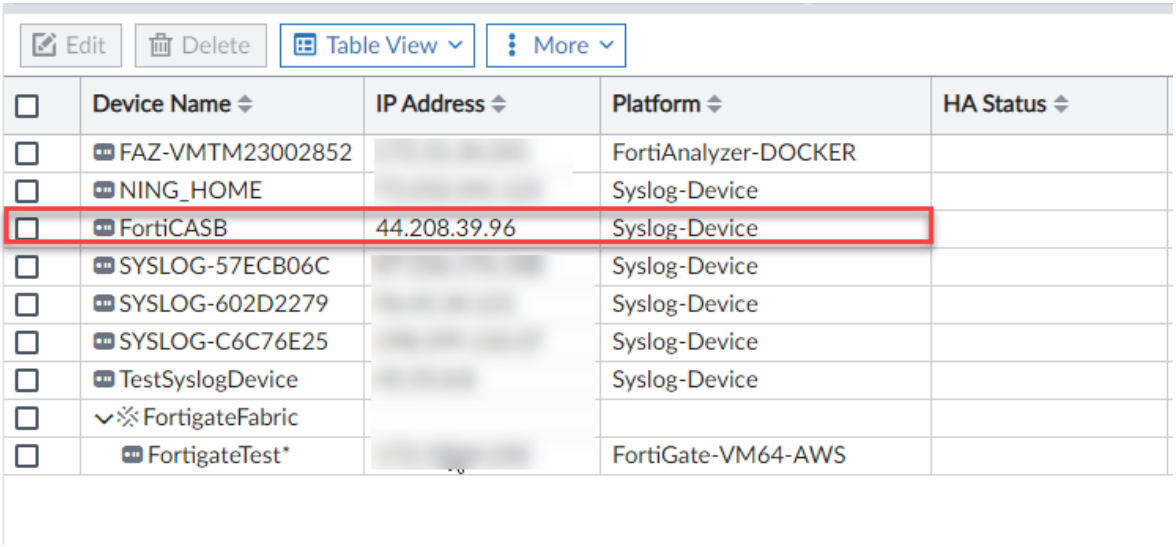
4. Check the FortiCASB device with **Connecting IP** as FortiCASB IP.



5. Click **Authorize**, and then click **OK** to confirm.
6. Select the device, click **Edit** and rename the device to "FortiCASB" or a name of your choice.(optional)



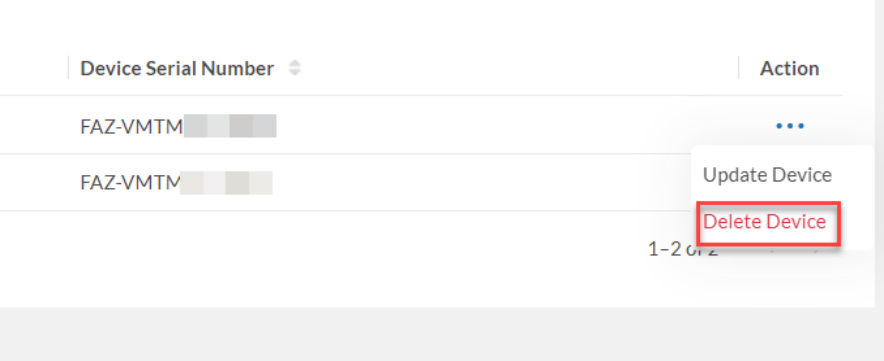
7. Now FortiCASB should be one of the authorized devices under **All Logging Devices**.



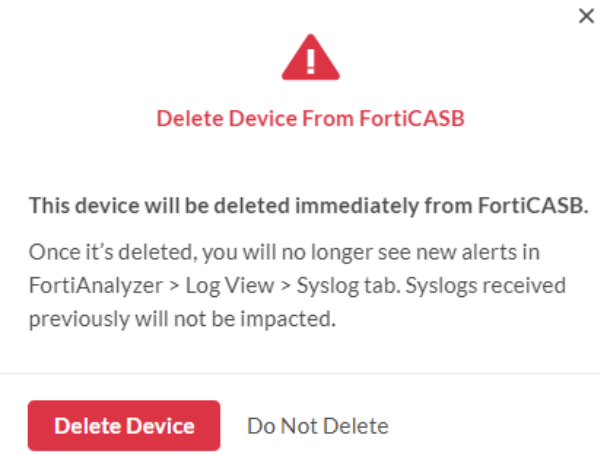
Remove Fortianalyzer from FortiCASB

When removing FortiAnalyzer from FortiCASB, FortiAnalyzer needs to be removed from FortiCASB, and FortiCASB needs to be removed in FortiAnalyzer list of devices to completely remove the fabric integration.

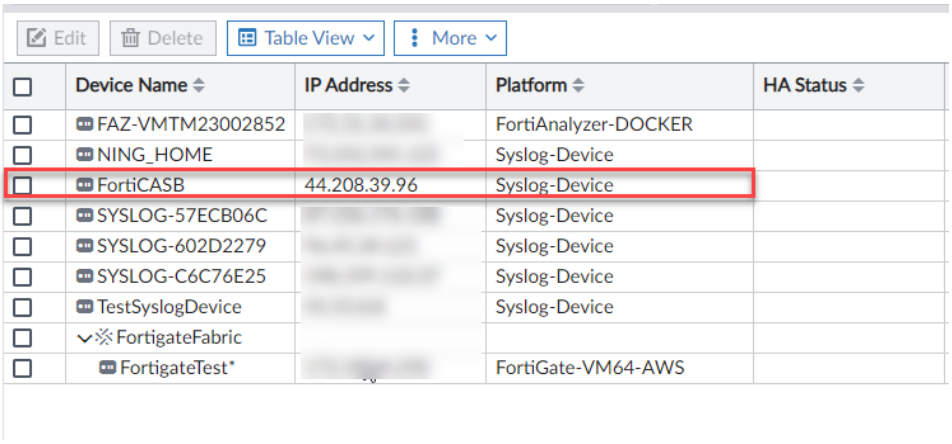
1. In FortiCASB, go to **Overview > Fabric Integration**
2. Locate the device to be removed, click **Action** and select **Delete Device**.



3. Click **Delete Device** again in the pop-up window to confirm.



4. Now log into FortiAnzlyzer, go to **Device Manager > All Logging Devices**.
5. Locate the device with FortiCASB IP address and delete the device.



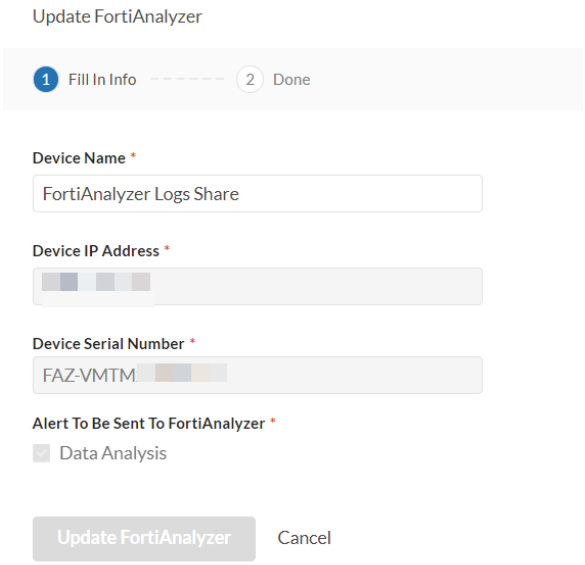
After the FortiAnalyzer removal procedure is completed , it will take about 5 minutes for FortiCASB to stop sending security alerts to FortiAnalyzer Syslogs.

Update FortiAnalyzer on FortiCASB

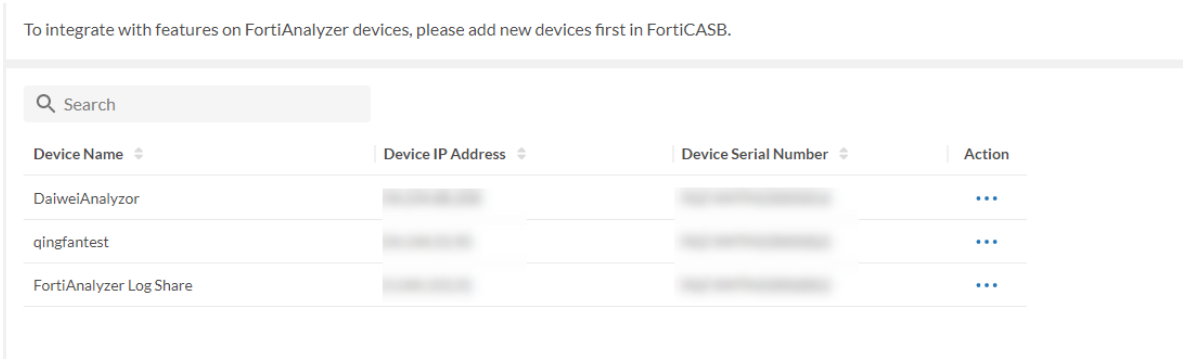
When updating FortiAnalyzer in FortiCASB, it allows you to rename the device in FortiCASB.

No action is required in the FortiAnalyzer side to update the FortiCASB configuration.

1. Go to **Overview > Fabric Integration**.
2. For the device to be updated, click **Action** and select **Update Device**.
3. Rename the **Device Name**.



4. Click **Update FortiAnalyzer** to finish device update.



Data Protection Features

This sections covers Data Protection features in FortiCASB. Data Protection are the fundamental features of FortiCASB where all SaaS application data are monitored and protected through Data Protection Policy and analyzed through Files and Discovery.

Data Protection Topics

Data Protection Discovery Analytic

Introduction

Discovery is located in **Data Protection > Discovery**. Discovery is an all-in-one analytics where all files from the supported SaaS applications on board are analyzed and categorized with emphasis on files and users who have access to the files that poses the most security vulnerability.

FortiCASB classifies data resides in cloud accounts as Data at Rest or Traffic Data.

Data At Rest is data uploaded onto the cloud application before the cloud account is added to FortiCASB.

Traffic Data is any data uploaded after the cloud account is added to FortiCASB and security monitoring has been initiated.

When the cloud account is on board in FortiCASB, the files are scanned individually when there is an access attempt. After the data scan is completed, depending on the **Data Analysis** policies enabled, FortiCASB will classify the files as either **sensitive** data or **non-sensitive** files.

Discovery currently only supports the following cloud application platforms:

Salesforce Office 365, Box, Dropbox, Google Workspace, Egnyte, Github, and **Webex**.

All Files Overview

Malware are malicious softwares or files that can steal sensitive or valuable information from the cloud accounts.

Click on Malware to review and remove malwares from cloud accounts before any data is compromised.

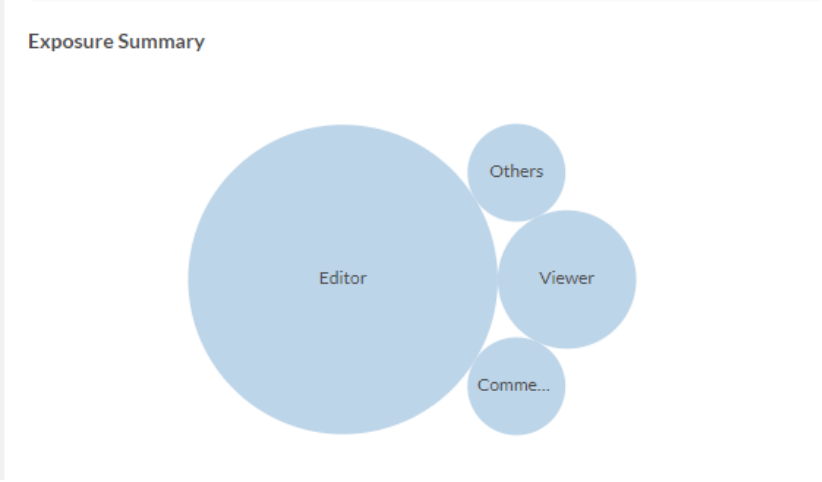
Sensitive Files are files that with **DLP(Data Loss Prevention) data** that contains personal information identified by Data Analysis policies.

Click on the Sensitive files to show all files that have sensitive data to protect the personal identity information from being exposed to unauthorized personnel.

Shared Files are files shared by the file creators to other users, groups, or any collaborators.

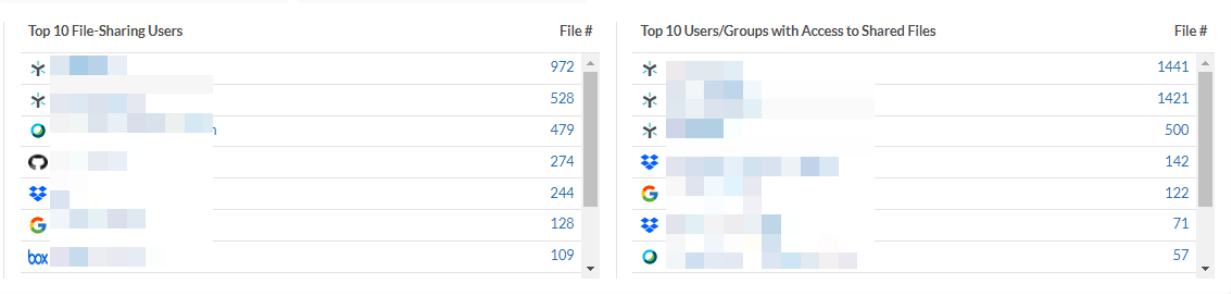
Click on Shared Files to review the cloud application files shared.

High Risk File Owner are users that are considered as high risk users who share sensitive files with other users.



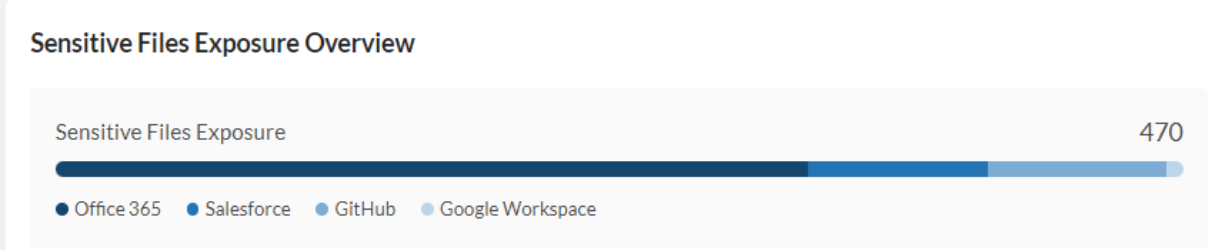
Exposure Summary categorizes users with access to files into different categorizes. **Viewer**, **Editor**, **Commenter**, and **Others** are normalized share types of all cloud platforms. For more details on normalized share types, see Appendix B - Normalized Share Types on page 541. Click on each normalized share type to show only files shared by the specific type of user.

Top 10 File-Sharing Users are the top 10 file sharing users across all on board cloud applications.



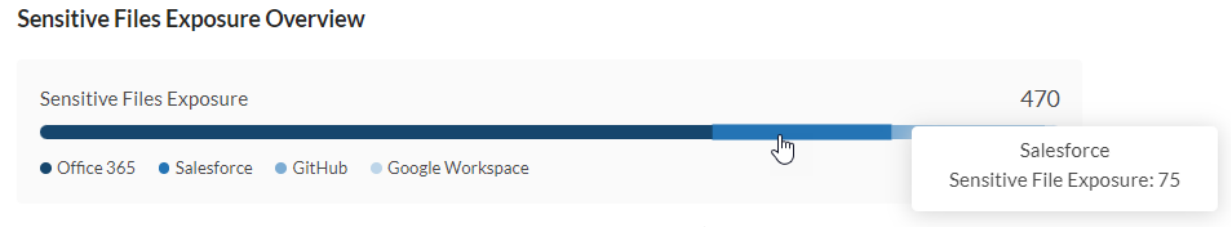
Top 10 Users/Groups with Access to Shared Files are the top 10 users that are grant the most number of file access.

Sensitive Files Exposure Overview



Sensitive Files Exposure Overview is an intuitive graphical distribution which reveals the number of Sensitive files shared per cloud application.

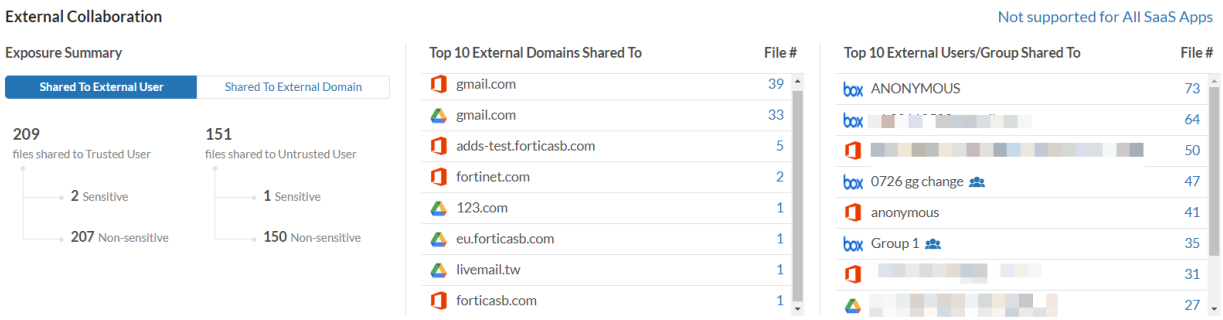
Hover the mouse over different colors to reveal the number of sensitive files shared from the targeted cloud application.



External Collaboration

External Collaboration Summary reveals the total number of sensitive and non-sensitive files shared to external users/group and external domains.

External Collaboration summary only supports **Office 365**, **Dropbox**, **Google Workspace**, and **Box**.



Top 10 External Domains Shared To outlines the top 10 external domains which the cloud application files are being shared with.

Top 10 External Users/Group Shared To depicts the top 10 external users/groups have access to the cloud application files.

Data Protection Files Analytics

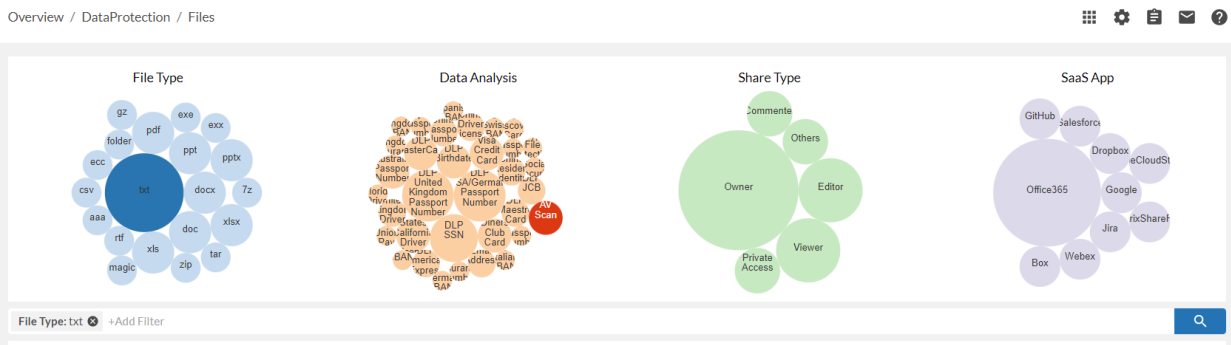
Introduction

Files is an all in one SaaS data storage security analytics located in **Data Protection > Files**. All files of all cloud application on board can be accessed in Files.

When a cloud account is first added to FortiCASB, files resided in the cloud account are pulled into the Files page. Then FortiCASB automatically updates the file status in Files page when users attempt to access files through the cloud application account.

Files is also available in each of the cloud application except **SAP IAS** and **Zoom**.

The files bubble chart gives an overview of the files categorized by **File Type**, **Data Analysis**, **Share Type**, and **SaaS App**. (SaaS App bubble chart is only available in the all in one Files in Data Protection.)



File Type captures all file types regardless of readability within the scope of cloud account storage/bucket.

Click on each file type bubble to show files with the specific file type.

Data Analysis scans and captures all files that contains DLP (Data Loss Prevention) data. Each bubble represents different Data Analysis policy.

Click on each Data Analysis bubble to show files only pertain to that Data Analysis policy.

Share Type is a normalized share type that normalized all cloud account users by grouping them together by access permission. For more detail on normalized share type, please see Appendix B - Normalized Share Types on page 541.

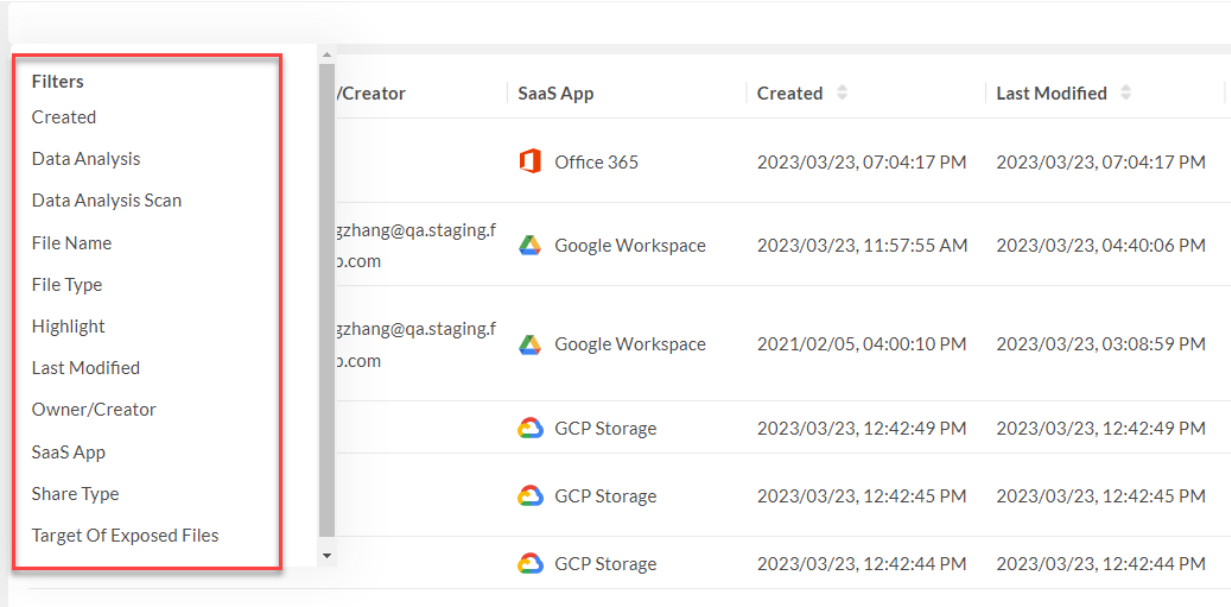
Click on each share type to see only files shared by the specific share type users.

SaaS App filters all cloud application files by cloud platform.

Click on each app bubble to filter the files by app.

Sort Cloud App Files by Filter

There are 11 filters that files can be sorted to identify the targeted files among all cloud applications:



For more information on **Highlight** and **Data Analysis Scan** filters, please see:

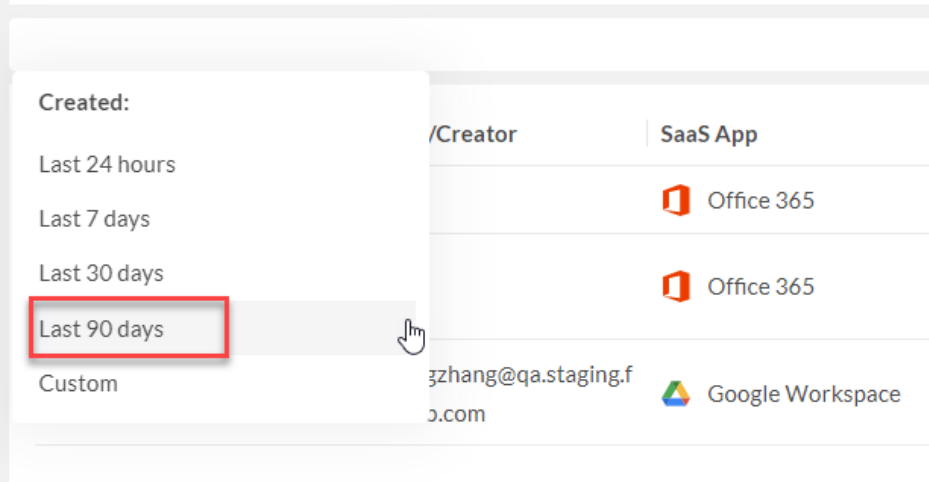
Highlight Filter on page 342

Data Analysis Scan Filter on page 343

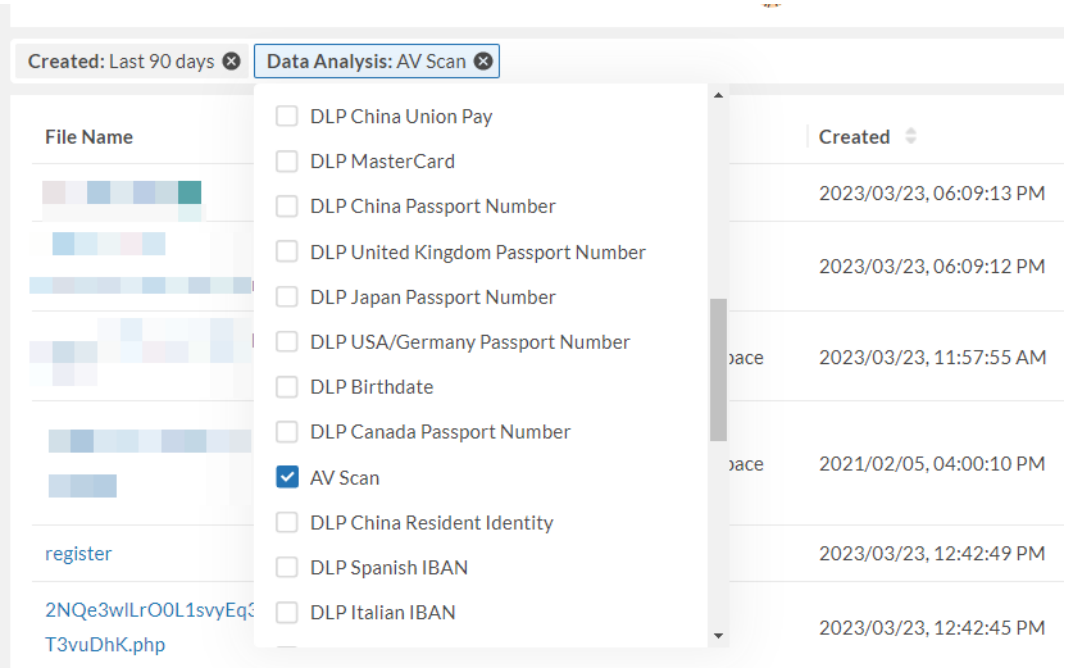
Example on using Files Filter

This example filters through all files for Malwares detected in the last 90 days among all cloud applications.

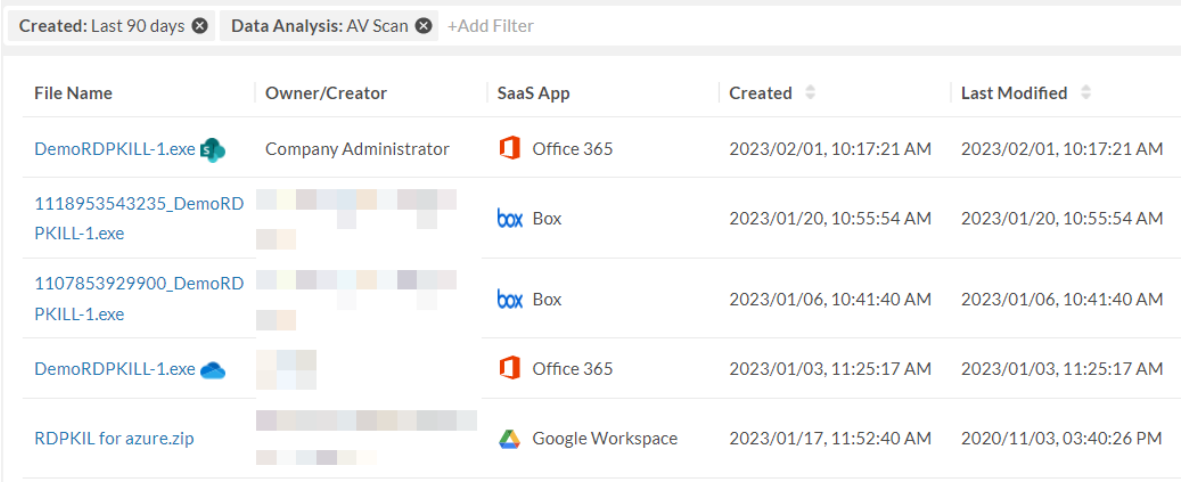
1. Click on **+Add Filter**.
2. Select **Created > Last 90 days**.



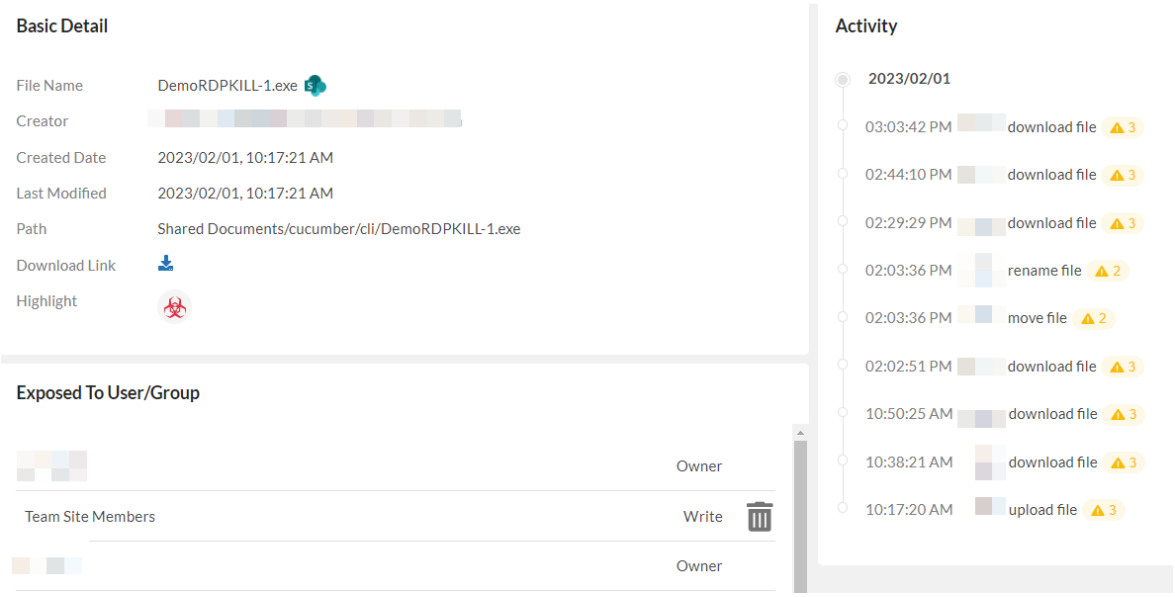
3. Click **+Add Filter** again.
4. Select **Data Analysis > AV Scan**.



5. Click **Search** sign and filter through all files.
6. All Malwares from the last 90 days are displayed.

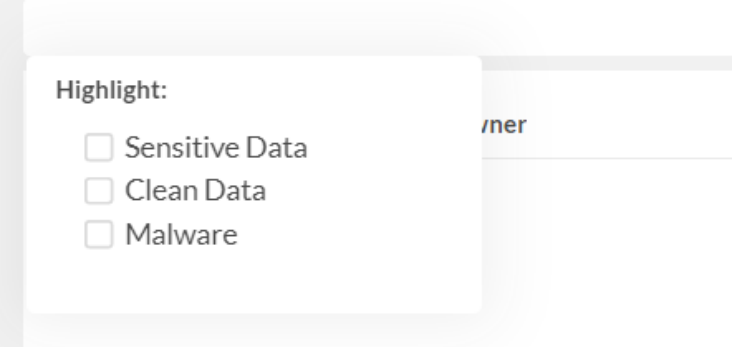


7. Click on any one of malware to view basic details, activity, users exposed, and data pattern violation.



Highlight Filter

The **Highlight** filter filters through all files for specific file type: **Sensitive**, **External**, and **Malware**.



Below is correlated Highlight and file type with description.

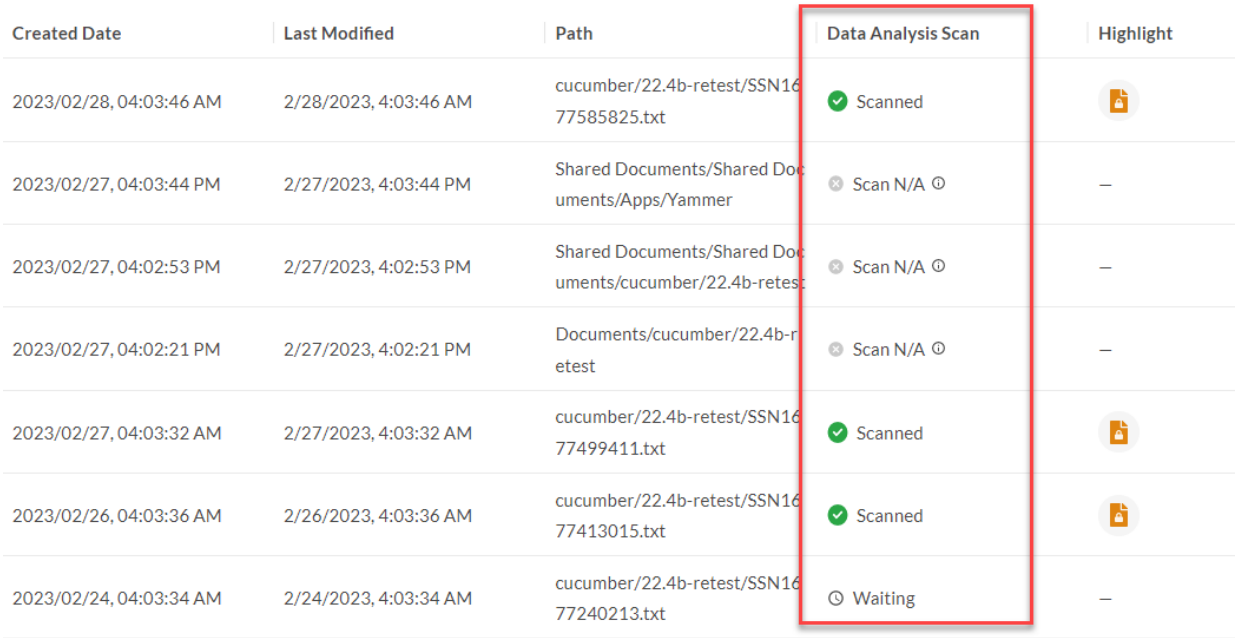
Highlight Icon	Document Type	Description
	Sensitive	Files with sensitive information searched and matched by DLP policies such as Social Security Number, Visa Credit Card number, etc.
	External	Files shared with the external users/groups.
	Malware	Infectious files searched and matched by the malware policies through AV scan.

Data Analysis Scan Filter

Data Analysis Scan, also called **DLP Scan (Data Loss Prevention scan)** identifies Personal Identification Information(PII) such as Driver License, Credit Card, Social Security Numbers, etc resting in the organization's cloud account. It gives cloud administrators the opportunity to take action against possible external or internal threat:

1. Possible network intrusion access on sensitive data.
2. Unauthorized internal storage of personal or sensitive data.
3. Detect potential malware and virus through Fortinet AV scan.

The Data Analysis scan is triggered when user activity is detected on the file resting in the cloud account. If the file is identified to be a type of personal identification information, it will be noted in the file details.



Created Date	Last Modified	Path	Data Analysis Scan	Highlight
2023/02/28, 04:03:46 AM	2/28/2023, 4:03:46 AM	cucumber/22.4b-retest/SSN16 77585825.txt	Scanned	
2023/02/27, 04:03:44 PM	2/27/2023, 4:03:44 PM	Shared Documents/Shared Doc uments/Apps/Yammer	Scan N/A	–
2023/02/27, 04:02:53 PM	2/27/2023, 4:02:53 PM	Shared Documents/Shared Doc uments/cucumber/22.4b-retest	Scan N/A	–
2023/02/27, 04:02:21 PM	2/27/2023, 4:02:21 PM	Documents/cucumber/22.4b-r etest	Scan N/A	–
2023/02/27, 04:03:32 AM	2/27/2023, 4:03:32 AM	cucumber/22.4b-retest/SSN16 77499411.txt	Scanned	
2023/02/26, 04:03:36 AM	2/26/2023, 4:03:36 AM	cucumber/22.4b-retest/SSN16 77413015.txt	Scanned	
2023/02/24, 04:03:34 AM	2/24/2023, 4:03:34 AM	cucumber/22.4b-retest/SSN16 77240213.txt	Waiting	–

Data Analysis Scan Status

Data Analysis Scan Status	Description
Scanned	The Data Analysis scan has completed and the scan result is available to the administrator.
Scan N/A	Data Analysis scan is not conducted on the file due to **Data Analysis Scan Limitations on page 344**.
Waiting	There has not been any user activity, thus the file is awaiting to be scanned by Data Analysis.

Data Analysis Scan Limitations

Data analysis scan become unavailable or **"Scan N/A"** status under the following circumstances:

1. The file size exceeds 20MB.
2. The file extension is not a supported type. (See for supported file type)
3. When all Data Analysis policies are disabled, the Data Analysis Scan become unavailable. (See **Policy Configuration on page 405** for Data Analysis Policy Configuration)

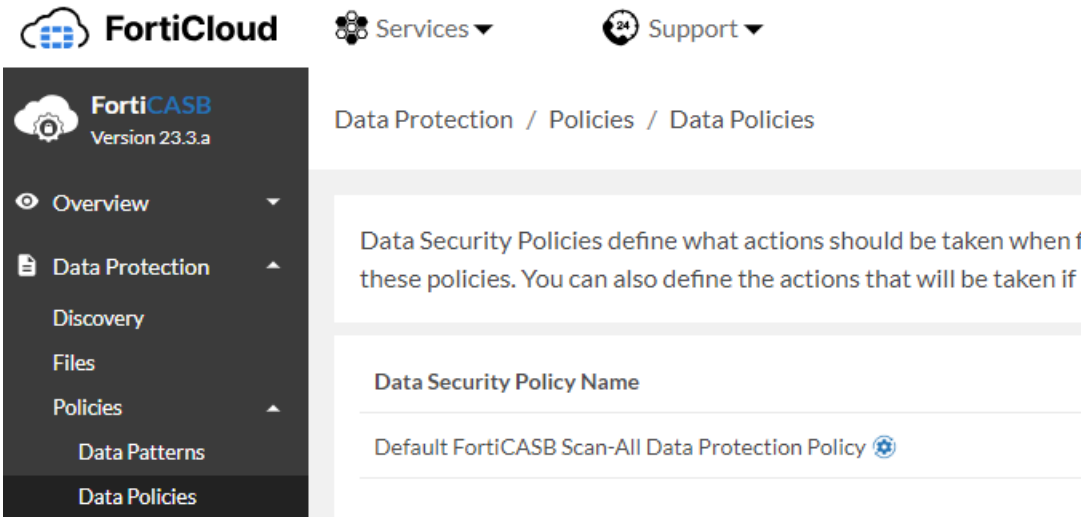
Data Security Policy

Introduction

Data Security Policy defines which DLP data patterns should be monitoring what type of files under which SaaS applications, and what activities would trigger an alert. In addition, when a data security alert is triggered, what action should be taken to mitigate.

In 2024, a major enhancement leveraging an Large Language Model framework with AI capability to accurately trigger DLP alerts that match Data Security policy, false positives and false negatives are minimized while providing better classification for text that can potentially match multiple data types.

Data Security Policy can be created in **Data Protection > Policies > Data Policies**.



File types Supported by Data Security Policy

These are the file types supported by Data Security Policy:

Compressed/UnCompressed	File Types
Uncompressed	Microsoft Word Document (.doc, .docx)
	Microsoft Powerpoint Document (.ppt, .pptx)
	Microsft Excel Document

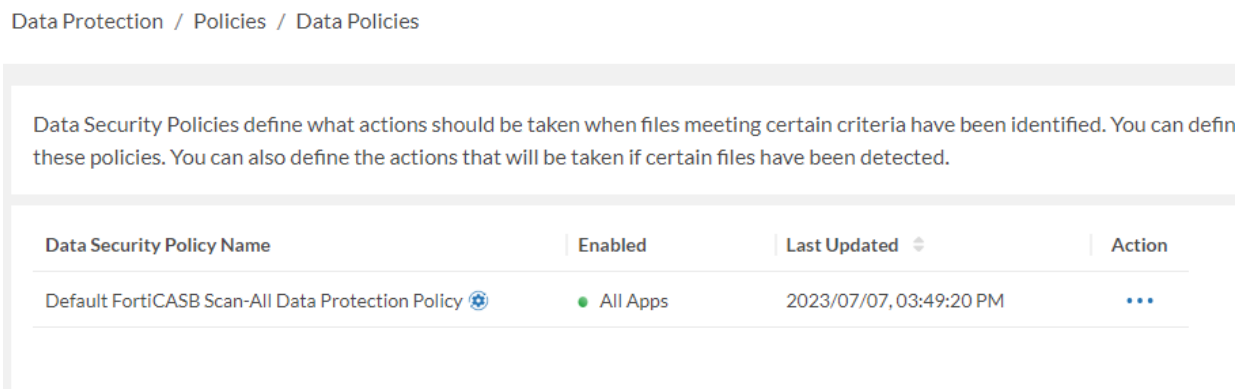
Compressed/UnCompressed	File Types
	(.xls, .xlsx)
	Text File (.txt, .rtf ,js)
	Portable Document Format (.pdf)
Compressed	.zip
	.tar
	.7z
	.gz
	.exe

FortiCASB DLP scan extracts and scans compressed files without limitation on the level of compressions.

For example, a zipped file that is zipped multiple times under a zip file will still be DLP scanned.

Predefined Data Protection Policy

Default FortiCASB Scan-All Data Protection Policy is the predefined default data security policy where all files under all onboarded SaaS accounts are monitored for all types of file activities using the 34 FortiCASB basic predefined data patterns. For the full list of basic predefined data patterns, please see Basic Predefined Data Patterns.

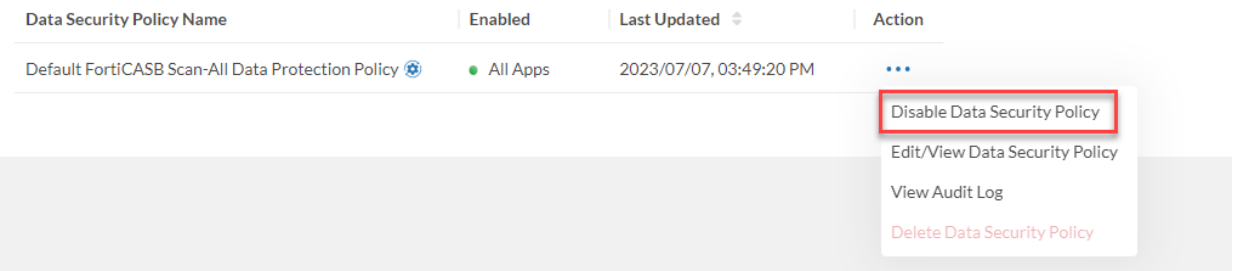


To utilize all 147 predefined data patterns and customized data pattern, create a Customized Data Protection policy to incorporate other predefined and customized data pattern.

Customized Data Protection Policy

Customized Data Protection policy can be created through **+Add New**.

Important: When a customized data protection policy is enabled, the **Default FortiCASB Scan-All Data Protection Policy** needs to be **disabled** to avoid two conflicting policies.



Data Security Policy Best Practice

1. Create a customized data protection for specific files you are monitoring. This practice can avoid conducting DLP scan on files that are not intended to be monitored.
2. When choosing DLP Patterns, only choose the DLP patterns that needs to be protected and monitored. This practice avoid conducting unnecessary DLP scans over time.
3. Always turn on **Email Notification** and **Notify File Owners** features to send alerts to relevant personnel to expedite the mitigation process.
4. Take advantage of **Send Alert to FortiAnalyer** feature if FortiCASB is one of the security fabrics in your organization.

Data Security Policy Match Criteria

There are eight match criteria that data security policies offers that can be customized when **Customized Data Security** policy is created.

Files Created After on page 348

File Types on page 348

Access Permissions on page 348

File Activity Triggers on page 349

Files Shared With Users/Domains NOT In Trust List (Google Workspace files only) on page 349

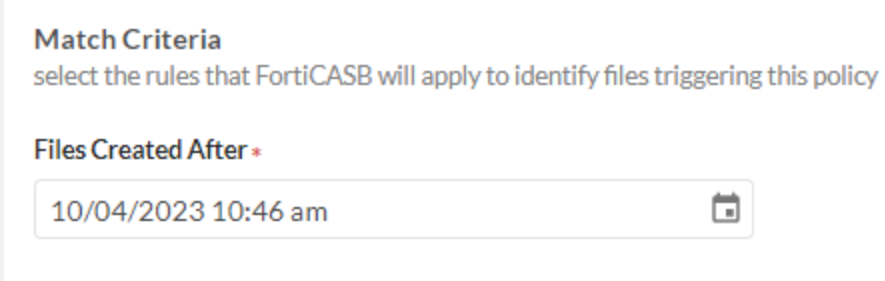
Label Triggers (Google Workspace Only) on page 351

SaaS Applications on page 350

Data Patterns on page 350

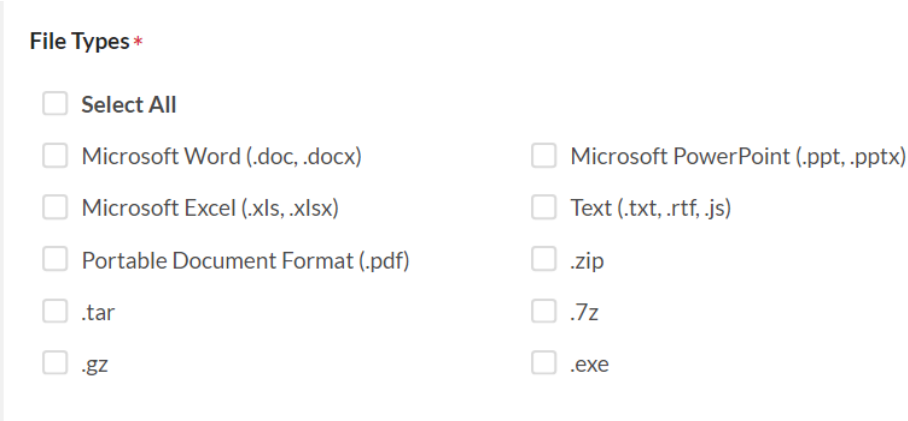
Files Created After

Time frame of the files being targeted, only the files on the SaaS application created after the designated day are targeted for data scan.



File Types

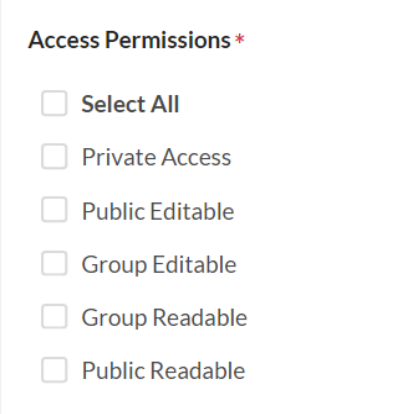
The file types being targeted for DLP scan, supported file types are **doc, ppt, pptx, xls, xlsx, txt, rtf, js, pdf, zip, tar, 7z, gz, exe**.



Access Permissions

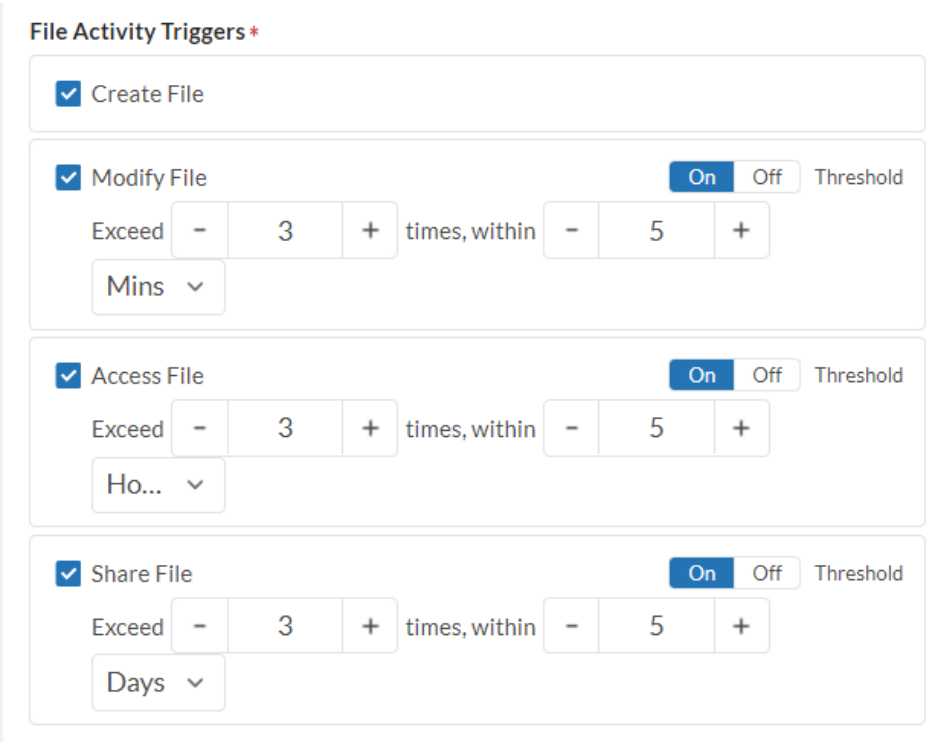
The access permission option can be customized to target specific share permissions of the files.

The supported file sharing types are **Private Access**, **Public Editable**, **Group Editable**, **Group Readable**, and **Public Readable**.



File Activity Triggers

The File Activity Triggers target specific file activities conducted on the file. Supported file activities are **Create File**, **Modify File**, **Access File**, and **Share File**. File Activity Triggers has configurable threshold that can be adjusted based on the number of times the activity is detected in a specified time frame.

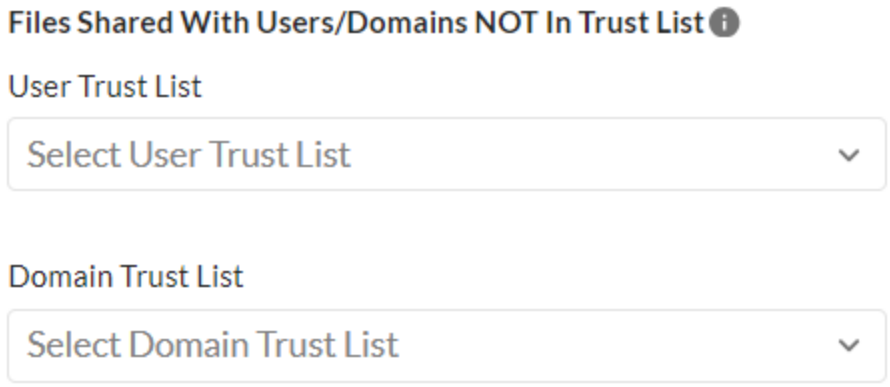


Files Shared With Users/Domains NOT In Trust List (Google Workspace files only)

The users and domains selected from the **User Trust List** and **Domain Trust List** will be monitored for files shared between the trusted users and external users. An alert will be triggered when a file is shared by a trusted user/domain with an external user.

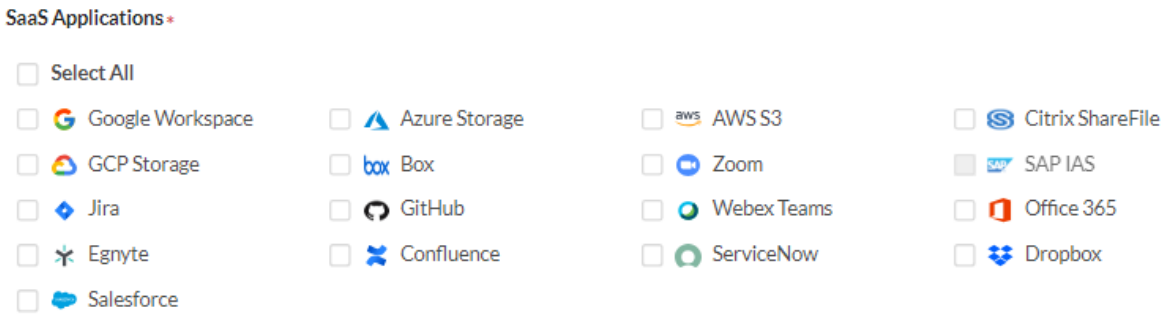
For example, when a trusted user named John Meyer shared a file with Mike Taylor who is not part of the Trust List. An alert will be triggered.

User Trust List and Domain Trust List can be configured in **Overview > Trusted List**.



SaaS Applications

In SaaS Applications option, only **onboarded** SaaS applications will appear in this section. Selected only the SaaS applications that will be targeted for DLP data scan.

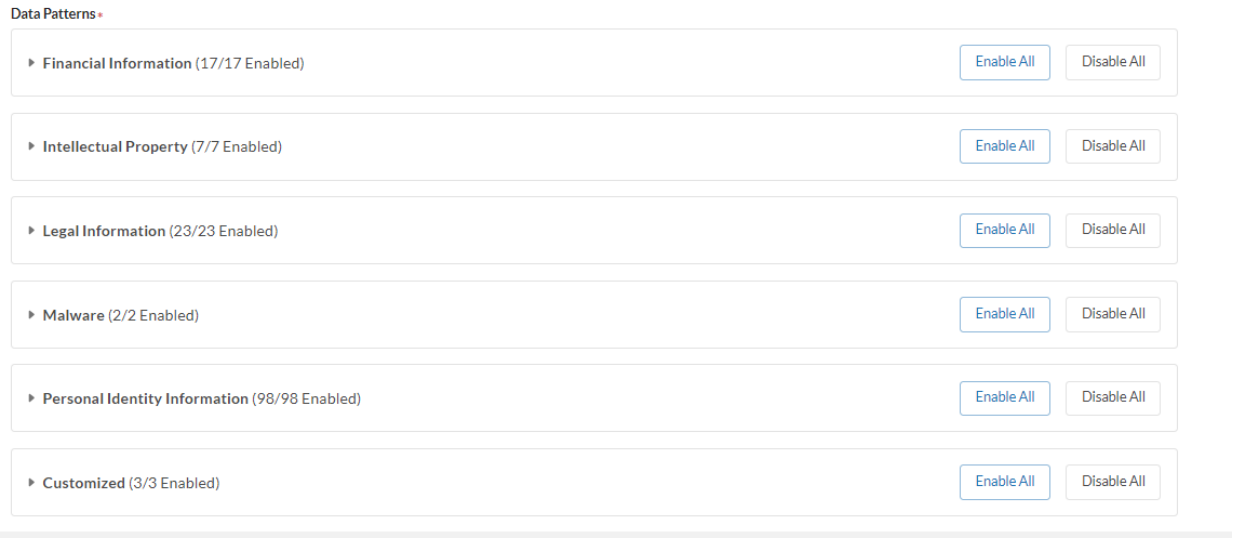


Note: **SAP IAS** is not supported in Data Security policy.

Data Patterns

DLP Patterns selection determines which data patterns will be used in the Data Security Policy. Both Predefined Data Patterns and Customized Data Patterns can be selected as the match criterias.

For more details on supported DLP patterns, please see Predefined Data Pattern on page 366 and Customized Data Pattern on page 374.



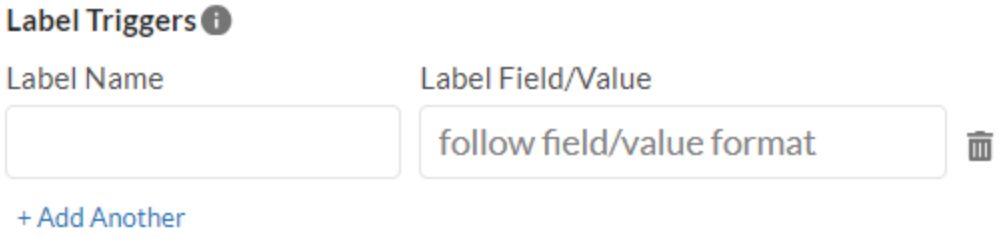
Label Triggers (Google Workspace Only)

Label Triggers only supports Google Workspace (Google Drive) files. Google Drive file label is a customizable label that can be attached to files in Google Drive.

For more information on Google Drive Labels please see Get Started as a Drive Labels admin.

Prerequisite

1. Before using Label Triggers as match criteria, Google Drive Labels APIs needs to be enabled. Please see Enable Drive Labels API (Google Workspace Only) on page 354
2. If this is your first time using Label Triggers, please first update the Google Workspace account in FortiCASB. Please see Update Google Workspace Account on page 158.



Label Name - the name of the Google file label.

Label Field/Value - Label Field is the field name and Value is the field value of the Google file label, separated by "/".

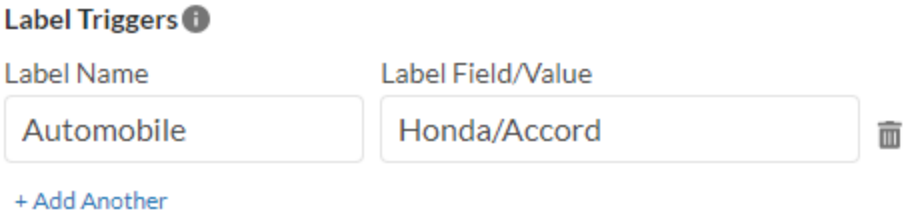
Depending on the label trigger created, Google Drive files will be matched only based on the label name and label field/value entered. And only the files matched will be data scanned. There are five types of Label Triggers Input:

Lable Type	Types of Label Triggers Input	Description
Standard Label	Label Name, Label Field/Value	All the file's label name, field name, and field value need to be matched.
Standard Label	Label Name, Field/	Only the file with the same label name and field name will be matched. If the label name and field name are the same, but has a value, then the file will be ignored.
Standard Label	Label Name	Only the file with the same label name and without any field name/value will be matched.
Badged Label	Lable Name, /Value	Both label name and label Value need to be matched. If the label name is the same but has not label value, it will not be matched.
Badged Label	Label Name	Only the file with the same label name will be matched. The file with the same label name but with a value will be ignored.

Label Trigger Input Examples

1. Standard Label - Label Name, Label Field/Value

In this example, only files with label name "Automobile" and label field/value "Honda/Accord" will be matched.



2. Standard Label - Label Name, Field

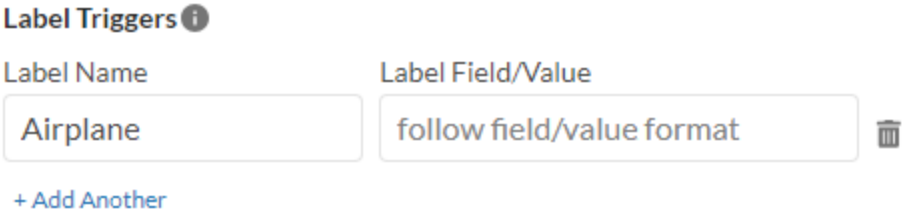
In this example, only files with label name "Mouse" and label field name "Test" will be matched.

If the file has a label name "Mouse", but with a different field name or no field name it will not be matched.

Lastly, if it has the same label name "Mouse" and field name "Test" but has a value, the file will not be matched.

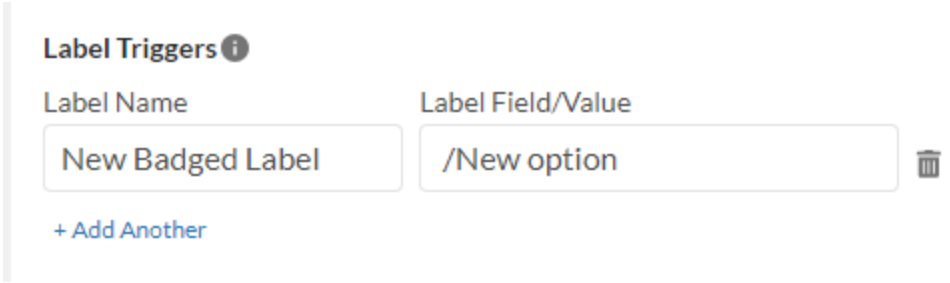
3. Standard Label - Label Name

In this example, only the file with the label name "Airplane" will be matched. If the file has the label name "Airplane", but with a field or value, the file will not be matched.



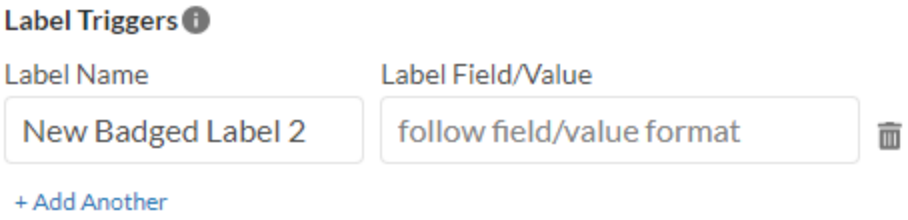
4. Badged Label Name - Label Name/Value

In this example, only files with the label name "New Badged Label" and value " /New Option" will be matched. If the file has the same label name but without a label value, it will not be matched.



5. Badged Label Name - Label Name

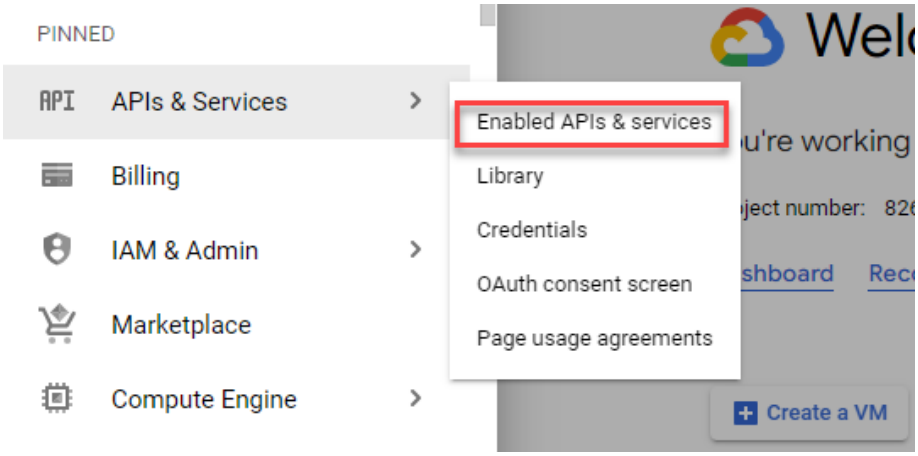
In this example, only file with the label name "New Badged Label 2" will be matched. If the file has the same label name but with a value, the file will not be matched.



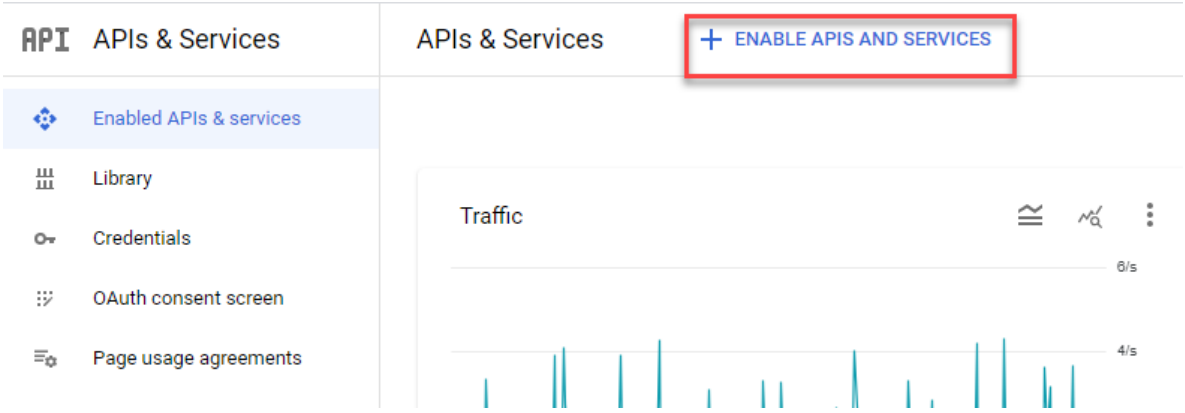
Enable Drive Labels API (Google Workspace Only)

The Drive Labels API need to be enabled for FortiCASB to collect Google Drive labels data for the purpose of Data Security Policy configuration and Google Workspace documents' basic profile labels.

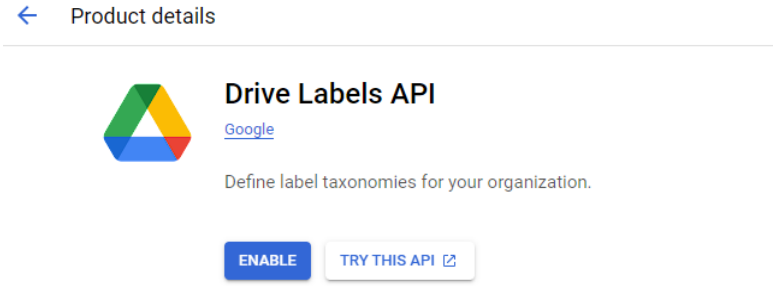
1. Log into Google Cloud Console with your Google Workspace account.
2. Click on the navigation menu button, and go to **APIs & Services > Enable APIs & Services**.



3. In **APIs & Services**, click **+ Enable APIs And Services**.



4. In **API Library**, search for "Drive Labels API", and click on **Drive Labels API**.
5. Click **Enable** to enable the Drive Labels API.



Data Security Policy Actions

All incidents matched by the Data Security Policy will trigger the action items that are enabled.

Quarantine Files on page 356

Change Access Permission (Google Workspace Only) on page 359

Write Label To Files (Google Workspace Only) on page 360

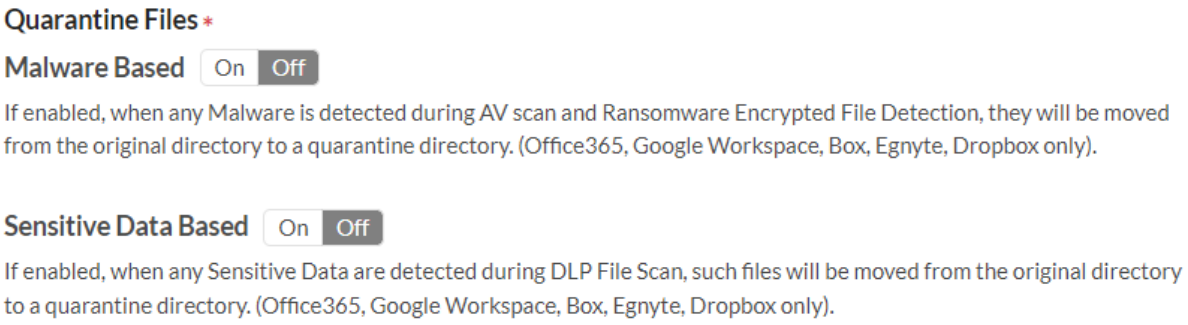
Send Email Notifications on page 362

Quarantine Files

The Quarantine File feature is designed to detect and move targeted files from the original directory to a quarantine directory and enable users to review the files later to determine the course of action that should be taken on the files.

At the moment, Quarantine Files feature is only available for **Office 365**, **Google Workspace**, **Box**, **Egnyte**, and **Dropbox**.

Types of Quarantine Files



There are two types of quarantine files:

Malware Based - when enabled, any malware(including virus and ransomewares) detected by the Fortinet Security Fabric during AV scan and Ransomeware Encrypted File Detection, will be moved from the original directory to a quarantine directory.

Senstive Data Based - when enabled, any type of sensitive data selected in the activated Data Security policy and detected during a DLP File Scan will be moved from the original directory to a quarantine directory.

Quarantine Directory

Files that are detected as malwares or deemed as sensitive data during AV scan or DLP file scan are moved from the original directory to a quarantine directory.

There are two types of quarantine directories.

1. **Default quarantine directory** - The default quarantine directory is preconfigured by FortiCASB as **forticasb_quarantine_directory~**. The quarantine directory will be placed at the root or top level of the file owner's account.
2. **Shared account quarantine directory** - If the infected file is in a shared account directory, the file will be removed from the shared account directory and placed at the root level of the **file owner's** account inside the directory, "**forticasb_quarantine_directory~**".

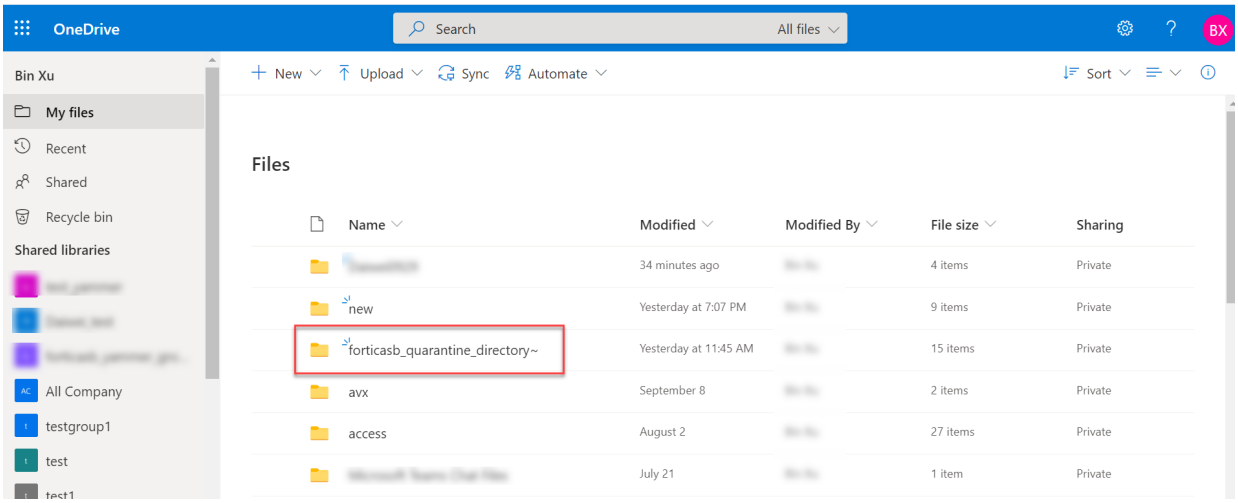
It is recommended for the file owner to review and remove the infected file from the quarantine directory.

Quarantine directory location by cloud account platform

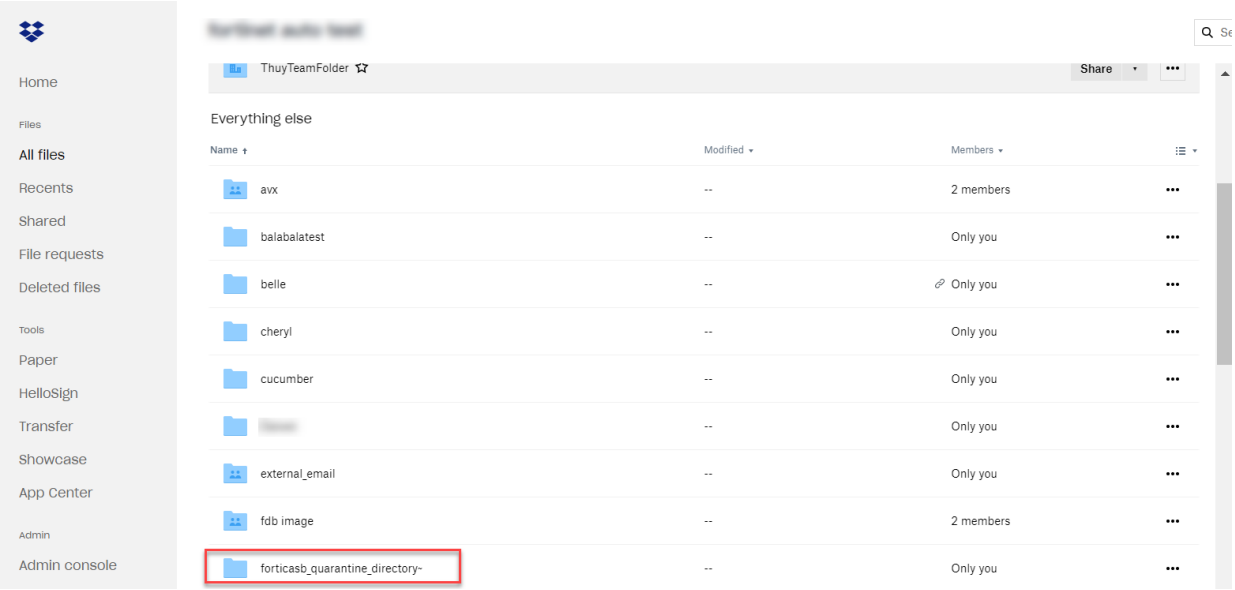
Cloud Account Platform	Quarantine Directory Location
Google Workspace	Root or top level of the file owner's account.
Office 365 One Drive	Root or top level of the file owner's account.
Office 365 SharePoint	Root or top level at the SharePoint Site of the file owner.
Box	Root or top level of the file owner's account.
Dropbox	Root or top level of the file owner's account.
Egnyte	Root or top level of the file owner's account.

Examples of quarantine directory on different cloud accounts

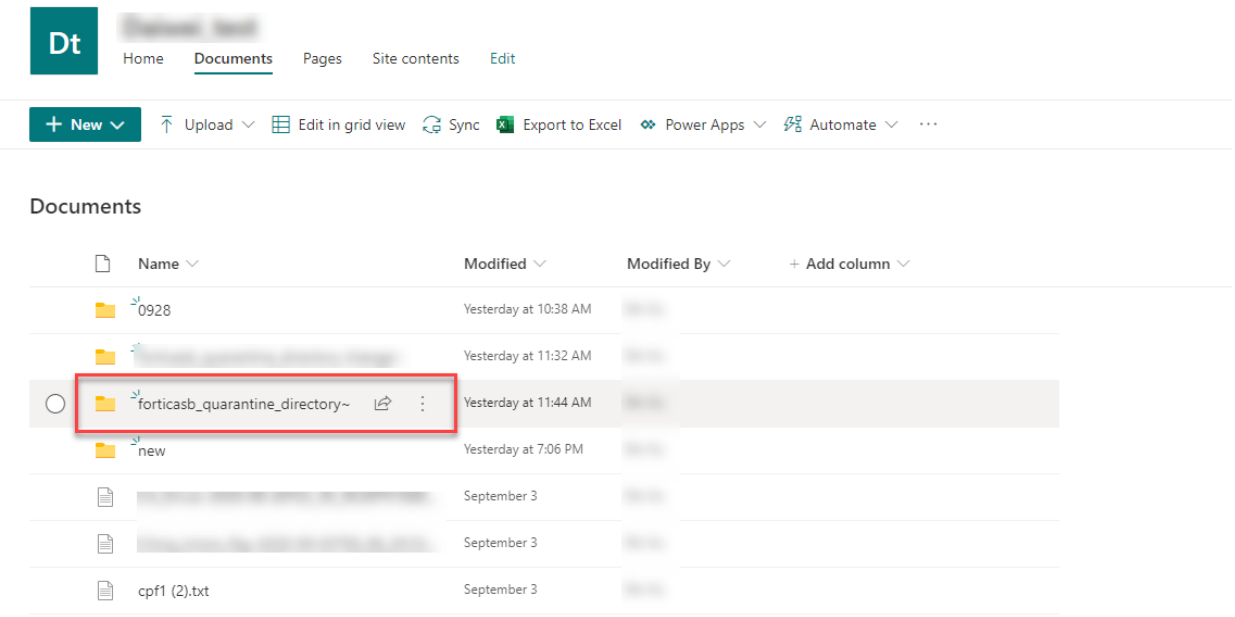
Quarantine directory on Office 365 One Drive



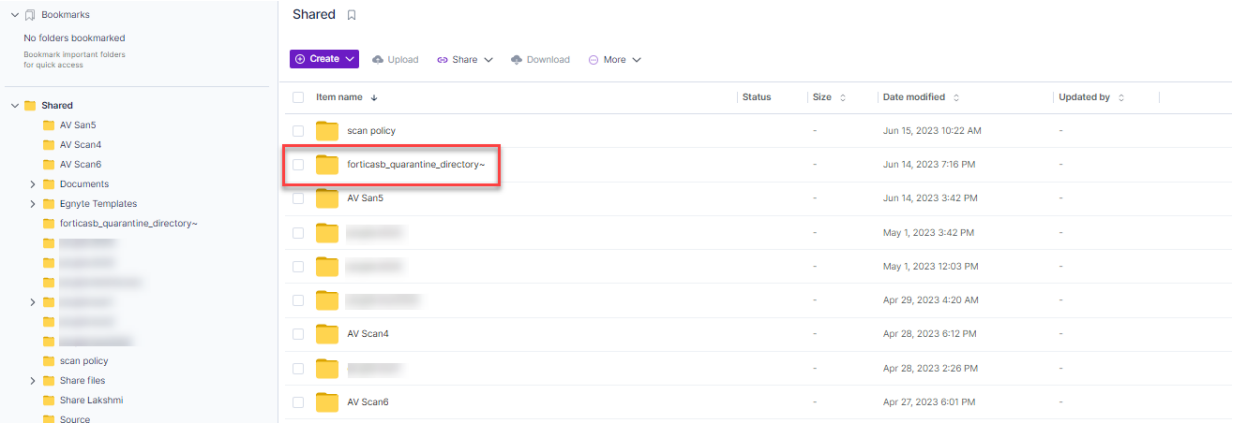
Quarantine directory on Dropbox Account



Quarantine directory on Office 365 SharePoint Site

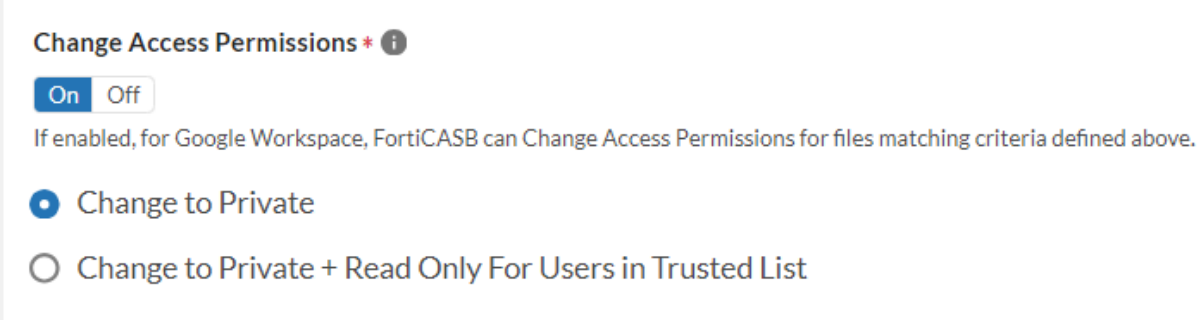


Quarantine directory on Egnyte account



Change Access Permission (Google Workspace Only)

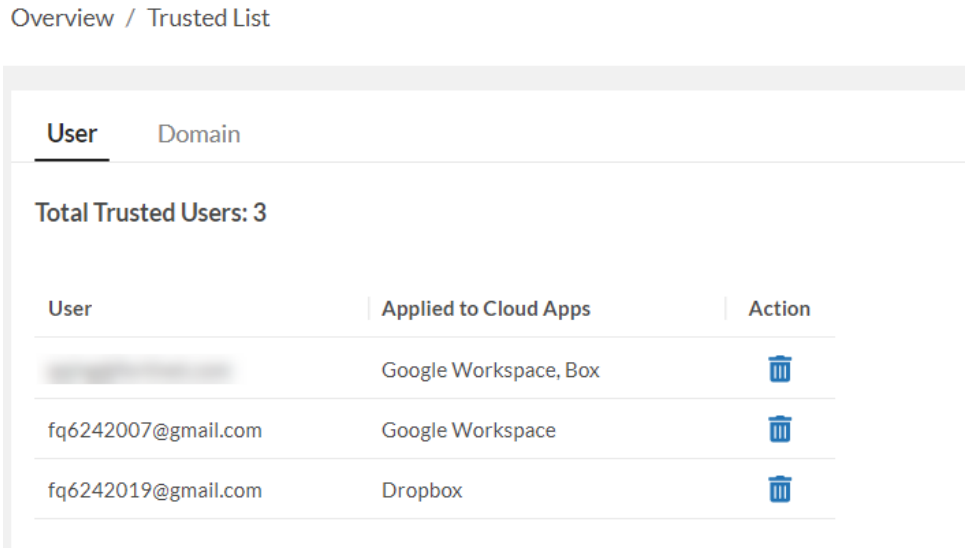
Change Access Permission is one of the action items on files found through the matching criteria of the Data Security Policy. Currently this feature is only available to **Google Workspace** Application.



There are two options to choose from in Change Access Permission:

1. **Change to Private** - when selected, the file access permission will be changed to Private.
2. **Change to Private + Read Only For Users in Trusted List** - when selected, the file access permission will be changed to Private and Read-Only only to users in Trusted List.

Trusted List is a list of users added in **Overview > Trusted List** through FortiCASB username or e-mail.



Write Label To Files (Google Workspace Only)

Prerequisite

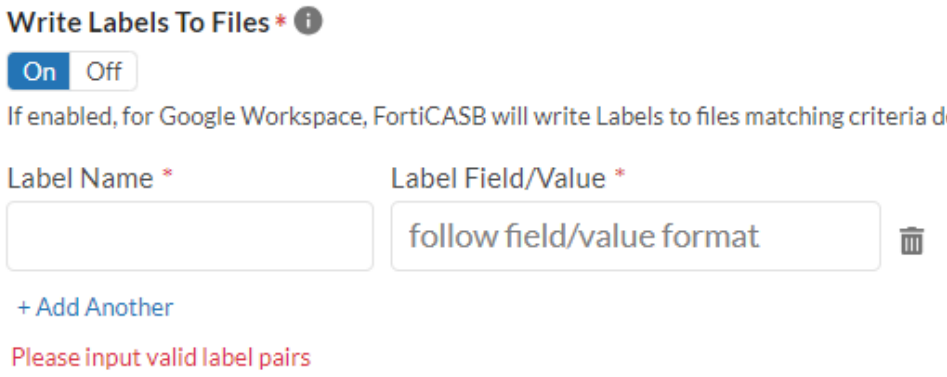
1. Before using Label Triggers as match criteria, Google Drive Labels APIs needs to be enabled. Please see Enable Drive Labels API (Google Workspace Only) on page 354
2. If this is your first time using Label Triggers, please update the Google Workspace account in FortiCASB. Please see Update Google Workspace Account on page 158.

Write Label To Files is one of the action items on Google Drive files found through the matching criteria of the Data Security Policy. Google Drive file label is a customizable label that can be attached to files in Google Drive.

For more information on Google Drive Labels please see Get Started as a Drive Labels admin.

1. When Write Label To Files is enabled, FortiCASB will apply the custom label to the Google Drive files found by the matching criteria.
2. The existing label will not be deleted, only new labels will be created.
3. If the new label name is the same as the old label name, but the label field name is different, then a new label will be created.

4. Each file on Google Drive can have a maximum of 5 user-applied labels, please check the file before applying this feature.

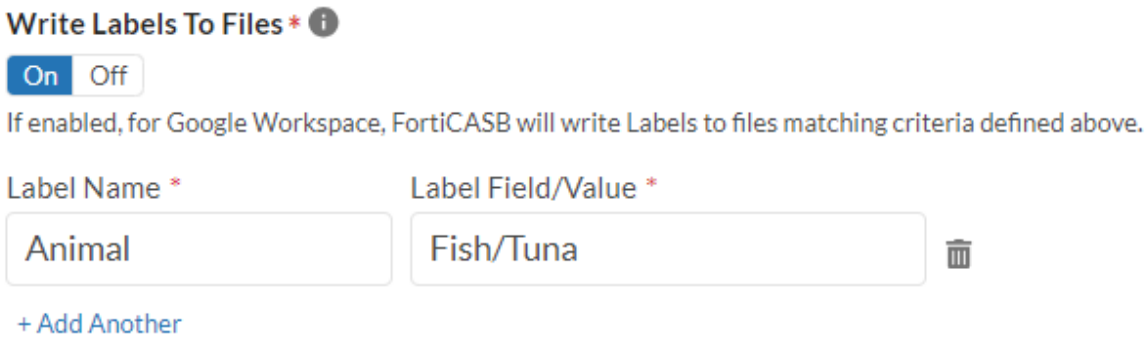


Label Name - the name of the Google file label.

Label Field/Value - Label Field is the field name and Value is the field value of the Google file label, separated by "/".

Example of Custom Label

In this example, the Google label name is "Animal", the label field is "Fish", and the label value is "Tuna"



Send Email Notifications

When the a data security policy is enabled, an alert will be triggered by specific user activity done on the targeted files with certain DLP patterns.

The alert also can be sent as notification to notify the relevant personnel to take immediate actions.

Types of Alert Notification

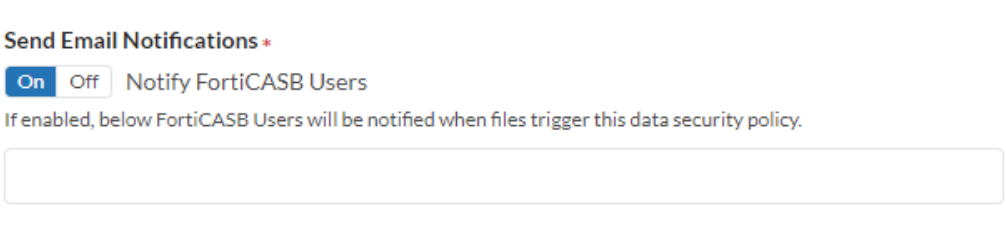
There are two types of alert notifications that can be generated to address the alert incident.

1. **Email Notification Alerts** can be sent to either the **FortiCASB Users** or the affected **File Owners**
2. **FortiAnalyzer Alerts** in the form of **Syslog messages** can be sent to FortiAnalyzer.
   In order to send alerts to FortiAnalyzer, a FortiAnalyer needs to be added first in **Overview > Fabric Integration**.
   See Fabric Integration Configuration on page 325 for more details

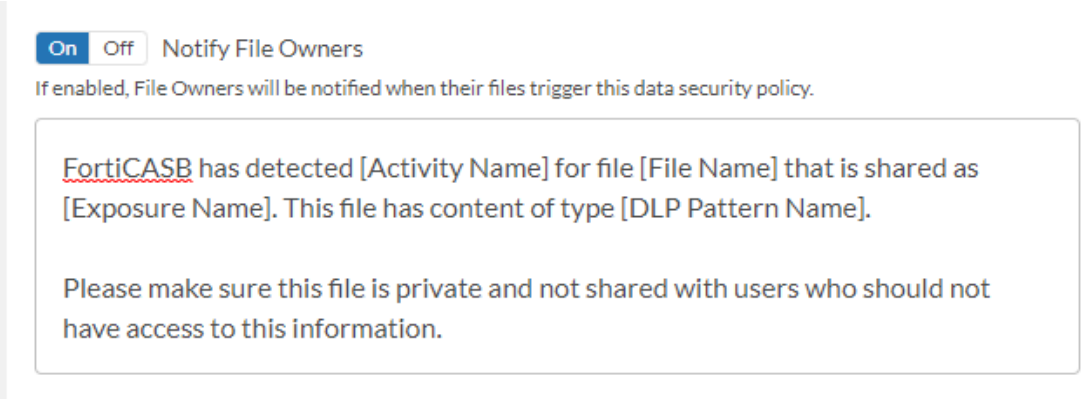
Email Notification or FortiAnalyzer alerts needs to be enabled in the Data Security Policy to send notifications.

Steps to Configure Email Notification in Data Security Policy

1. Go to **Data Protection > Policies > Scan Policies** from the main menu.
2. Click **+Add New** to create a new **Data Security Policy**.
3. After **Data Security Policy Name** and **Match Criteria** are filled, go to **Action** section.
4. In **Send Email Notification**, click **On** to enable email notifications.

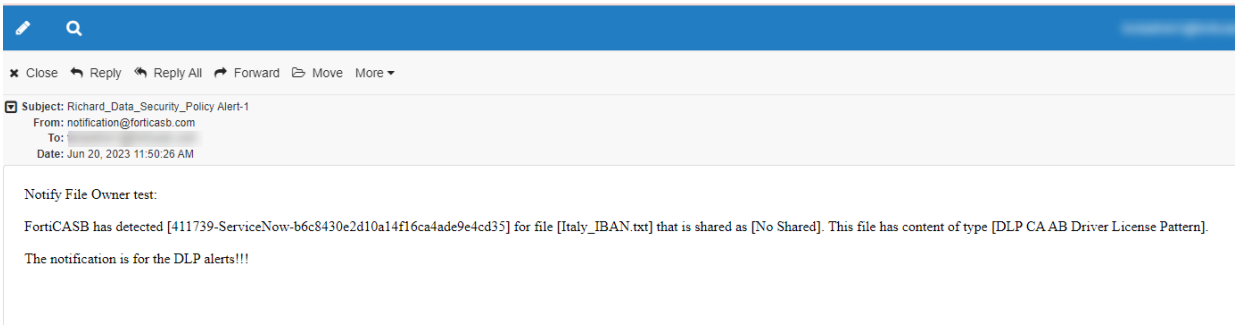


5. Enter the recipient's e-mail address in the field below.
6. In **Notify File Owners**, click **On** to enable file owner notification.



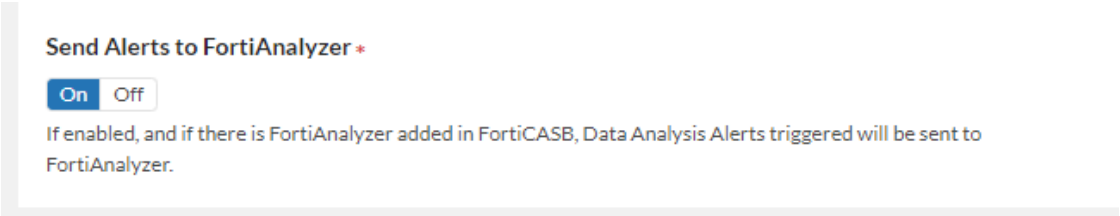
7. Edit the alert notification field below. The following parameters will be send as part of the notification to the file owner.
   a. **Activity Name** - the type of activity conducted on the file.
   b. **File Name** - The file that contains the targeted DLP pattern.
   c. **DLP Pattern Name** - the DLP pattern that triggers the alert.
8. Click **Add New Data Security Policy** to finish.

Example of File Owner Notification Alert



Steps to Configure FortiAnalyzer Notification

1. Go to **Data Protection > Policies > Scan Policies** from the main menu.
2. Click **+Add New** to create a new **Data Security Policies**.
3. After **Data Security Policy Name** and **Match Criteria** are filled, go to **Action** section.
4. In **Send Alerts to FortiAnalyer**, click **On** to enable alerts to be sent to FortiAnalyzer.

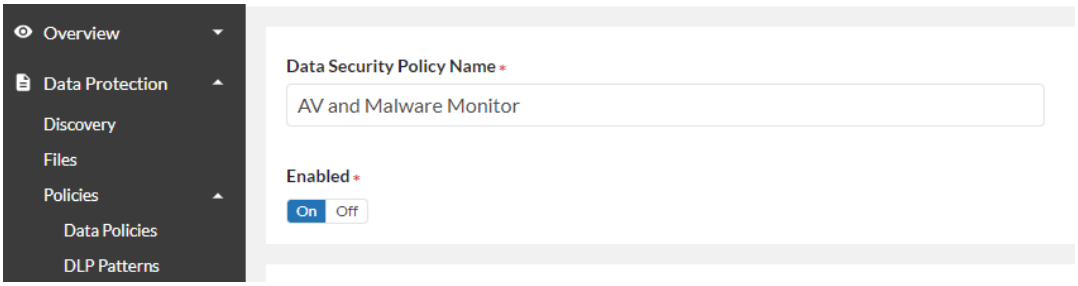


5. Click **Add New Data Security Policy** to finish.

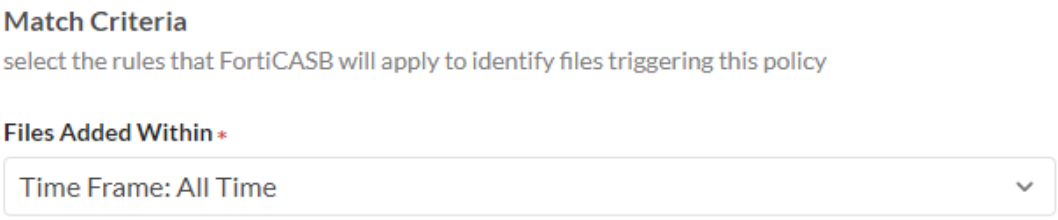
Create Data Security Policy Example

In this example, a data security policy will be created for monitoring for any malicious file containing malware or virus. Alert notification will be sent to the FortiCASB user, file owner, and FortiAnalyzer.

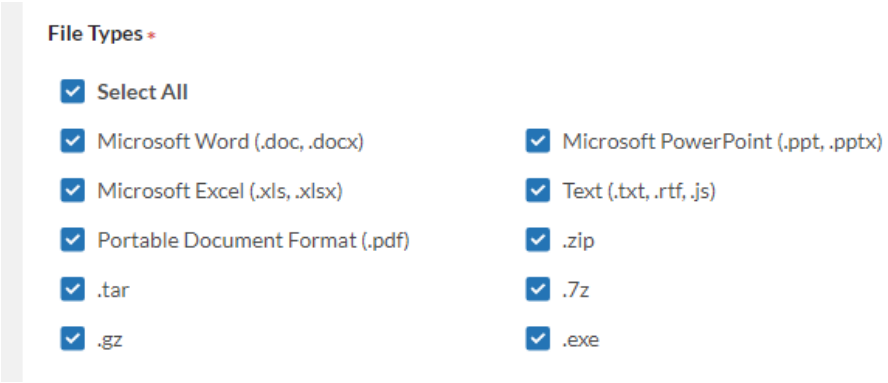
1. Go to **Data Protection > Policies > Scan Policies**.
2. Click **+Add New** to add new data security policy.
3. In **Data Security Policy Name**, name the policy as "AV and Malware Monitor"



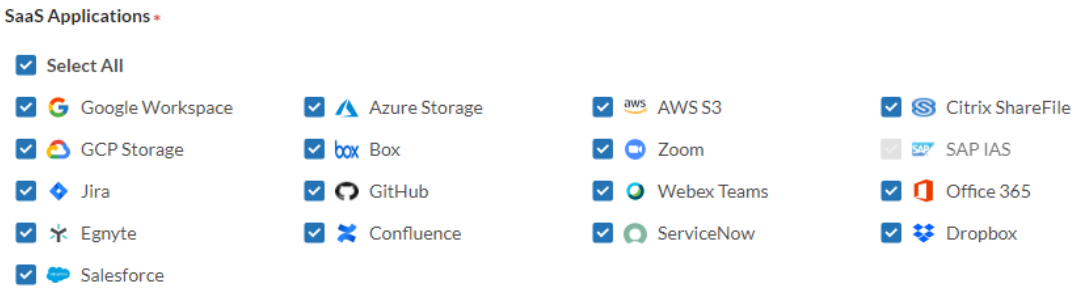
4. Click **Enabled** toggle switch button to enable the policy.
5. In **Match Criteria** section, click **Files Added Within** drop down menu, select "Time Frame: All Time".



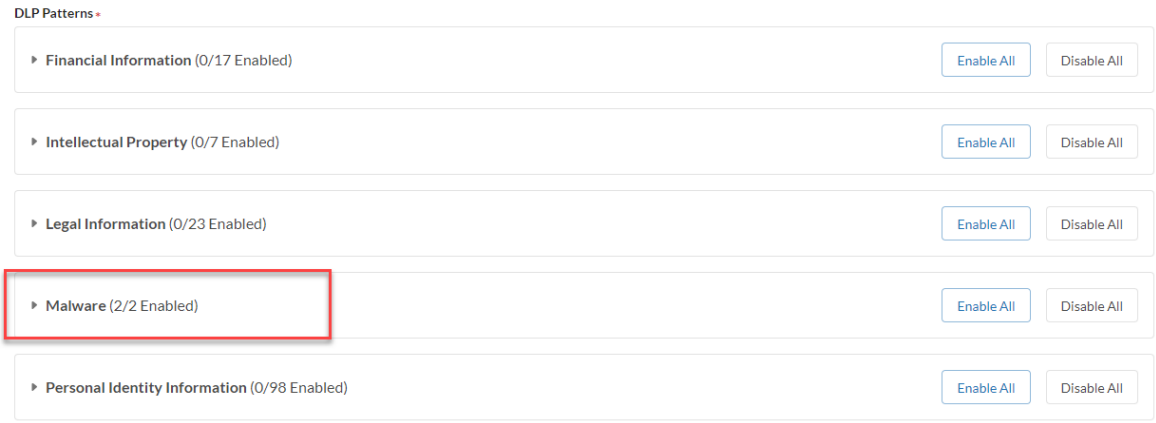
6. In **File Types**, click **Select All**.



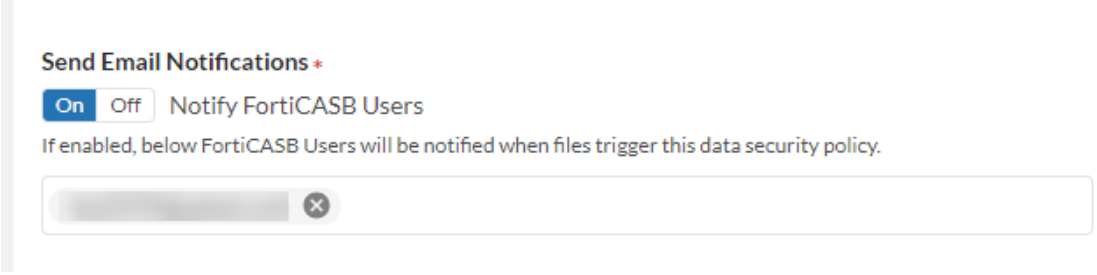
7. In **Access Permissions**, click **Select All**
8. In **File Activity Triggers**, click **Select All**
9. In **SaaS Applications**, click **Select All**.



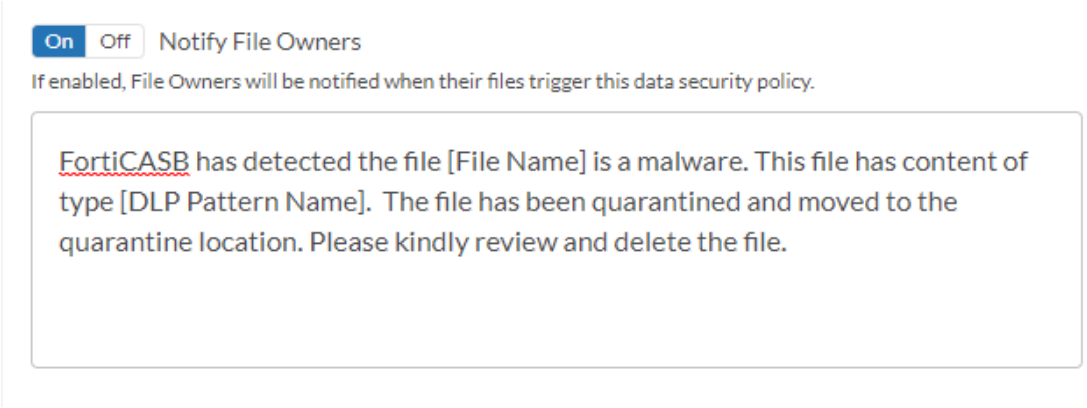
10. In **DLP Pattern**, only enable all **Malware** type DLP patterns and disable the rest.



11. In **Action** section, turn on **Quarantine Files** to quarantine malwares if detected.
12. In **Send Email Notification**, turn on FortiCASB Users, and enter a user below to be notified.



13. Turn on **Notify File Owners** alert and edit the notification contents.



14. Turn on **Send Alerts to FortiAnalyzer** to send alerts to FortiAnalyzer.
15. Click **Add New Data Security Policy** to finish.

Predefined Data Pattern

Predefined Data Pattern defines the default **DLP (Data Loss Prevention) patterns** and classify private and confidential data that should be regulated in accordance to regulatory compliance requirements.

Predefined data patterns are located in **Data Protection > Policies > Data Patterns > Predefined** tab.

FortiCASB identifies SaaS account activities on files with these predefined data patterns and alert the administrators.

For example, when a file containing Social Security Numbers (SSN) is accessed by a SaaS user, FortiCASB will notify the file owner or the administrator.

In 2023, additional data patterns are added with the support through FortiGuard, resulting a total of 113 data patterns with 3 pattern categories:

- **Personal Identity Information on page 366**
- **Financial Information on page 372**
- **Malware and Ransomware on page 373**

The maximum uncompressed/compressed file size that the data patterns supports is 20 MB.

For the latest data pattern updates, please refer to **FortiGuard DLP updates**.

Personal Identity Information

FortiCASB scans for the Personal Identity Information data patterns during Data Security Policy scans, and triggers an alert when the specific data pattern is accessed.

Below are different types of personal identity information that FortiCASB supports in DLP scan.

Personal Identity Number	Description
DLP Birthdate Pattern	Birthdate
DLP SSN Pattern	United States social security number
DLP Polish Social Security Number Pattern	Poland social security number
DLP CN Resident Identity Pattern	China resident identity

Personal Identity Number	Description
	number
DLP Email Address Pattern	Email address

Passport Number	Description
DLP USA/Germany Passport Number Pattern	United States and Germany Passport number
DLP JP Passport Number Pattern	Japan passport number
DLP AU Passport Number Pattern	Australia passport number
DLP UK Passport Number Pattern	United Kingdom passport number
DLP CA Passport Number Pattern	Canada passport number
DLP CN Passport Number Pattern	China passport number
DLP FR Passport Number Pattern	France passport number

International Bank Account Number (IBAN)	Description
DLP German IBAN Pattern	Germany Bank International Bank Account Number
DLP Italian IBAN Pattern	Italian Bank International Bank Account Number
DLP Spanish IBAN Pattern	Spanish International Bank Account Number
DLP Swedish IBAN Pattern	Swedish International Bank Account Number
DLP Swiss IBAN Pattern	Swiss International Bank Account Number
DLP UK IBAN Pattern	United Kingdom International Bank Account Number

Driver License	Description
DLP CN Driver License Pattern	China driver's license number
DLP UK Driver License Pattern	United Kingdom driver's license number
DLP US AL Driver License Pattern	United States Alabama driver's license number
DLP US AK Driver License Pattern	United States Alaska driver's license number
DLP US AZ Driver License Pattern	United States Arizona driver's license number
DLP US AR Driver License Pattern	United States Arkansas driver's license number
DLP US CA Driver License Pattern	United States California driver's license number
DLP US CO Driver License Pattern	United States Colorado driver's license number
DLP US CT Driver License Pattern	United States Connecticut driver's license number
DLP US DE Driver License Pattern	United States Delaware driver's license number
DLP US DC Driver License Pattern	United States Washington DC driver's license number
DLP US FL Driver License	United States Florida driver's license number
DLP US GA Driver License Pattern	United States Georgia driver's license number
DLP US HI Driver License Pattern	United States Hawaii driver's license number
DLP US ID Driver License Pattern	United States Idaho driver's license number
DLP US IL Driver License Pattern	United States Illinois driver's license number
DLP US IN Driver License Pattern	United States Indiana driver's license number
DLP US IA Driver License Pattern	United States Iowa driver's license number

Driver License	Description
DLP US KS Driver License Pattern	United States Kansas driver's license number
DLP US KY Driver License Pattern	United States Kentucky driver's license number
DLP US LA Driver License Pattern	United States Louisiana driver's license number
DLP US ME Driver License Pattern	United States Maine driver's license number
DLP US MD Driver License Pattern	United States Maryland driver's license number
DLP US MA Driver License Pattern	United States Massachusetts driver's license number
DLP US MI Driver License Pattern	United States Michigan driver's license number
DLP US MN Driver License Pattern	United States Minnesota driver's license number
DLP US MS Driver License Pattern	United States Mississippi driver's license number
DLP US MO Driver License Pattern	United States Missouri driver's license number
DLP US MT Driver License Pattern	United States Montana driver's license number
DLP US ND Driver License Pattern	United States North Dakota driver's license number
DLP US NE Driver License Pattern	United States Nebraska driver's license number
DLP US NV Driver License Pattern	United States Nevada driver's license number
DLP US NH Driver License Pattern	United States New Hampshire driver's license number
DLP US NJ Driver License Pattern	United States New Jersey driver's license number
DLP US NM Driver License Pattern	United States New Mexico driver's license number
DLP US NY Driver License Pattern	United States New York driver's license number

Driver License	Description
DLP US NC Driver License Pattern	United States North Carolina driver's license number
DLP US OH Driver License Pattern	United States Ohio driver's license number
DLP US OK Driver License Pattern	United States Oklahoma driver's license number
DLP US OR Driver License Pattern	United States Oregon driver's license number
DLP US PA Driver License Pattern	United States Pennsylvania driver's license number
DLP US RI Driver License Pattern	United States Rhode Island driver's license number
DLP US SC Driver License Pattern	United States South Carolina driver's license number
DLP US SD Driver License Pattern	United States South Dakota driver's license number
DLP US TN Driver License Pattern	United States Tennessee driver's license number
DLP US TX Driver License Pattern	United States Texas driver's license number
DLP US UT Driver License Pattern	United States Utah driver's license number
DLP US VT Driver License Pattern	United States Vermont driver's license number
DLP US VA Driver License Pattern	United States Virginia driver's license number
DLP US WA Driver License Pattern	United States Washington driver's license number
DLP US WV Driver License Pattern	United States West Virginia driver's license number
DLP US WI Driver License Pattern	United States Wisconsin driver's license number
DLP US WY Driver License Pattern	United States Wyoming driver's license number
DLP CA AB Driver License Pattern	Canada Alberta driver's license number

Driver License	Description
DLP CA BC Driver License Pattern	Canada British Columbia driver's license number
DLP CA MB Driver License Pattern	Canada Manitoba driver's license number
DLP CA NB Driver License Pattern	Canada New Brunswick driver's license number
DLP CA NL-1 Driver License Pattern	Canada Newfoundland and Labrador driver's license number
DLP CA NL-2 Driver License Pattern	Canada Newfoundland and Labrador driver's license number
DLP CA NT Driver License Pattern	Canada Northwest Territories driver's license number
DLP CA NS Driver License Pattern	Canada Nova Scotia driver's license number
DLP CA NU Driver License Pattern	Canada Nunavut driver's license number
DLP CA ON Driver License Pattern	Canada Ontario driver's license number
DLP CA PE-1 Driver License Pattern	Canada Prince Edward Island driver's license number
DLP CA PE-2 Driver License Pattern	Canada Prince Edward Island driver's license number
DLP CA QC Driver License Pattern	Canada Quebec driver's license number
DLP CA SK Driver License Pattern	Canada Saskatchewan driver's license number
DLP CA YT Driver License Pattern	Canada Yukon driver's license number

Financial Information

FortiCASB scans for the financial information data patterns during Data Security Policy scans, and triggers an alert when the specific data pattern is accessed.

Financial Information Patterns	Description
DLP JCB Pattern	JCB credit card number
DLP Maestro Card Pattern	Maestro debit card number
DLP MasterCard Pattern	Master credit card number
DLP American Express Pattern	American Express credit card number
DLP Diners Club Card Pattern	Diners Cloud credit card number
DLP Discover Card Pattern	Discover credit card number
DLP China Union Pay Pattern	China Union Pay credit card number
DLP Visa Credit Card Pattern	Visa credit card number
DLP BC Global Credit Card Pattern	Korean BC credit card number
DLP Carte Blanche Credit Card Pattern	Carte Blanche credit card number
DLP Insta Payment Credit Card Pattern	Instant payments are credit transfers that make funds available in a payee's account within ten seconds of a payment order being made.
DLP Korean Local Credit Card Pattern	Korean local credit card number (Samsung, Lotte, Hyundai, Hana, BC, NG, Shinhan, and KB)
DLP Laser Credit Card Pattern	Laser was primarily an electronic point of sale debit card, but could also be used by telephone and internet, at ATMs and to pay regular bills by direct debit.
DLP Solo Credit Card Pattern	Solo credit card number

Financial Information Patterns	Description
DLP Switch Credit Card Pattern	Switch credit card number
DLP CA Insurance Number Pattern	Canadian Insurance number
DLP UK Insurance Number Pattern	United Kingdom Insurance number
DLP VSMC Pattern	Victoria Secret Master Card
DLP Australia SWIFT Code Pattern	Australia SWIFT code number
DLP China SWIFT Code Pattern	China SWIFT code number
DLP Germany SWIFT Code Pattern	Germany SWIFT code number
DLP France SWIFT Code Pattern	France SWIFT code number
DLP Japan SWIFT Code Pattern	Japan SWIFT code number
DLP United Kingdom SWIFT Code Pattern	United Kingdom SWIFT code number
DLP USA SWIFT Code Pattern	United States SWIFT code number

Malware and Ransomware

FortiCASB scans for malware and ransomware data patterns during Data Security Policy scans, and triggers an alert when a malware or ransomware is detected.

Malware/Ransomware	Description
Ransomware Encrypted File Detection Pattern	Scans for ransomware encrypted file utilizing Fortinet Security Fabric.
AV Scan Pattern	Scans for malware and virus utilizing Fortinet Security Fabric.

Customized Data Pattern

Customized Data Pattern is user defined **DLP (Data Loss Prevention) patterns** and can be applied to Data Security Policy just as Predefined Data Patterns.

Customized Data pattern is located in **Data Protection > Policies > Data Patterns > Customized Data Pattern** tab.

Regex or **PCRE**(Perl Compatible Regular Expressions) plays the major role in determining the data pattern that the Customized Data Pattern should search for. Regex is regular expression that combines special character operators that can be constructed to search specific strings in files.

Configurable Parameters in Customized Data Pattern

Name	Enter a name for the data pattern.
Description	Enter a description for the data pattern.
Category	Select a data category from the list.
Uncompressed File Size	Specify the upper bound of an object size, in MB, for a full content scan.
Compressed File Size	Specify the upper bound of a zip file size, in MB, for a full content scan.
Regex Context	Enter in a Regex to search for specific string

Exact Data Match Category

EDM (Exact Data Match) is a category of Customized DLP Data Patterns. EDM allows specific sensitive data to be scanned by a predefined dataset and triggers an alert when a match is detected. Users can define predefined dataset through a CSV file, upload it through Exact Data Match category when creating a Customized Data Pattern.

Characteristics of EDM Customized Data Pattern

- There is a match only if the sensitive data is matched exactly as the predefined dataset.
- Symbols in the predefined dataset as well as ", . And" all need to have exact match as the sensitive data scanned.
- When a matching threshold is specified in the EDM data pattern, an alert will be triggered when the number of matched values in the CSV file is equal or greater than the matching threshold. Please see Customized Data Pattern Example - Exact Data Match on page 377 for example.

CSV File Requirements

- The CSV files should have no header row.
- Only English (Latin script) is supported.
- A maximum of 120 rows and 30 columns are supported per data set.
- The CSV file format is recommended to adhere to RFC-4180 standard.
- First Normal Form(1NF) recommended in data design, meaning all columns should have only scalar or atomic values. **For example**, first name and last name should be separated into two separate columns, city and zip code should be separated into two columns.

CSV File Example

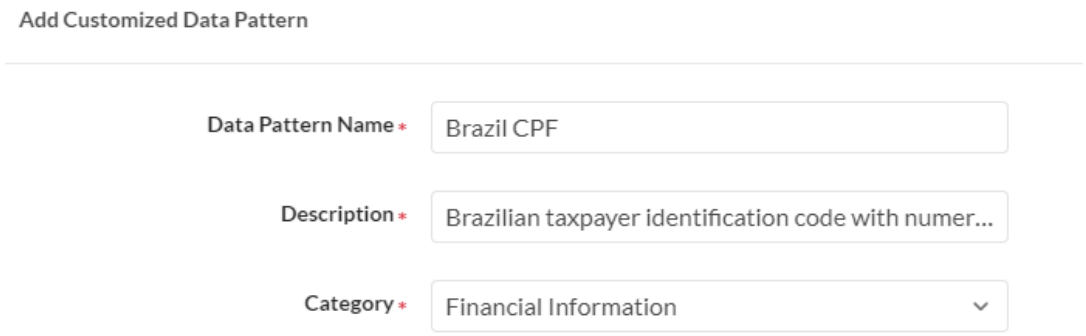
This is an example where the data format fulfills the CSV file requirement for EDM Customized Data Pattern.

Jason	Valentino	120 Jefferson St.	Riverside	CA	92504
Marry	Baxter	415 W Willow Grove Ave	Philadelphia	PA	19118
David	Solace	555 Pierce Street APT #123	Albany	CA	94706
Thomas	Jefferson	1600 Pennsylvania Avenue NW	Washington	DC	20500

Customized Data Pattern Example - Regex

The following customized data pattern will search for a Brazilian CPF, an 11 digit taxpayer identification code issued by Brazillian Federal Reserve. This data pattern will monitor for the presence of Brazilian taxpayer identification code in the cloud accounts.

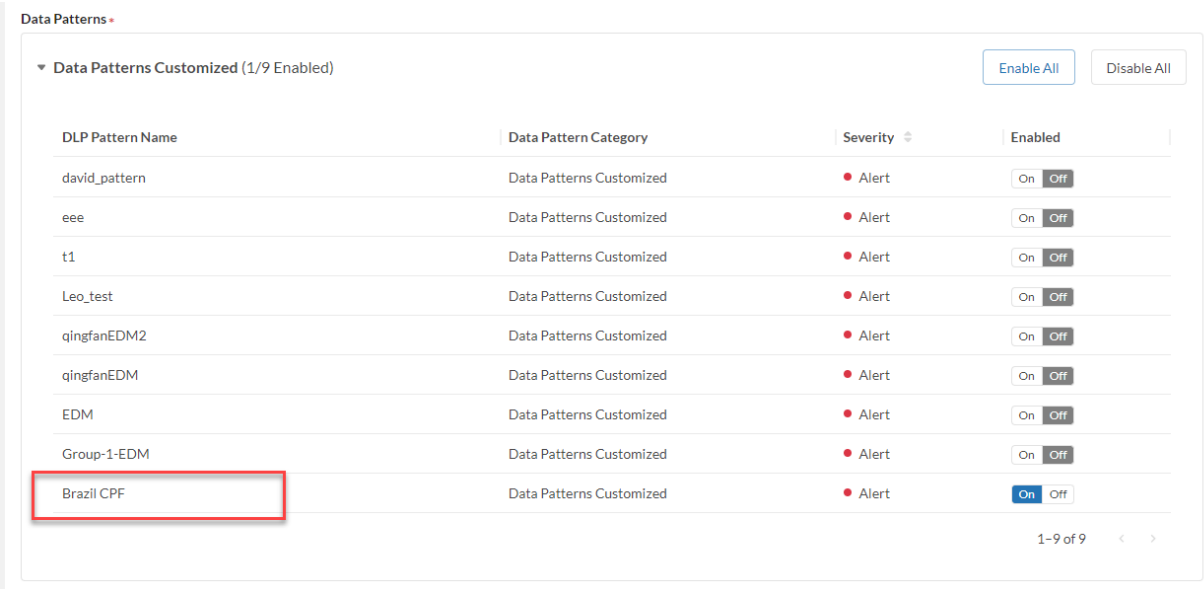
1. Go to **Data Protection > Policies > Data Pattern**, and click on **Customized** tab.
2. Click on **+ADD NEW** to add a customized data pattern.
3. In **Data Pattern Name**, enter "Brazil CPF".



4. In **Description**, enter "Brazilian taxpayer identification code with numerical format in xxx.xxx.xxx-xx".
5. In **Category**, select "Financial Information".
6. In **Max Uncompressed File Size** and **Max Compressed File Size**, use the default value "10MB".

7. In **Regex (PCRE)**, enter the regex: "^\d{3}\.\d{3}\.\d{3}\-\d{2}$".
8. Click **Add Customized Data Pattern** to finish.

Now the Customized Data Pattern is ready to be added and enabled in Data Security Policy configuration.



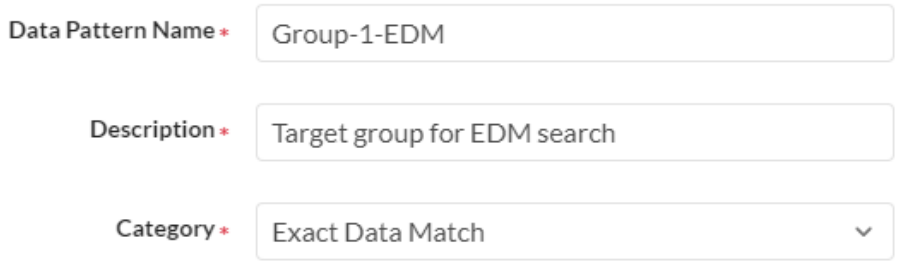
Customized Data Pattern Example - Exact Data Match

Before the Customized Data Pattern can be added, create a CSV file named "Group1EDM.csv" with the following content.

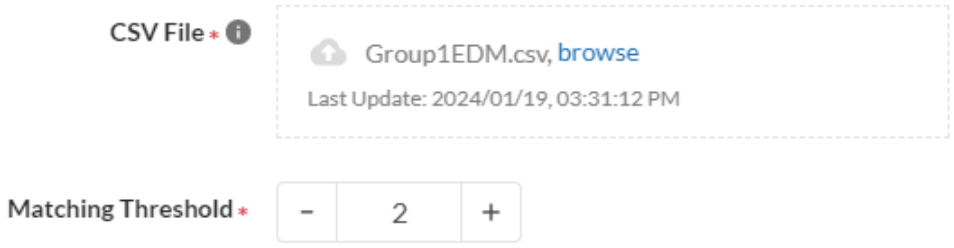
Jason	Valentino	120 Jefferson St.	Riverside	CA	92504
Marry	Baxter	415 W Willow Grove Ave	Philadelphia	PA	19118
David	Solace	555 Pierce Street APT #123	Albany	CA	94706
Thomas	Jefferson	1600 Pennsylvania Avenue NW	Washington	DC	20500

The following Customized Data Pattern will utilize the Exact Data Match category and a CSV file provided to search for a match against the sensitive data in a Data Protection Policy.

1. Go to **Data Protection > Policies > Data Pattern**, and click on **Customized** tab.
2. Click on **+ADD NEW** to add a customized data pattern.
3. In **Data Pattern Name**, enter "Group-1-EDM".

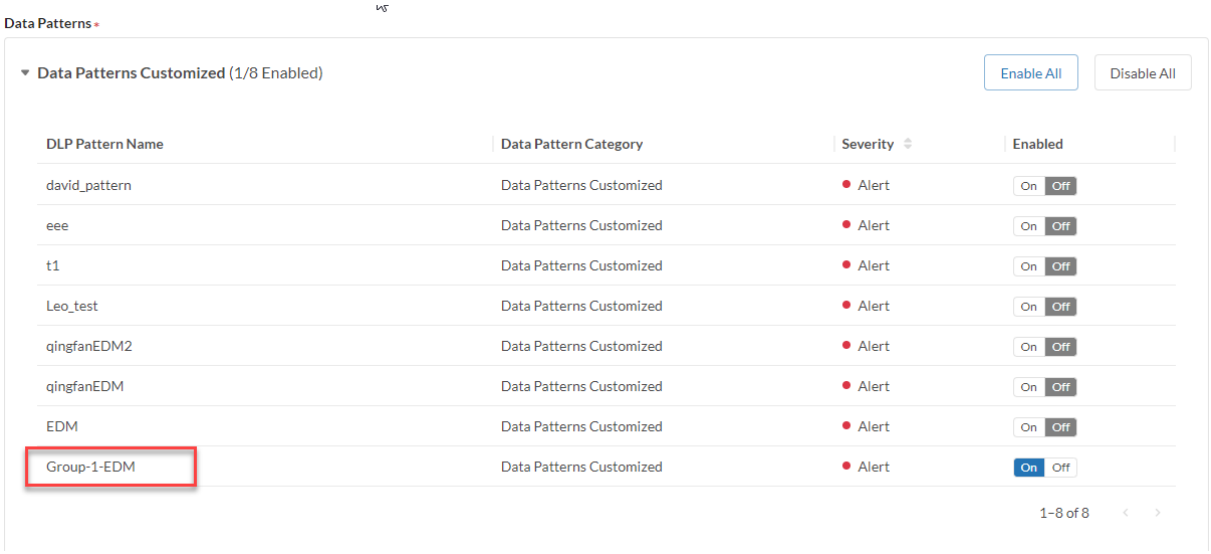


4. In **Description**, enter "Target group for EDM search".
5. In **Category**, select **Exact Data Match**.
6. In **Max Uncompressed File Size** and **Max Compressed File Size**, use the default value "10MB".
7. In **CSV File**, browse and upload the CSV file.



8. In **Matching Threshold**, press **+** to select 2
   Note: When the Matching Threshold value of 2 is selected, it means if there are any 2 cell values that matched between the CSV file and the sensitive data during file scan, a DLP alert will be triggered.
   For example, when both the values from the CSV file - "Thomas" and "Albany" are found in the targeted sensitive file, a DLP alert will be triggered. If only "Thomas" is matched, then an alert will not be triggered.
9. Click **Add Customized Data Pattern** to finish.

Now the Customized Data Pattern is ready to be added and enabled in Data Security Policy configuration.



Cloud Application Features

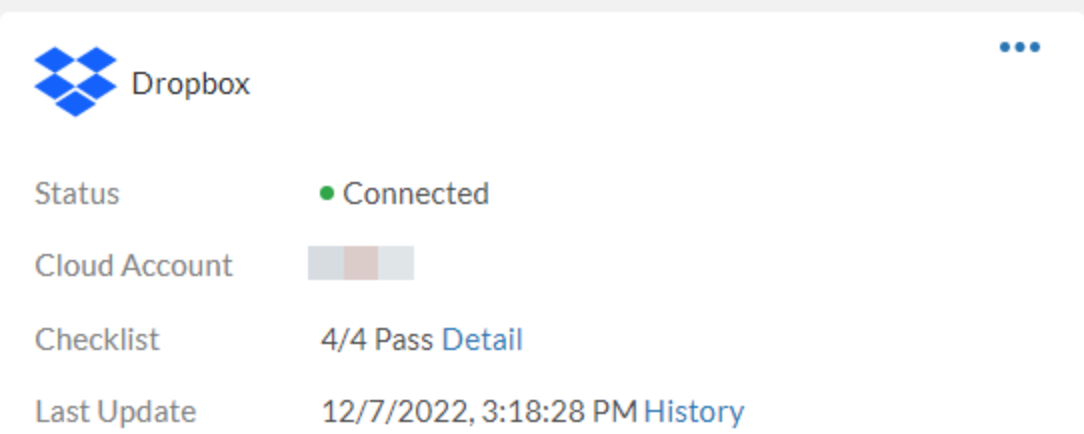
This section covers features specific to cloud application installed on FortiCASB.

Dashboard

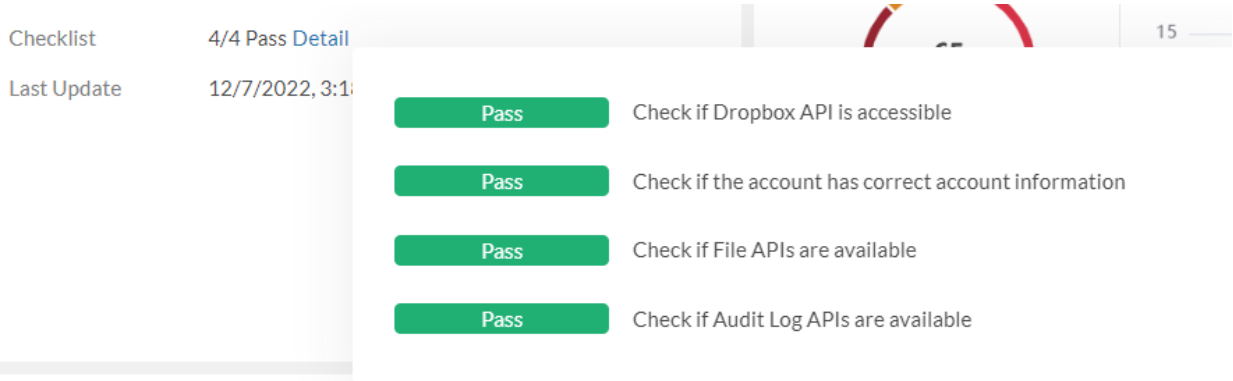
The cloud application dashboard shows account status, **Alert Overview**, **Policy Overview**, **Document Overview**, **Activity Overview**, and **Top 5 Policy Violation**, **High Risk Activities**, and **High Risk Documents**.

Account Status and Checklist

When the cloud account is successfully onboarded, it should show **Connected** status.



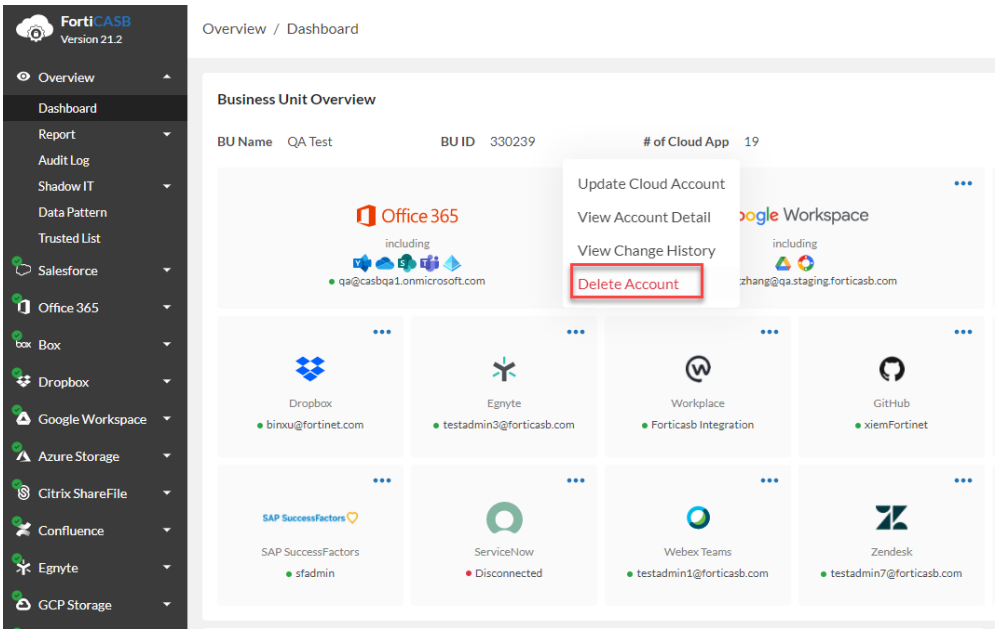
Click on the **Checklist > Details** button to show the onboarding checklist. All checklist items need to be in **Pass** status for FortiCASB to retrieve security data on the cloud account.



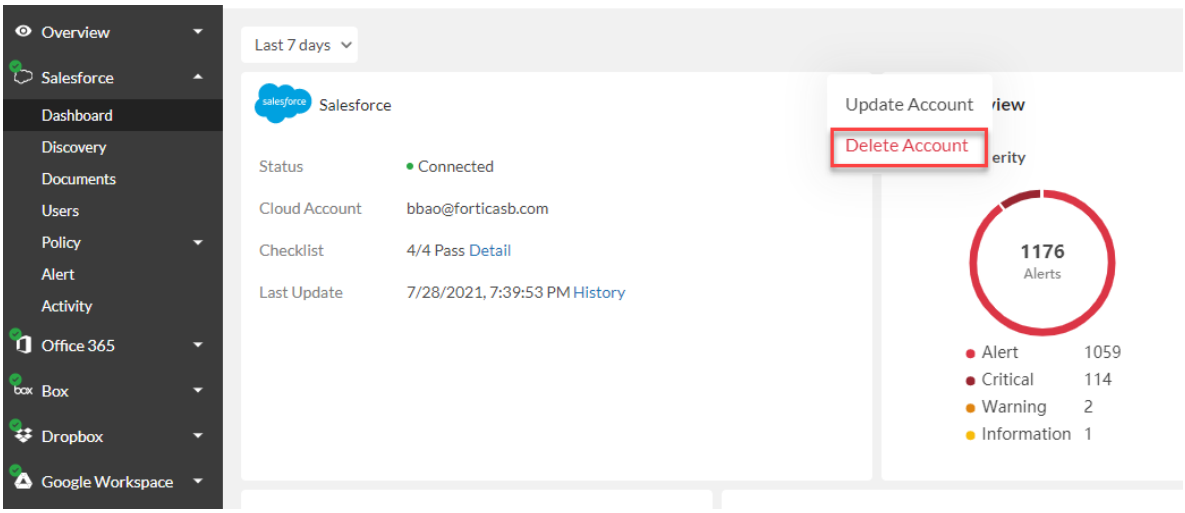
Delete Cloud Account

Cloud account can be deleted when no longer needed. There are two ways to delete a cloud account.

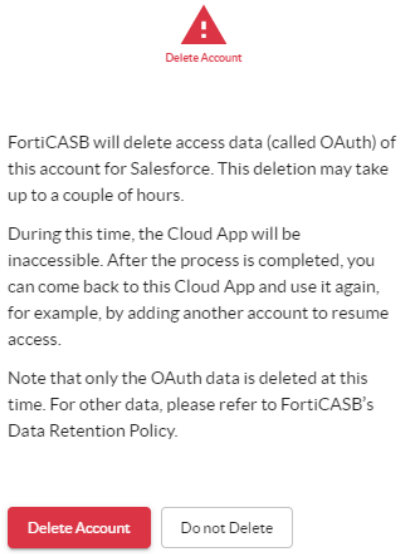
1. Go to **Overview > Dashboard**, click on the configuration button ••• and select **Delete Account**.



2. Go to the cloud app drop down menu, e.g. **Salesforce**, click on the configuration button ••• and select **Delete Account**.



A prompt to delete notice will pop up, select **Delete Account** to confirm deleting the account.



Note: It will take a couple hours to delete the cloud account, and during this time you will not be able to add another account. Please check back after a couple hours to add another cloud account.

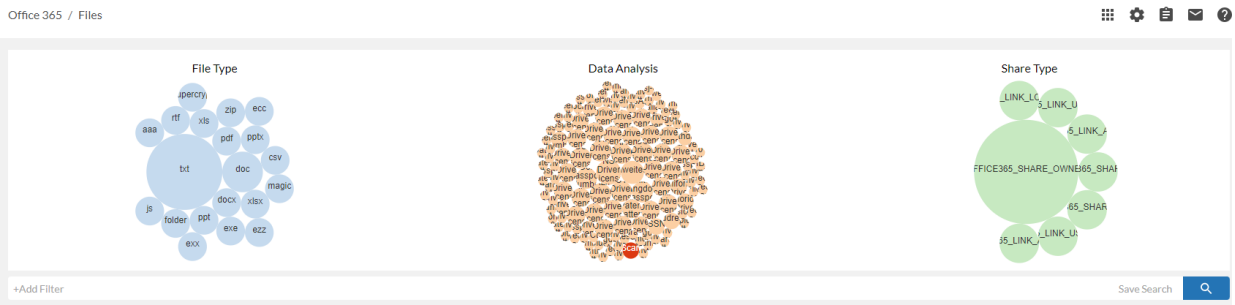
Files

Introduction

Files is a SaaS data storage security analytics located in each cloud application except **SAP IAS** and **Zoom**.

When a cloud account is first added to FortiCASB, files resided in the cloud account are pulled into the Files page. Then FortiCASB automatically updates the file status in Files page when users attempt to access files through the cloud application account.

The files bubble chart gives an overview of the files categorized by **File Type**, **Data Analysis**, and **Share Type**.



File Type captures all file types regardless of readability within the scope of cloud account storage/bucket.

Click on each file type bubble to show files with the specific file type.

Data Analysis scans and captures all files that contains DLP (Data Loss Prevention) data. Each bubble represents different Data Analysis policy.

Click on each Data Analysis bubble to show files only pertain to that Data Analysis policy.

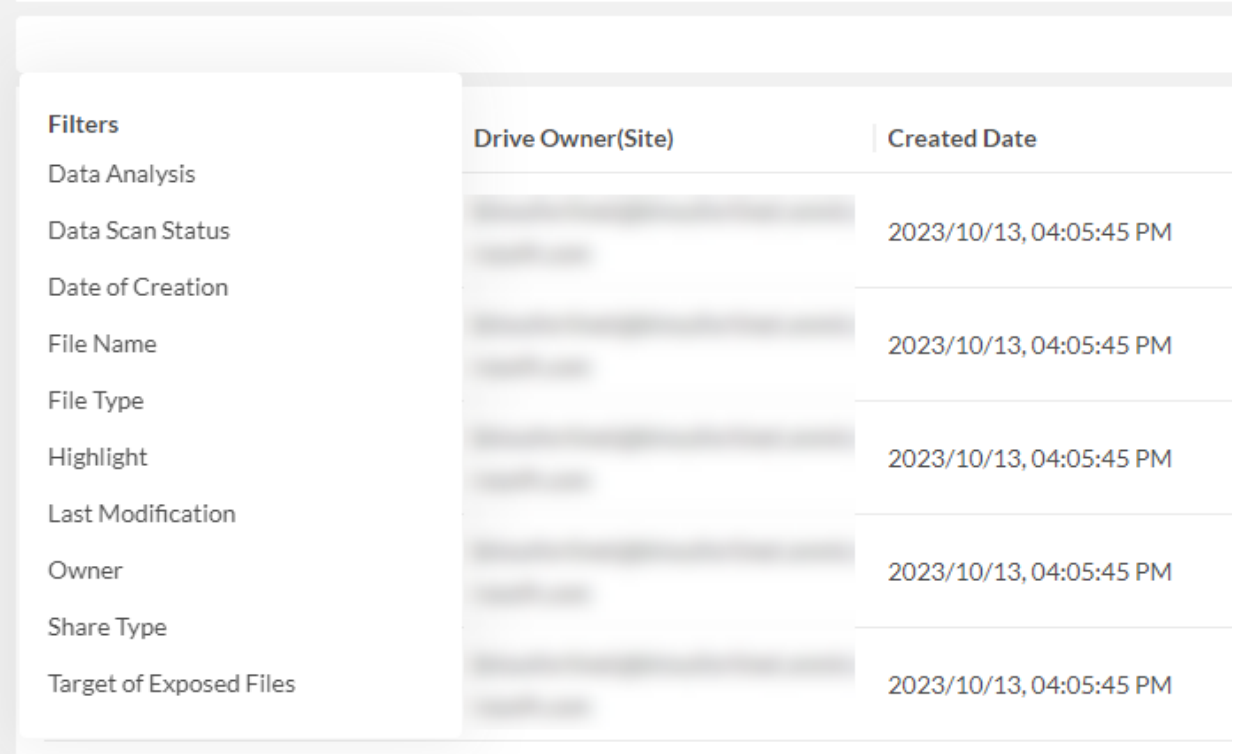
Share Type is a normalized share type that normalized all cloud account users by grouping them together by access permission. For more detail on normalized share type, please see Appendix B - Normalized Share Types on page 541.

Click on each share type to see only files shared by the specific share type users.

Click on each app bubble to filter the files by app.

Sort Cloud App Files by Filter

There are 11 filters that files can be sorted to identify the targeted files among all cloud applications:



For more information on **Highlight** and **Data Analysis Scan** filters, please see:

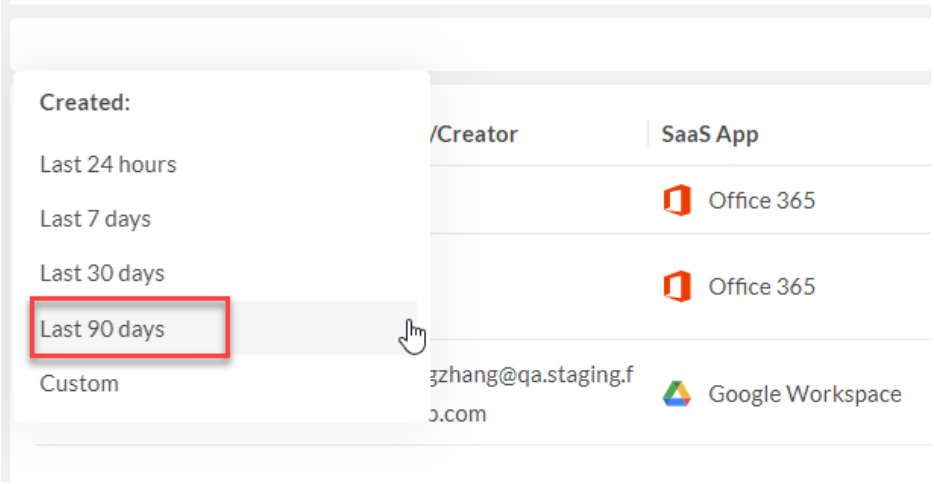
Highlight Filter on page 385

Data Scan Status on page 386

Example on using Files Filter

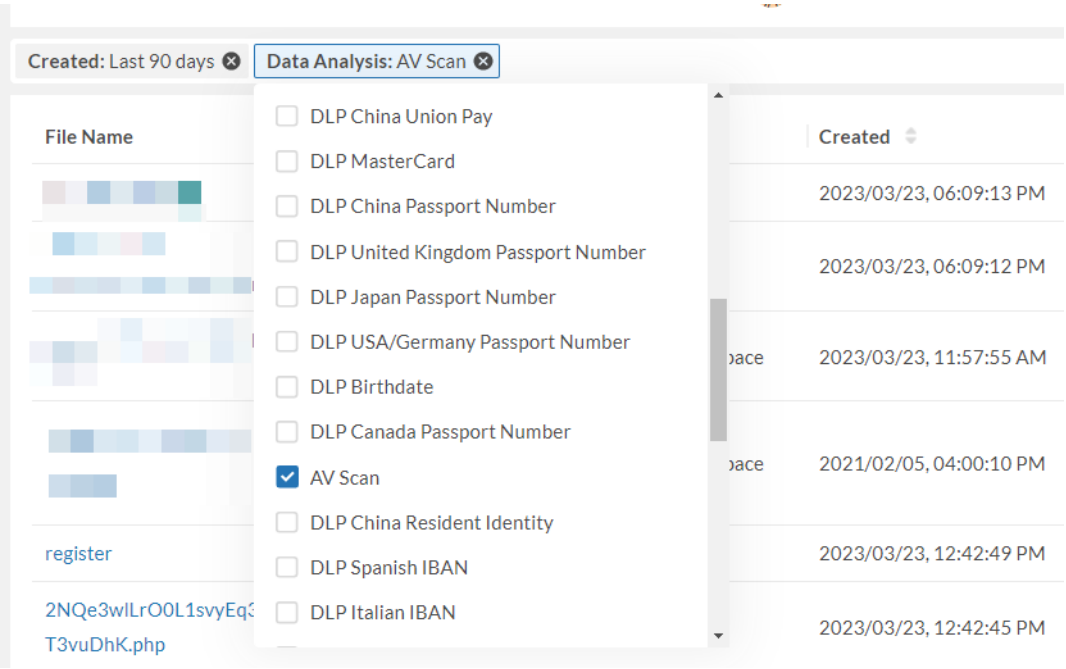
This example filters through all files for Malwares detected in the last 90 days among all cloud applications.

1. Click on **+Add Filter**.
2. Select **Created > Last 90 days**.

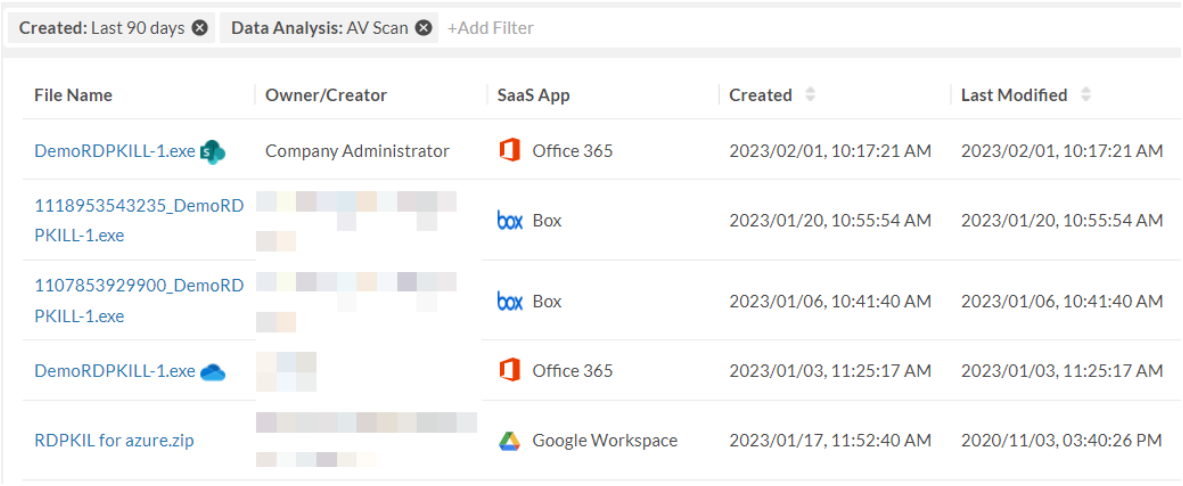


3. Click **+Add Filter** again.

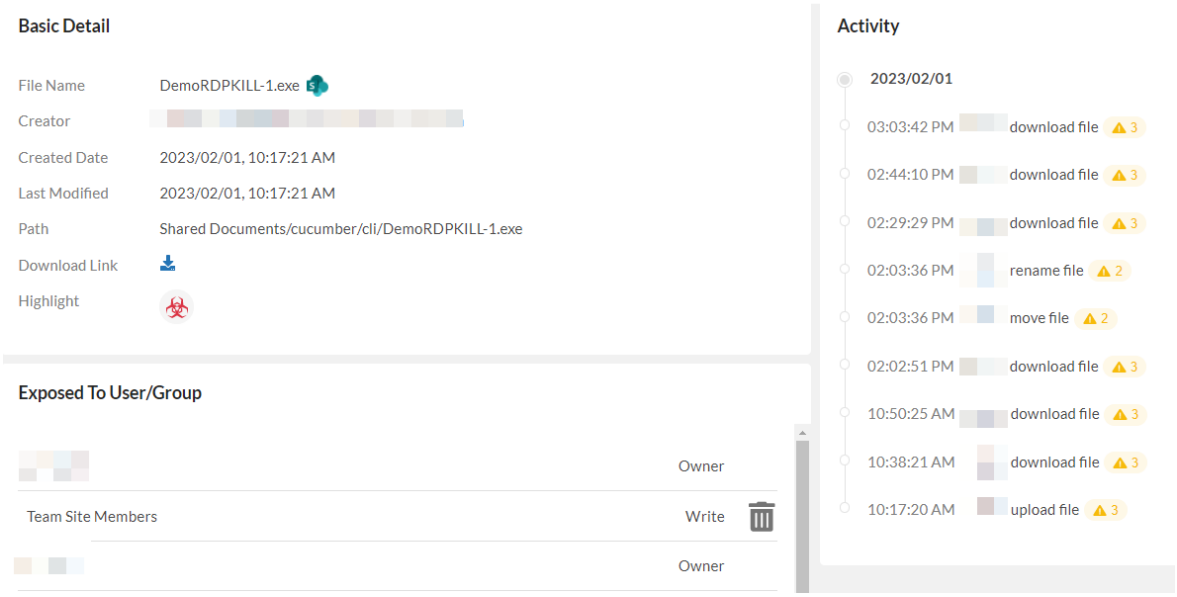
4. Select **Data Analysis > AV Scan**.



5. Click **Search** sign and filter through all files.
6. All Malwares from the last 90 days are displayed.

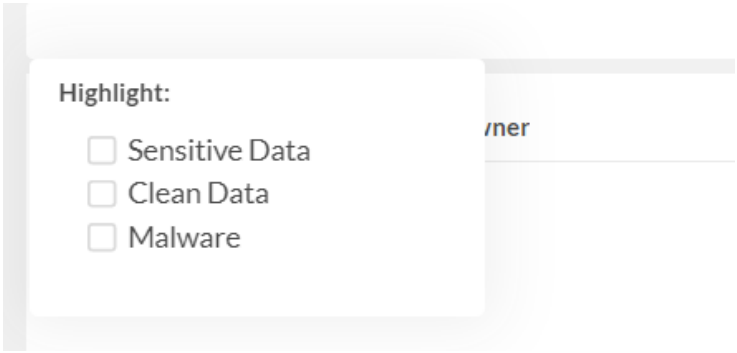


7. Click on any one of malware to view basic details, activity, users exposed, and data pattern violation.



Highlight Filter

The **Highlight** filter filters through all files for specific file type: **Sensitive**, **External**, and **Malware**.



Below is correlated Highlight and file type with description.

Highlight Icon	Document Type	Description
	Sensitive	Files with sensitive information searched and matched by DLP policies such as Social Security Number, Visa Credit Card number, etc.
	External	Files shared with the external users/groups.
	Malware	Infectious files searched and matched by the malware policies through AV scan.

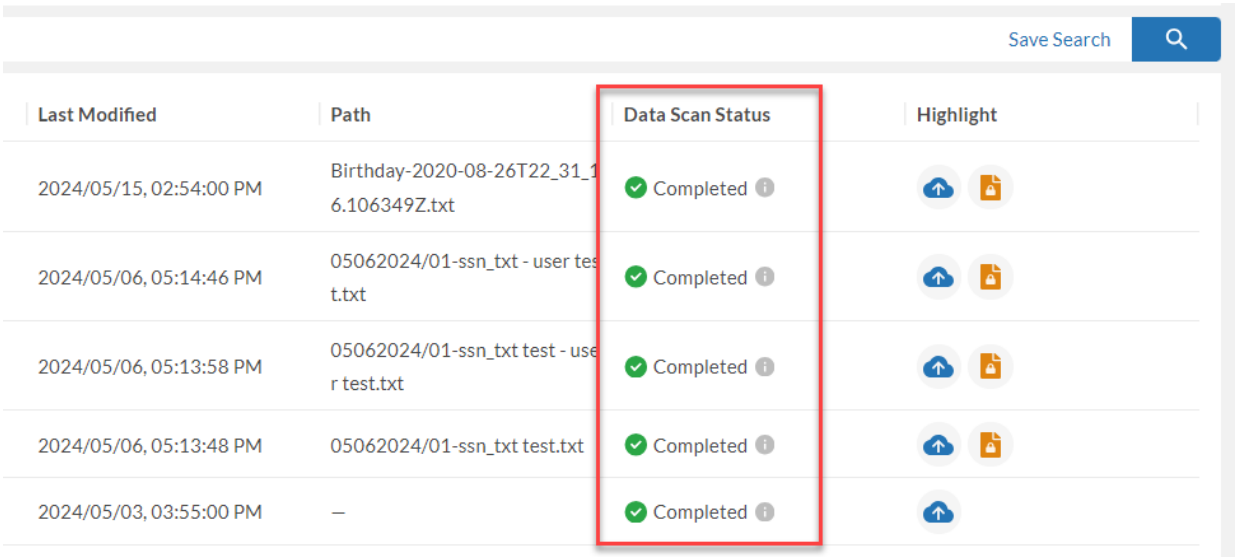
Data Scan Status

Data Scan Status shows the status of **DLP Scan (Data Loss Prevention scan)** which identifies Personal Identification Information(PII) such as Driver License, Credit Card, Social Security Numbers, etc resting in the organization's cloud account. It gives cloud administrators the opportunity to take action against possible external or internal threat:

1. Possible network intrusion access on sensitive data.
2. Unauthorized internal storage of personal or sensitive data.
3. Detect potential malware and virus through Fortinet AV scan.

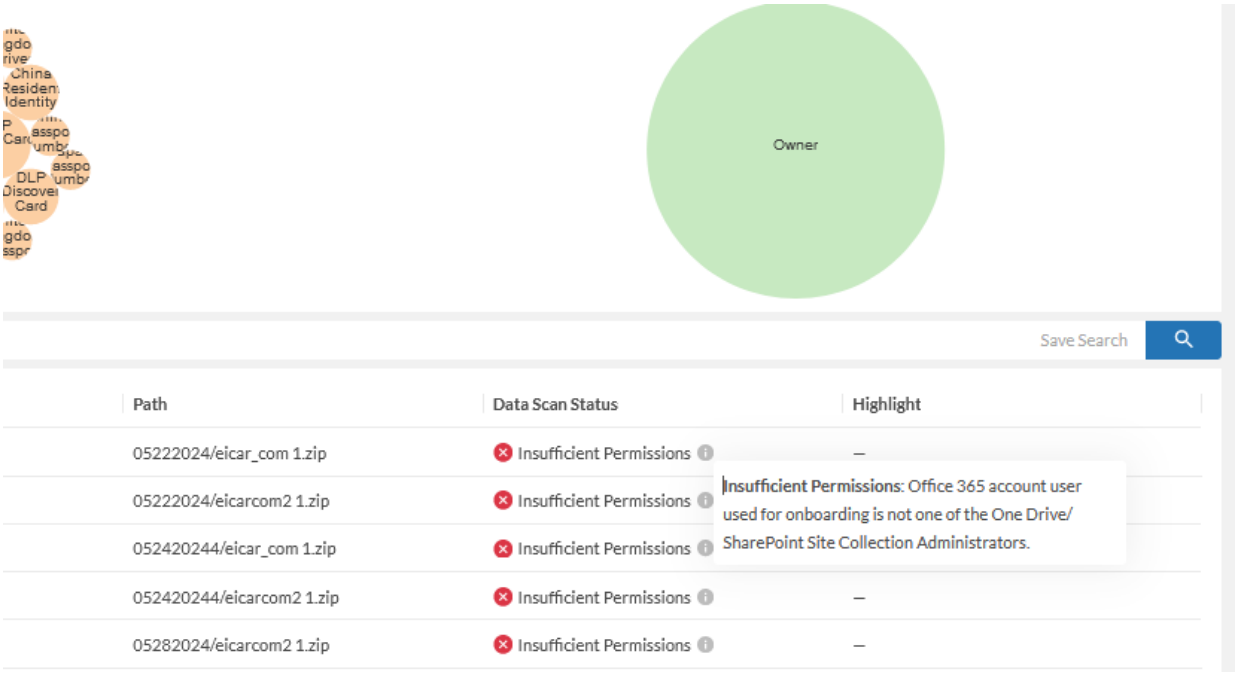
The DLP scan is triggered when user activity is detected on the file resting in the cloud account. If the file is identified to be a type of personal identification information, it will be noted in the file details.

Data Scan Status is located in any supported Cloud Application under **Files**:



Data Scan Status Description

When hover the mouse over the tooltip, it will show detailed description on the file scan status.



List of Data Scan Status

There are 17 Data Scan statuses that reflects the current state or the result of DLP Scan. Depending on the cloud application platform, not all data scan statuses are supported in a single cloud application.

Data Scan Status
Initiating
In Scan Queue
In Progress
Completed
Cannot Be Scanned
Scan Failure
API Threshold Error
Data Protection Exceeded
Empty File
File Not Found
File Transfer Error

Data Scan Status
Insufficient Permissions
Internal Error
No Scan Policy
Unknown Error
Unsupported File Size
Unsupported File Type

Normalized Share Types

Normalized Share types categorize file access permissions of all supported cloud applications in FortiCASB.

Instead of having files retaining their share permissions from different cloud applications, all share permissions are normalized and converted into 5 share types:

- **Private Access Share Type on page 388**
- **Public Editable Share Type on page 390**
- **Group Editable Share Type on page 391**
- **Group Readable Share Type on page 393**
- **Public Readable Share Type on page 395**

Private Access Share Type

Private Access Share Type is a normalized share permission that represents the supported cloud applications share permissions that is only accessible by the file owner.

The following are the share permissions from each cloud applications that the Private Access Share Type covers.

Cloud Application	Share Permission	Description
AWS S3	S3_OBJECT_OWNER_WRITE_OBJ	Owner Write Object
AWS S3	S3_OBJECT_OWNER_WRITE_OBJ_PERM	Owner Write Object Permissions
Azure	AZURE_BLOBCONTAINER_PUBLICACCESS_NONE	Private Only
Azure	AZURE_BLOB_PRIVATE	Private Only
Box	BOX_SHARE_VIEWER	Viewer
Box	BOX_SHARE_OWNER	Owner
Box	BOX_SHARE_VIEWER_UPLOADER	Viewer Uploader
Box	BOX_SHARE_PREVIEWER_UPLOADER	Previewer Uploader
Confluence	CONFLUENCE_SHARE_OWNER	Users Own File
Dropbox	DROPBOX_SHARE_VIEWER	Viewer
Dropbox	DROPBOX_SHARE_OWNER	Owner
Dropbox	DROPBOX_LINK_PASSWORD	Link_password
Egnyte	EGNYTE_SHARE_EDITOR	User Can Edit Folder content
Egnyte	EGNYTE_SHARE_VIEWER	User Can View Folder content
Egnyte	EGNYTE_SHARE_OWNER	Users Own Folder
Egnyte	EGNYTE_SHARE_FULL_ACCESS	User has Full Access
Github	GITHUB_REPO_READ	Read
GitHub	GITHUB_REPO_ADMIN	Admin
Github	GITHUB_REPO_NONE	None
Github	GITHUB_REPO_TRIAGE	Triage
Github	GITHUB_REPO_MAINTAIN	Maintain
Google Workspace	GOOGLE_USER_READER	User View
Google Workspace	GOOGLE_USER_OWNER	User Owner
Google Cloud	GOOGLECLOUD_BUCKET_USER_EDIT_BKT	User Can Edit Bucket
Google Cloud	GOOGLECLOUD_BUCKET_SERVICEACCOUNT_EDIT_BKT	Service Account Can Edit Bucket
Google Cloud	22	User reads Object

Cloud Application	Share Permission	Description
Google Cloud	GOOGLECLOUD_OBJECT_OWNPROJECT_READ_OBJ	Own project reads Object
Google Cloud	GOOGLECLOUD_OBJECT_PROJECT_READ_OBJ	Project reads Object
Google Cloud	GOOGLECLOUD_OBJECT_OWNER_READ_OBJ	Owner reads Object
Google Cloud	GOOGLECLOUD_BUCKET_USER_READ_BKT	User Can Read Bucket
Google Cloud	GOOGLECLOUD_BUCKET_SERVICEACCOUNT_READ_BKT	Service Account Can Read Bucket
Google Cloud	GOOGLECLOUD_OBJECT_OWNER_OWN_OBJ	Owner owns Object
Google Cloud	GOOGLECLOUD_OBJECT_USER_OWN_OBJ	User owns Object
Google Cloud	GOOGLECLOUD_OBJECT_OWNER_OWN_OBJ	Owner owns Object
Google Cloud	GOOGLECLOUD_OBJECT_USER_OWN_OBJ	User owns Object
Google Workspace	GOOGLE_USER_WRITER	User Edit
Google Workspace	GOOGLE_USER_COMMENTER	User Comment
Google Workspace	GOOGLE_USER_ORGANIZER	User TeamDrive Member
Office365	OFFICE365_SHARE_READ	View
Office365	OFFICE365_SHARE_OWNER	Owner
Salesforce	SALESFORCE_SHARE_READ	Viewer
Webex	WEBEX_SHARE_OWNER	202
Webex	WEBEX_SHARE_DIRECT	File Direct Recipient

Public Editable Share Type

Public Editable Share Type is a normalized share permission that represents the supported cloud applications share permissions that is accessible and editable by any user.

The following are the share permissions from each cloud applications that the Public Editable Share Type covers.

Cloud Application	Share Permission	Description
AWS S3	S3_OBJECT_PUBLIC_WRITE_OBJ	Public Write Object
Confluence	CONFLUENCE_SHARE_EDITOR	User Can Edit File
Dropbox	DROPBOX_SHARE_EDITOR	Editor
Dropbox	DROPBOX_LINK	Link_public
Egnyte	EGNYTE_LINK_ANYONE_DOWNLOAD	Link Shared with Anyone Read and Download
Google Workspace	GOOGLE_ANYONE_COMMENTER	Anyone Can Comment
Google Workspace	GOOGLE_ANYONE_WRITER	Anyone Can Edit
Google Workspace	GOOGLE_LINK_ANYONE_ COMMENTER	Anyone With Link Can Edit
Google Workspace	GOOGLE_LINK_ANYONE_WRITER	Anyone With Link Can Edit
Google Cloud	GOOGLECLOUD_OBJECT_ ALLUSERS_OWN_OBJ	All users own Object
Google Cloud	GOOGLECLOUD_OBJECT_ ALLAUTHUSERS_OWN_OBJ	All users own Object
Google Cloud	GOOGLECLOUD_OBJECT_ ALLUSERS_OWN_OBJ	All users own Object
Google Cloud	GOOGLECLOUD_OBJECT_ ALLAUTHUSERS_OWN_OBJ	All users own Object
Office365	OFFICE365_LINK_ALL_EDIT	Anyone Edit Link

Group Editable Share Type

Group Editable Share Type is a normalized share permission that represents the supported cloud applications share permissions that is only accessible and editable by the group.

The following are the share permissions from each cloud applications that the Group Editable Share Type covers.

Cloud Application	Share Permission	Description
AWS S3	S3_OBJECT_CROSS_WRITE_OBJ	Cross-account Write Object
Box	BOX_SHARE_EDITOR	Editor

Cloud Application	Share Permission	Description
Box	BOX_LINK	Link
Box	BOX_SHARE_COOWNER	Coowner
Dropbox	DROPBOX_LINK_TEAM_ONLY	Link_team_only
Egnyte	EGNYTE_GROUP_SHARE_EDITOR	Group Can Edit Folder content
Egnyte	EGNYTE_GROUP_SHARE_OWNER	Group Own Folder
Egnyte	EGNYTE_LINK_DOMAIN_DOWNLOAD	Link Shared to Domain - Read and Download
Egnyte	EGNYTE_LINK_PASSWORD_ DOWNLOAD	Link Shared with Password Protection - Read and Download
Egnyte	EGNYTE_LINK_RECIPIENTS_ DOWNLOAD	Link Shared to specific User Recepients - Read and Download
Egnyte	EGNYTE_LINK_GROUP_DOWNLOAD	Link Shared to Group - Read and Download
Egnyte	EGNYTE_GROUP_SHARE_FULL_ ACCESS	Group has Full Access
Google Cloud	GOOGLECLOUD_BUCKET_GROUP_ EDIT_BKT	Group Can Edit Bucket
Google Cloud	GOOGLECLOUD_BUCKET_DOMAIN_ EDIT_BKT	Domain Can Edit Bucket
Google Cloud	GOOGLECLOUD_BUCKET_PROJECT_ EDIT_BKT	Project Can Edit Bucket
Google Cloud	GOOGLECLOUD_BUCKET_ ALLUSERS_EDIT_BKT	All Users Can Edit Bucket
Google Cloud	GOOGLECLOUD_BUCKET_ ALLAUTHUSERS_EDIT_BKT	All Authenticated Users Can Edit Bucket
Google Cloud	GOOGLECLOUD_OBJECT_GROUP_ OWN_OBJ	Group owns Object
Google Cloud	GOOGLECLOUD_OBJECT_DOMAIN_ OWN_OBJ	Domain owns Object
Google Cloud	GOOGLECLOUD_OBJECT_ OWNPROJECT_OWN_OBJ	Own project owns Object
Google Cloud	GOOGLECLOUD_OBJECT_PROJECT_ OWN_OBJ	Project owns Object
Google Cloud	GOOGLECLOUD_OBJECT_GROUP_ OWN_OBJ	Group owns Object

Cloud Application	Share Permission	Description
Google Cloud	GOOGLECLOUD_OBJECT_DOMAIN_OWN_OBJ	Domain owns Object
Google Cloud	GOOGLECLOUD_OBJECT_OWNPROJECT_OWN_OBJ	Own project owns Object
Google Cloud	GOOGLECLOUD_OBJECT_PROJECT_OWN_OBJ	Project owns Object
Google Workspace	GOOGLE_GROUP_WRITER	Group Edit
Google Workspace	GOOGLE_DOMAIN_WRITER	People In The Domain Can Edit
Google Workspace	GOOGLE_LINK_DOMAIN_WRITER	People In The Domain With Link Can Edit
Google Workspace	GOOGLE_LINK_DOMAIN_COMMENTER	People In The Domain With Link Can Comment
Google Workspace	GOOGLE_DOMAIN_COMMENTER	People In The Domain Can Comment
Google Workspace	GOOGLE_GROUP_COMMENTER	Group Comment
Office365	OFFICE365_SHARE_EDIT	Edit
Office365	OFFICE365_LINK_LOGIN_EDIT	People In Organization Can Edit
Office365	OFFICE365_LINK_USER_EDIT	People With The Link Can Edit
Salesforce	SALESFORCE_SHARE_EDIT	Collaborator
Salesforce	SALESFORCE_LINK	Link
Webex	WEBEX_SHARE_GROUP	File Group Recipient

Group Readable Share Type

Group Readable Share Type is a normalized share permission that represents the supported cloud applications share permissions that is only readable by a specific group of users.

The following are the share permissions from each cloud applications that the Group Readable Share Type covers.

Cloud Application	Share Permission	Description
AWS S3	S3_OBJECT_CROSS_READ_OBJ	Cross-account Read Object
AWS S3	S3_OBJECT_CROSS_READ_OBJ_PERM	Cross-account Read Object Permissions
AWS S3	S3_OBJECT_CROSS_WRITE_OBJ_PERM	Cross-account Write Object Permissions
Egnyte	EGNYTE_GROUP_SHARE_VIEWER	Group Can View Folder content
Egnyte	EGNYTE_LINK_DOMAIN_PREVIEW	Link Shared to Domain - Read only
Egnyte	EGNYTE_LINK_PASSWORD_PREVIEW	Link Shared with Password Protection - Read only
Egnyte	EGNYTE_LINK_RECIPIENTS_PREVIEW	Link Shared to specificUser Recepients - Read Only
Egnyte	EGNYTE_LINK_GROUP_PREVIEW	Link Shared to Group - Read Only
Google Cloud	GOOGLECLOUD_OBJECT_GROUP_READ_OBJ	Group reads Object
Google Cloud	GOOGLECLOUD_OBJECT_ALLAUTHUSERS_READ_OBJ	All Authenticated users reads Object
Google Cloud	GOOGLECLOUD_BUCKET_GROUP_READ_BKT	Group Can Read Bucket
Google Cloud	GOOGLECLOUD_BUCKET_DOMAIN_READ_BKT	Domain Can Read Bucket
Google Cloud	GOOGLECLOUD_BUCKET_PROJECT_READ_BKT	Project Can Read Bucket
Google Cloud	GOOGLECLOUD_BUCKET_ALLAUTHUSERS_READ_BKT	All Authenticated Users Can Read Bucket
Google Workspace	GOOGLE_GROUP_READER	Group View
Google Workspace	GOOGLE_DOMAIN_READER	People In The Domain Can View
Google Workspace	GOOGLE_LINK_DOMAIN_READER	People In The Domain With Link Can View
Office365	OFFICE365_LINK_LOGIN_READ	People In Organization Can View
Office365	OFFICE365_LINK_USER_READ	People With The Link Can View

Public Readable Share Type

Public Readable Share Type is a normalized share permission that represents the supported cloud applications share permissions that is only readable by any user.

The following are the share permissions from each cloud applications that the Public Readable Share Type covers.

Cloud Application	Share Permission	Description
AWS S3	S3_OBJECT_PUBLIC_READ_OBJ	Public Read Object
AWS S3	S3_OBJECT_PUBLIC_READ_OBJ_PERM	Public Read Object Permissions
AWS S3	S3_OBJECT_PUBLIC_WRITE_OBJ_PERM	Public Write Object Permissions
Azure	AZURE_BLOBCONTAINER_PUBLICACCESS_CONTAINER	Public Read Access on Container Level
Azure	AZURE_BLOBCONTAINER_PUBLICACCESS_BLOB	Public Read Access on Container and Blob Level
Azure	AZURE_BLOB_PUBLIC_READ	Public Read Access on Blob
Confluence	CONFLUENCE_SHARE_VIEWER	User Can View File
Egnyte	EGNYTE_LINK_ANYONE_PREVIEW	Link Shared with Anyone - Read only
Google Cloud	GOOGLECLOUD_OBJECT_ALLUSERS_READ_OBJ	All users reads Object
Google Cloud	GOOGLECLOUD_BUCKET_ALLUSERS_READ_BKT	All Users Can Read Bucket
Google Workspace	GOOGLE_ANYONE_READER	Anyone Can View
Google Workspace	GOOGLE_LINK_ANYONE_READER	Anyone With Link Can View
Office365	OFFICE365_LINK_ALL_READ	Anyone View Link

Microsoft Online Apps Integration (Office 365 Only)

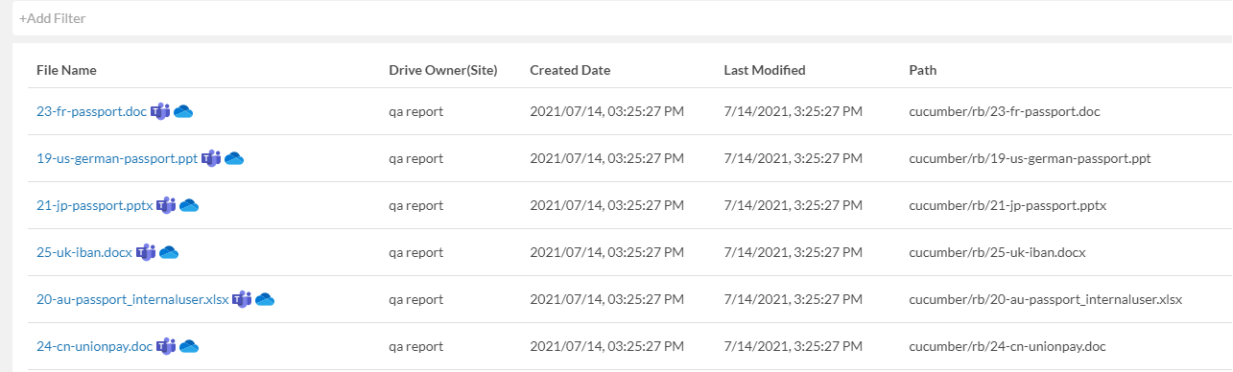
The Microsoft online application integration monitors **Microsoft Yammer, Microsoft One Drive, Microsoft Sharepoint**, and **Microsoft Teams**.

In Files page, all shared files from Microsoft Online Application are shown with corresponding logos.

Microsoft Online Application and Logos

Microsoft Online Application	Logo
Microsoft Yammer	
Microsoft One Drive	
Microsoft Sharepoint	
Microsoft Teams	
Azure Active Directory	

For example, the following files are on both Microsoft Teams and Microsoft One Drive.



Google Drive Label Integration (Google Workspace Only)

Introduction

Google Drivel Label is a feature of Google Drive where labels can be attached to files stored in Google Drive to provide better organization.

For more details on Google Drive Labels, please see Get Started as a Drive labels admin.

Google Drive Label Integration

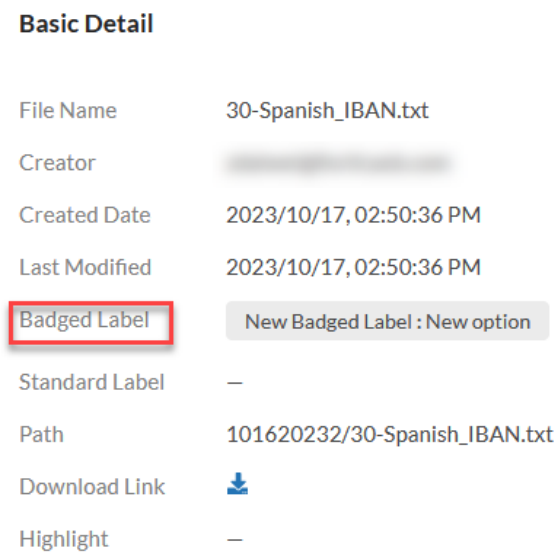
FortiCASB integrates Google Drive Label in Google Workspace files' profiles to provide additional details on the metadata of the files to give more insights.

There are two types of labels, Badged labels and Standard Labels.

Basic Detail - Badged Label

Badged Labels are critical metadata of an organization, and are the most visible labels next to the file name when opened in Google Doc, Sheets, etc.

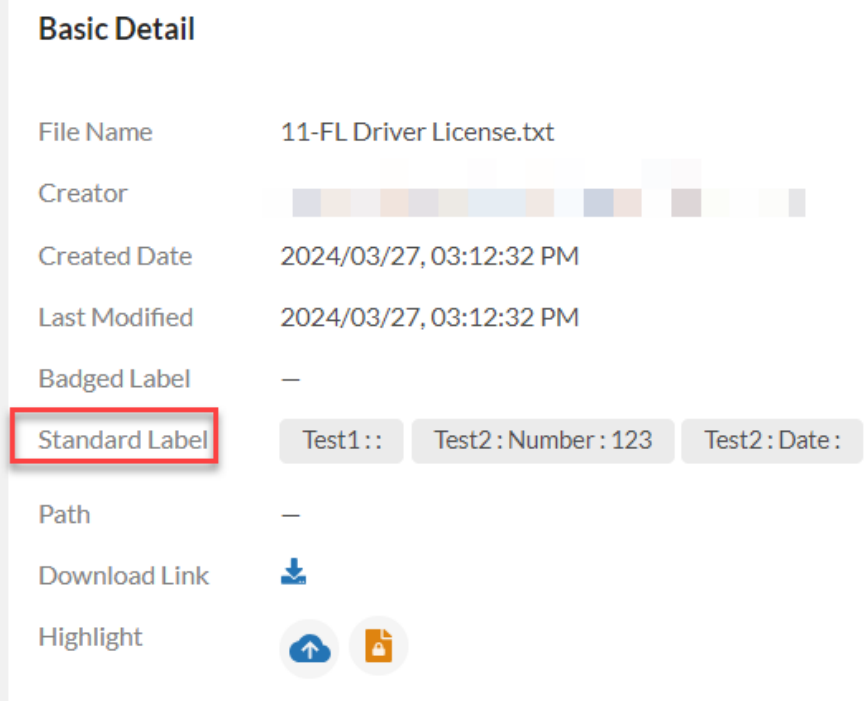
There is only one badged label per organization.



Basic Detail - Standard Label

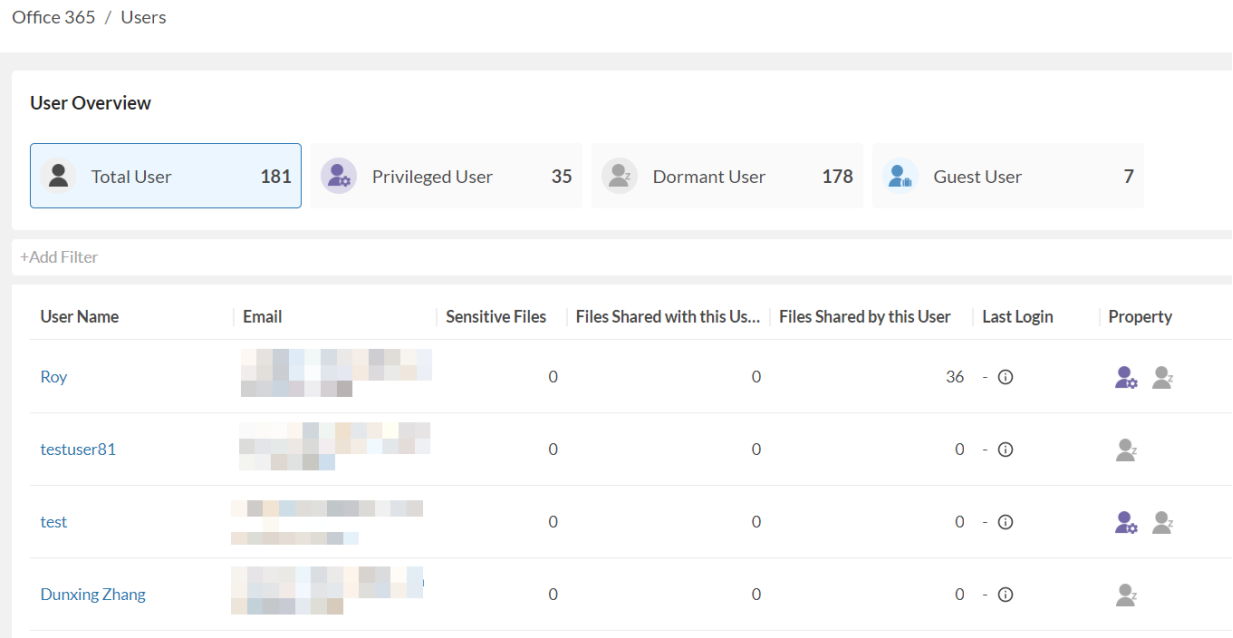
Standard Labels are other metadata of an organization that can be used like tags where fields and values can be attached for additional information.

There can be a maximum of 150 standard labels per organization.



Users

Users page displays user access privilege to cloud application and the files shared or shared by the users.



Click on the **User Name** for more details about the user.

The type of user is displayed in **Property** column.

Type of User	Description
Privileged User	Any user with specific administrative privileges. For a list of these specific privileges, see Administrative Privileges on page 400.
Dormant User	Any user that has not accessed the cloud application for at least 30 days.
Guest User	Any user from an external company with access to your cloud application.

If the User page cannot retrieve privileged roles information from your Office 365 account, make sure you have **Global Administrator Privileges** and **Azure Active Directory Premium P2**.

Administrative Privileges

Box

An admin with all of the following permissions is considered a privileged user:

- Manage users and groups
- Make calls on behalf of users
- View all data

Confluence

A user with any of the following administrator roles is considered a privileged user:

- Site Admin
- Administrator
- Trusted User

Dropbox Business

A Team Admin is considered a privileged user.

Egnyte

A user with any of the following administrator roles is considered a privileged user:

- Administrator
- Power User

Google Workspace

A user with any of the following administrator roles is considered a privileged user:

- Super Administrator
- Groups Administrator
- User Management Administrator
- Help Desk Administrator
- Services Administrator
- User Customized Administrator

Jira

A user with any of the following administrator roles is considered a privileged user:

- Site Admin
- Administrator
- Jira-Administrator

Github

Only the Account owner is considered as a privilege user.

Office 365

A user with any of the following administrator roles is considered a privileged user:

- global administrator
- billing administrator
- password administrator
- service administrator
- user management administrator
- Exchange administrator
- SharePoint administrator
- Skype for Business administrator

SAP IAS

A user with any of the following administrator roles is considered a privileged user:

- Admin user or user with user type: Public

Salesforce

A user with any of the following administrative permissions is considered a privileged user:

- Assign Permission Sets
- Manage Sharing
- Modify All Data
- Manage Encryption Keys
- View All Data
- View All Users

ServiceNow

A user with any of the following administrator roles is considered a privileged user:

- Administrative User (Any user with admin role)

Webex Teams

A user with any of the following administrator roles is considered a privileged user:

- User Administrator
- Read-only Administrator

- Support Administrator
- Device Administrator
- Sales Administrator
- Help Desk Administrator
- Full Administrator

Zoom

A user with any of the following administrator roles is considered a privileged user:

- Owner
- Admin
- Custom role user with all privileges of an Admin role.

Policy

In addition to the Data Security policy from Data Protection, there are also Threat Protection and Compliance policies that are specific to each SaaS application.

Threat protection policies track suspicious user behavior.

Compliance policies monitor cloud accounts in compliance with various compliance standards (SOX-COBIT, PCI, HIPAA, etc.).

- **Threat Protection on page 403**
- **Compliance Policy on page 404**

To activate a policy to trigger alert, please refer to Policy Configuration on page 405.

Threat Protection

Threat Protection policies track suspicious user behavior. **For example**, if a user fails to enter his or her password correctly multiple times in a row and you have the Excessive Login Failures policy active, FortiCASB will send you an alert.

Threat Protection feature is currently only available for **Salesforce**, **Office 365**, **Box**, **Dropbox**, **Confluence, Egnyte, GitHub, Jira, SAP IAS, ServiceNow, Webex Teams**, and **Zoom**.

Threat protection policies

Access	Description
Excessive Login Failures	Triggers an alert when the number of failed logins for a user exceeds a set threshold.
Password Change	Triggers an alert when passwords are changed.
Suspicious Movement	Triggers an alert when a change in a user's geographic location exceeds threshold parameters.
Unapproved Login Location	Triggers an alert when a user logs in from an unapproved geographic location.

Suspicious Activity	Description
Restricted User	Triggers an alert when a monitored user performs select activities.
Suspicious IP	Triggers an alert when there is activity from a suspicious IP.
Suspicious Time	Triggers an alert when there is activity outside of work hours.
Suspicious Location	Triggers an alert when there is activity from suspicious locations.

Sensitive Activity	Description
Sensitive Event	Triggers an alert when a sensitive event occurs.
Sensitive File	Triggers an alert when a specified sensitive file is accessed.
Ransomware Behavior Detection	Triggers an alert when the directory's file (s) had been replaced.

Abnormal Traffic	Description
Large File Upload	Triggers an alert when a file upload exceeds a size threshold.

Compliance Policy

Compliance policies monitor cloud accounts in compliance with various compliance standards (SOX-COBIT, PCI, HIPAA, etc.).

Only polices with in **Alert** column will generate alerts. All other compliance polices will generate data in **compliance report**.

The compliance reports are designed to fulfill the compliance requirements of your organization.

For example, if a user accesses a file containing private heath information and you have the corresponding HIPAA policy enabled, FortiCASB will add the corresponding access logs in the Compliance report.

The prerequisite to generate Compliance report is to enable and configure compliance policies required by your organization. For more details on configuring compliance policies, please refer to Policy Configuration on page 405.

List of Compliance policies

See **Policy Configuration on page 405** for instructions/examples on setting policies.

SOX-COBIT

SOX-COBIT policies help your organization track and show compliance with the Sarbanes-Oxley (SOX) Act of 2002 using COBIT guidelines. Use these policies to monitor your cloud applications for SOX compliance, then use the Report feature to print a report detailing compliance specifics.

PCI-DSS

PCI-DSS (Payment Card Industry Data Security Standard) utilizes the current industry standard version 3.2.1 to help your organization track and stay in compliant with the current industry payment standard. FortiCNP uses these policies to monitor your cloud applications for PCI-DSS compliance, and use the Reporting feature to generate reports.

HIPAA

HIPAA policies help your organization track and show compliance with the Health Insurance Portability and Accountability Act (HIPAA). Use these policies to monitor your cloud applications for HIPAA compliance, then use the Report feature to print a report detailing compliance specifics.

GDPR

GDPR policies help your organization track and show compliance with the EU General Data protection Regulation (GDPR). Use these policies to monitor your cloud applications for GDPR compliance, then use the Report feature to print a report detailing compliance specifics. Personal data type can be setup inside GDPR policy configuration for monitoring.

ISO 270001

ISO 270001 is the best-known standard in the family in providing requirements for an information security management system (ISMS). ISO 270001 policies help your organization manage the security of assets, such as financial information, intellectual property, employee details, and information entrusted to you by third parties.

NIST 800-53 V4

NIST 800-53 V4 is the recommended security controls for federal information systems and organizations. It documents security controls for all federal information systems.

NIST 800-171

NIST 800-171 can help to protect controlled unclassified information in non-federal Information systems and organizations.

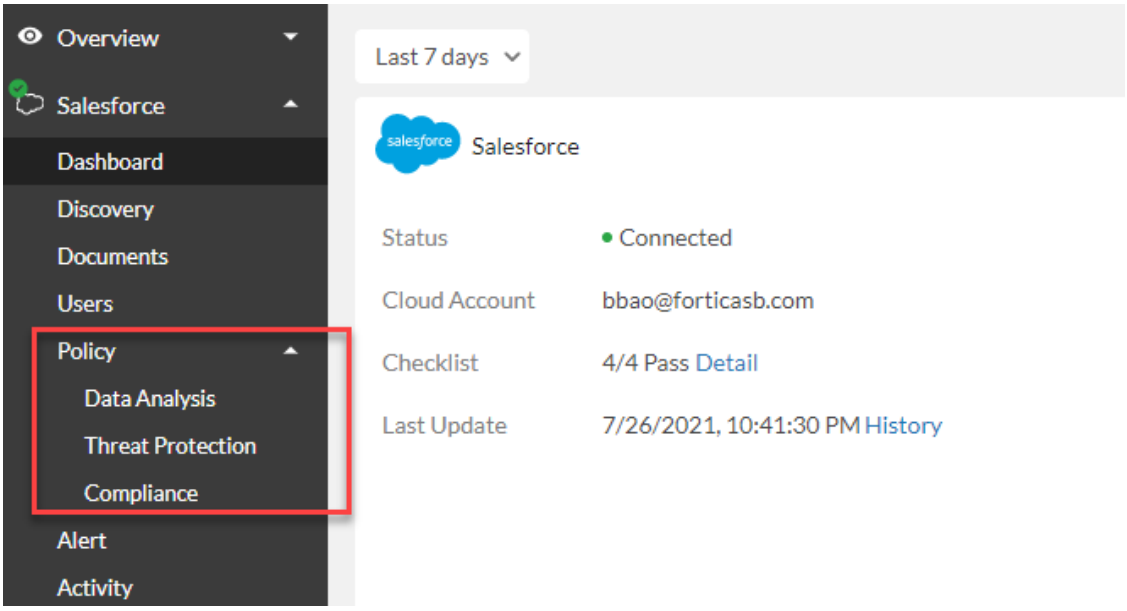
Policy Configuration

One important note on policy configuration is that only the policy that is turned **On** can **trigger alerts** or **generate reports**.

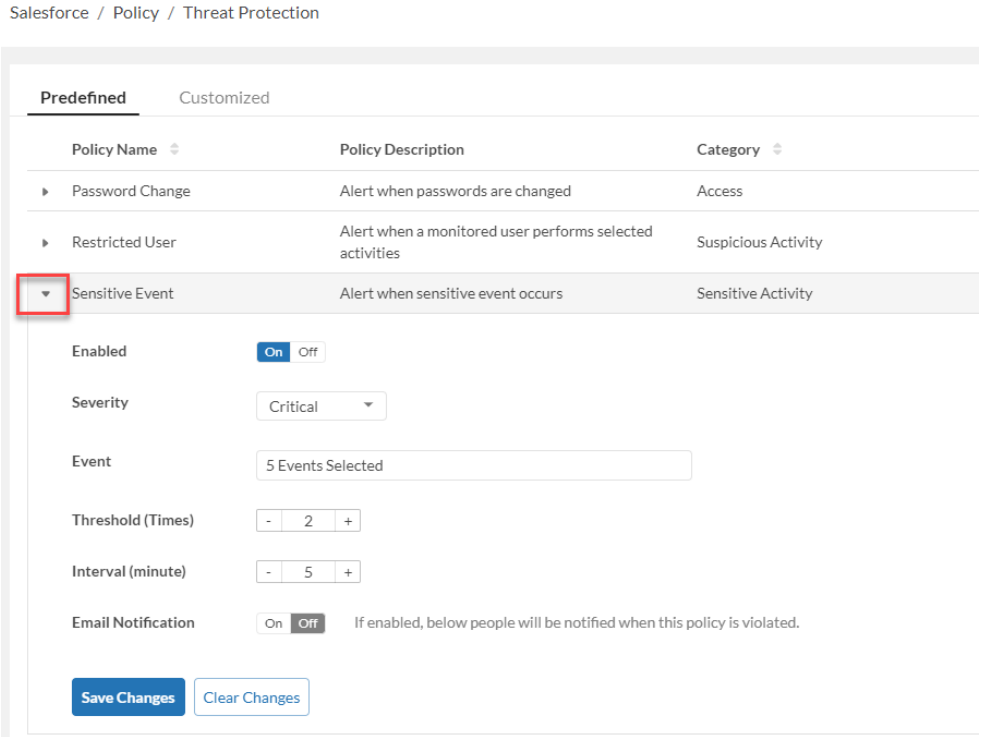
Enable Policy

Policy setting allows you to configure each policy depending on the requirement of your organization. Follow the steps below to configure policies.

1. Select a cloud application from FortiCASB main dashboard.
2. Click on the **Policy** drop down menu, and select any type of Policy (**Data Analysis**, **Threat Protection** or **Compliance**)



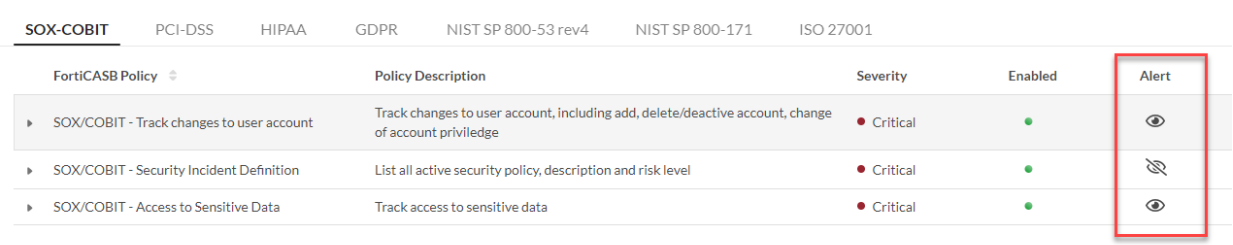
3. Click on any policy drop down menu. **For example**, "Sensitive Event".



4. Enable the policy by setting it to **On**.
5. Click **Save Changes** to complete the configuration.

The policy you set should be active after a few minutes.

Note: For **Compliance Policies**, only polices with in Alert column will generate alerts. All other Compliance polices will still generate data in Compliance reports.



General Configuration

These are the common parameters in Policy Configuration. Every policy has different setting parameters. Not all parameters are available in any given policy setting.

Parameter Name	Description
Enabled	Specify whether or not the policy is enabled to trigger alert. A policy is active when it is set to **On**.
Severity Level	The severity level for the policy, you can set the severity level as **Critical**, **Alert**, **Warning**, or **Information**.
Matching Threshold	Specify the minimum threshold for an alert to be triggered. For example, **DLP Visa Card Policy** with a matching threshold of 2 will trigger an alert when 2 or more credit card numbers are detected.
Interval (minute)	The minimum threshold between each time the policy is triggered by the user activity for an alert to be triggered. For example, **Sensitive Event** with an interval of 5 minutes will trigger an alert when a sensitive event occurs every 5 minutes.
Data Pattern	Specify the DLP or customized data pattern to be associated with the policy to protect the type of sensitive data. FortiCASB will search for the selected DLP data pattern during Discovery scans.
File Path Regex	Specify the targeted regular expression pattern of the cloud storage files which FortiCASB will run DLP scan on.
Email Notification (Notify FortiCASB Users)	When the email notification is turned on, FortiCASB users can be added to be notified when an alert is triggered by the policy.
Email Notification (Notify File Owners)	This feature is only available in customized Threat Protection policies. When the policy is turned on, the file owner will be notified on the file exposure with editable notification.

For more details on policy configurations, please see

Threat Protection Policy Configuration on page 408

Compliance Policy Configuration on page 423

Customized Policy Configurations on page 430

Threat Protection Policy Configuration

List of all Threat Protection Policy Configuration guides

Excessive Login Failures

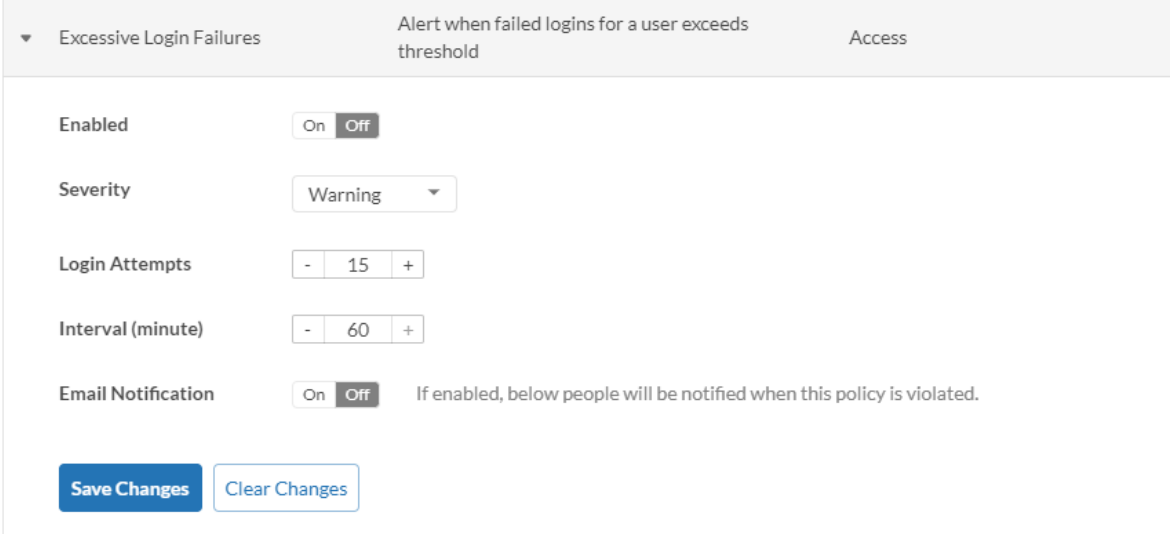
Description

Excessive Login Failures monitors for excessive login attempts of unidentified user in a time interval. Administrators are able to customize the threshold of number of failed login attempts and the time interval (minutes) before an alert is generated.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Excessive Login Failures** and click on the right arrow key **>** button to expand the policy.
4. Click On in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Login Attempts,** enter the threshold of the number of failed login attempts before an alert is generated.
7. In **Interval** (minute), enter the time interval of the first failed login attempt of the same user.
8. Click **Save Changes** to save and update the configuration.

After the policy is enabled and configured, whenever an unidentified user exceeded the login attempts threshold within in the given time interval, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Suspicious Movement

Description

Suspicious Movement policy monitors changes in users geographical location. When the speed (mph) of traveling between the original and the new location exceeds the maximum threshold, an alert will be generated to inform on the unidentified cloud account intrusion.

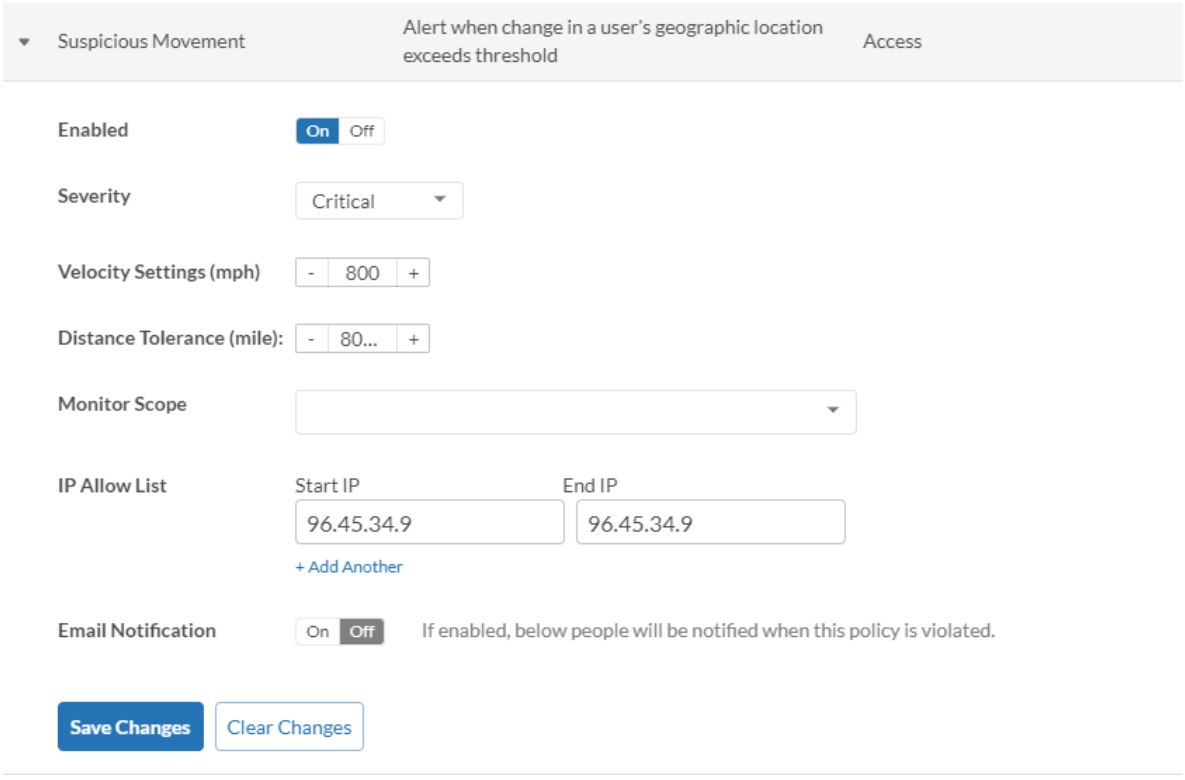
The policy also takes in account of the proximity distance of the new location before checking for the speed in which the user traveled.

In exception cases, known users can be excluded from being monitored by placing them on the IP allow list.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Suspicious Movement** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Velocity Setting (mph)**, enter the maximum speed in which a user can travel between two locations in any given time before being viewed as suspicious movement. The most commonly used value for this parameter is commercial flight speed, 600 mph.
7. In **Distance Tolerance (mile)** field, enter a proximity distance that will not be accounted for in monitoring for suspicious movement.
   For example, if you entered 50 miles, any login within 50 miles of the origin will not be taken as suspicious movement.
8. In **IP Allow List**, enter sets of IP ranges to be excluded from being monitored for suspicious movements. This is useful when you know the users who travel periodically.
9. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever the new user login location exceeded the maximum speed threshold, an alert will be sent on the illegal login, for more details, please refer to Alert on page 434.

Unapproved Login Location

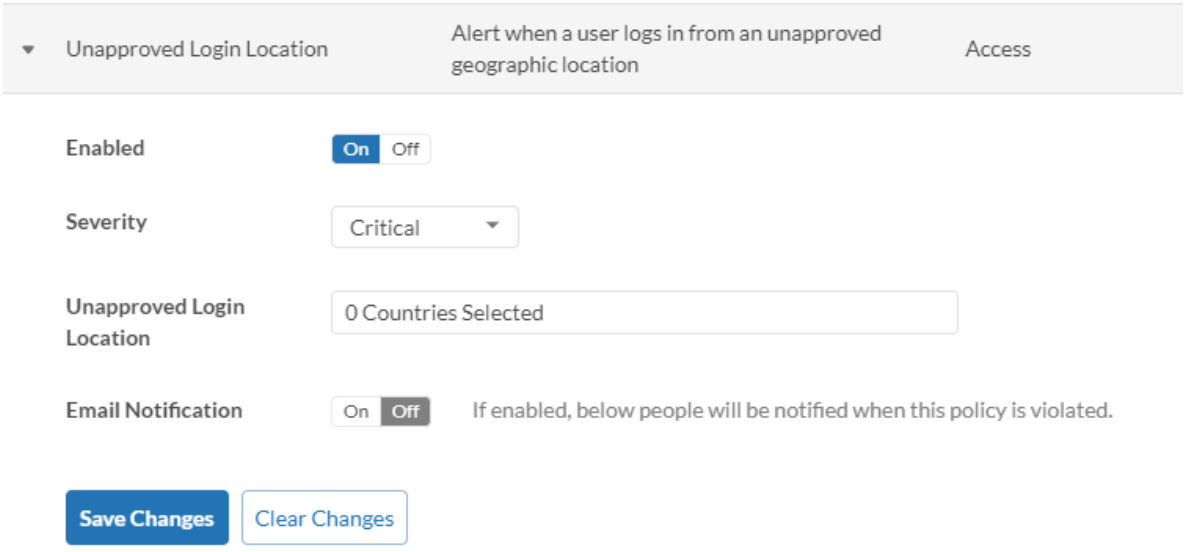
Description

Unapproved Login Location policy monitors for logins from block listed country.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Unapproved Login Location** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).

6. Click **Unapproved Location List** to select the countries. This will generate an alert whenever there is a login attempt from the block listed countries.
7. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever an unidentified user login from the block listed location, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Restricted User

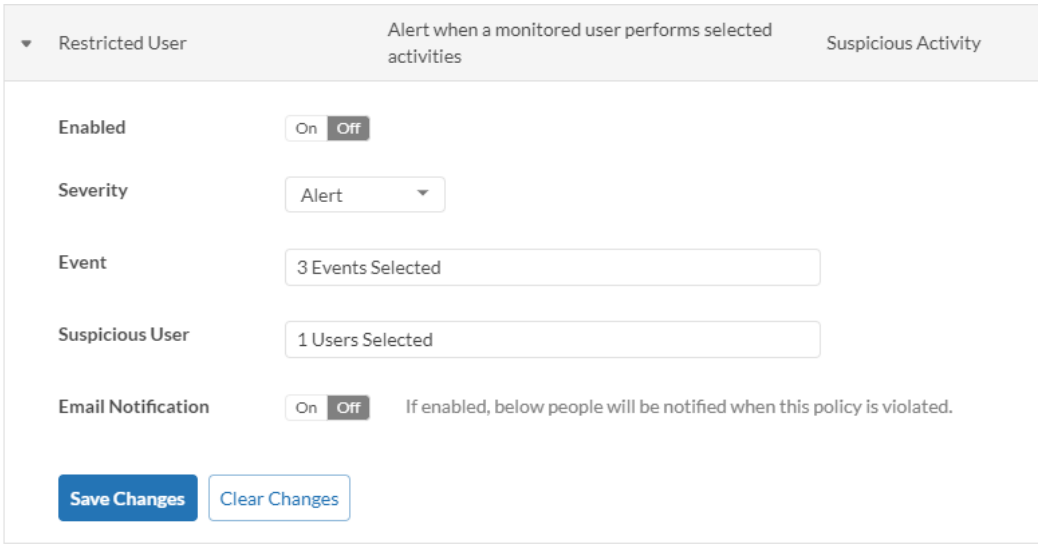
Description

Restricted User policy monitors for cloud account activities conducted by targeted users. An alert will be sent whenever targeted user(s) performs certain activities.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Restricted User** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Event** section, click to select **Specific events** then click the drop down field under it to select specific event(s). To select all events instead, click on **Select all events**.
7. In **Suspicious User** section, click to select **Specify users** and click the **Select User** drop down field to select user(s). To select all users instead, click **Select all users**.
8. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever the targeted users perform certain activities, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Suspicious IP

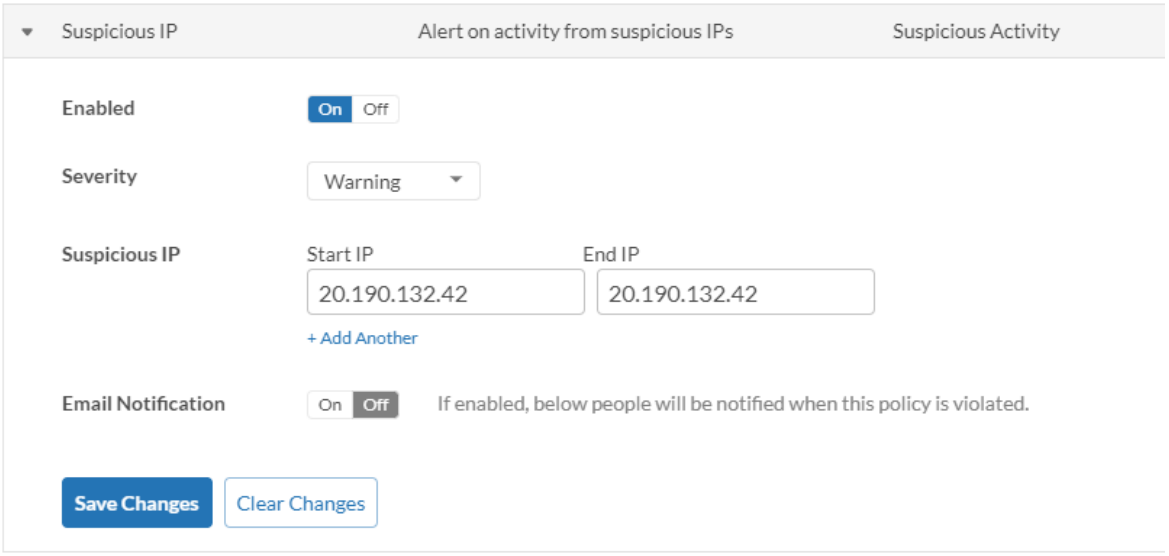
Description

Suspicious IP policy monitors cloud account activities conducted by targeted IP addresses. Alerts will be sent when any activities are performed by the targeted IPs.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Suspicious IP** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level **(Critical, Alert, Warning, Information**).
6. In **Suspicious IP** section, click to enter the beginning and ending IP range, and click **+** to add. Repeat this step to enter more IP ranges,
7. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever a targeted IP performs any activity, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Suspicious Time

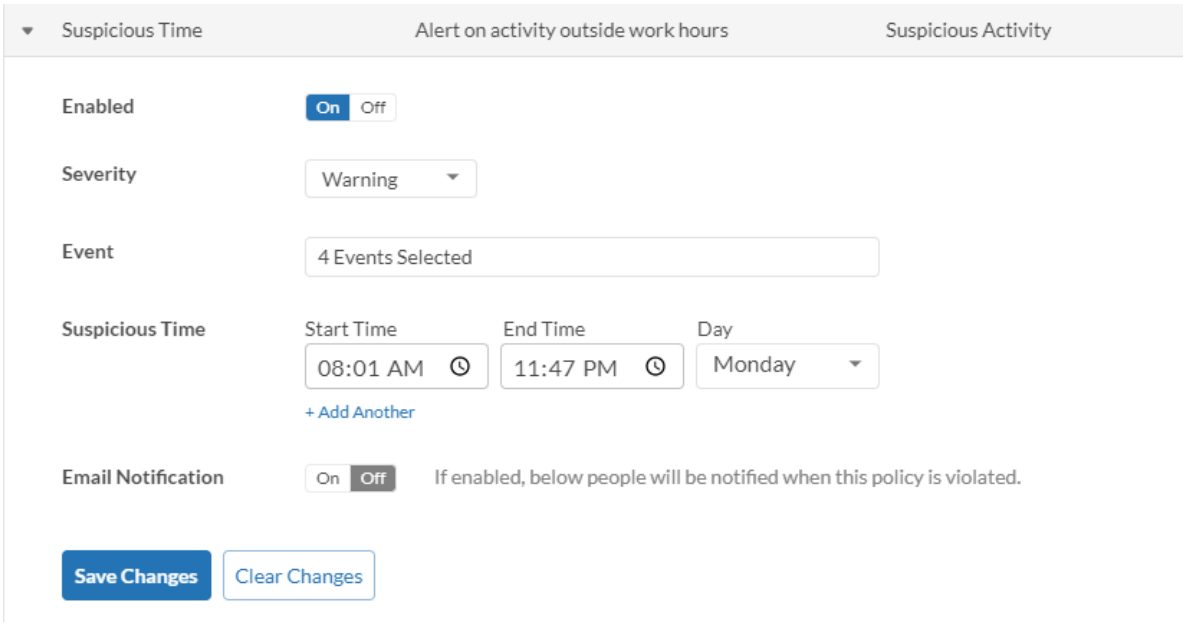
Description

Suspicious Time policy monitors cloud account activities outside of regular working hours.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Suspicious Time** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Event** section, click to select **Specific events** then click the drop down field under it to select specific event(s). To select all events instead, click on **Select all events**.
7. In **Suspicious Time** section, click on **Select day in week** drop down menu to select a day in the week to monitor for suspicious event. Then enter the beginning and end time of the day to monitor the event.
8. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever the specific activity is conducted in the suspicions time frame during the target day of the week, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Suspicious Location

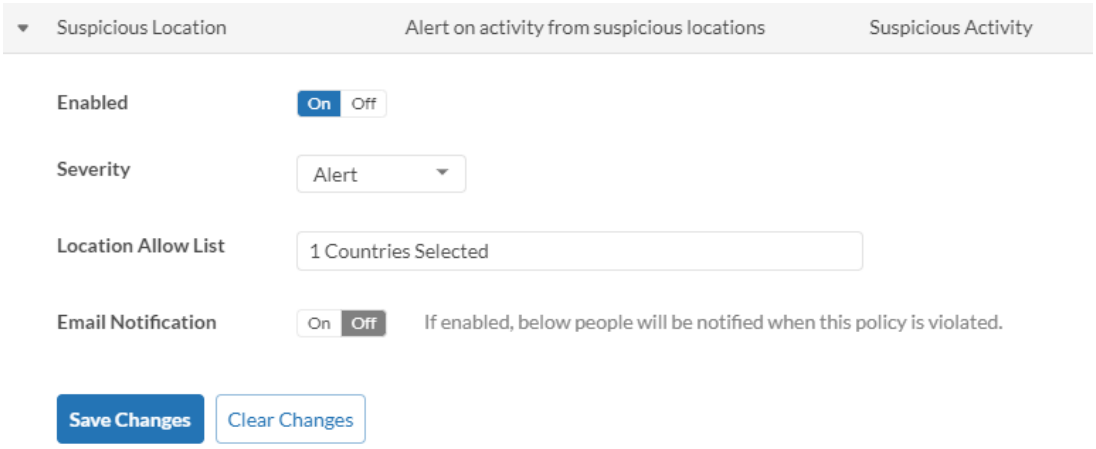
Description

Suspicious Location policy monitors for cloud account activities not shown on location allow list.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Suspicious Location** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Location Allow List**, click **Select Country** drop down menu to select a country to be added to the location Allow list. Click **Add** to finish adding the location. Repeat the same process to add more location.
7. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever there is any cloud account activity outside of the allow list locations, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Sensitive File

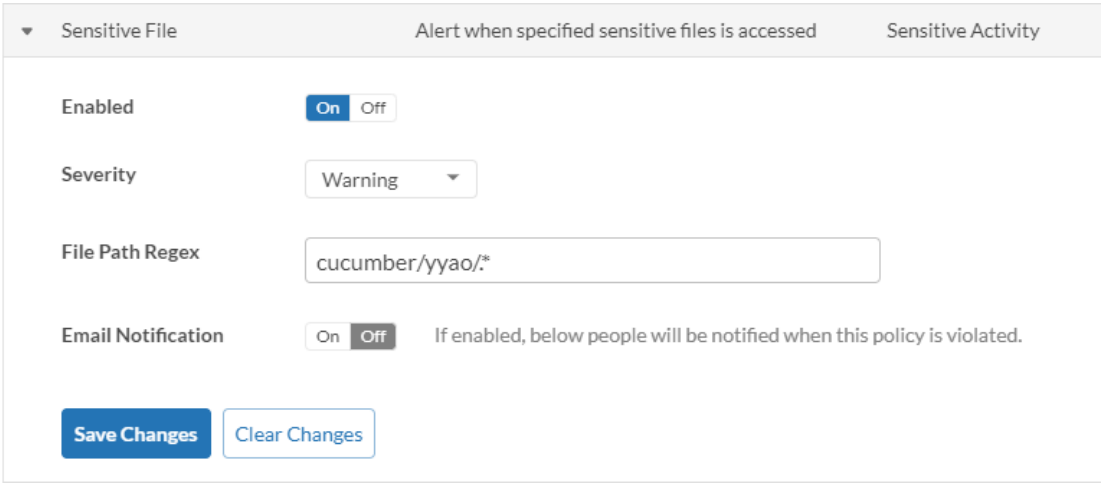
Description

Sensitive File policy monitors and sends an alert when targeted cloud account files are being accessed. The location of the cloud account file path is configured through Regex.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Sensitive File** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **File Path Regex**, enter a valid Regex of the target file path to be monitored. Here are examples of file path Regex:
   a. ".*" targets all files in the cloud account.
   b. "^(?:[\w]\:|\\)(\\[a-z_\-\s0-9\.]+)+\.(txt|gif|pdf|doc|docx|xls|xlsx)$" targets files begin with x:\ or \\ with files ending in the following types of extensions: txt, gif, pdf, doc, docx, xls, xlsx. Here are the file paths that will this file path Regex matches:
      i. \\192.168.0.1\folder\file.pdf
      ii. c:\my folder\abc abc.docx

   Reference: https://www.codeproject.com/Tips/216238/Regular-Expression-to-Validate-File-Path-and-Exten
7. Click **Save Changes** to update the policy configuration.

After the policy is enabled and configured, whenever any file targeted by the file path Regex is accessed on the cloud account, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Sensitive Event

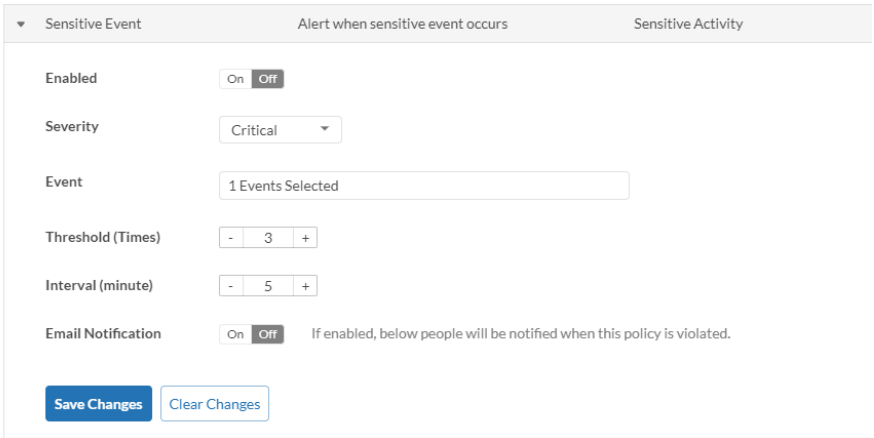
Description

Sensitive Event policy monitors specific cloud account activities and triggers alerts.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Sensitive Event** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Event** section, click to select **Specific events** then click the drop down field under it to select specific event(s). To select all events instead, click on **Select all events**.

7. In **Threshold (Times)**, enter the maximum number of times the event or activity is being performed by the same user before an alert is triggered.
8. In **Interval (Minutes)**, specify the amount of time that the user conducts the targeted activities before triggering an alert.
9. Click **Save Changes** to update the configuration.

A typical example for the policy usage is downloading or uploading multiple files in a given amount of time would trigger an alert.

After the policy is enabled and configured, whenever the specific activity is conducted repeatedly by the same user in a given time frame, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Large File Upload

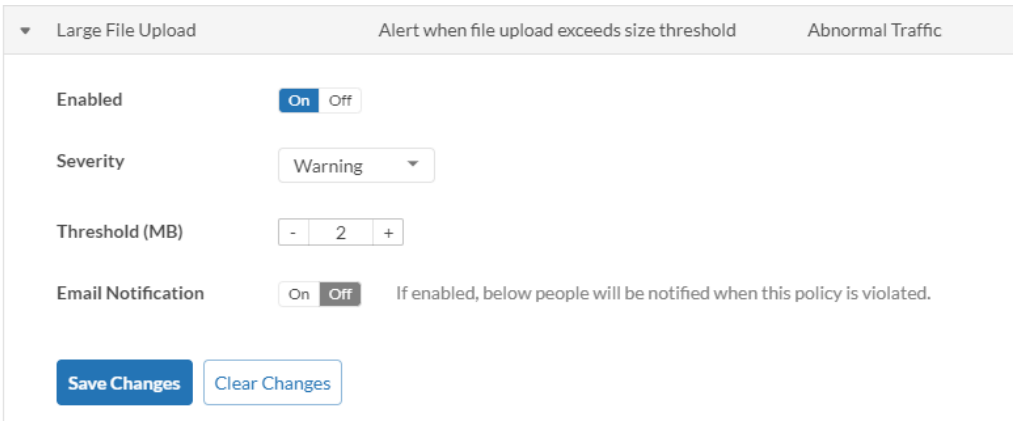
Description

Large File Upload policy monitor and tracks for file size uploaded to the cloud account, an alert will be sent when the file uploaded exceeded file size threshold.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Threat Protection**.
3. Locate **Large File Upload** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.

5. 

6. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
7. Enter the maximum file size (MB) of the file to be uploaded to the cloud account without triggering an alert.
8. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever a file larger than the file size threshold is uploaded to the cloud account, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Suspicious Label Activity (Google Workspace Only)

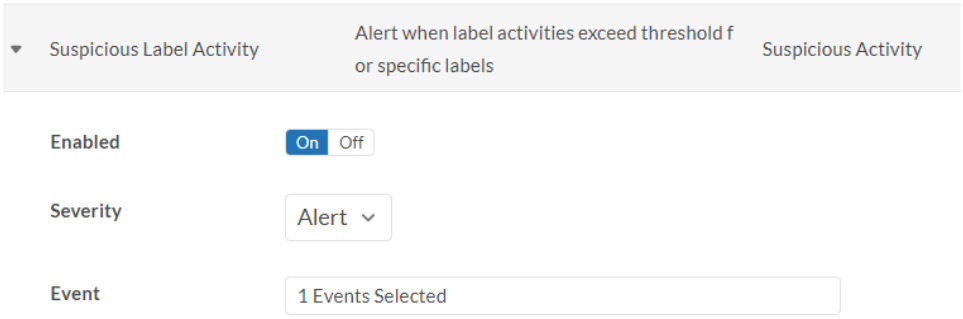
Description

Suspicious Label Activity alerts when targeted Google Drive label activities exceed threshold for specific labels.

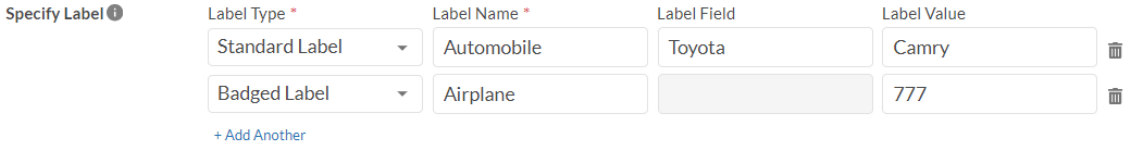
Policy Configuration

Follow the steps below to enable and configure the policy

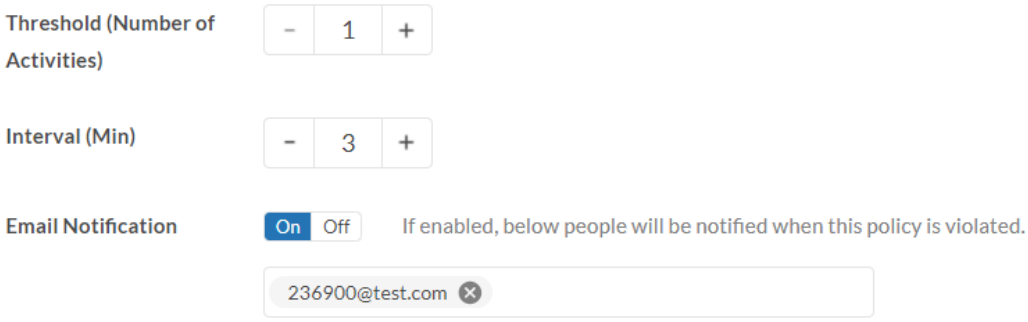
1. Go to **Google Workspace > Policy > Threat Protection**.
2. Locate **Suspicious Label Activity** and click on the right arrow key **>** button to expand the policy.
3. Click **On** in **Enabled** to enable the policy.



4. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
5. Click **Event** drop down menu and select the event(s) that would trigger the alert.
   a. **Attach label to file** - alert will trigger if a new label is attach to the file.
   b. **Remove label from file** - alert will trigger if an existing label is removed from the file.
   c. **Edit label from file** - alert will trigger if an existing label is modified.
6. In **Specify Label**, click **Label Type** drop down menu to select a label Type, and fill in appropriate fills.
   a. **Standard Labels** have Label Name, Label Field (optional), and Label Values (optional).
   b. **Badged Labels** only have Label Name and Label Value (optional)



7. Click to select **Threshold (Number of Activities)** needed to trigger the alert.



8. In **Interval**, select number of minutes between each activity to trigger an alert.
9. Click **On** turn on **Email Notification** and enter the email address to receive notification alert.
10. Click **Saves Changes** to finish.

Compliance Policy Configuration

Compliance Policy Configurations offers oppurtunities to look for violation of compliance policies in cloud account usage.

Regex is used in Compliance Policy Configurations to target specific data.

Compliance Policy - Regex Configuration on page 423

Other examples of Compliance Policy Configurations:

- SOX-COBIT - Access to Sensitive Data on page 425
- PCI - Failed Access Attempt Detection on page 426
- PCI - Privileged Account Activity on page 428
- PCI - Retention Violation for Cardholder Data on page 429

Compliance Policy - Regex Configuration

Introduction

Regex or Regular Expression is a set of pattern matching rules used in search for specific data patterns in files located in the cloud accounts.

Here are some common search queries and the corresponding Regex:

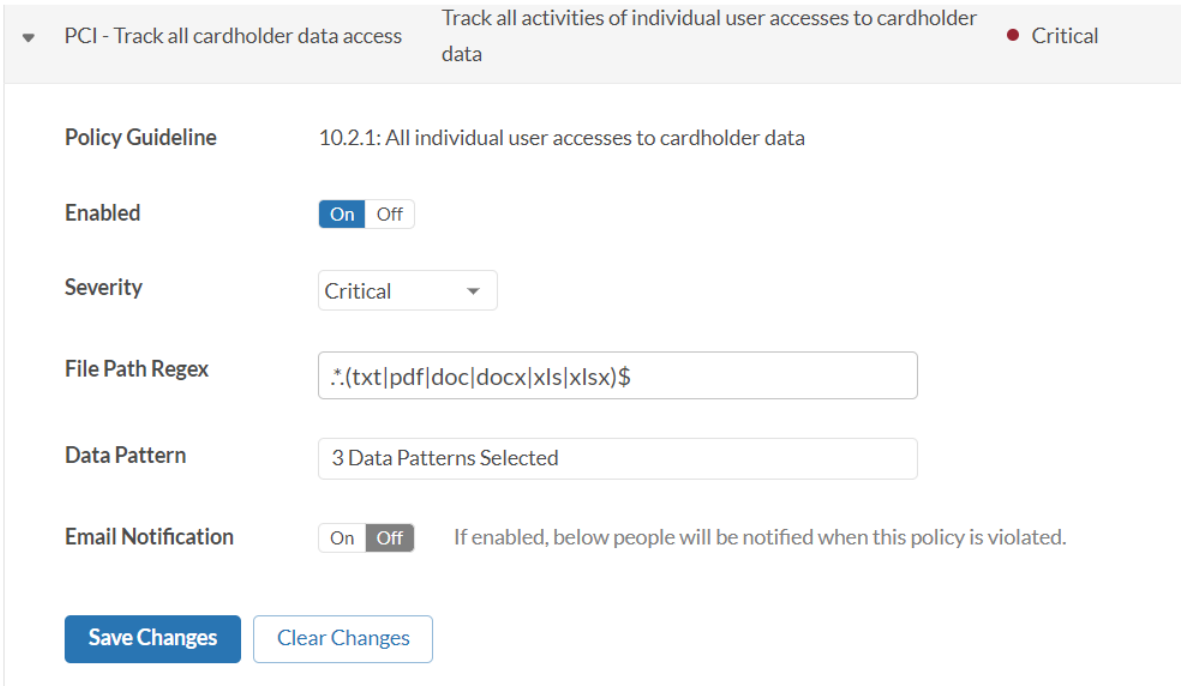
Search Queries	Regex
Specific Extension	.*.(txt|pdf|doc|docx|xls|xlsx)$
Folder	.*\/cucumber\/.*
File Name	.*ssn.*
All Path	.*

Example on using Regex search queries

PCI - Track all cardholder data access

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Go to **Policy > Compliance**, then select **PCI-DSS** tab.
3. Go to **PCI - Track all cardholder data access** and click **>** to expand the policy.
4. Click on **Enabled** toggle switch button to enable the policy.
5. Click on **Severity level** drop down menu to select the severity level (Critical, Alert, Warning, Information). **Note**: this policy generates both alert in **Alert** page and data in **Compliance Report**.
6. In **File Path Regex**, enter .*.(txt|pdf|doc|docx|xls|xlsx)$ to track all files with extensions in txt, pdf, doc, docx, xls, and xlsx.



7. In **Data Patterns**, click on the field and select **DLP SSN**, **DLP Visa Credit Card**, and **DLP JCB** to be monitored.
8. Click **Save Changes** to finish.

Now all files with extensions in txt, pdf, doc, docx, xls, and xlsx will look for the presences of Social Security, Visa Credit card, and JCB card numbers.

SOX-COBIT - Access to Sensitive Data

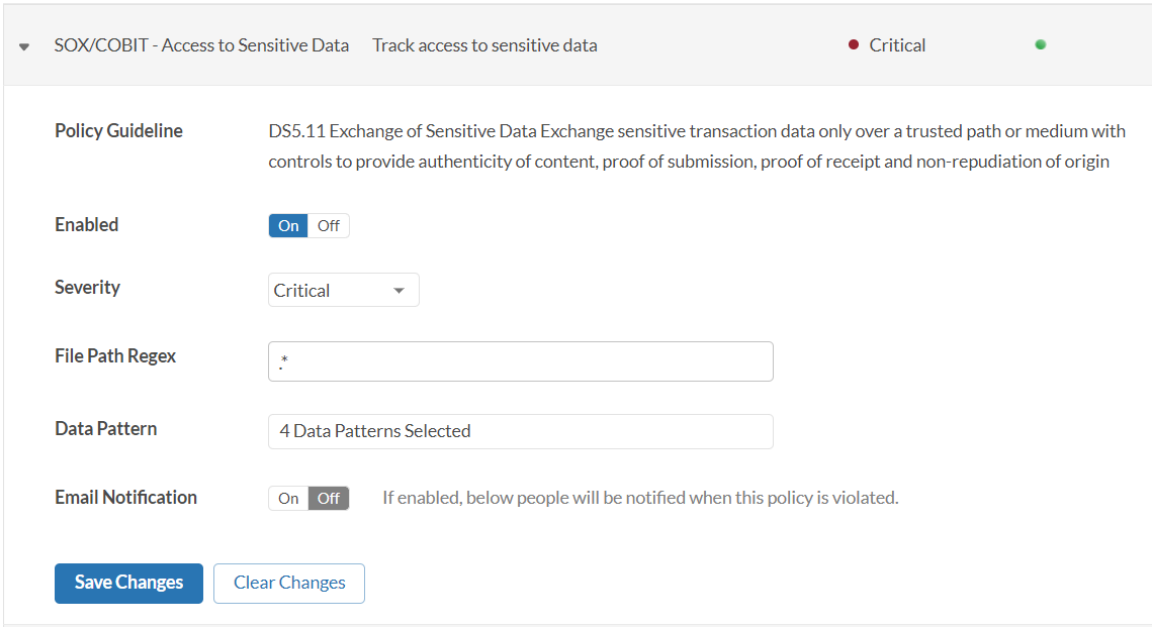
Description

Access to Sensitive Data policy monitors and tracks access to sensitive data located in the cloud account. Sensitive data location can be configured through file path Regex.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Go to **Policy > Compliance**, then select **SOX-COBIT** tab.
3. Expand **SOX/COBIT - Access to Sensitive Data** by clicking **>** button.
4. **Enable** the policy by clicking to toggle switch button.



5. Click on **Severity level** drop down menu to select a severity level (Critical, Alert, Warning, Information). **Note**: this policy generates both alert in **Alert** page and data in **Compliance Report**.
6. In **File Path Regex**, enter a valid Regex of the target file path to be monitored. Here are examples of file path Regex:
   a. ".*" targets all files in the cloud account.
   b. "^(?:[\w]\:|\\)(\\[a-z_\-\s0-9\.]+)+\.(txt|gif|pdf|doc|docx|xls|xlsx)$" targets files begin with x:\ or \\ with files ending in the following types of extensions: txt, gif, pdf, doc, docx, xls, xlsx. Here are the file paths that will this file path Regex matches:
      i. \\192.168.0.1\folder\file.pdf
      ii. c:\my folder\abc abc.docx

7. In **Data Patterns**, click on the field and select the data patterns (financial, personal identity information, etc.) to be monitored.
8. Click **Save Changes** to upgrade the configuration.

After the policy is enabled and configured, whenever any targeted sensitive file is accessed, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Compliance report will also record any alerts generated by this policy, for more details, please see Generate Compliance Report on page 281.

PCI - Failed Access Attempt Detection

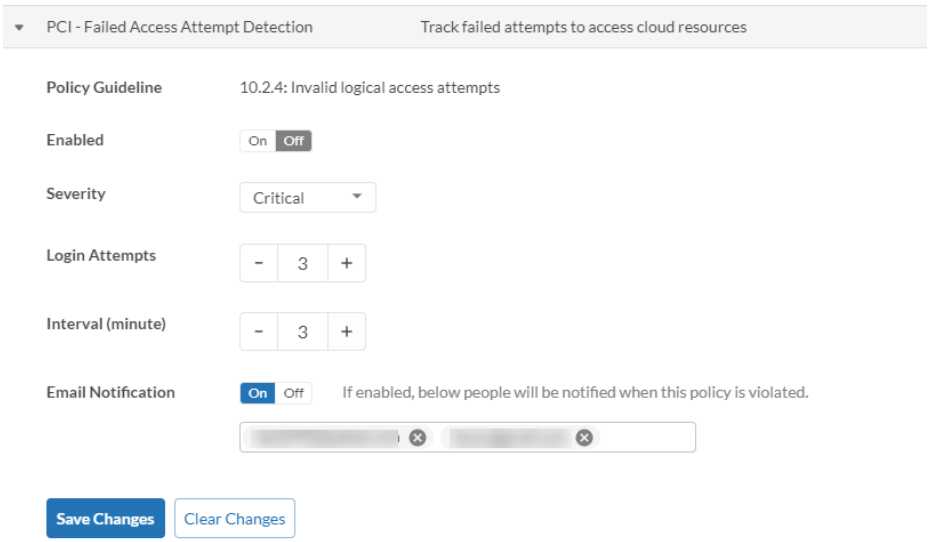
Description

Privileged Account Activity policy monitors and tracks targeted users' activities on the cloud accounts. The policy allows configuration on which user and what type of activities to be monitored.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Compliance**, then select **PCI-DSS** tab.
3. Locate **PCI - Failed Access Attempt Detection** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enabled the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
   Note: this policy generates both alert in **Alert** page and data in **Compliance Report**.
6. In **Login Attempts**, enter the threshold for the number of failed login attempts before an alert is generated.
7. In **Interval (minute)**, enter the time frame for all failed login attempts before an alert is generated.
   For example, given an interval of 3 minutes and login attempts of 5. If a user had more than 5 failed login attempts in 3 minutes, an alert will be sent to inform on the suspicious login attempts on the cloud account.
8. Click **Save Changes** to update the configuration.

After the policy is enabled and configured, whenever there are excessive failed login attempts on the cloud account, an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Compliance report will also record any alerts generated by this policy, for more details, please see Generate Compliance Report on page 281.

PCI - Privileged Account Activity

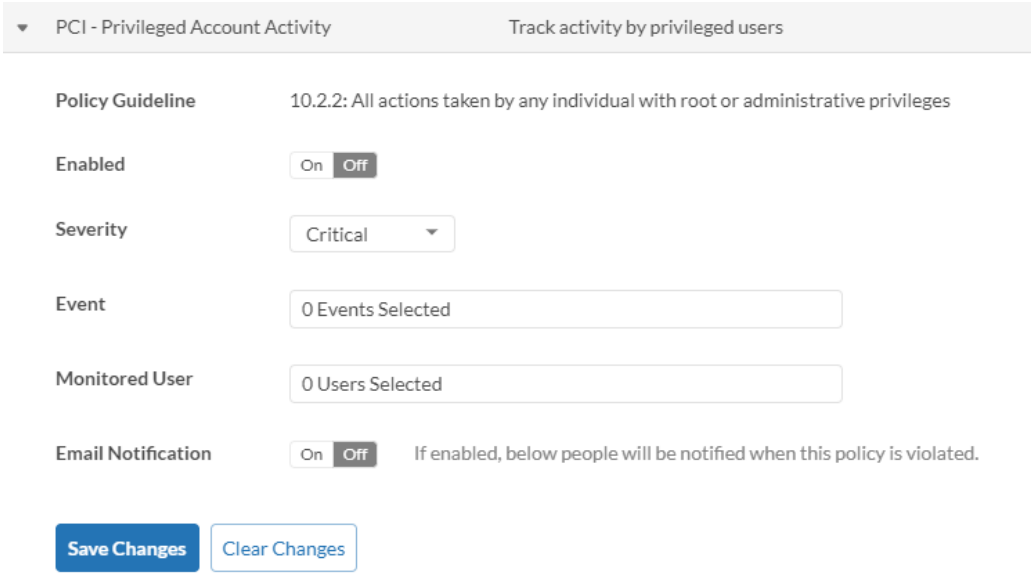
Description

Privileged Account Activity policy monitors and tracks targeted users' activities on the cloud accounts. The policy allows configuration on which user and what type of activities to be monitored.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Compliance**, then select **PCI-DSS** tab.
3. Locate **PCI - Privileged Account Activity** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enabled the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
   Note: this policy generates both alert in **Alert** page and data in **Compliance Report**.
6. In **Event** section, click to select specific event(s). To select all events instead, click on **Select all events**.
7. In **Monitored User** section, and select user(s) to be monitored. To select all users, click **Select all users**.
8. Click **Save Changes** to update the configurations.

After the policy is enabled and configured, whenever there is any specific activity conducted by targeted user(s), an alert will be triggered in the alert page. For more details, please refer to Alert on page 434.

Compliance report will also record any alerts generated by this policy, for more details, please see Generate Compliance Report on page 281.

PCI - Retention Violation for Cardholder Data

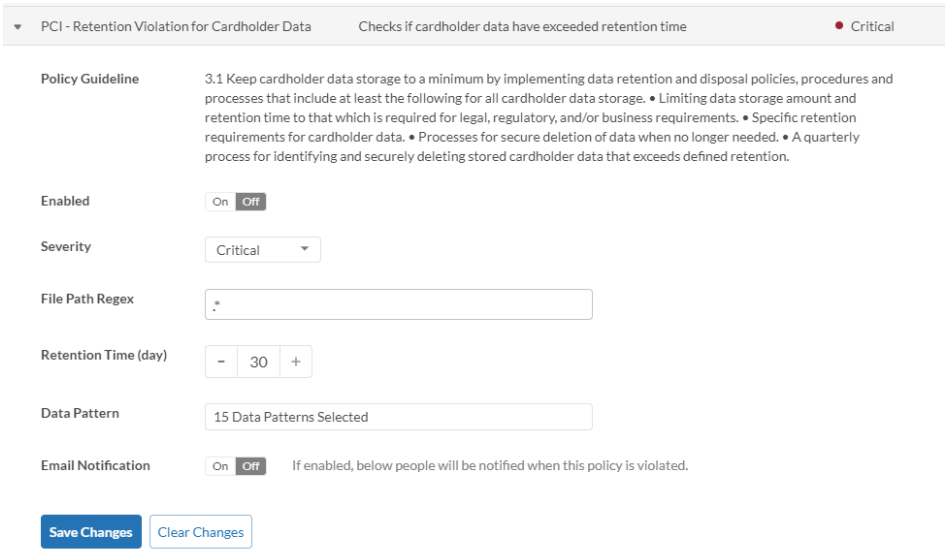
Description

Check if the designated cloud storage data has exceeded the retention time set by the cardholder. The cardholder is able to set the cloud storage file path with the designated retention time.

Policy Configuration

Follow the steps below to enable and configure the policy

1. Click on any Cloud Account drop down menu from FortiCASB dashboard, e.g. **Salesforce**, **Office365**, etc.
2. Click on **Policy** drop down menu and select **Compliance**, then select **PCI-DSS** tab.
3. Locate **PCI - Retention Violation for Cardholder Data** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enabled the policy.



5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
   Note: this policy only generates data in **Compliance Report**.
6. In **File Path Regex**, enter a valid Regex of the target file path for the storage data under the retention restriction. Here are examples of file path Regex:

a. ".*" targets all files in the cloud account.
b. "^(?:[\w]\:|\\)(\\[a-z_\-\s0-9\.]+)+\.(txt|gif|pdf|doc|docx|xls|xlsx)$" targets files begin with x:\ or \\ with files ending in the following types of extensions: txt, gif, pdf, doc, docx, xls, xlsx. Here are the file paths that will this file path Regex matches:
   i. \\192.168.0.1\folder\file.pdf
   ii. c:\my folder\abc abc.docx

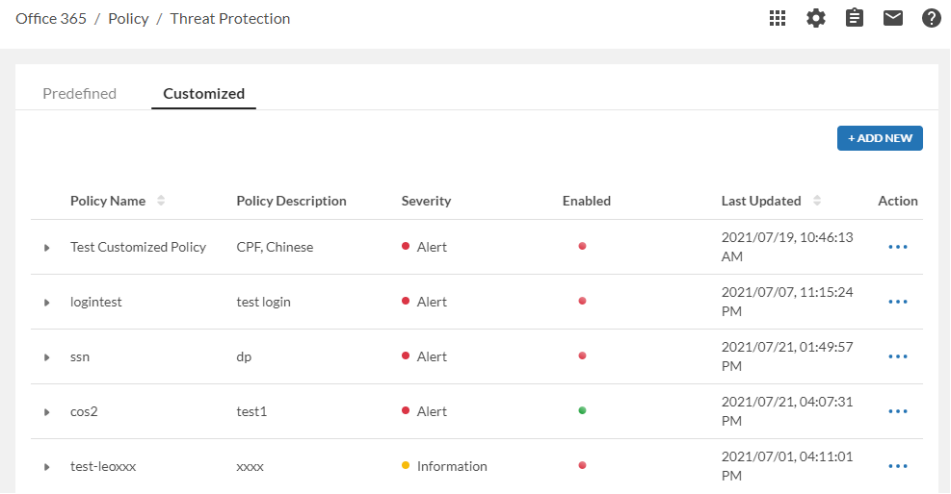
7. In **Retention Time (day)**, enter the number of days as the retention time for the cloud storage data.
8. In **Data Patterns**, click on the field and select the data patterns (financial, personal identity information, etc.) that shall be under the retention restriction.
9. Click **Save Changes** to upgrade the configuration.

After the policy is enabled and configured, when the targeted data exceeded the maximum retention time, Compliance report will record retention violation generated , for more details, please see Generate Compliance Report on page 281.

Customized Policy Configurations

FortiCASB allows you to create personalized policies to suit your organization needs.

To add a customized policy, select a cloud application, and go to **Threat Protection > Customized**, scroll to the bottom of the page and click **+ Add New**.



Customized policies focus on two aspects, **Content Monitoring** and **Activity Monitoring**.

Content monitoring: Content monitoring monitors and look for sensitive data in the cloud accounts.

Activity Monitoring: Activity monitoring monitors user activities for suspicions activities.

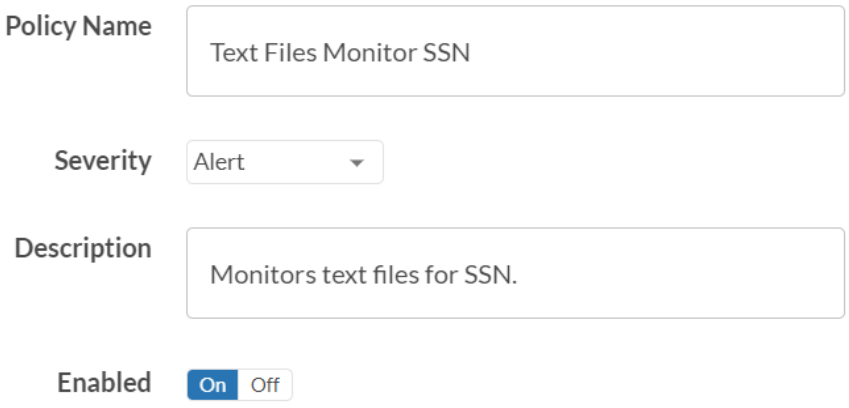
The following example illustrate how to create a common customized policies:

Customized Policy example: Monitor file download links with Social Security number on page 431

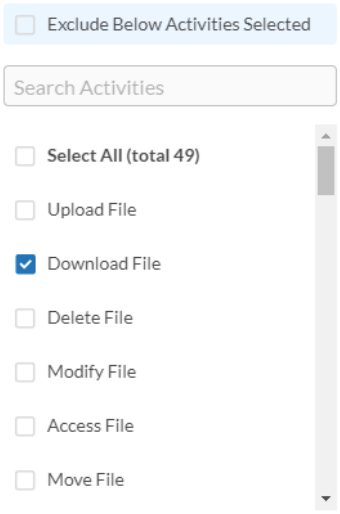
Customized Policy example: Monitor file download links with Social Security number

This example generates an alert when any Salesforce text file sharing link that contains a social security number is downloaded.

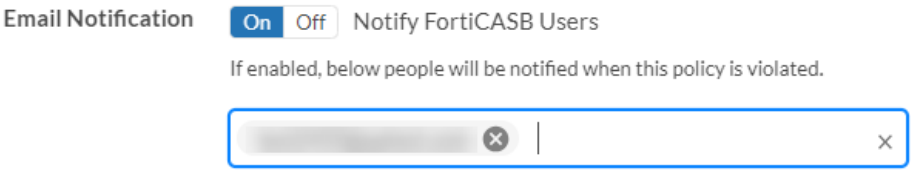
1. Enter a **Policy Name** and **Description** for the policy, e.g. "Text Files Monitors SSN".



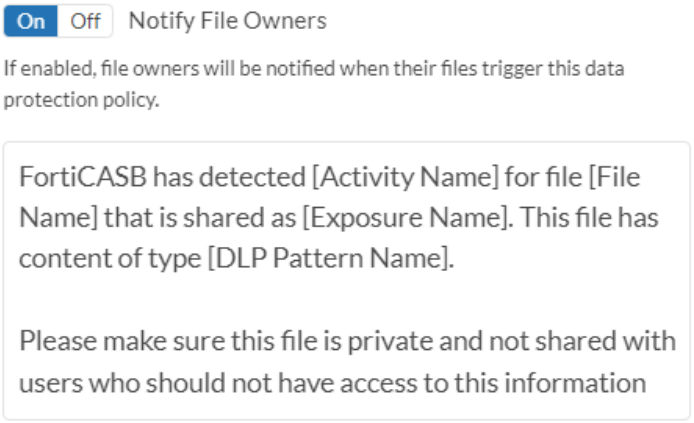
2. Click on **Activity** drop down menu, and select the **Download File** option.



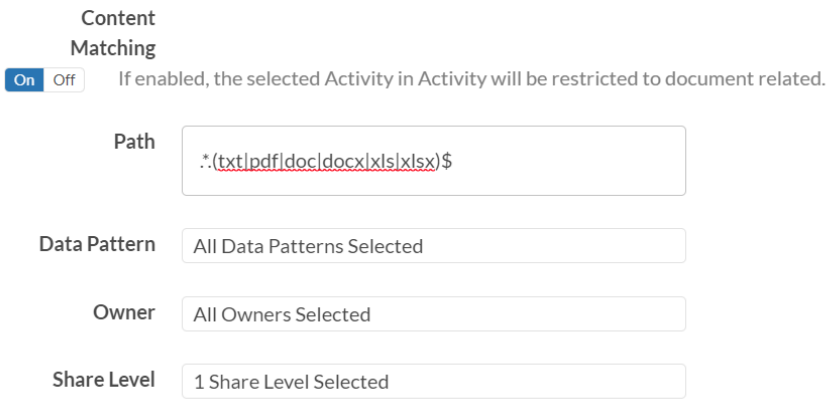
3. In Email Notification turn on to notify **FortiCASB users** and **File Owners**.
4. In Notify FortiCASB Users field, enter the FortiCASB user which the alert should be sent to.



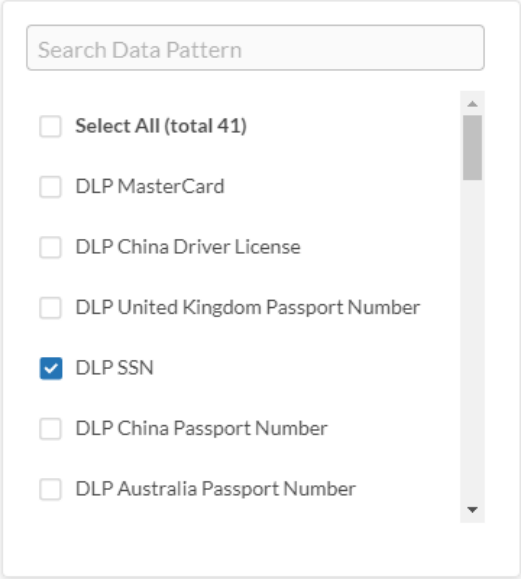
5. In Notify File Owners field, edit the alert content with the file name, activity name, and exposure name parameter.



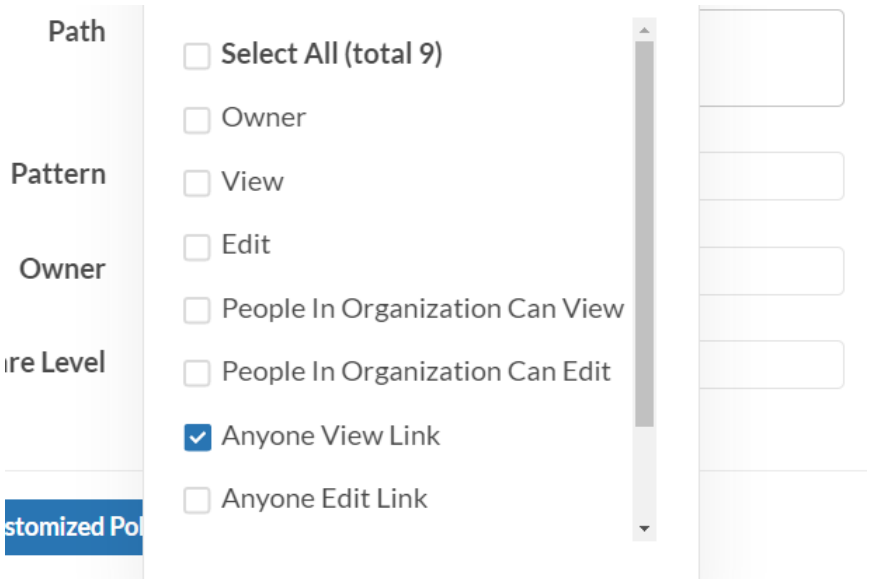
6. Turn on **Content Matching** to reveal **Data Patterns** selection.
7. In **Path** field, enter .*.(txt|pdf|doc|docx|xls|xlsx)$ to monitor all text files downloads.



8. Click on **Data Patterns** drop down menu, and select **DLP SSN**.



9. Click on **Share Level** drop down menu, and select **Anyone View Link**.



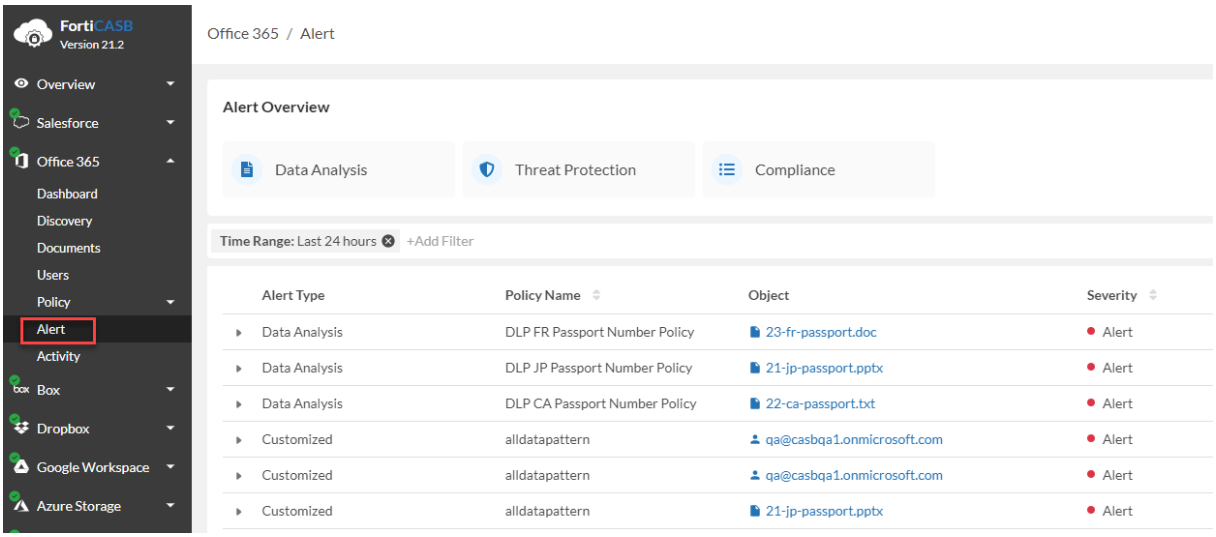
10. Click **Add Customized Policy** to finish adding the policy.

Alert

FortiCASB sends you alerts when any of the **enabled** policy is triggered by user activity.

- **Data Analysis** policies pertain to the types of data stored in the cloud application.
- **Threat protection** policies pertain to suspicious user activity.
- **Compliance** policies pertain to specific regulations, such as HIPAA, PCI, and SOX.

To view alerts of each cloud application, click on a cloud application drop down menu and click on **Alert**.



All alerts are triggered by user activities that violated the corresponding policies.

Click on the right arrow key ❯ of an alert to show alert summary.

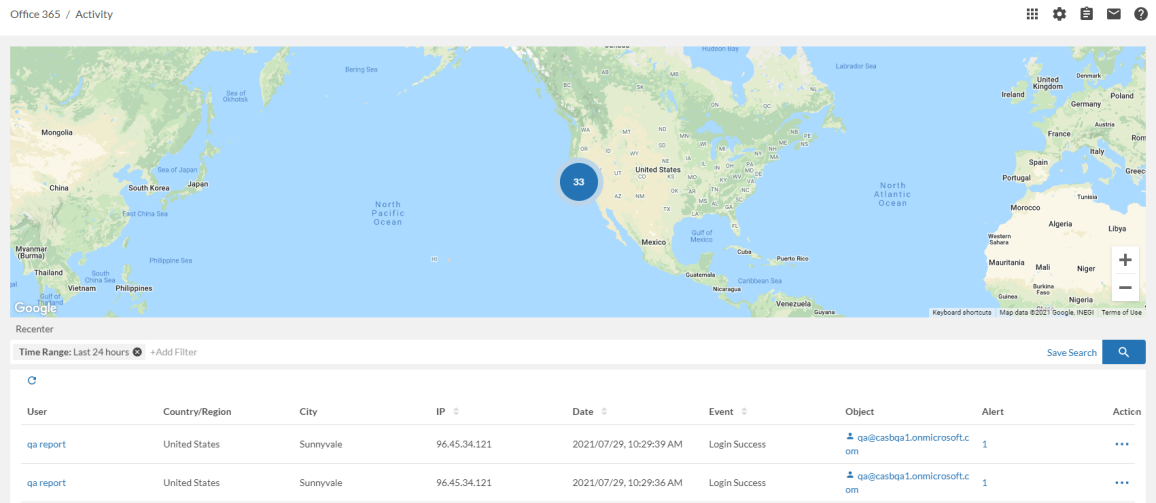
To enable a policy to trigger alert, please refer to Policy Configuration on page 405.

Daily alerts can be compiled into Alert reports for export, please see Generate Alert Report on page 284.

Activity

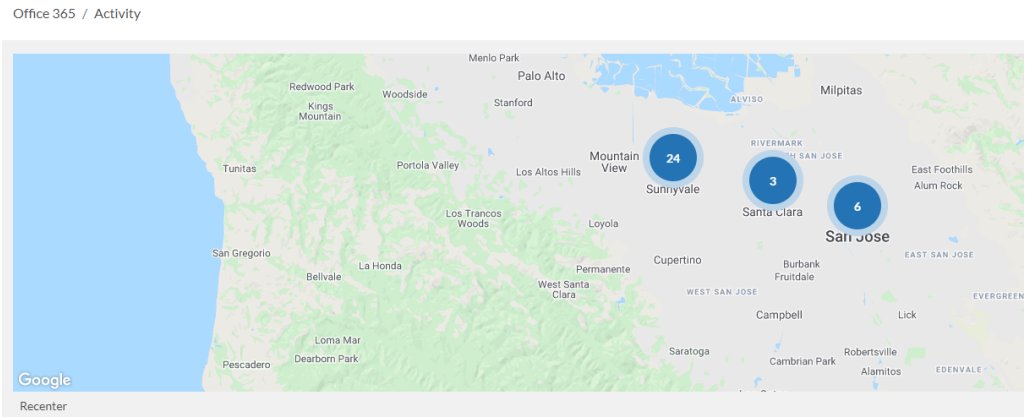
FortiCASB monitors and tracks user data traffic and activities on your cloud platforms.

The Activity page contains both a map displaying (approximate) geolocations of events and activities list.



Activity Map options

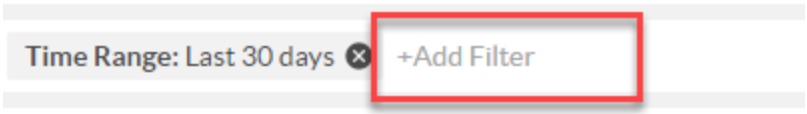
- **Activity**—Click on an activity bubble on the map to bring up an activities at that specific location.



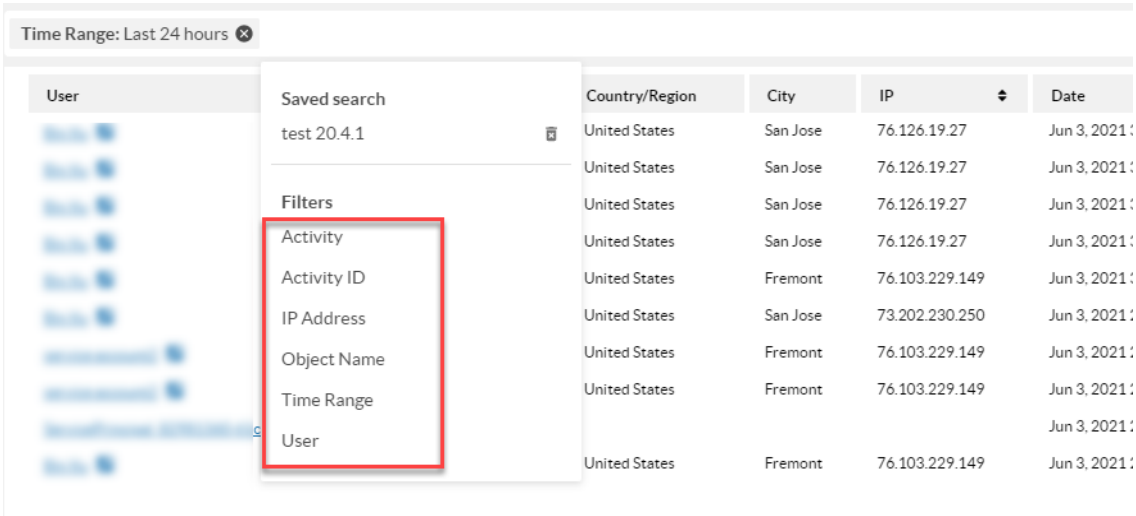
- **Move**—Move the map by clicking any point on the map and dragging with your mouse.
- **Zoom**—Use the buttons on the bottom-right corner of the map to zoom in and out.
- **Refresh**—Click the **Refresh** button to refresh the map.

Activity Filter Example

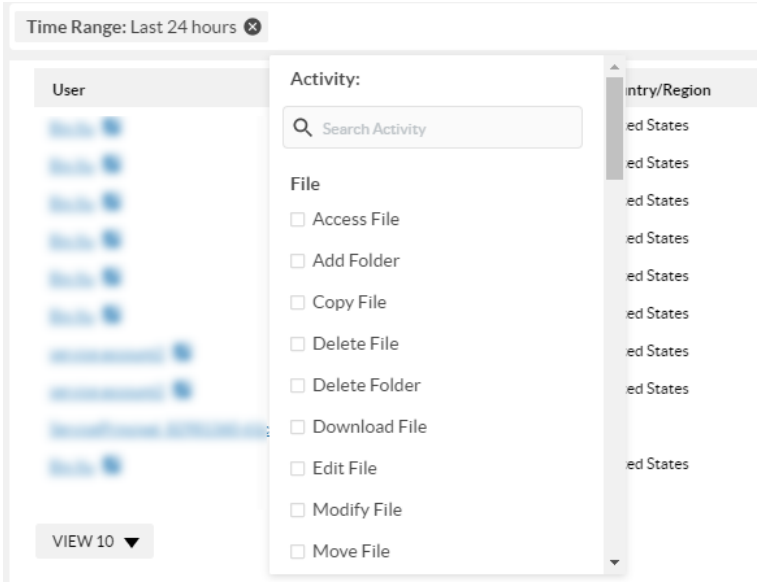
1. Click on **+Add Filter** drop down menu.



2. Select a filter type, "Activity".

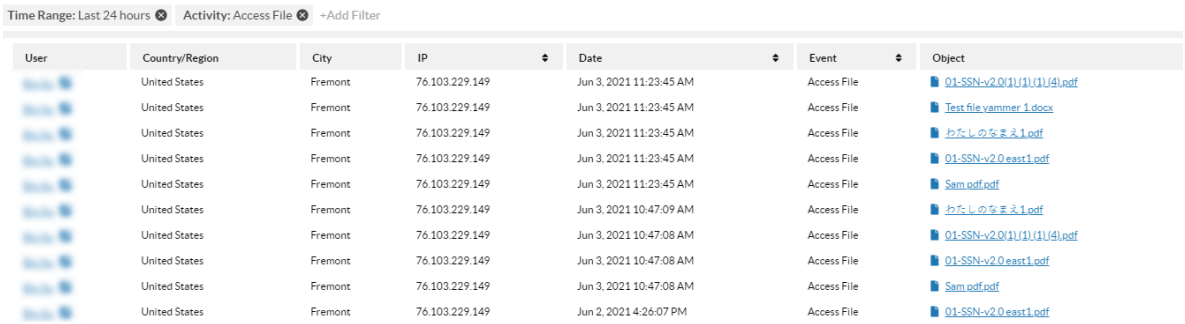


3. Then scroll down to select a type of activity, "Access File".



4. Then click Search button  to update the search with the filter, only "Access File" activities will be

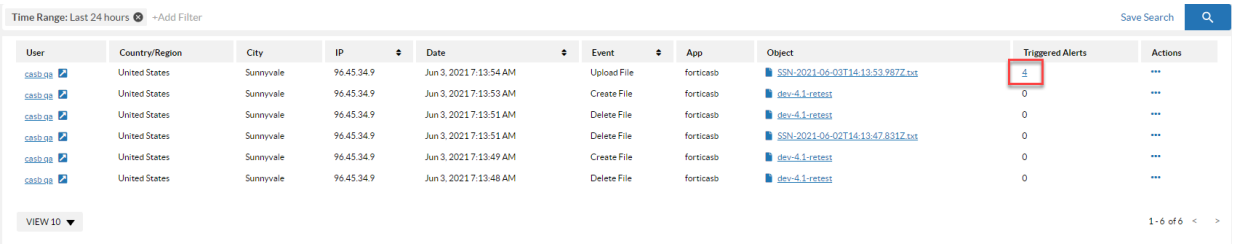
shown in the time range.



Activity Alert Correlation

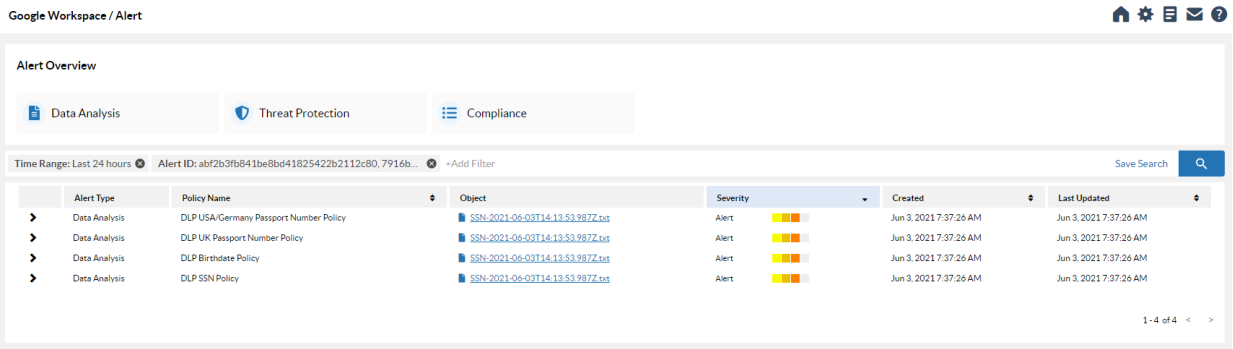
One activity may trigger multiple alerts, the multiple alerts are triggered by different policies.

For example, the Google Workspace event "Upload File" triggered 4 alerts, click on the alert button to see **Alert Overview**.



The **Alert Overview** page shows that this activity has triggered 4 different DLP policies:

DLP USA/Germany Passport Number Policy, DLP UK Passport Number Policy, DLP Birthday Policy, and DLP SSN Policy.

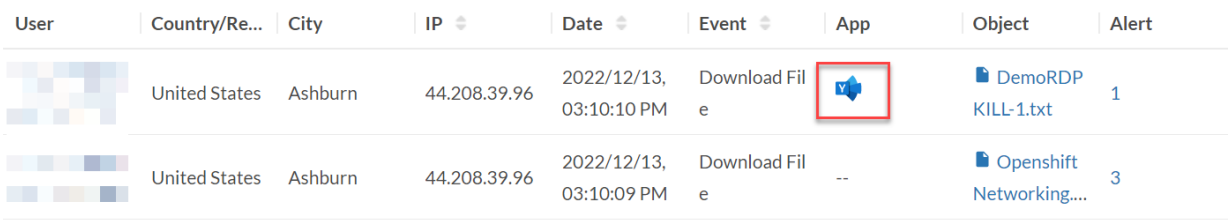


Daily cloud account activities will be compiled into Activity reports for export, please see Generate Activity Report on page 287.

Microsoft App Integration (Office 365 Accounts Only)

Microsoft App integration shows the location of the files on **Microsoft Yammer** or **Microsoft Teams** Apps.

Go to **Office 365 > Activity**, the **App** Column shows the documents currently located in **Microsoft Yammer** or **Microsoft Teams** App.

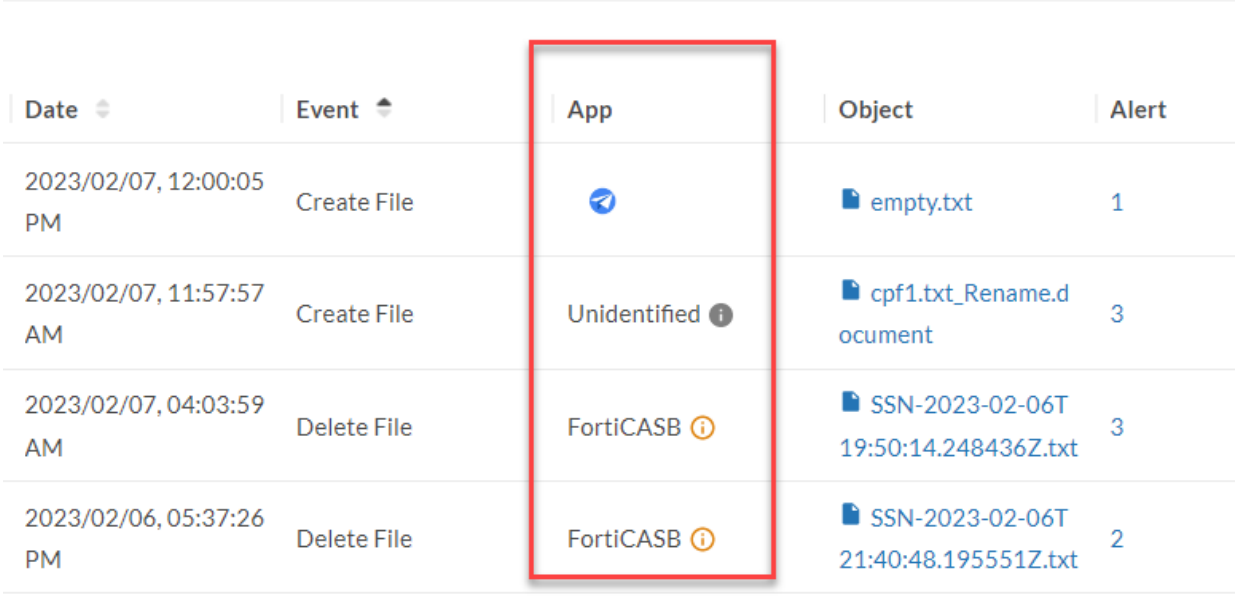


User	Country/Re...	City	IP	Date	Event	App	Object	Alert
[redacted]	United States	Ashburn	44.208.39.96	2022/12/13, 03:10:10 PM	Download File		DemoRDP KILL-1.txt	1
[redacted]	United States	Ashburn	44.208.39.96	2022/12/13, 03:10:09 PM	Download File	--	Openshift Networking....	3

Microsoft App	App Logo
Microsoft Yammer	
Microsoft Teams	

Google Third-Party App Verification (Google Workspace Accounts Only)

The third-party apps under Google Workspace are reviewed by Google to ensure compliance with Google's security and privacy requirements. The third-party apps that are not verified by Google are subject to restrictions. The **App** column in Activity reflects the Google verification status of the third-party apps.



Date	Event	App	Object	Alert
2023/02/07, 12:00:05 PM	Create File		empty.txt	1
2023/02/07, 11:57:57 AM	Create File	Unidentified	cpf1.txt_Rename.document	3
2023/02/07, 04:03:59 AM	Delete File	FortiCASB	SSN-2023-02-06T19:50:14.248436Z.txt	3
2023/02/06, 05:37:26 PM	Delete File	FortiCASB	SSN-2023-02-06T21:40:48.195551Z.txt	2

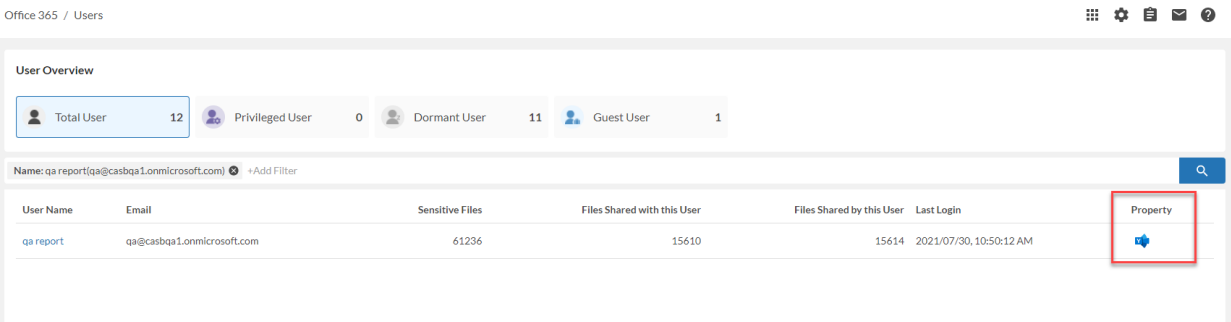
Google Third-Party App Verification Status and Description

Third-Party App Status	Description
(App Name)	The third-party app has **Not** gone through Google verification process.
Unidentified	The third-party app can be one of the following Apps: **Google Docs**, **Google Sheets**, **Google Slides**, **Google Forms**, **Google Drawing**, etc.
App name (icon) with no status	The third-party app is verified by Google.

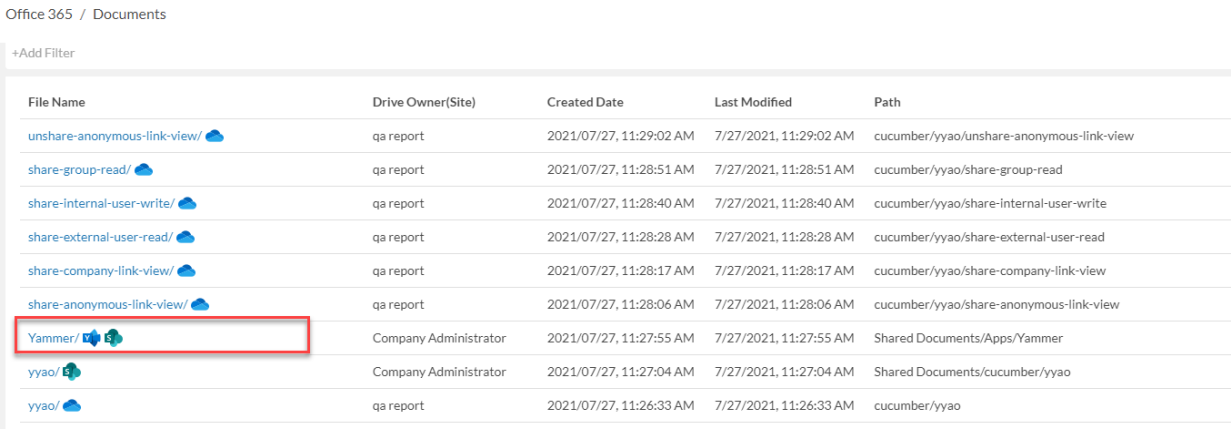
Yammer Integration

FortiCASB Yammer integration allows you to monitor and inspect all the files posted on Yammer by users within your organization. All users within your organization that is also a Yammer user, will show as "Yammer Licensed" on FortiCASB.

From FortiCASB control panel, go to **Office 365 > Users** to see the FortiCASB users that are also on Yammer, notice that all Yammer user will have the Yammer icon under **Property**.



All Yammer uploaded files by the Yammer Licensed user are able to be viewed in FortiCASB Office 365 Documents. All Yammer files can be distinguished through **File Name** column with icon in **Office 365 > Documents** in FortiCASB.



When clicking on a Yammer uploaded file name, you can view detailed file information such as creator, created date, last modified, date, file path, and etc.

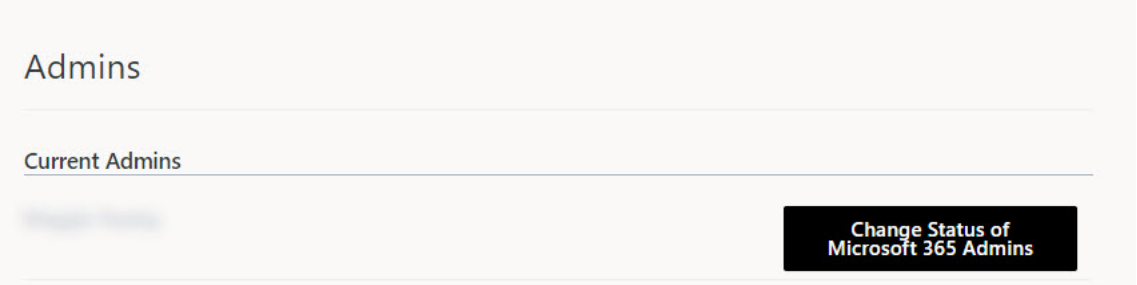
Prerequisites

Yammer integration in FortiCASB requires enforcing Office 365 identity in Yammer. When turning this setting on, it may disrupt Yammer users' access to Yammer, especially those who do not have Office 365 account, they will be locked out of Yammer. Therefore, before making this change, please inform your Yammer users to do the following:

- Make sure that all Yammer users have Azure AD account. You can figure out who does not have an Azure AD account by comparing the list of users on Yammer with the list of users in Office 365. From Yammer, go to **Settings > Edit Network Settings > Export Users** to export all users.
- Help the Yammer users who do not have Azure AD account to get Azure AD account before enforcing Office 365 identity.

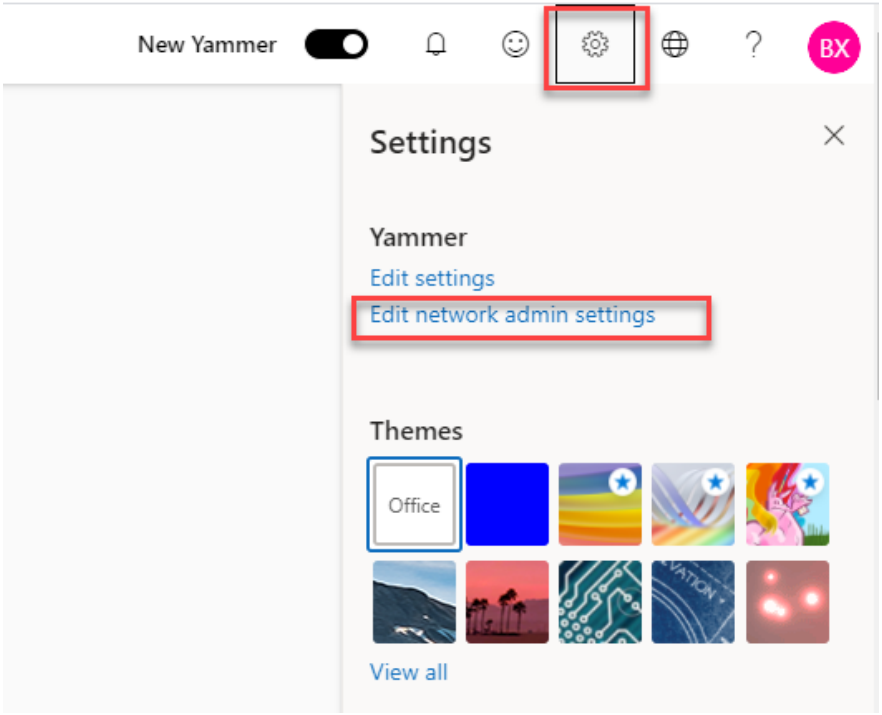
You need to be a **global administrator** on Office 365 and be synchronized to Yammer as verified administrator to enforce Office 365 identity in Yammer.

From your Yammer account, go to **Settings > Edit Network Settings > Admins** to verify your Yammer admin account is synchronized to Office 365 global administrator account. Below is a screen shot of a synced admin in Yammer:

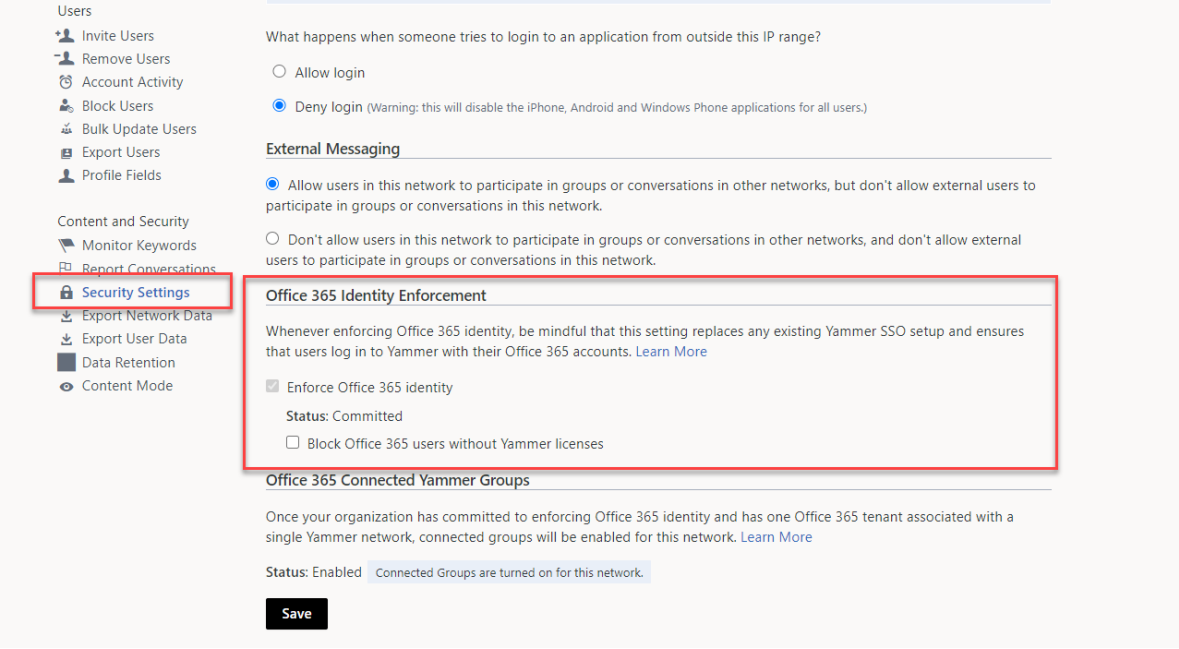


Enforce Office 365 Identity in Yammer

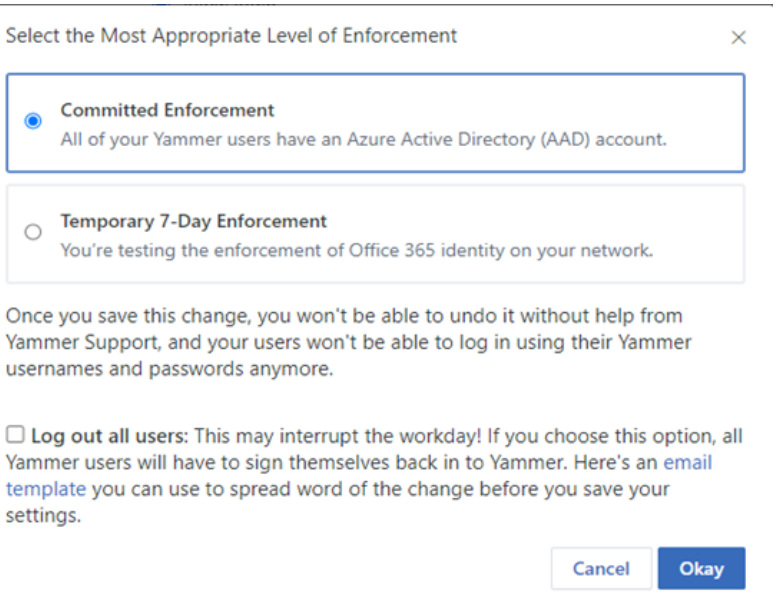
1. Log into Yammer with your Yammer admin account.
2. If you are using the new Yammer, go to **Settings > Edit Network Admin Settings** in the upper right hand side.



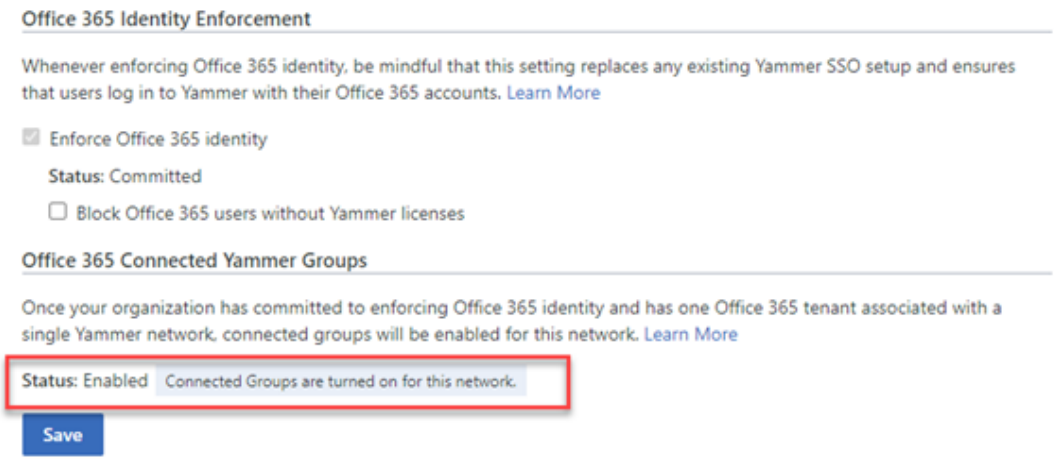
   If you are using the old Yammer, go to **Settings > Network Admin** at the upper left hand side.
3. Click **Security Settings** under **Content and Security**.
4. Scroll down to **Office 365 Identity Enforcement**, click on **Enforce Office 365 identity** checkbox.



5. A confirmation message will ask you to select the appropriate level of enforcement.



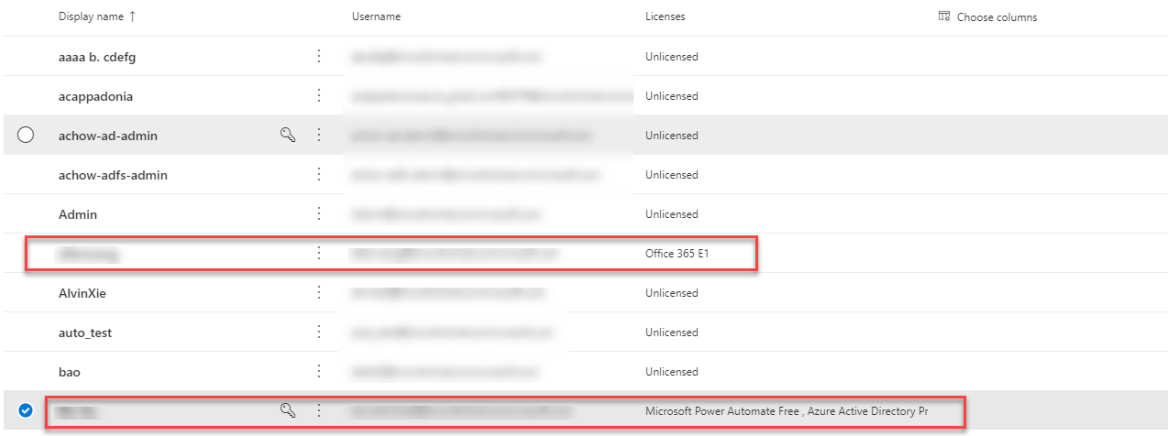
6. Select **Committed Enforcement** and press **okay**.
   Note: Once you made this change, you will not be able to undo it, your users will not be able to log in with their Yammer user accounts anymore, only Yammer users with Azure Active Directory accounts will be able to log in to Yammer moving forward.
7. Click **Save** to save your settings.
8. Go back to **Security Settings** after at least 15 minutes, and check the status under **Office 365 Connected Yammer Groups**, it should be **enabled**.



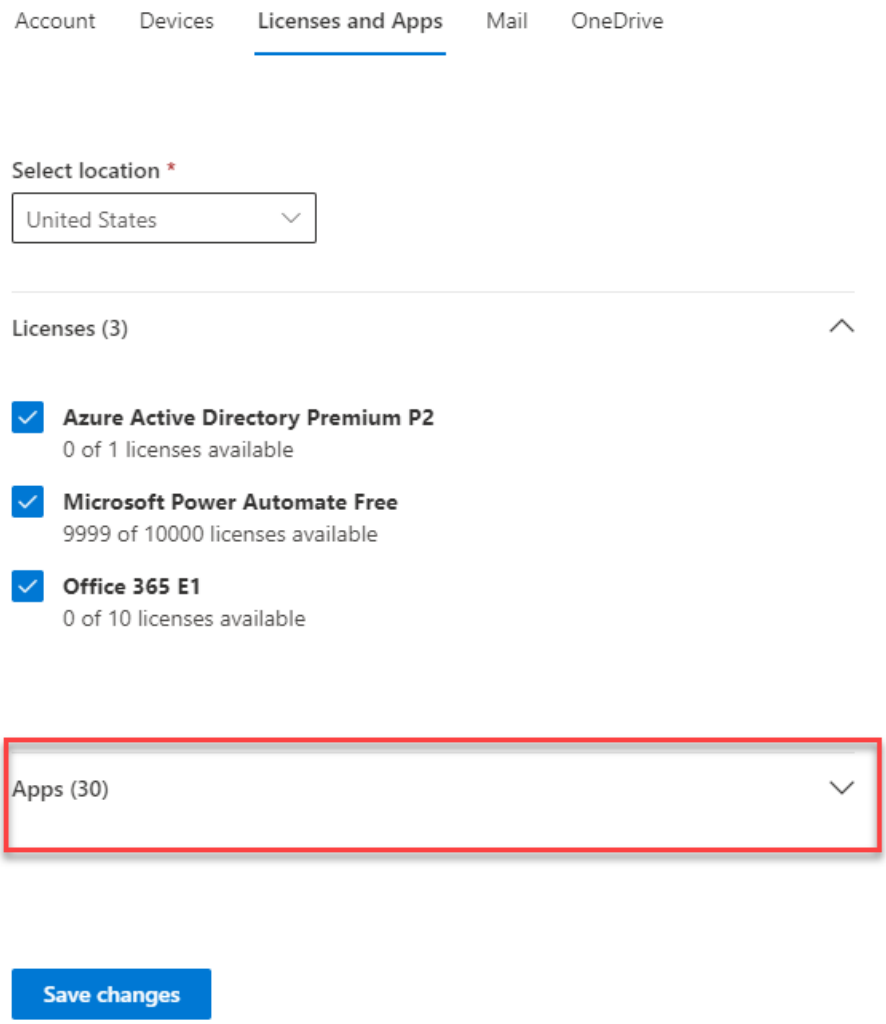
Yammer License Verification

After enforcing Office 365 identity on all Yammer users, you can verify the Yammer user has integrated into FortiCASB through Microsoft Office Administrator. You must be the Office 365 global administrator in order to verify the user license info. Follow these steps to verify the user credentials:

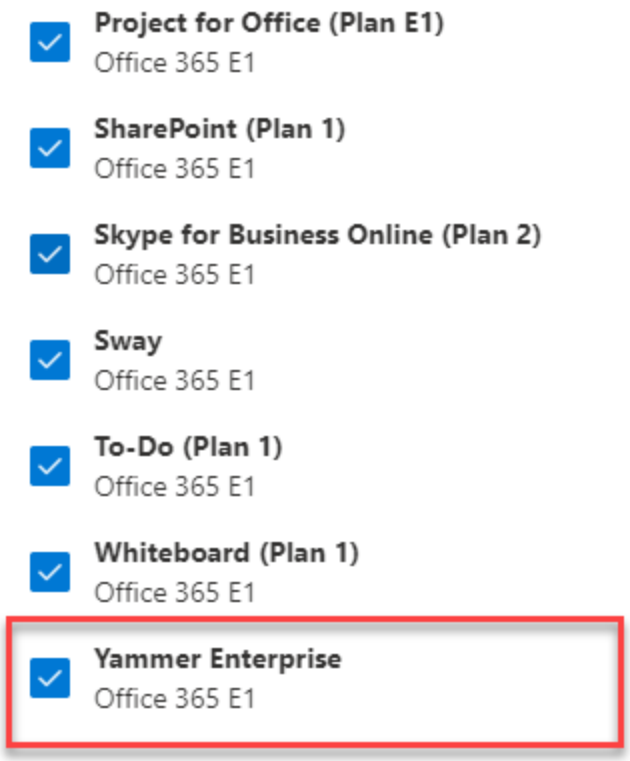
1. Log into **Office 365** (https://www.office.com/) as the global administrator.
2. Click on **Admin** to access **Microsoft 365 admin center**.
3. On the left control panel, expand **Users** and select **Active Users**.
4. Click on any licensed user, and the user profile will pop up.



5. In the user profile, Select **Licenses and Apps** tab, and expand **Apps** section.



6. Scroll all the way down, and you will see **Yammer Enterprise** checkbox. The user needs to have **Yammer Enterprise** checked in order to be integrated with FortiCASB.

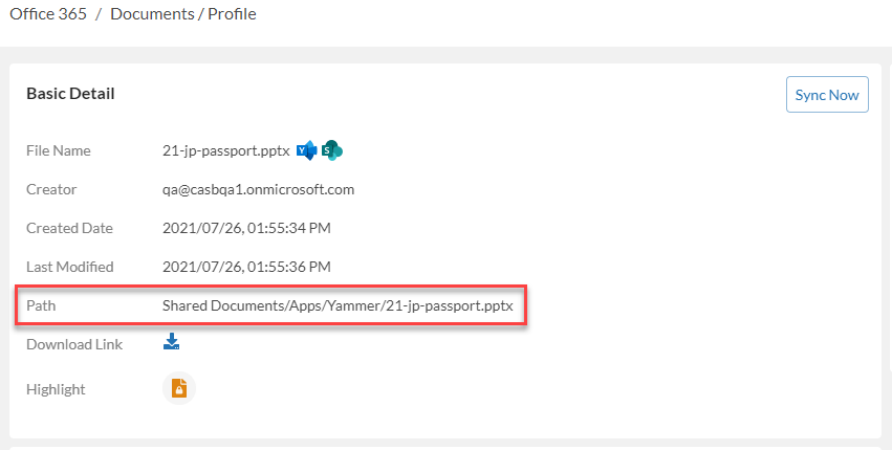


7. Repeat step **4-6** on all Yammer users.

Yammer File Path

After Office 365 identity is enforced in Yammer, all files uploaded to Yammer will be relocated to the folder **Shared Document/Apps/Yammer/** in the user SharePoint. FortiCASB will retrieve all the files metadata

through this file path on SharePoint. Therefore, please keep this file path without changing it to let FortiCASB obtain file metadata in Yammer. This is the Yammer file path shown in FortiCASB.



FortiCASB APIs

FortiCASB service endpoints supports HTTP requests through the use of REST APIs. This section contains documentation for FortiCASB REST API service endpoints. FortiCASB provides one endpoint with single authentication token to simplify developer experience. All the service endpoints can be accessed through a single access/bearer token. The HTTP requests provide access to valuable FortiCASB cloud resources. All FortiCASB REST APIs, such as Get, POST, etc. require access/bearer token in assembling HTTPS requests.

Request Authorization Methods

There are 3 methods of acquiring the access/bearer token from FortiCASB to assemble a REST API request to access FortiCASB resources.

1. Client Credential

Client credential can be used to generate access/bearer token to form request headers. First, you will need to log into FortiCASB and generate a FortiCASB credential, please follow the guide in Generate API Credential on page 41. This is only a one-time process, and only one credential is necessary to generate access/bearer token.

After you have acquired a client credential, it can be used permanently to assemble the request header to obtain an access/bearer token as long as the client credential is not revoked.

Follow the example in Get Credentials Token on page 453 to use client credential to assemble HTTPS POST request header to acquire access/bearer token.

2. Username and Password

Another method of acquiring access/bearer token is through your FortiCASB account username and password. Follow the example in Get Authorization Token on page 451 to assemble HTTPS POST request header to acquire access/bearer token using your username and password.

3. Refresh Token

The use of refresh token requires one of the two methods above. Once you get the response through client credential or username/password, you may use the refresh token in the response body to acquire more bearer tokens without using client credential or user/name password. Follow the example in Post Refresh Token on page 454 to generate access/bearer token using refresh token. The refresh token will expire 8 hours after generated.

Fabricate Request Header and Body

After acquiring access/bearer token, use the bearer token to assemble a REST API request. Like all other REST APIT requests, FortiCASB operate through a secured channel: URI request with HTTPS protocol. The details of the request parameters are determined by the specific REST API specification.

You may take a closer look in each REST API specification to determine what additional fields are necessary to fulfill the request. Request body is an optional field, depending on the API specification, some parameters may be required and others are optional.

Send Request

There are 5 request headers that are often used in FortiCASB REST API requests. The first 3 are default request headers.

Request Header	Description
Host	The domain name of the REST service endpoint or the IP address
Authorization	Access/bearer token generated earlier through one of the get token methods
Content-Type	This default header is set as "application/json"
Company ID	The company ID of the company which the username or the credential is originated from. Company ID can be obtained from Get Resource Map on page 456.
Role ID	Role ID is the login user ID, can be obtained through Get Resource Map on page 456.
Business Unit ID	Business unit ID is the ID of the business unit which the user is entitled to access. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456

When you have assembled the request header and body, the request is ready to be sent to the REST endpoint. Here is a GET request example in HTTPS:

```
GET /api/v1/country/list? HTTP/1.1
Host: www.forticasb.com
Authorization: Bearer
     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzY29wZSI6IkFQSSIsImlzcyI6ImZhdXRoLXNlcnZlc
     iIsImhvc3QiOlsiRkNXUCJdLCJleHAiOjE1ODY5MTUxNjQsImFpZCI6InFhLmNhc2IxQGdtYWlsLmNvbSJ
     9.Hh2yVHEEd73BJ31rEjB2C-iclodmMigEPIwtuRwCObo
Content-Type: application/json
```

REST API Response

After you sent the request to FortiCASB service endpoint, you will receive a response header and a response body. The above request calls for the list of countries, and here is a part of the response in JSON format:

```
[
   {
      "id":"US",
      "country":"United States of America"
   }
]
```

API Throttling

API throttling refers to the limit that FortiCASB sets on the number of requests in a range of time to prevent the application sending too many requests. The API throttling of FortiCASB is 100TPM (times per minute), meaning there can have 100 requests in one minute.

Get Authorization Token

Description

Get FortiCASB access token by the FortiCASB username and password.

URL

/api/v1/auth/token

Method: POST

Request Header

Key	Value	Type	Description
Content-Type	application/x-www-form-urlencoded	String	

Request Body Parameters

Name	Required	Value	Description
grant_type	Required	password	
username	Required	<username>	FortiCASB account user name
password	Required	<password>	FortiCASB account password

Sample Request

Request URL	`POST https://www.forticasb.com/api/v1/auth/token`
Request Header	`Content-Type: application/x-www-form-urlencoded`

Request Body	`grant_type: password`
	`username: XXXXXXXXXX`
	`password: XXXXXXXXXX`

Response Variables

Name	Type	Description
access_token	String	Access token returned
refresh_token	String	Refresh token returned
token_type	String	Type of token
expires	String	Timestamp of when the token will expire

Sample Response

```
{
   "token_type": "bearer",
   "expires": 1.585002117836E12,
   "access_token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzY29wZSI6IkFQSSIsImlzcyI6ImZhdXRoLXNlc
        nZlciIsImhvc3QiOlsiRkNXUCJdLCJleHAiOjE1ODUwMDIxMTcsImFpZCI6InFhLmNhc2IxQGdtYWls
        LmNvbSJ9.TFfhF3jRDnoj1W96gFOuMnxvAhdwU55IQdO6tpkOpH0",
   "refresh_token": "I4WnuRUY0xHEsoNMDvmurq_
        J45VHyuxa4DRWq5mevlYB1YT1yL2TUAA8vRRNNyOyy5RwEww62j0cAM8yxa4B5kU8GbTrty2kgSD7nf
        bmYEaPNQIBIi5Mv7jq0fHkn0Z-5z43CwI5yWF3pfGygvYoqaL0_YC5np5AKSPP3S49KhA"
}
```

Get Credentials Token

Description

Get the FortiCASB OAuth 2.0 bearer token by the credentials generated on FortiCASB. Before using this API, first generate a credential on FortiCASB through Generate API Credential on page 41.

URL

/api/v1/auth/credentials/token/

Method: POST

Request Headers

Key	Value	Type	Description
Authorization	Basic <FortiCASB credentials>	String	Authorization credential generated by FortiCASB
Content-Type	application/x-www-form-urlencoded	String	

Request Body Parameters

Name	Required	Value	Description
grant_type	Required	client_credentials	

Sample Request

Request URL	`POST https://www.forticasb.com/api/v1/auth/credentials/token/`
Request Header	`Authorization: Basic a0eddbf4-6840-4bb7-9789-acffd4ffac02` `Content-Type: application/x-www-form-urlencoded`
Request Body	`grant_type=client_credentials`

Response Variables

Name	Type	Description
access_token	String	Access token returned
refresh_token	String	Refresh token returned

Name	Type	Description
token_type	String	Type of token
expires	String	Timestamp of when the token will expire

Sample Response


```
{
   "token_type": "bearer",
   "expires": 1.585248581336E12,
   "access_token":
         "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzY29wZSI6IkFQSSIsImlzcyI6ImZhdXRoLXNlc
         nZlciIsImhvc3QiOlsiRkNBU0IiXSwiZXhwIjoxNTg1MjQ4NTgxLCJhaWQiOiJxYS5jYXNiMUBnbWFp
         bC5jb20ifQ.PVfdrQ7NJYdYTu0PmIQnNUJJTWq3ZmW-iw2ux_8LLCM",
   "refresh_token": "I4WnuRUY0xHEsoNMDvmuronKCCut-
         9FKHZOT4Pfuancwh46UUz5irXDK98bRmDKREdg05VQmjbN8zrcvsyatl9DvuuSOBfhQ4Kztmwu5Vrho
         Ml3tpq1U_feWjs866PcMix9BUO2DYRzLXWucyjiyyT7uHZMwakKhps9vbWm9gzq3XpCej-
         yeX7ze0TNrWSG3WLh5n5sydU5NMNI_Stt-WycO05ZQL4FvRmqjn1-8Hz0"
}
```


Post Refresh Token

Description

Get refresh token uses the short-lived refresh token from past access token requests (**Get Authorization Token** or **Get Credentials Token**) without having to use credentials or username/password.

URL

/api/v1/auth/token/refresh

Method: POST

Request Header

Key	Value	Type	Description
Content-Type	application/x-www-form-urlencoded	String	

Request Body Parameters

Name	Required	Value	Description
grant_type	Required	refresh_token	
refresh_token	Required	<Refresh Token>	Refresh token generated from the past Get Authorization Token and Get Credentials Token request responses.

Sample Request

Request URL	`POST https://www.forticasb.com/api/v1/auth/token/refresh`
Request Header	`Content-Type: application/x-www-form-urlencoded`
Request Body	`grant_type: refresh_token` `refresh_token: 2j0cAM8yxa4B5kU8GbTrty2kgSD7nfbmYEaPNQ`

Response Variables

Name	Type	Description
access_token	String	Access token returned
token_type	String	Type of token
expires	String	Timestamp of when the token will expire

Sample Response

```
{
   "token_type": "bearer",
   "expires": 1.585002361532E12,
   "access_token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzY29wZSI6IkFQSSIsImlzcyI6ImZhdXRoLXNlc
```

```
        nZlciIsImhvc3QiOlsiRkNXUCJdLCJleHAiOjE1ODUwMDIzNjEsImFpZCI6InFhLmNhc2IxQGdtYWls
        LmNvbSJ9.Y7RGkrRn6hvfqCbPF9LGNchYGMiEIK2WljPqSbffsk0"
}
```

Get Resource Map

Description

Get the user and account basic information from FortiCASB, including the company ID, role ID, user name, bushiness unit IDs, etc.

Company ID (**companyID**), role ID (**roleId**), and business unit ID (**buId**) are the response variables that you will need to call many other FortiCASB REST APIs.

URL

/api/v1/resourceURLMap

Method: GET

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/resourceURLMap**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json

Response Variables

Name	Type	Description
resourceURL	String	API request endpoint
roleId	Long	Login user identity

Name	Type	Description
username	String	Login user name
buMapSet.companyId	Long	Company ID (**companyId**) of which the business unit is under.
buMapSet.buId	Long	Business unit ID (**buId**) of which the user account is under.
buMapSet.buName	String	Business unit name

Sample Response


```
[
   {
      "resourceURL":"https://qa1.staging.forticasb.com",
      "roleId":1,
      "username":"casb qacasb1",
      "buMapSet":[
         {
            "buName":"research authentication",
            "companyId":6,
            "buId":238187
         },
         {
            "buName":"aaa",
            "companyId":6,
            "buId":6384
         }
      ]
   }
]
```


Post Alert List

Description

Get cloud service account alert details.

URL

/api/v1/alert/list

Request Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456

Request Body Parameters

Name	Required	Type	Description
service	<Cloud Service>	String	Cloud service name such as Salesforce,Office365, etc.
startTime	Required	long	Timestamp, filter to get open alert time after start date
endTime	Required	long	Timestamp, filter to get open alert time before start date
skip	Required	integer	Indexes in a result set. Used to exclude response from the first N items of a resource collection.
limit	Required	integer	Maximum number of return items
user	Optional	List<String>	Filter to search user email
policy	Optional	List<String>	Filter to search alert id

Name	Required	Type	Description
activity	Optional	List<String>	Filter to search alert by activities
objectIdList	Optional	List<String>	Filter to search alert by object identity
objectName	Optional	String	Filter to search alert by object name
severity	Optional	List<String>	Filter to search alert by severity
status	Optional	List<String>	Filter to search by status
idList	Optional	List<String>	Filter to search alert by alert IDs
alertType	Optional	List<String>	Filter to search alert by alert types
countryList	Optional	List<String>	Filter to search alert by countries
asc	Optional	String	Sort and display all alerts by ascending order. The optional string parameters provide sort options: "**policyName**": sort by the policy names that triggered the alert. "**severity**": sort by the severity levels of the alert. "**createTimestamp**": sort by the alert creation time. "**timestamp**": sort by the last updated alerts.
desc	Optional	String	Sort and display all alerts by descending order. The optional string parameters provide sort options: "**policyName**": sort by the policy names that triggered the alert. "**severity**": sort by the severity levels of the alert. "**createTimestamp**": sort by the alert creation time. "**timestamp**": sort by the last updated alerts.

Sample Request

Request URL	`POST https://www.forticasb.com/api/v1/alert/list`

Request Header	`Authorization: Bearer <Authorization_Token>`
	`Content-Type: application/json`
	`buid: 6384`
	`service: Salesforce`
	`roleId:36241`
	`companyId: 62598`

Request Body


```
{
   "service":"Salesforce",
   "startTime":1583792777000,
   "endTime":1583879177000,
   "id":"",
   "user":[
   ],
   "policy":[
   ],
   "activity":[
   ],
   "objectid":[
   ],
   "severity":[
   ],
   "status":[
   ],
   "city":[
   ],
   "idList":[
   ],
   "alertType":[
   ],
   "asc":"severity",
   "desc":"",
   "end_dt":"2020-03-10T15:26:17-0700",
   "start_dt":"2020-03-09T15:26:17-0700",
   "id_list":[
   ],
   "skip":0,
   "limit":20
}
```


Response Variables

Name	Type	Description
buId	Long	Business ID
companyId	String	Company ID
id	String	Alert ID
object	String	Object name that triggered the alert
objectType	String	Object type of alert
objectId	String	Object id that triggered the alert
severity	String	Severity of the alert
serviceId	String	ID to distinguish different account of the cloud service

Name	Type	Description
violationActivity	String	Activity violation that triggered alert
displayOperation	String	Operation that triggered alert
createTime	long	Timestamp of when the alert is created in UTC
updateTime	long	Timestamp of when the alert is updated in UTC
policyName	String	Violation policy name
policyId	String	Name of the policy that alert is triggered by
policyCode	String	ID of the policy that alert is triggered by
contextName	String	Context name of violation policy
userId	String	ID of the user who trigger the alert
eventId	String	ID of the event
eventIdList	Array	List id of the events
service	Application	Cloud service
resultDesc	String	Description for violation context
geoLocationList	Array	Place where the activity occurred.
alertType	String	Classification of the alert
alertSubType	String	Sub classification of the alert
defineType	String	Type of policy, predefined or customized
state	String	Alert state
totalPage	long	Total page of alert results
skip	integer	Indexes in a result set. Used to exclude a response from the first N items of a resource collection.
limit	integer	Maximum number of return alerts in one page
totalCount	integer	Total number of activities on file
user	String	The registered user name of FCASB
userName	String	The registered user email of FCASB

Sample Response


```
{
  "data":[
  {
        "buId":6384,
        "companyId":"6",
        "timestampUUID":"203A8qR797nn390d6CQhOH6DjrdiGx9A",
        "id":"203A8qR797nn390d6CQhOH6DjrdiGx9A",
        "objectType":"USER",
```

```
        "objectId":"0050P000006d7J1QAI",
        "user":"0050P000006d7J1QAI",
        "userName":"0050P000006d7J1QAI",
        "severity":"Alert",
        "applicationId":"00D0P000000Db1XUAS",
        "violationActivity":"SALESFORCE_MODIFY_PERMISSION_SET",
        "displayOperation":"Modify Permission Set",
        "createTime":1583830347799,
        "updateTime":1583830347000,
        "policyName":"Restricted User",
        "policyId":"16615",
        "policyCode":"FC-ACT-010",
        "contextName":"Restricted User",
        "userId":"0050P000006d7J1QAI",
        "eventId":"203A8hk004-akeXpvvQdWBzRhXAwDyJw",
        "eventIdList":[
        "203A8hk004-akeXpvvQdWBzRhXAwDyJw"
        ],
        "service":"Salesforce",
        "resultDesc":"hit the rule: all user include and all event
             include",
        "matches":0,
        "geoLocationList":[
        ],
        "alertType":"Threat protection",
        "defineType":"Predefined",
        "state":"Open"
     },
     {
        "buId":6384,
        "companyId":"6",
        "timestampUUID":"203A8qR796Xvf-yGqIQvSPwS7831UnKA",
        "id":"203A8qR796Xvf-yGqIQvSPwS7831UnKA",
        "objectType":"USER",
        "objectId":"0050P000006d7J1QAI",
        "user":"0050P000006d7J1QAI",
        "userName":"0050P000006d7J1QAI",
        "severity":"Alert",
        "applicationId":"00D0P000000Db1XUAS",
        "violationActivity":"SALESFORCE_MODIFY_PERMISSION_SET",
        "displayOperation":"Modify Permission Set",
        "createTime":1583830347798,
        "updateTime":1583830347000,
        "policyName":"Restricted User",
        "policyId":"16615",
        "policyCode":"FC-ACT-010",
        "contextName":"Restricted User",
        "userId":"0050P000006d7J1QAI",
        "eventId":"203A8hk003U7DBS8g5ScuSgpxwM_TUTw",
        "eventIdList":[
        "203A8hk003U7DBS8g5ScuSgpxwM_TUTw"
        ],
        "service":"Salesforce",
        "resultDesc":"hit the rule: all user include and all event
             include",
        "matches":0,
        "geoLocationList":[
```

```
        ],
        "alertType":"Threat protection",
        "defineType":"Predefined",
        "state":"Open"
     },
     {
        "buId":6384,
        "companyId":"6",
        "timestampUUID":"203A8qR661F8irdySGQZ2gT5BxOk3plg",
        "id":"203A8qR661F8irdySGQZ2gT5BxOk3plg",
        "objectType":"USER",
        "objectId":"0050P000006d7J1QAI",
        "user":"0050P000006d7J1QAI",
        "userName":"0050P000006d7J1QAI",
        "severity":"Alert",
        "applicationId":"00D0P000000Db1XUAS",
        "violationActivity":"SALESFORCE_MODIFY_PERMISSION_SET",
        "displayOperation":"Modify Permission Set",
        "createTime":1583830347664,
        "updateTime":1583830347000,
        "policyName":"Restricted User",
        "policyId":"16615",
        "policyCode":"FC-ACT-010",
        "contextName":"Restricted User",
        "userId":"0050P000006d7J1QAI",
        "eventId":"203A8hk002J2FkUSUIQjaCHtr9UDBLXQ",
        "eventIdList":[
        "203A8hk002J2FkUSUIQjaCHtr9UDBLXQ"
        ],
        "service":"Salesforce",
        "resultDesc":"hit the rule: all user include and all event
             include",
        "matches":0,
        "geoLocationList":[
        ],
        "alertType":"Threat protection",
        "defineType":"Predefined",
        "state":"Open"
     },
  ],
  "totalPage":0,
  "limit":20,
  "skip":0,
  "totalCount":6
}
```


Get Business Unit Info

Description

Get details of the business unit.

URL

/api/v1/businessUnit/info

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/businessUnit/info**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **companyId:** 62598 **roleId:** 36241

Response Variables

Name	Required	Type	Description
companyId	Required	Long	Company ID
companyName	Required	String	The registered parent company name in FortiCASB

Name	Required	Type	Description
buId	Required	Long	Business unit ID
displayName	Required	String	Business unit display name
region	Required	String	Registered region
companyEmail	Optional	String	Registered email
primary	Optional	Boolean	Is primary or not
users	Optional	long	Number of users

Sample Response

```
{
   "companyId":6,
   "companyName":"qa",
   "buId":6384,
   "displayName":"aaa",
   "region":"global",
   "companyEmail":"",
   "primary":false,
   "users":0
}
```

Get Country List

Description

Get a list of all countries.

URL

/api/v1/country/list

Method: GET

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB

Key	Value	Type	Description
Content-Type	application/json	String	
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/country/list**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **roleId:** 36241 **companyId:** 62598

Response Variables

Name	Type	Description
id	String	The country code, represents "Country" for filtering alerts
country	String	The country name, represent "Country Name" for filtering alerts

Sample Response

```
[
   {
      "id":"AU",
      "country":"Australia"
   },
   {
      "id":"CN",
      "country":"China"
   },
   {
      "id":"DE",
      "country":"Germany"
   },
   {
      "id":"ES",
      "country":"Spain"
   },
   {
      "id":"JP",
      "country":"Japan"
   },
```

```
   {
      "id":"US",
      "country":"United States of America"
   },
]
```

Post Dashboard Risk

Description

Get all risk trend data of all monitoring accounts in the business unit.

URL

/api/v1/dashboard/risk

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Account Number>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
timeZone	<Time Zone>	String	Numeric representation of time zone of the user, ex. +0800
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Request Body Parameters

Name	Required	Type	Description
startTime	Required	long	Timestamp, starting time of filtered open alerts
endTime	Required	long	Timestamp, ending time of filtered open alerts

Sample Request

Request URL	**POST https://www.forticasb.com/api/v1/dashboard/risk**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **roleId:** 36241 **companyId:** 62598 **buid:** 6384 **timezone:** -0700
Request Body	{ "startTime":1585518361548, "endTime":1585604761548 }

Response Variables

Name	Type	Description
name	String	Cloud service name
id	String	Risk sequence number
key	String	The time that the risk was detected
value	long	The risk number on this date

Sample Response

```
{
   "data":[
   {
      "name":"Box",
      "values":[
         {
            "id":"0",
            "key":"2020-03-10T18:00:00+0000",
            "value":0
```

```
        },
        {
           "id":"1",
           "key":"2020-03-10T18:30:00+0000",
           "value":0
        }
        ]
     },
     {
     "name":"Salesforce",
     "values":[
        {
           "id":"0",
           "key":"2020-03-10T18:00:00+0000",
           "value":0
        },
        {
           "id":"1",
           "key":"2020-03-10T18:30:00+0000",
           "value":0
        }
     ]
  },
  {
  "name":"Dropbox",
  "values":[
     {
        "id":"0",
        "key":"2020-03-10T18:00:00+0000",
        "value":0
     },
     {
        "id":"1",
        "key":"2020-03-10T18:30:00+0000",
        "value":0
     }
  ]
  },
  {
  "name":"Google",
  "values":[
        {
           "id":"0",
           "key":"2020-03-10T18:00:00+0000",
           "value":0
        },
        {
           "id":"1",
           "key":"2020-03-10T18:30:00+0000",
           "value":0
        }
     ]
  },
  {
  "name":"Office365",
  "values":[
     {
```

```
        "id":"0",
        "key":"2020-03-10T18:00:00+0000",
        "value":0
     },
     {
        "id":"1",
        "key":"2020-03-10T18:30:00+0000",
        "value":0
     }
  ]
  }
  ]
}
```


Post Dashboard Statistics

Description

Get crucial statistics data from the cloud service in the business unit.

URL

/api/v1/dashboard/statistics

Method: POST

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
timeZone	<Time Zone>	String	Numeric representation of time zone of the user, ex. +0800.
service	<Salesforce>	String	Cloud service account

Key	Value	Type	Description
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Request Body Parameters

Name	Type	Description
startTime	long	Timestamp, starting time of filtered open alerts
endTime	long	Timestamp, ending time of filtered open alerts

Sample Request

Request URL	`POST https://www.forticasb.com/api/v1/dashboard/statistics`

Request Header	`Authorization: Bearer <Authorization_Token>`
	`Content-Type: application/json`
	`timeZone: +0800`
	`Service: Salesforce`
	`buid: 6384`
	`roleId: 36241`
	`companyId: 62598`

Request Body	`{`
	`"startTime":1583865778729,`
	`"endTime":1583952178729`
	`}`

Response Variables

Name	Type	Description
topRiskUsers	List	Top risk users in a time period
topRiskObjects	List	Top risk objects in a time period
topHitPolicies	List	Top hit policies in a time period
topRiskEventType	List	Top risk event type in a time period
topRiskPositions	List	Top risk positions in a time period
topActivityPositions	List	Top activity positions in a time period
alertTrend	List	The trend of alert in a time period

Name	Type	Description
usageTrend	List	The trend of usage in a time period
riskSeverity	List	The risk severity statistics
name	String	Position of the alert
id	String	Corresponding ID number of the event, policy, risk user, risk object, risk position
key	String	The event name, risk user name, policy name, activity name, alert name, risk object name, trend time
value	long	The number of the statics items

Sample Response


```
{
  "topRiskUsers":[
        {
           "id":"0050P000006k18GQAQ",
           "key":"yue zhang",
           "value":2
        }
     ],
     "topRiskObjects":[
        {
           "id":"0690P000006mwkbQAA",
           "key":"SSN2020-03-11T17:00:24.746Z.txt",
           "value":4
        },
     {
        "id":"0690P000006mwlPQAQ",
        "key":"CA_Driver2020-03-
             11T17:00:30.133Z.txt",
        "value":4
     },
     {
        "id":"0690P000006mwloQAA",
        "key":"CN_Passport2020-03-
             11T17:00:32.464Z.txt",
        "value":4
     },
     {
        "id":"0690P000006mwkgQAA",
        "key":"CNID2020-03-11T17:00:25.632Z.txt",
        "value":3
     },
     {
        "id":"0690P000006mwlUQAQ",
        "key":"CN_Driver2020-03-
             11T17:00:30.566Z.txt",
        "value":3
     }
     ],
     "topHitPolicies":[
```

```
    {
       "id":"16615",
       "key":"Restricted User",
       "value":35
    },
    {
       "id":"16598",
       "key":"DLP UK Passport Number Policy",
       "value":4
    },
    {
       "id":"16601",
       "key":"DLP USA/Germany Passport Number
            Policy",
       "value":4
    },
    {
       "id":"16599",
       "key":"DLP AU Passport Number Policy",
       "value":3
    },
    {
       "id":"16603",
       "key":"DLP CA Driver License Policy",
       "value":3
    }
    ],
    "topRiskEventType":[
    {
       "id":"202",
       "key":"Upload File",
       "value":76
    },
    {
       "id":"238",
       "key":"Post",
       "value":4
    },
    {
       "id":"214",
       "key":"Login Success",
       "value":2
    },
    {
       "id":"239",
       "key":"Comment",
       "value":1
    }
    ],
    "topRiskPositions":[
    {
       "name":"United States of America",
       "key":"US",
       "value":83
    }
    ],
    "topActivityPositions":[
```

```
      {
         "name":"United States of America",
         "key":"US",
         "value":35
      }
      ],
      "alertTrend":[
      {
         "id":"0",
         "key":"2020-03-10T21:00:00+0000",
         "value":0
      }
      ],
      "usageTrend":[
      {
         "id":"0",
         "key":"2020-03-10T21:00:00+0000",
         "value":0
      }
      ],
      "riskSeverity":[
      {
         "id":"0",
         "key":"Alert",
         "value":82
      },
      {
         "id":"1",
         "key":"Critical",
         "value":1
      }
   ]
}
```


Get Dashboard Summary

Description

Get dashboard summary.

URL

/api/v1/dashboard/summary

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	`GET https://www.forticasb.com/api/v1/dashboard/summary`

Request Header	`Authorization: Bearer <Authorization_Token>`
	`Content-Type: application/json`
	`companyId: 6`
	`buid: 6384`
	`companyId: 62598`
	`roleId: 36241`

Response Variables

Name	Type	Description
loginUser	String	The login user e-mail.
alertsCount	long	Number of alerts in the last 30 days
activitiesCount	long	Number of activities in the last 30 days

Name	Type	Description
fileScannedCount	long	Number of files scanned in the last 30 days

Sample Response

```
{
   "loginUser":"qa.casb1@gmail.com",
   "alertsCount":3220,
   "activitiesCount":9514,
   "fileScannedCount":340
}
```

Post Dashboard Usage

Description

Get all activity usage trend data of all the monitoring cloud accounts in the business unit.

URL

/api/v1/dashboard/usage

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
timeZone	<Time Zone>	String	Numeric representation of time zone of the user, ex. +0800.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page

Key	Value	Type	Description
			456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Request Body Parameters

Name	Type	Description
startTime	long	Timestamp, starting time of filtered open alerts
endTime	long	Timestamp, ending time of filtered open alerts

Sample Request

Request URL	`POST https://www.forticasb.com/api/v1/dashboard/usage`

Request Header	`Authorization: Bearer <Authorization_Token>`
	`Content-Type: application/json`
	`timeZone: +0800`
	`buid: 6384`
	`roleId: 36241`
	`companyId: 62598`

Request Body	`{`
	`"startTime":1583865778729,`
	`"endTime":1583952178729`
	`}`

Response Variables

Name	Type	Description
name	String	Cloud service name
id	String	Usage sequence number
key	String	The time that the usage was detected
value	long	The usage number at the date

Sample Response

```
{
"data": [
  {
     "name": "Box",
     "values": [
```

```
        {
           "id": "0",
           "key": "2020-03-10T18:30:00+0000",
           "value": 0
        }
     ]
  },
  {
  "name": "Salesforce",
  "values": [
        {
           "id": "0",
           "key": "2020-03-10T18:30:00+0000",
           "value": 0
        }
     ]
  },
  {
  "name": "Dropbox",
  "values": [
        {
           "id": "0",
           "key": "2020-03-10T18:30:00+0000",
           "value": 0
        }
     ]
  },
  {
  "name": "Google",
  "values": [
        {
           "id": "0",
           "key": "2020-03-10T18:30:00+0000",
           "value": 0
        }
     ]
  },
  {
  "name": "Office365",
  "values": [
        {
           "id": "0",
           "key": "2020-03-10T18:30:00+0000",
           "value": 0
        }
     ]
  }
  ]
}
```

Get Event

Description

Get activity events definition from FortiCASB.

URL

/api/v1/event

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
service	<Cloud Service>	String	Cloud service name such as Salesforce, Office365, etc.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/event**
Request Header	**Authorization:** Bearer <Authorization_Token> **service:** Salesforce **Content-Type:** application/json **roleId:** 36241 **companyId:** 62598

Response Variables

Name	Type	Description
id	integer	The activity id, represents "Activity ID" for filtering alerts and activity
name	String	Name of the activity operation, represents "Activity Name" for filtering alerts and activity
nameEnum	OperationNameEnum	The activity operation type, represents "Activity" enum for filtering alerts and activity
value	String	The activity ID, represents "Activity" for filtering alerts and activity
category	String	The category of activity, represents "Activity Category" for filtering alerts and activity
searchField	String	The search field of the filter

Sample Response


```
[
   {
      "id":202,
      "name":"Upload File",
      "nameEnum":"UPLOAD_FILE",
      "value":"202",
      "category":"FILE",
      "searchField":"activity"
   },
   {
      "id":203,
      "name":"Download File",
      "nameEnum":"DOWNLOAD_FILE",
      "value":"203",
      "category":"FILE",
      "searchField":"activity"
   },
   {
      "id":206,
      "name":"Upload New Version",
      "nameEnum":"UPLOAD_NEW_VERSION",
      "value":"206",
      "category":"FILE",
      "searchField":"activity"
   },
]
```

Get Filter List

Description

Get all users created filter lists in the specific cloud service under the targeted business unit.

URL

/api/v1/filter/list

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
service	<Cloud Service Name>	String	Cloud service name such as Salesforce, Office365, etc.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/filter/list**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Office365 **roleId:** 36241 **companyId:** 62598

Response Variables

Name	Type	Description
id	Integer	The serial number
name	String	The filter name that user created
filter	String	The filter that the user saved
source	String	The filter source page

Sample Response


```
[
   {
      "id":36156,
      "name":"casb test",
      "filter":"{\"selectPolicyObject\":[],\"selectFileTypeObject\":
            [],\"selectShareTypeObject\":[],\"selectSensitiveDataObject\":
            [],\"selectOwnerObject\":[],\"selectShareToInternalObject\":
            [],\"selectShareToGuestObject\":[],\"selectUserObject\":
            [],\"selectSharedUserObject\":[],\"selectActivityObject\":
            [{\"id\":2,\"name\":\"Upload
            File\",\"category\":\"FILE\"}],\"selectSeverityObject\":
            [],\"selectAlertTypeObject\":[],\"selectStatusObject\":
            [],\"selectCountryObject\":[],\"ipList\":[],\"selectAuditOperateObject\":
            [],\"selectAuditModuleObject\":[],\"selectAuditVendorObject\":
            [],\"isShare\":false,\"isLink\":false,\"isNewFinding\":false,\"isViolation\":
            false,\"isSuccess\":null,\"object\":\"\",\"selectedHistoryPeriod\":
            {\"time\":\"Last 24 hours\",\"displayTime\":\"Last 24
            hours\"},\"selectedPeriod\":{\"start_dt\":\"2020-03-10T23:38:45.069Z\",\"end_
            dt\":\"2020-03-11T23:38:45.069Z\",\"value\":{\"time\":\"Last 24
            hours\",\"displayTime\":\"Last 24 hours\"}}}",
      "source":"alert"
   }
]
```


Get Service History

Description

Get cloud service OAuth history of the business unit.

URL

/api/v1/service/history/{application}

Method: GET

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
application	<Cloud Service application>	String	Cloud service application name such as Salesforce, Office365, etc.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/service/history/Salesforce**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **companyId:** 62598 **roleId:** 36241

Response Variables

Name	Required	Type	Description
id	Required	long	The OAuth history ID
buId	Required	Long	Business unit ID
application	Required	String	Cloud service application name

Name	Required	Type	Description
scanId	Optional	String	Application name + company name
actionStatusCode	Optional	String	The user name that is registered with this cloud service
message	Optional	String	The returned message of cloud service status history
date	Optional	long	Timestamp, the time that processed this step
lastStep	Optional	String	The last process step
casbUser	Optional	String	The user email that is used in FortiCASB
cloudUser	Optional	String	The user name that is registered in this cloud service account

Sample Response


```
[
   {
      "id":31289,
      "scanId":"SALESFORCEVb-gvLgmSLCWw8U_BSh6Vw",
      "buId":6384,
      "application":"SALESFORCE",
      "actionStatusCode":"Success",
      "message":"",
      "date":1583432356528,
      "lastStep":"Update OAuth Data",
      "casbUser":"qa.casb1@gmail.com",
      "cloudUser":"yuezhang@yue.com"
   },
   {
      "id":31267,
      "scanId":"SALESFORCEVb-gvLgmSLCWw8U_BSh6Vw",
      "buId":6384,
      "application":"SALESFORCE",
      "actionStatusCode":"Success",
      "message":"",
      "date":1583378643280,
      "lastStep":"Update OAuth Data",
      "casbUser":"qa.casb1@gmail.com",
      "cloudUser":"mhuang@fortinet-uk.com"
   },
   {
      "id":24433,
      "scanId":"SALESFORCEVb-gvLgmSLCWw8U_BSh6Vw",
      "buId":6384,
      "application":"SALESFORCE",
```

```
        "actionStatusCode":"Success",
        "message":"",
        "date":1582918837831,
        "lastStep":"Update OAuth Data",
        "casbUser":"qa.casb1@gmail.com",
        "cloudUser":"yuezhang@yue.com"
    },
    {
        "id":16572,
        "scanId":"SALESFORCEVb-gvLgmSLCWw8U_BSh6Vw",
        "buId":6384,
        "application":"SALESFORCE",
        "actionStatusCode":"Success",
        "message":"",
        "date":1582585855516,
        "lastStep":"Save OAuth Data",
        "casbUser":"qa.casb1@gmail.com",
        "cloudUser":"mh20170918@126.com"
    }
]
```


Get Application Status

Description

Get the cloud service information and authentication status under the same business unit.

URL

/api/v1/application/status

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	

Key	Value	Type	Description
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/application/status**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **roleId:** 36241 **companyId:** 62598 **buid:** 84

Response Variables

Name	Required	Type	Description
service	Required	String	Cloud service account such as "Salesforce", "Office365", etc.
applicationId	Required	String	The id of the cloud service account.
applicationStatus	Required	int	The onboarding status of the cloud service account.
cloudAccount	Required	String	Cloud service account username.

Sample Response


```
[
   {
      "companyId": 62598,
      "buId": 84,
      "service": "AWSS3",
      "applicationId": "239187241191",
      "update": false,
      "enable": true,
      "applicationStatus": "RUNNING",
      "lastUpdate": 1680311539918,
      "cloudAccount": "239187241191"
   },
   {
      "companyId": 62598,
      "buId": 84,
      "service": "SAPSuccessFactors",
      "applicationId": "SFCPART000289",
      "update": false,
      "enable": true,
      "applicationStatus": "RUNNING",
      "lastUpdate": 1705083754298,
      "cloudAccount": "sfadmin"
   },
   {
      "companyId": 62598,
      "buId": 84,
      "service": "CitrixShareFile",
      "applicationId": "a4205de9-ca5b-8c96-4cb3-802ffe209b84",
      "update": true,
      "enable": true,
      "applicationStatus": "RUNNING",
      "lastUpdate": 1705070917370,
      "cloudAccount": "testadmin1@forticasb.com"
   }
]
```


Get Severity

Description

Get all alert severity definitions from FortiCASB.

URL

/api/v1/severity

Method: GET

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/severity**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **roleId:** 36241 **companyId:** 62598

Response Variables

Name	Type	Description
id	String	The severity code, represents "Severity" code filter in filtering alerts
name	String	The severity name, represents "Severity" name filter for filtering alerts

Sample Response

```
[
   {
      "id":"1",
```

```
        "name":"Critical"
      },
      {
        "id":"2",
        "name":"Alert"
      },
      {
        "id":"3",
        "name":"Warning"
      },
      {
        "id":"4",
        "name":"Information"
      },
      {
        "id":"5",
        "name":"Pass"
      }
]
```


Get Status

Description

Get status definition from FortiCASB system.

URL

/api/v1/status

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/status**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **companyId:** 62598 **roleId:** 36241

Response Variables

Name	Type	Description
id	String	Status ID
name	String	Service Status

Sample Response

```
[
   {
      "id":"1",
      "name":"New"
   },
   {
      "id":"2",
      "name":"In progress"
   },
   {
      "id":"3",
      "name":"Resolved"
   },
   {
      "id":"4",
      "name":"Discard"
   }
]
```

Get User List

Description

Get details of all users of the cloud services under the same company and business unit.

URL

/api/v1/profile/user/list

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
service	<Cloud Service>	String	Name of the cloud service such as Salesforce, Office365, etc.
skip	<Skip Number>	Integer	Indexes in a result set. Used to exclude response from the first N items of a resource collection.
limit	<Limit per Page>	Integer	Maximum number of return items per page.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/profile/user/list**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **companyId:** 62598 **roleId:** 36241 **service:** Salesforce **buid:** 8 **companyid:** 7 **skip:** 0 **limit:** 2

Response Variables

Name	Required	Type	Description
companyId	Required	String	Company ID
userId	Required	String	The user identity
origUserId	Required	String	The original user identity
deleted	Required	boolean	The current user information deleted or not
createdDate	Required	long	Timestamp, user created date
service	Required	Application	Cloud service name
isActive	Required	boolean	User active status
buId	optional	Long	Business unit ID
createdById	optional	String	The ID which created this user
lastModifiedDate	optional	long	Timestamp, the last time that this user has been modified
lastModifiedById	optional	String	The last user id that modified this user information
lastLoginDate	optional	long	Timestamp, the last time that this user login into FortiCASB
systemModstamp	optional	long	Timestamp of the system
email	optional	String	The email of the registered user
userName	optional	String	The user name of the registered user
name	optional	String	This user's name
firstName	optional	String	This user's first name
lastName	optional	String	This user's last name
userType	optional	UserTypeEnum	User type
profileId	optional	String	This user's profile ID
userRoleId	optional	String	This user's role ID

Sample Response


```
[
   {
      "companyId": "7",
      "buId": 8,
      "userId": "0050P000006kOBcQAM",
      "origUserId": "0050P000006kOBcQAM",
      "deleted": false,
      "createdDate": 1492555111000,
      "createdById": "0050P000006d7J0QAI",
      "lastModifiedDate": 1583370489000,
      "systemModstamp": 1545262127000,
      "email": "xxxxxxx@gmail.com",
      "userName": "xxxxxxx@guest.hotmail.com",
      "name": "forti3 net3",
      "firstName": "forti3",
      "lastName": "net3",
      "service": "SALESFORCE",
      "lastLoginDate": 1545262127000,
      "userType": "CsnOnly",
      "isActive": true,
      "profileId": "00e0P000000JYKPQA4"
   },
   {
      "companyId": "7",
      "buId": 8,
      "userId": "0054U000009GCaMQAW",
      "origUserId": "0054U000009GCaMQAW",
      "deleted": false,
      "createdDate": 1595303943000,
      "createdById": "0050P000006d7J1QAI",
      "lastModifiedDate": 1595303943000,
      "systemModstamp": 0,
      "email": "xxxxx@salesforce.com",
      "userName": "xxxxxx@00d0p000000db1xuas",
      "name": "Platform Integration User",
      "lastName": "Platform Integration User",
      "service": "SALESFORCE",
      "lastLoginDate": 0,
      "isActive": true,
      "profileId": "00e0P000000a7HVQAY"
   }
]
```


Get Data Security Policy List

Description

Return all FortiCASB Data Security Policies and details from Data Protection.

URL

/api/v1/scan/policy/list

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/scan/policy/list**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Salesforce **roleId:** 36241 **companyId:** 62598

Response Variables

Name	Type	Description
name	String	Data Security Policy name.
category	String	Category of the policy
code	String	Policy code for identifying the policy

Sample Response


```
{
   "data": {
      "datas": [
         {
            "selectAllFileTypes": false,
            "selectAllAccessPermissions": false,
            "selectAllFileActivities": false,
            "selectAllSaasApps": true,
            "filesAddedWithin": {
            "name": "ALL_TIME",
            "displayName": "All Time",
            "code": 6
         },
            "customizedPatterns": [],
            "permitQuarantine": true,
            "notifyUsers": false,
            "usersToNotify": [],
            "notifyOwners": false,
            "fazLog": false,
            "startTime": 0,
            "changeAccessPermission": false,
            "changeAccessPermissionType": 0,
            "writeLabels": false,
            "id": 1,
            "companyId": "62598",
            "bizUnitId": 84,
            "name": "data_security_test",
            "predefined": false,
            "enabled": true,
            "lastUpdated": 1702402793153
         },
         {
            "selectAllFileTypes": false,
            "selectAllAccessPermissions": false,
            "selectAllFileActivities": false,
            "selectAllSaasApps": true,
            "filesAddedWithin": {
            "name": "ALL_TIME",
            "displayName": "All Time",
            "code": 6
         },
            "customizedPatterns": [],
            "permitQuarantine": true,
            "notifyUsers": false,
            "usersToNotify": [],
            "notifyOwners": false,
            "fazLog": false,
            "startTime": 0,
            "changeAccessPermission": false,
            "changeAccessPermissionType": 0,
            "writeLabels": false,
            "id": 35,
            "companyId": "62598",
            "bizUnitId": 84,
```

```
            "name": "Default FortiCASB Scan-All Data Protection
                 Policy",
            "predefined": true,
            "enabled": false,
            "lastUpdated": 1699312350281
        }
    ],
    "totalPage": 0,
    "limit": 0,
    "skip": 0,
    "totalCount": 2
  },
  "code": 0,
  "msg": "success",
  "httpCode": 200
}
```


Get Threat Protection Policy List

Description

Return all FortiCASB Threat Protection Policies and details of the specified cloud service account.

URL

/api/v1/policy/tpList

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
service	<Salesforce>	String	Cloud service account

Key	Value	Type	Description
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/policy/tplist**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Office365 **companyId:** 62598

Response Variables

Name	Type	Description
name	String	Threat Protection Policy name
policyCategory	String	Category of the policy
policyId	String	Policy Id for identifying the policy

Sample Response

```
[
   {
      "policyId": 179,
      "name": "Excessive Login Failures",
      "service": "OFFICE365",
      "description": "Alert when failed logins for a user exceeds
           threshold",
      "type": "Access",
      "severity": "Alert",
      "enable": true,
      "threshold": 1,
      "interval": 2,
      "alert": true,
      "lastUpdatedBy": "",
      "lastUpdated": 1696375132181,
      "enableWorkflow": true,
      "operatorType": "trigger",
      "workflowSubject": "Policy '%s' added to workflow",
      "workflowMessage": "Policy '%s' was added to your workflow. You
           will be notified when the alert's status changes.",
      "enableEmail": false,
      "emailSubject": "%s Alert",
      "emailMessage": "An event matched '%s'. Please verify sensitive
           information is not exposed.",
      "policyCategory": "Threat protection",
      "regexPattern": ".*",
      "receivers": [],
```

```
      "vi": {
         "velocity": true,
         "vs": 0,
         "vd": 0
      },
      "object": {
         "nameMatch": true,
         "extension": true,
         "contextMatch": false,
         "objSize": false,
         "objNum": false,
         "mFile": [],
         "mContext": ".*",
         "sizeThreshold": 10.0,
         "zipThreshold": 0.0,
         "numThreshold": 50,
         "size": [],
         "num": []
      },
      "isSelectAllEvents": false,
      "isSelectAllUsers": false,
      "dataPatterns": [],
      "enableActivityMatching": false,
      "enableContentMatching": false,
      "allDatapattern": false,
      "policyCode": "FC-ACT-001",
      "storageConfig": {},
      "enableCreatorEmail": false
   }
]
```


Get Compliance Policy List

Description

Return all FortiCASB Compliance Policies and details of the specified cloud service account.

URL

/api/v1/policy/cList

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
service	<Salesforce>	String	Cloud service account
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/policy/cList**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Office365 **companyId:** 62598 **roleid:** 36241

Response Variables

Name	Type	Description
name	String	Compliance Policy name
policyCategory	String	Category of the policy
policyId	String	Policy Id for identifying the policy

Sample Response


```
[
   {
      "policyId": 31054,
      "name": "HIPAA - Access to EPHI Data",
      "service": "OFFICE365",
      "description": "Track access to EPHI data",
      "type": "HIPAA",
      "severity": "Critical",
      "enable": true,
      "exposure": "",
      "threshold": 30,
      "interval": 60,
      "alert": true,
      "lastUpdatedBy": "fcasbdemo@gmail.com",
      "lastUpdated": 1631078491154,
      "guideline": "Audit Controls (§ 164.312(b))Implement procedural
           mechanisms that record and examine activity in information
           systems that contain or use electronic protected health
           information.",
      "enableWorkflow": true,
      "workflowSubject": "Policy '%s' added to workflow",
      "workflowMessage": "Policy '%s' was added to your workflow. You
           will be notified when the alert's status changes.",
      "enableEmail": false,
      "emailSubject": "%s Alert",
      "emailMessage": "An event matched '%s'. Please verify sensitive
           information is not exposed.",
      "policyCategory": "compliance",
      "regexPattern": ".*",
      "receivers": [
         "qqin@fortinet.com"
      ],
      "isSelectAllEvents": false,
      "isSelectAllUsers": false,
      "contentMatching": {
         "enable": false,
         "fileExtExclusion": false,
         "fileSize": 0,
         "compressedFileSize": 0,
         "filePaths": [
         ""
         ],
         "filePathsExclusion": false,
         "ownersExclusion": false,
         "exposureExclusion": false
      },
      "enableActivityMatching": true,
      "enableContentMatching": true,
      "allDatapattern": false,
      "policyCode": "FC-ACT-047",
      "isolateMalwareFile": false,
      "storageConfig": {},
      "enableCreatorEmail": false
   }
]
```

Post Document Profile Summary

Description

Return all document profile summaries of the specified cloud service account.

URL

/api/v1/profile/document/summary

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
service	<Salesforce>	String	Cloud service account
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**POST https://www.forticasb.com/api/v1/profile/document/summary**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Office365 **companyId:** 62598 **roleid:** 36241
Request Body	{

```
                        "limit": 10,
                        "skip": 0,
                        "filterDataList": [
                           {
                              "name": "File Type",
                              "valueList": []
                           },
                           {
                              "name": "Sensitive Data",
                              "valueList": [],
                              "byOthers": false,
                              "byAll": false
                           },
                           {
                              "name": "Share Type",
                              "valueList": [],
                              "byOthers": false,
                              "byAll": false
                           }
                        ]
                     }
```


Response Variables

Name	Type	Description
name	String	Data type of the file.
bubbleList	String	List of file types in the bubble diagram.
id	String	The id of the file type.

Sample Response


```
{
   "data": [
      {
         "name": "File Type",
         "bubbleOther": {
            "name": "Non-Extension",
            "id": "Non-Extension",
            "size": 1
         },
         "bubbleTotal": {
            "name": "With-Extension",
            "id": "With-Extension",
            "size": 20198
         },
         "bubbleList": [
         {
            "name": "7z_014tix27s33cczubi4vbhzeeq3kspwwqpa",
            "id": "7z_014TIX27S33CCZUBI4VBHZEEQ3KSPWWQPA",
            "size": 2
         },
         {
            "name": "exe_014tix27q4xmeysomhibdzllu3s7z65piw",
```

```
            "id": "exe_014TIX27Q4XMEYSOMHIBDZLLU3S7Z65PIW",
            "size": 2
         },
         ]
      },
      {
         "name": "Sensitive Data",
         "bubbleOther": {
            "name": "Non-Extension",
            "id": "Non-Extension",
            "size": 0
         },
         "bubbleTotal": {
            "name": "With-Extension",
            "id": "With-Extension",
            "size": 80545
         },
         "bubbleList": [
            {
               "name": "DLP US WA-1 Driver License Pattern",
               "id": "1545",
               "size": 1
            }
         ]
      },
      {
         "name": "Share Type",
         "bubbleOther": {
            "name": "Non-Extension",
            "id": "Non-Extension",
            "size": 0
         },
         "bubbleTotal": {
            "name": "With-Extension",
            "id": "With-Extension",
            "size": 15427
         },
         "bubbleList": [
            {
               "name": "Anyone Edit Link",
               "id": "OFFICE365_LINK_ALL_EDIT",
               "size": 1
            }
         ]
      },
      {
         "name": "SaaS App",
         "bubbleOther": {
            "name": "Non-Extension",
            "id": "Non-Extension",
            "size": 0
         },
         "bubbleTotal": {
            "name": "With-Extension",
            "id": "With-Extension",
            "size": 20199
         },
```

```
        "bubbleList": [
           {
              "name": "Office365",
              "id": "OFFICE365",
              "size": 20199
           }
        ]
     }
  ],
  "code": 0,
  "msg": "success",
  "httpCode": 200
}
```


Post Document Profile List

Description

Return all document profile details of the specified cloud service account.

URL

/api/v1/profile/document/fileList

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
service	<Salesforce>	String	Cloud service account
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**POST https://www.forticasb.com/api/v1/profile/document/fileList**
Request Header	**Authorization**: Bearer <Authorization_Token> **Content-Type**: application/json **buid**: 6384 **service**: Office365 **companyId**: 62598 **roleid**: 36241

Request Body	<pre>{
	"limit": 1,
	"skip": 0,
	"filterDataList": [
	{
	"name": "File Type",
	"valueList": []
	},
	{
	"name": "Sensitive Data",
	"valueList": [],
	"byOthers": false,
	"byAll": false
	},
	{
	"name": "Share Type",
	"valueList": [],
	"byOthers": false,
	"byAll": false
	}
	]
	}</pre>

Response Variables

Name	Type	Description
filename	String	The name of the file
fileId	String	The Id of the file.
service	String	The cloud service account provider that host the file.

Sample Response

<pre>{
"data": {
"datas": [
{
"fileId": "74c3f925-34bc-49da-8b88-d5f5973b1272",
"fileName": "EMD232add3.txt",
"buId": 84,
"serviceId": "fa16a6de-8e28-46fb-a400-7f881ba9bcea",
"companyId": "62598",
"service": "Office365",</pre>

```
            "vendorCode": "Office365",
            "path": "011220248/EMD232add3.txt",
            "lastModifiedUser": "",
            "lastModifiedUserName": "",
            "docCreatedAt": "2024-01-13T00:02:53.000Z",
            "docLastUpdatedAt": "2024-01-13T00:02:53.000Z",
            "link": "/download/Office365/users/null/74c3f925-34bc-49da-
                 8b88-d5f5973b1272",
            "size": 4224,
            "dlp": false,
            "exposure": false,
            "sharing": false,
            "sensitive": false,
            "malware": false,
            "isLink": false,
            "resourceType": "users",
            "isDelete": false,
            "folder": false,
            "location": false,
            "root": true,
            "states": [
            "SCANNING"
            ],
            "processedResult": "Data scan is in progress.",
            "pathInfo": {}
         }
      ],
      "totalPage": 20202,
      "limit": 1,
      "skip": 0,
      "totalCount": 20202
   },
   "code": 0,
   "msg": "success",
   "httpCode": 200
}
```


Post C-Level Report Summary

Description

Return all C-Level reports instances generated on FortiCASB.

URL

/api/v1/report/clevel/page

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**POST https://www.forticasb.com/api/v1/report/clevel/page**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Office365 **companyId:** 62598 **roleid:** 36241
Request Body	{ "skip": 0, "limit": 1 }

Response Variables

Name	Type	Description
filename	String	C-Level report name.

Name	Type	Description
date	String	Date the C-Level report generated.
id	String	Id of the C-Level report.

Sample Response


```
{
   "data": {
      "datas": [
         {
            "id": 3840,
            "name": "2024 Annual",
            "date": "2024-01-13T00:29:14.556Z",
            "cLevel": true,
            "status": "completed_success",
            "finished": true,
            "timezoneOffset": 0
         }
      ],
      "totalPage": 0,
      "limit": 1,
      "skip": 0,
      "totalCount": 617
   },
   "code": 0,
   "msg": "success",
   "httpCode": 200
}
```


Post Compliance Report Summary

Description

Return all Compliance reports instances generated on FortiCASB.

URL

/api/v1/report/compliance/filtered

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**POST https://www.forticasb.com/api/v1/report/compliance/filtered**
Request Header	**Authorization**: Bearer <Authorization_Token> **Content-Type**: application/json **buid**: 6384 **service**: Office365 **companyId**: 62598 **roleid**: 36241
Request Body	{ "skip": 0, "limit": 1, "timezoneOffset": "-0800", "reportTypes": [], "cloudApps": [], "scheduled": [] }

Response Variables

Name	Type	Description
name	String	Compliance report name.
date	String	Date the Compliance report generated.
id	String	Id of the Compliance report.

Sample Response


```
{
   "data": {
      "datas": [
         {
            "id": 129593,
            "name": "SAAS Box PCI-DSS Compliance Report December 2023
                  UTC.zip",
            "generator": "SAAS",
            "date": "2024-01-01T01:21:23.858Z",
            "available": true,
            "complete": true,
            "scheduled": true
         }
      ],
      "totalPage": 0,
      "limit": 1,
      "skip": 0,
      "totalCount": 4655
   },
   "code": 0,
   "msg": "success",
   "httpCode": 200
}
```


Post Shadow IT Report Summary

Description

Return all Shadow IT reports instances generated on FortiCASB.

URL

/api/v1/report/shadowIt/page

Method: Post

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.

Sample Request

Request URL	**POST https://www.forticasb.com/api/v1/report/shadowIt/page**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Office365 **companyId:** 62598 **roleid:** 36241
Request Body	{ "skip": 0, "limit": 1 }

Response Variables

Name	Type	Description
name	String	Shadow IT report name.

Name	Type	Description
date	String	Date the Shadow IT report generated.
id	String	Id of the Shadow IT report.

Sample Response


```
{
   "data": {
      "datas": [
         {
            "id": 512,
            "name": "SAAS_Shadow_IT_Report_2023-11-06-14-47-42.pdf",
            "generator": "SAAS",
            "date": "2023-11-06T22:47:42.086Z",
            "available": true,
            "complete": true
         }
      ],
      "totalPage": 0,
      "limit": 1,
      "skip": 0,
      "totalCount": 217
   },
   "code": 0,
   "msg": "success",
   "httpCode": 200
}
```


Get Alert Report Summary

Description

Return all alert reports instances generated with specification on the year generated and if is generated on a monthly basis.

URL

/api/v1/report/alert/reportList

Method: Get

Request Headers

Key	Value	Type	Description
Authorization	Bearer <Authorization Token>	String	Authorization credential generated by FortiCASB
Content-Type	application/json	String	
buId	<Business Unit ID>	Long	The targeted business unit ID on FortiCASB. Business unit ID can be obtained through . Alternatively, it can also be obtained from the REST API Get Resource Map on page 456
roleId	<User ID>	Integer	Login user ID, can be obtained through Get Resource Map on page 456.
companyId	<Company ID>	Integer	Company ID of which the business unit is under, can be obtained through Get Resource Map on page 456.
service	<Salesforce>	String	Cloud service account
year	<Year>	Integer	Year the report generated.
isMonthly	<True>	Boolean	True if the report is monthly, false if the report is not a monthly report.

Sample Request

Request URL	**GET https://www.forticasb.com/api/v1/report/alert/reportList**
Request Header	**Authorization:** Bearer <Authorization_Token> **Content-Type:** application/json **buid:** 6384 **service:** Salesforce **companyId:** 62598 **roleid:** 36241 **isMonthly:** false **year:** 2024

Response Variables

Name	Type	Description
name	String	Alert report name.
size	String	The size of the Alert report.
timestamp	String	Date the Alert report generated.

Sample Response


```
{
   "data": [
      {
         "name": "Salesforce_Alert_Report20240101_UTC.csv",
         "size": 14108,
         "timestamp": "Jan 2, 2024, 9:18:06 PM"
      },
      {
         "name": "Salesforce_Alert_Report20240102_UTC.csv",
         "size": 15990,
         "timestamp": "Jan 3, 2024, 9:18:09 PM"
      },
      {
         "name": "Salesforce_Alert_Report20240103_UTC.csv",
         "size": 15116,
         "timestamp": "Jan 4, 2024, 9:18:06 PM"
      }
   ],
   "code": 0,
   "msg": "success",
   "httpCode": 200
}
```

Troubleshooting

Information and solutions for the following problems are included in this section:

Getting Started

- **I have a new account but no license**
- **I have renewed my license, but cannot use it.**

Salesforce

- I get an **OAuth Request** error.

Office 365

- I get a **Add Site Collection Admin errors on page 520**.
- I get a **Add Users errors on page 522**
- I get a **Add Groups errors on page 522**
- I get a **System Automatic Sync NOT Completed error on page 523**
- I get a **Insufficient Permissions(Access Denied) Error (One Drive) on page 525**
- I get a **Insufficient Permissions(Access Denied) Error (SharePoint) on page 528**

Dropbox Business

- I get an **OAuth Request** error.

Google Workspace

- **I can't connect Google Workspace to FortiCASB**.

All SaaS Applications

- I get an **API Throttling Limitation Message (All Apps) on page 534**

Getting Started Issues

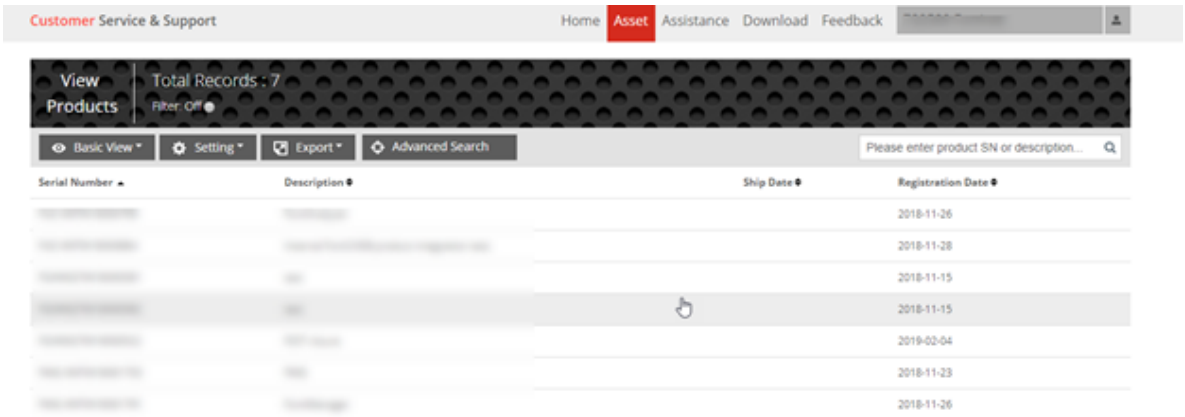
Information and solutions for the following problems are included in this section:

- **New account with No License Error on page 516**
- **Renew License error on page 517**

New account with No License Error

Please check on your primary FortiCloud account to see if the license is present with these steps:

1. Log into FortiCloud https://support.fortinet.com/ with your primary FortiCloud account.
2. From the top main menu click on **Asset > Manage/View Products**.
3. Check and see if the licenses you purchased is shown in the product list.

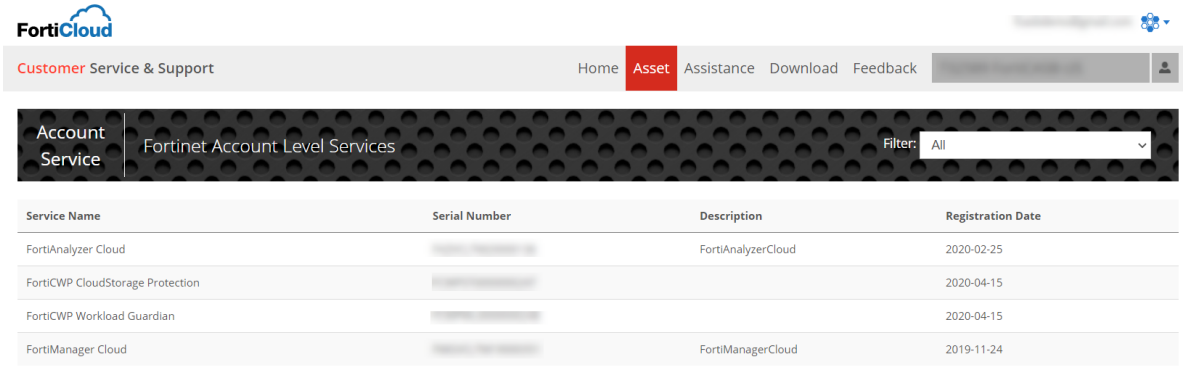


4. If you find your license on the list, then you can add the license through creating a company. Please see Company Management on page 23.
5. If you do not see the license you purchased is on the list, please contact FortiCloud support.

Renew License error

When you have renewed your license but cannot find it on your FortiCASB Dashboard, follow these steps to see if the license appears in your FortiCloud account.

1. Log into FortiCloud https://support.fortinet.com/ with your primary FortiCloud account.
2. From the top main menu click on **Asset > View Account Service**.
3. Check and see if the license/contract you purchased is shown in the product list.



4. If you do not see the license/contract you purchased is on the list, please contact FortiCloud support.
5. If your license is on the list, then it only need to be assigned to the company/business unit on FortiCASB.

Salesforce

OAuth Request errors

If an error occurs, an error message will be displayed on the Salesforce panel.

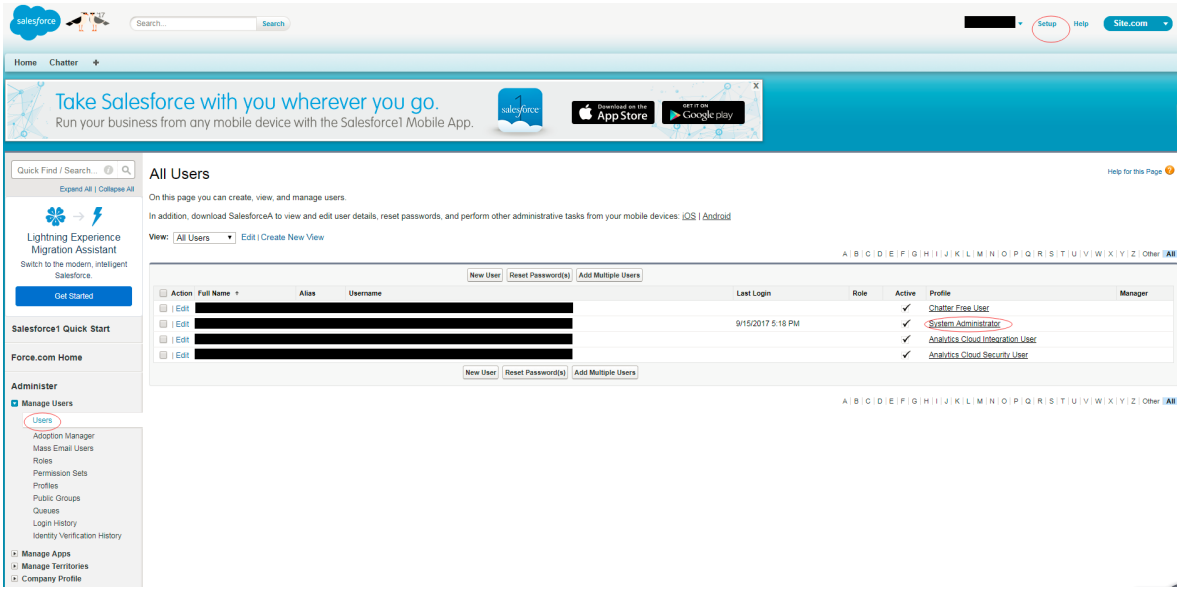
The following sections show some common error messages, as well as possible solutions:

- If your error message says "Saas application API gateway not accessible", go to Saas application API gateway not accessible error on page 518

Saas application API gateway not accessible error

FortiCASB requires users to have three specific Salesforce permissions. To check your Salesforce permissions, follow these steps:

1. From your Salesforce menu, go to **Setup > Manage Users > Users.**
2. Click on the profile of the integrated user.
   For example, if the integrated user is listed as a "**System Administrator**", click on System Administrator under "Profile".



3. Make sure you have the "API Enabled", "View All Data", and "View All Users" permissions enabled.

If you have all these permissions and still encounter the error, your organization could have reached Salesforce's daily API request limit. To check if you have reached this limit, follow these steps:

1. From your Salesforce menu, go to **Setup > Company Profile > Company Information**.
2. Check "API Requests, Last 24 Hours" to see if you have reached your maximum limit.

If you have reached this limit, wait for the next 24 hour period to try again.

Salesforce enforces API call limits based on a per-organization basis, not a per-user basis. If your organization has multiple applications sharing Salesforce API requests, please consolidate usage between applications.

Office 365

Add Site Collection Admin errors

The following sections show some common causes for this error, as well as possible solutions.

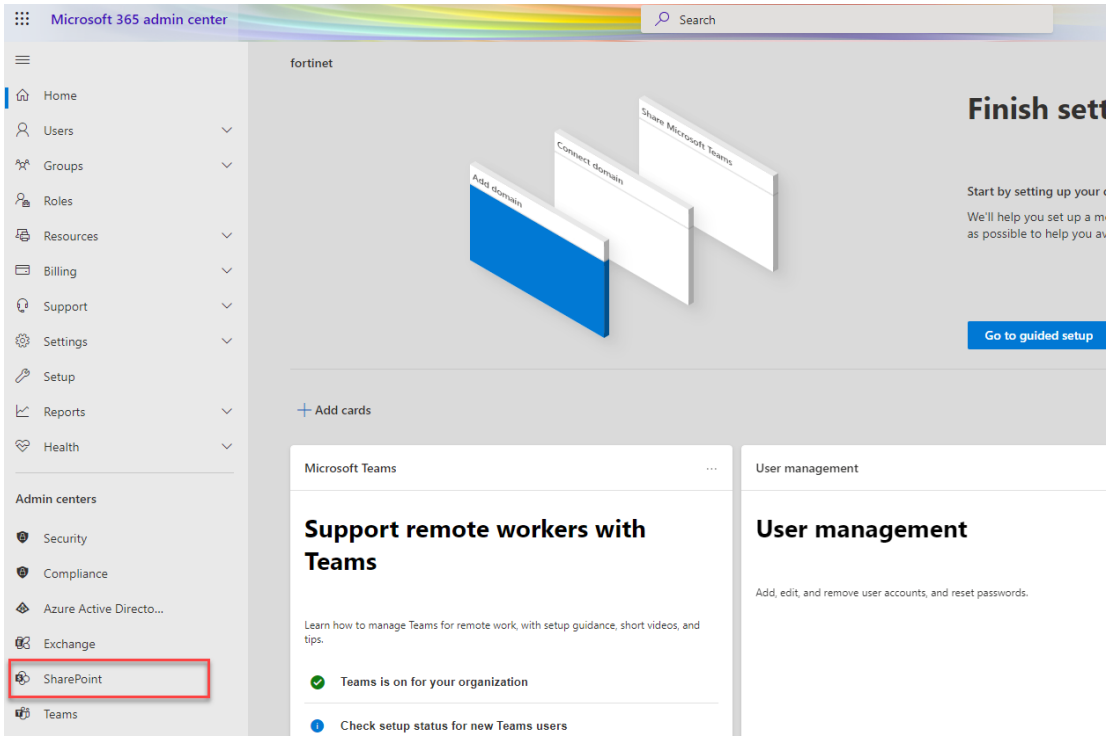
- If your azure domain does not end in ".onmicrosoft.com", follow the steps in Customized SharePoint homepage URL on page 520 to allow collection manually.

Customized SharePoint homepage URL

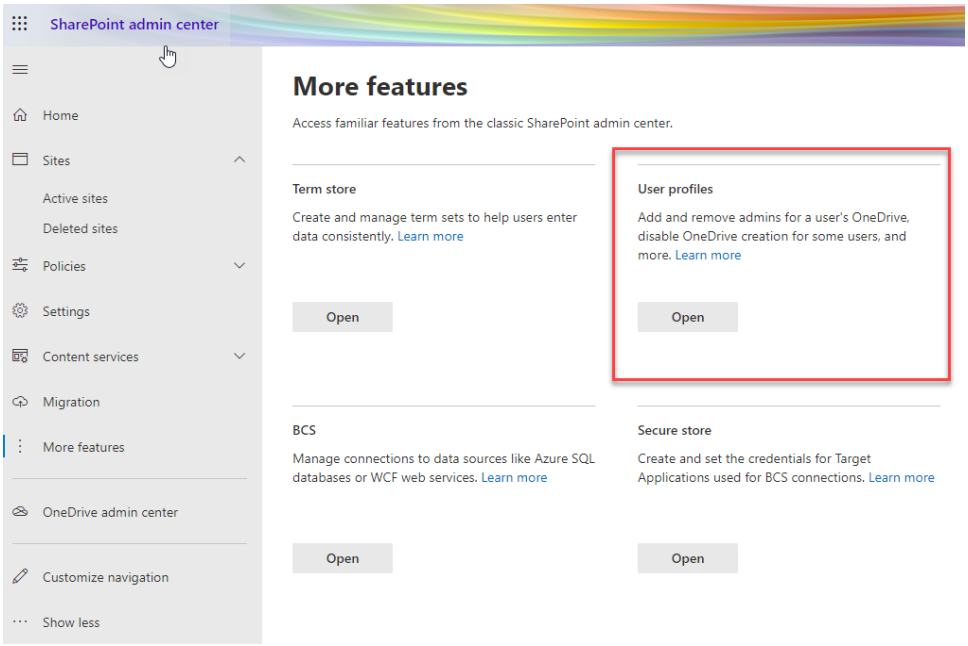
FortiCASB's "Add Site Collection Admin" feature currently only supports the default azure domain format (abc.onmicrosoft.com).

If you have a custom SharePoint homepage URL, you will have to allow collection manually.

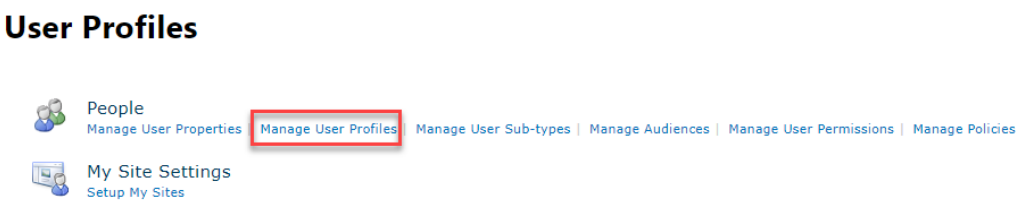
1. Go to Microsoft 365 Admin Center, click on **show all** in the navigation pane, then click **SharePoint**.



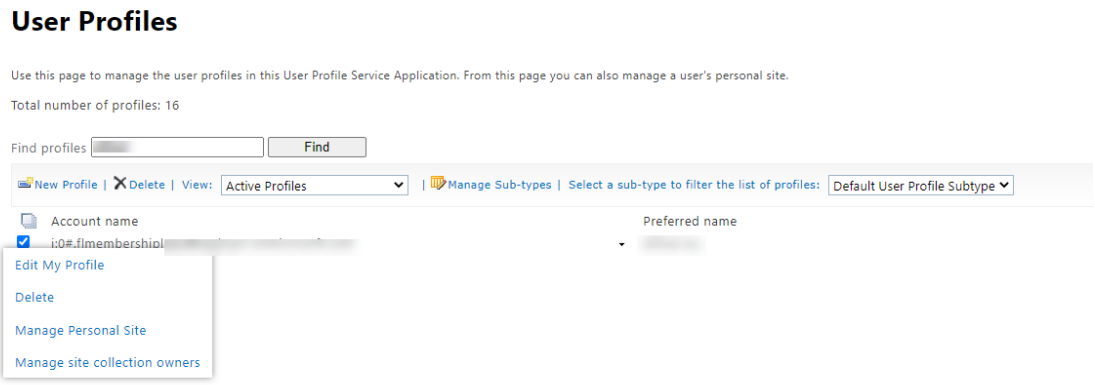
2. In **SharePoint Admin Center** navigation pane, click **More features**. Under **User profiles**, click **Open**.



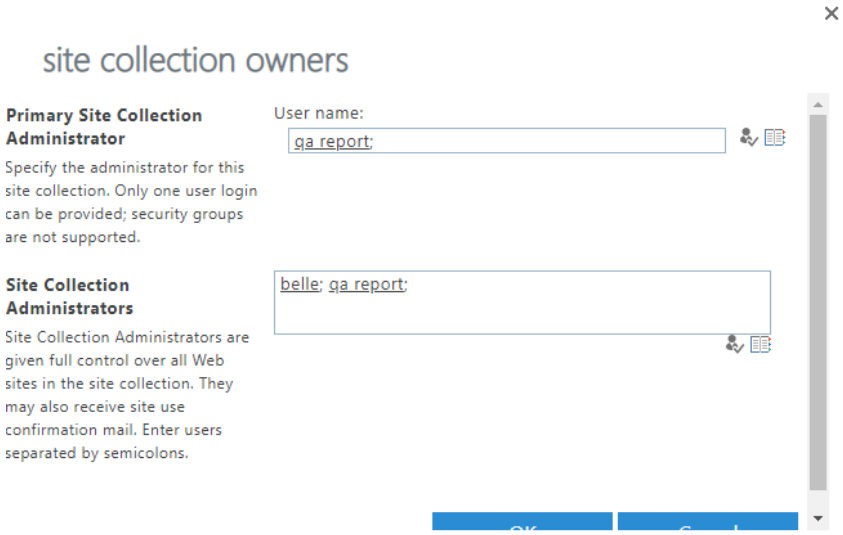
3. In **User Profiles** , click **Manage User Profiles**.



4. Find the user, click on user account name, then select **Manage site collection owners.**



5. In the **Site Collection Administrators** box, enter your admin username, then click **Ok**.



FortiCASB can now audit this user's OneDrives. Repeat steps one through four for each user you wish to audit.

Add Users errors

Even if such an error occurs, FortiCASB will still monitor users that do not trigger this error. For example, in this case, FortiCASB will monitor the 37 users that were added successfully, even if this error is not corrected.

The following sections show some common causes for this error, as well as possible solutions.

- If these users have never logged into their Office 365 accounts before, go to Adding users with new Office 365 accounts on page 522.

Adding users with new Office 365 accounts

Office 365 activates a new user's SharePoint portal when he or she logs in for the first time. For a brand new O365 account, log into the account once to activate the portal, then add the user in FortiCASB.

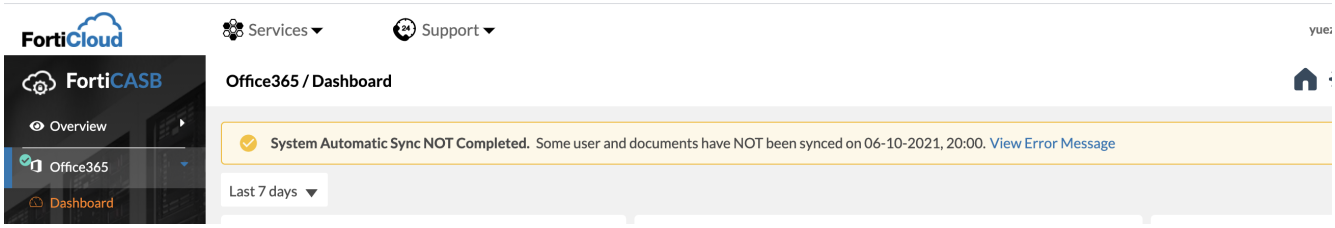
Add Groups errors

Some groups do not generate or manipulate files. FortiCASB will not monitor these groups. FortiCASB will also not monitor groups the site administrator does not have permission to monitor.

Even if such an error occurs, FortiCASB will still monitor groups that do not trigger this error.

System Automatic Sync NOT Completed error

When you received the error "**System Automatic Sync NOT Completed. Some users and documents Not been synced on ..**" on Office 365 Dashboard, click **View Error Message** to see the details.



The error messages contains a list of users using the same Office 365 account, but have not been granted with permission to be monitored by FortiCASB.

This error **Will Not** prevent FortiCASB from providing account monitoring and protection for the Office 365 account.

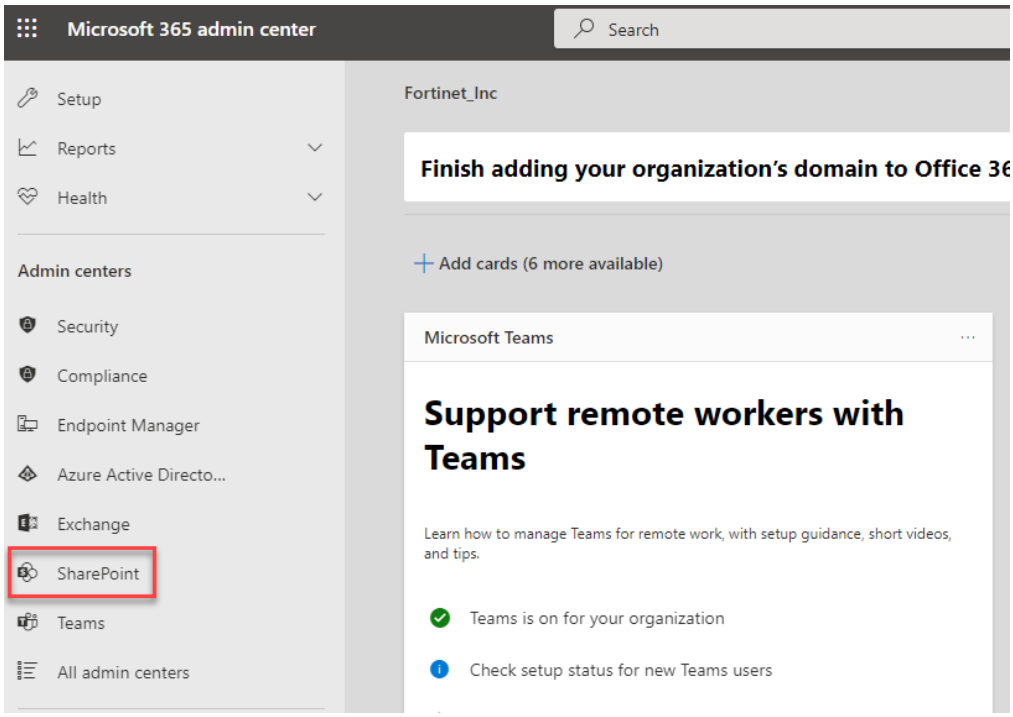
However, DLP (Data Analysis) scan can not be performed on the list of users' Office 365 OneDrive Accounts.

To fix the error, please follow the instruction in **Manually Activate Sites Collection on page 523** to add the global administrator or sharepoint administrator to the **Site Collection Administrators** to grant users to be connected to FortiCASB.

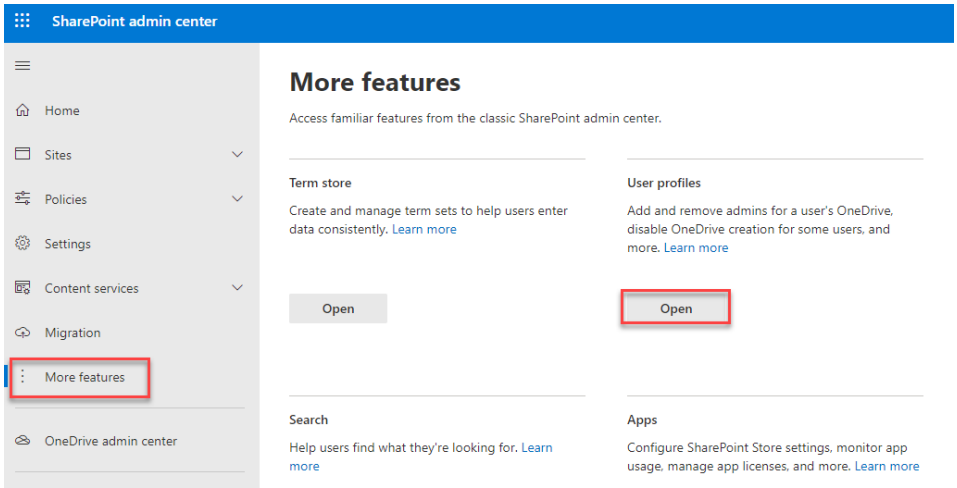
Manually Activate Sites Collection

Follow these steps to make OneDrive data accessible:

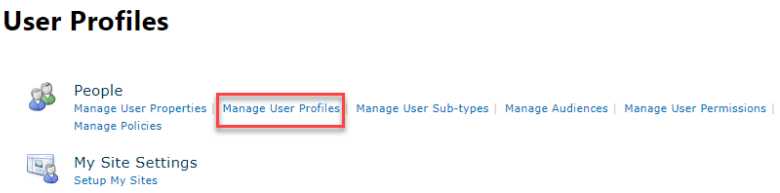
1. Log into https://admin.microsoft.com/ using your global administrator account.
2. In the left pane, under **Admin centers**, click **SharePoint**.



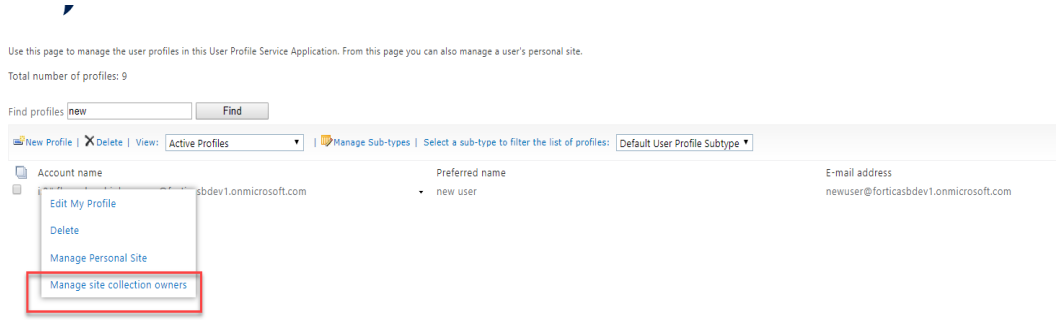
3. After **SharePoint admin center** pop-up, click **More features**, and open **User profiles.**



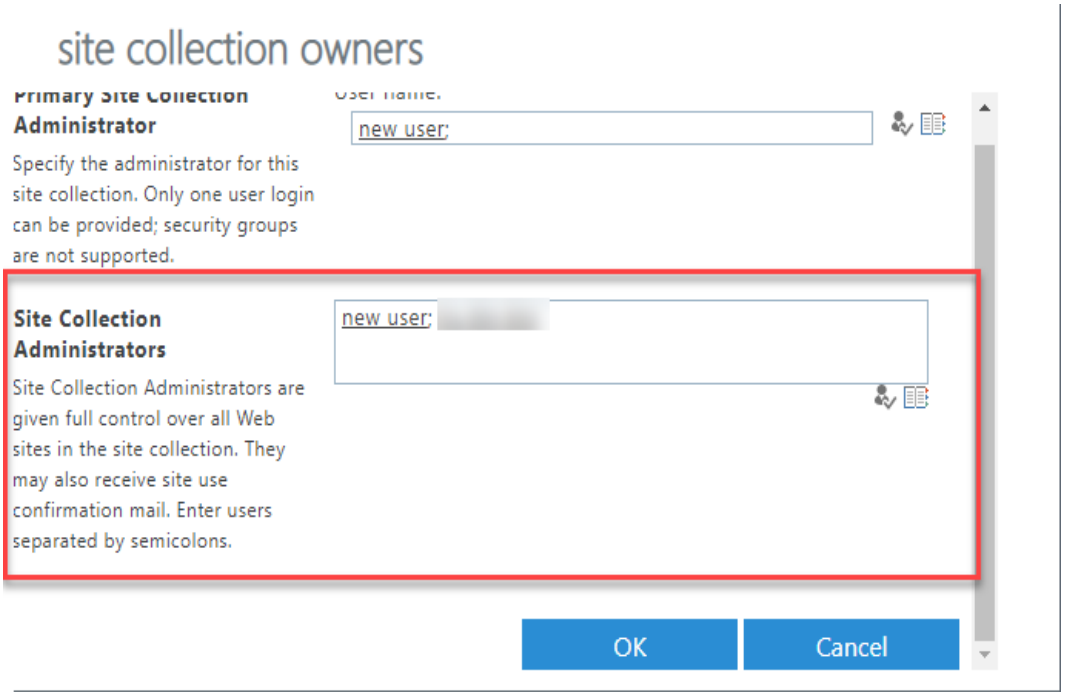
4. In **User Profiles** page, under **People**, select **Manager User Profiles**.



5. In **Find profiles** box, enter a licensed user under the global account administrator and click **Find**.
6. Right click on the account name and select **Manage site collections owners**.



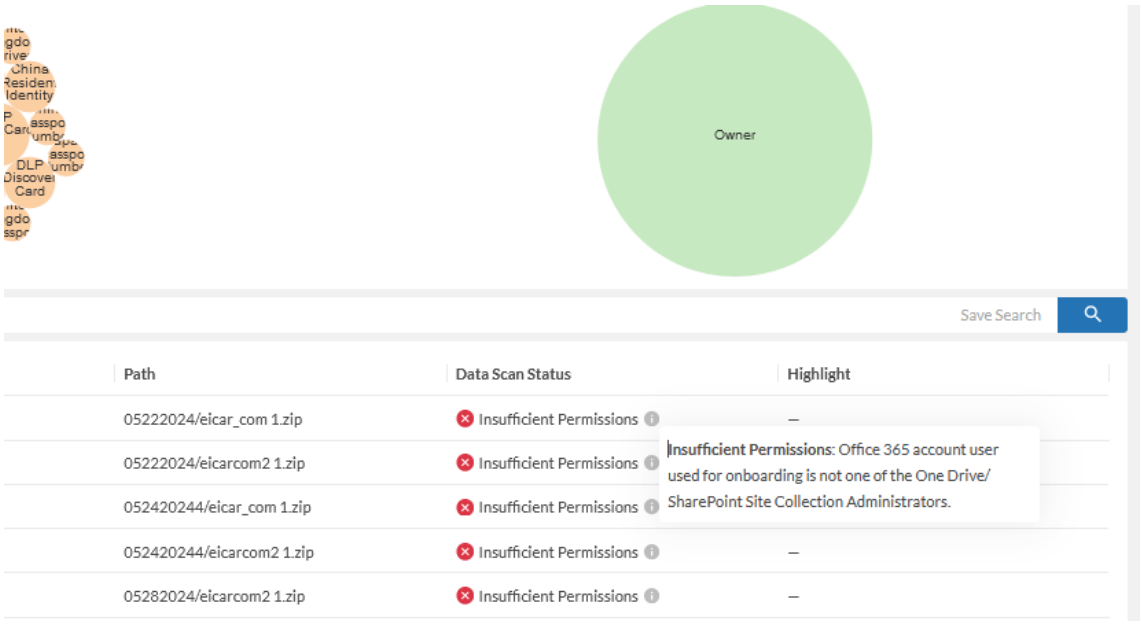
7. In the field for **Site Collection Administrators**, add the global or sharepoint administrator account's user name or e-mail address and press Enter.



8. Click on **Ok** button to complete adding the global or sharepoint administrator as one of the site collection administrators.

Insufficient Permissions(Access Denied) Error (One Drive)

Insufficient Permissions(Access Denied) error is one of the **Data Scan Status** in **Office 365 > Files** page. This guide is targeted on the files in **Microsoft OneDrive** account.

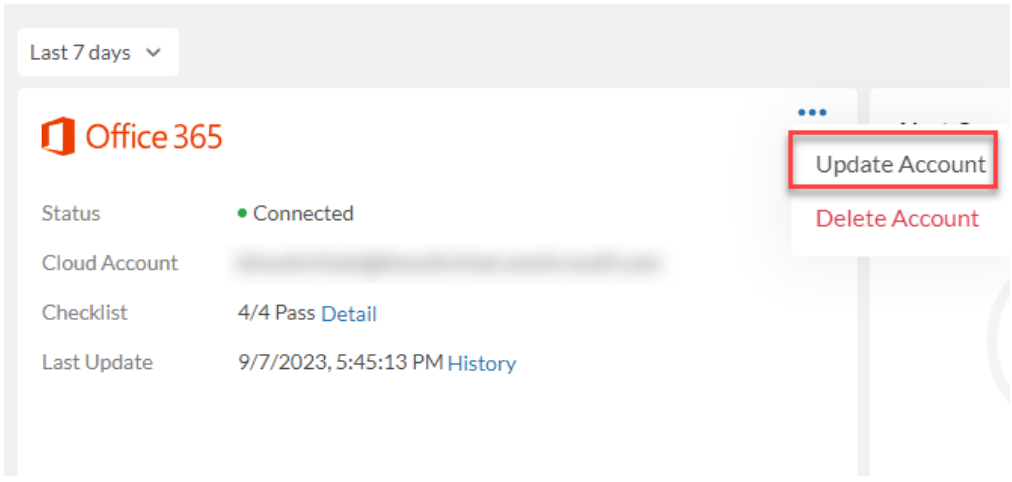


Root Cause Analysis

The file resided in OneDrive is not accessible for data scan, thus returning the "Insufficient Permissions" error. This error occurs when the Office 365 service account used for the FortiCASB onboarding process is not part of the new Office 365 user's OneDrive **Site Collection Administrators**.

Solution 1: Update Office 365 Account

In FortiCASB, update the Office 365 Account and follow the instructions to update the account. The service account should be added automatically to the new user's OneDrive Site Collection Administrator when the account is successfully updated.



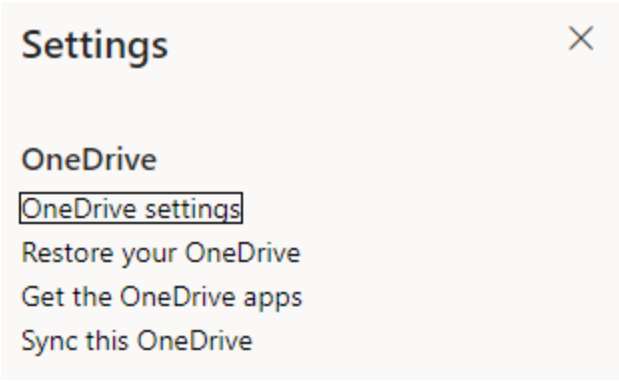
Solution 2 - Add Admin Account to One Drive Site

The service account or the Office 365 account used in the FortiCASB onboarding process needs to be added to the new Office 365 user's OneDrive **site collection administrator**.

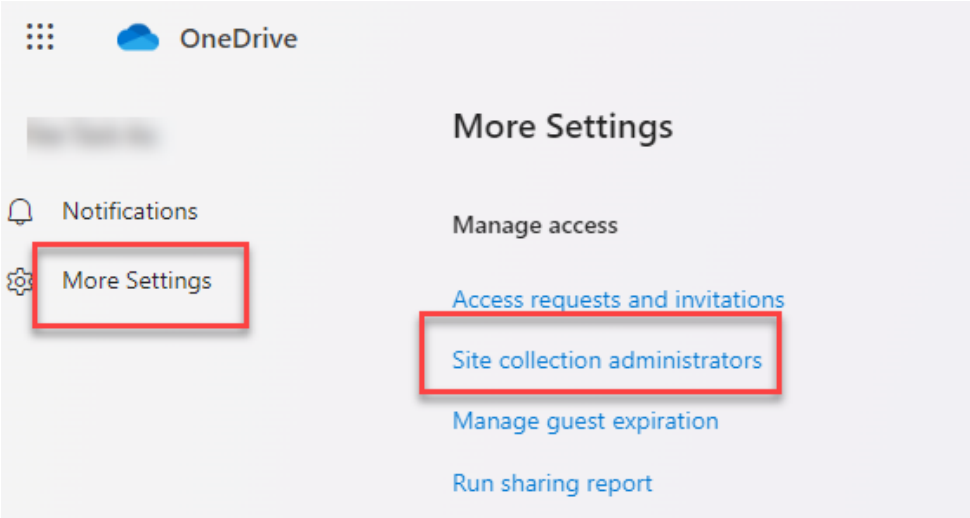
By completing this configuration, the data stored in OneDrive will be accessible for FortiCASB data scan.

1. Log into the new user's Office 365 account, click on the Apps menu and select **OneDrive**.
2. Click on the **setting** icon in the top right corner.

3. In **Settings**, click **OneDrive setting**.

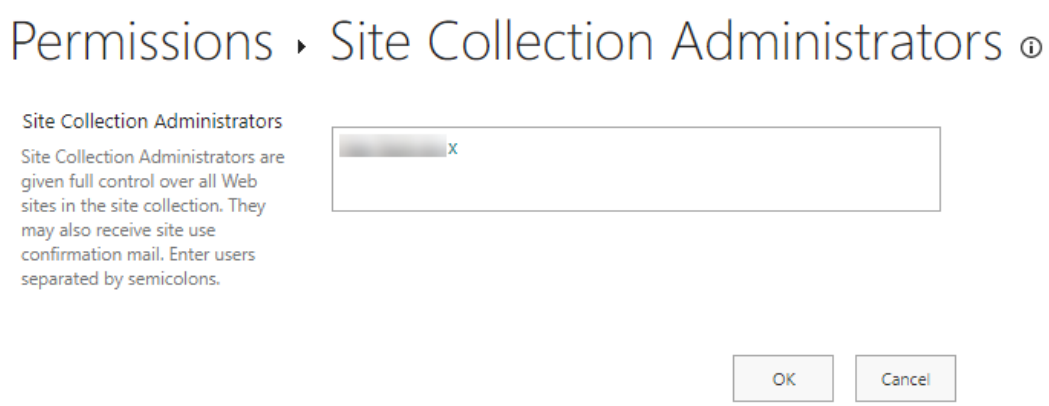


4. Click **More Settings**, inside **Manage access**, click **Site Collection administrators**.



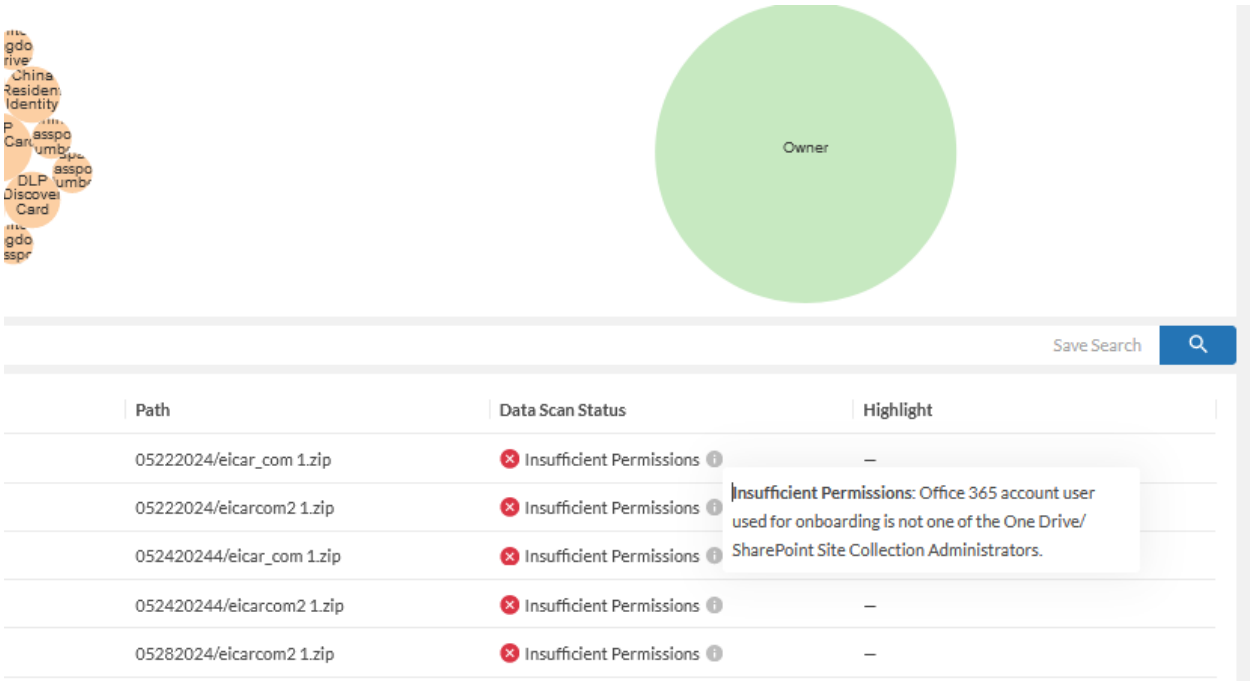
5. Check to see if the Office 365 service account used for FortiCASB onboarding is one of the Site Collection

Administrators. If not, add the account in the list and click **Ok**.



Insufficient Permissions(Access Denied) Error (SharePoint)

Insufficient Permissions(Access Denied) error is one of the **Data Scan Status** in **Office 365 > Files** page. This guide is targeted on files on **Microsoft SharePoint** sites.



Root Cause Analysis

The file resided on the Microsoft SharePoint Site is not accessible for data scan, thus returning "Insufficient Permissions" error. This error occurs when the Office 365 service account used for the FortiCASB onboarding process is not one of the SharePoint Site's admins.

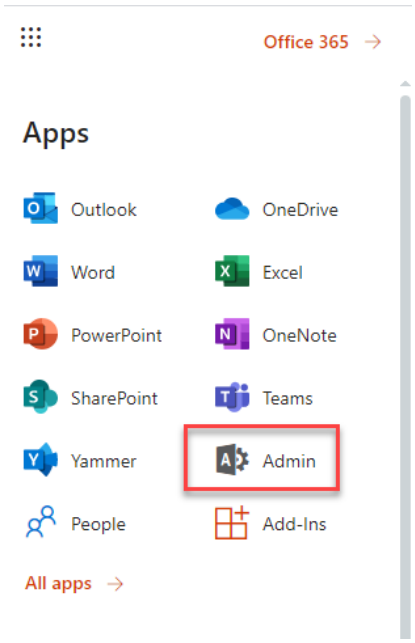
Solution 1: Update Office 365 Account

In FortiCASB, update the Office 365 account and follow the instructions to update the account. The service account should be added automatically to the Sharepoint Site Administrators when the account is successfully updated.

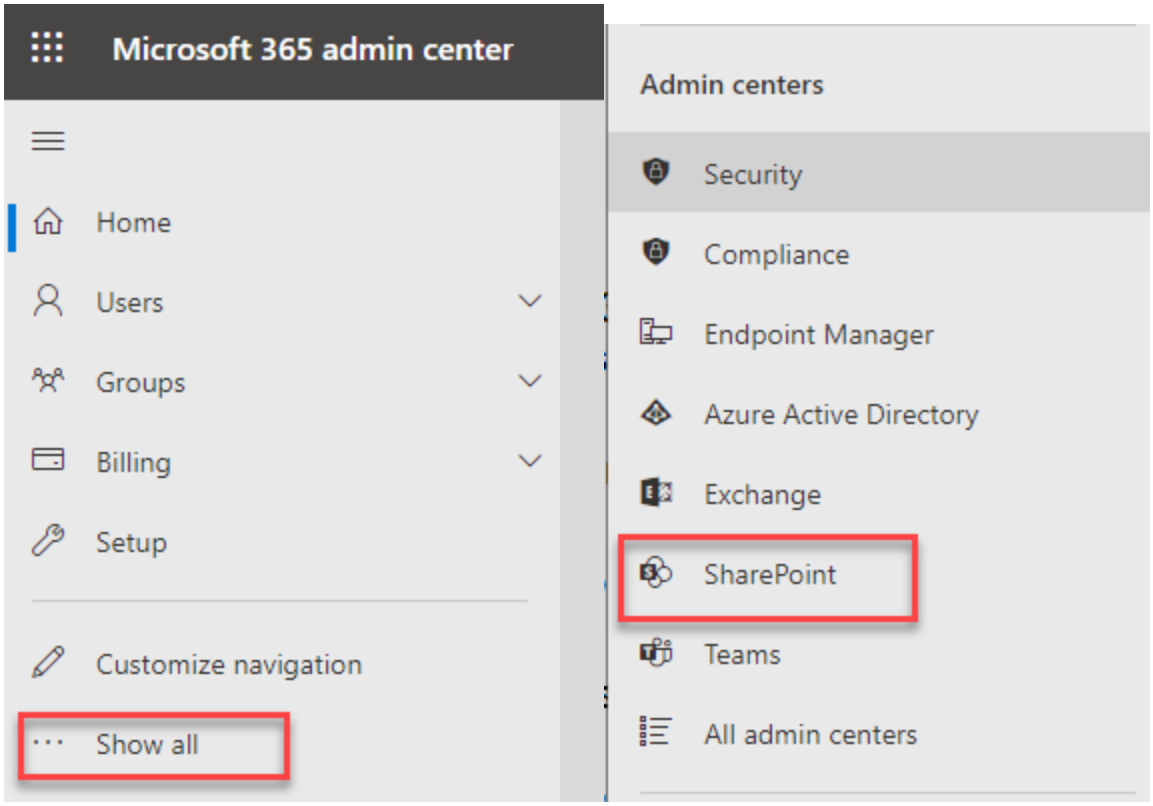
Solution 2 - Add Admin Account to SharePoint Site Admin Group

Before adding an administrator account to the SharePoint Site admin group, please verify that the account is one of the **Company Administrators**, and this account will be used for Office 365 onboarding process on FortiCASB.

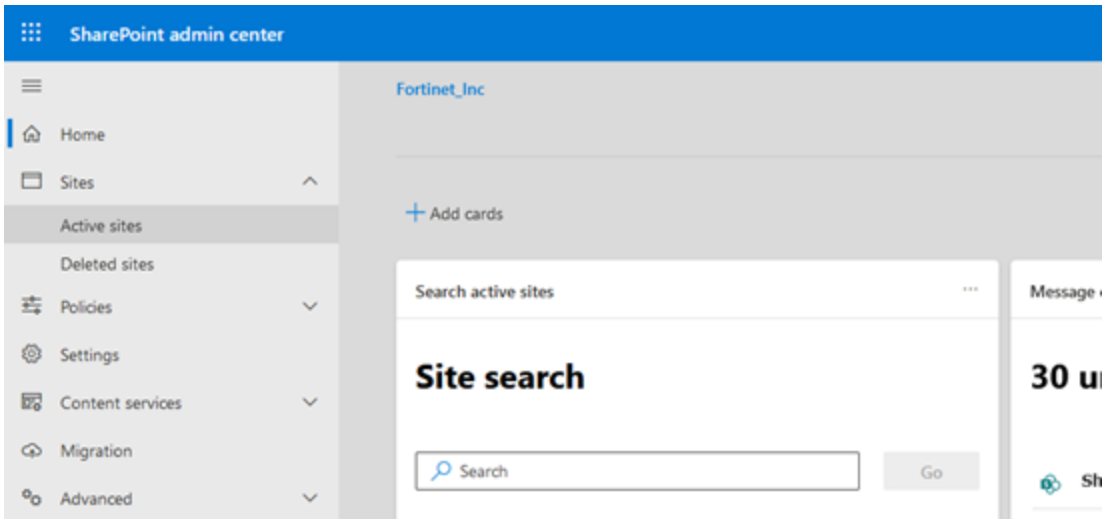
1. Log into Office 365 (https://office.com) with your account to be added to FortiCASB.
2. Click on the App Launcher button  at the top left corner, and select **Admin**.



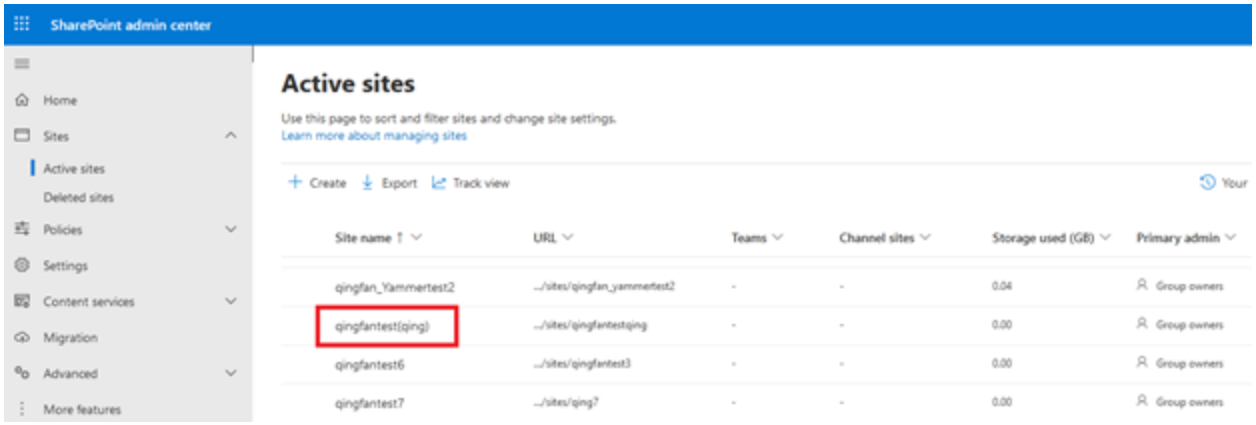
3. In **Microsoft 365 admin center** left navigation menu, , click on **Show all** to show other options. Scroll down to **Admin Centers** and click **SharePoint** to access **SharePoint admin center**.



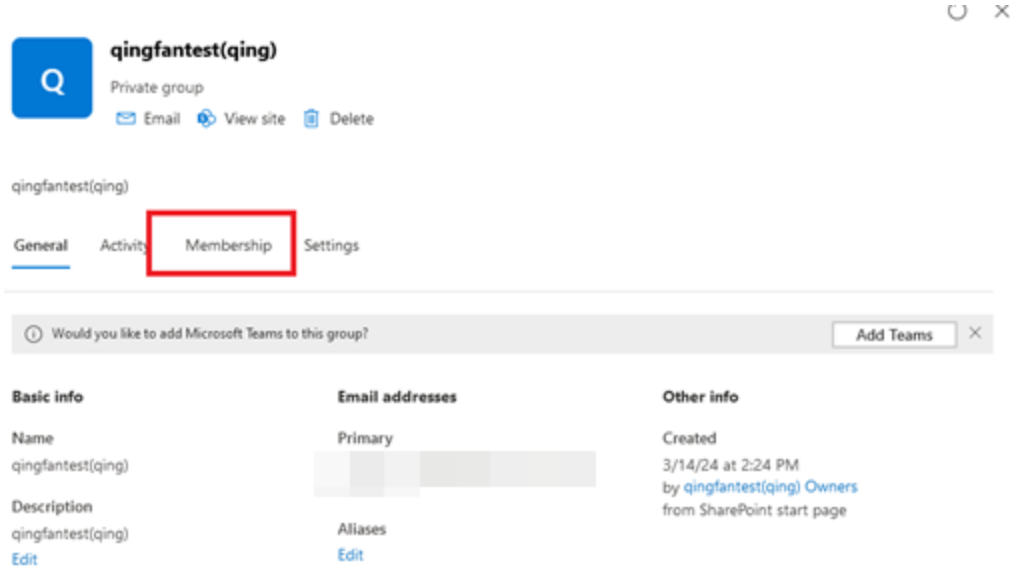
4. In **SharePoint admin center**, click on **Sites** drop down menu, and select **Active Sties**.



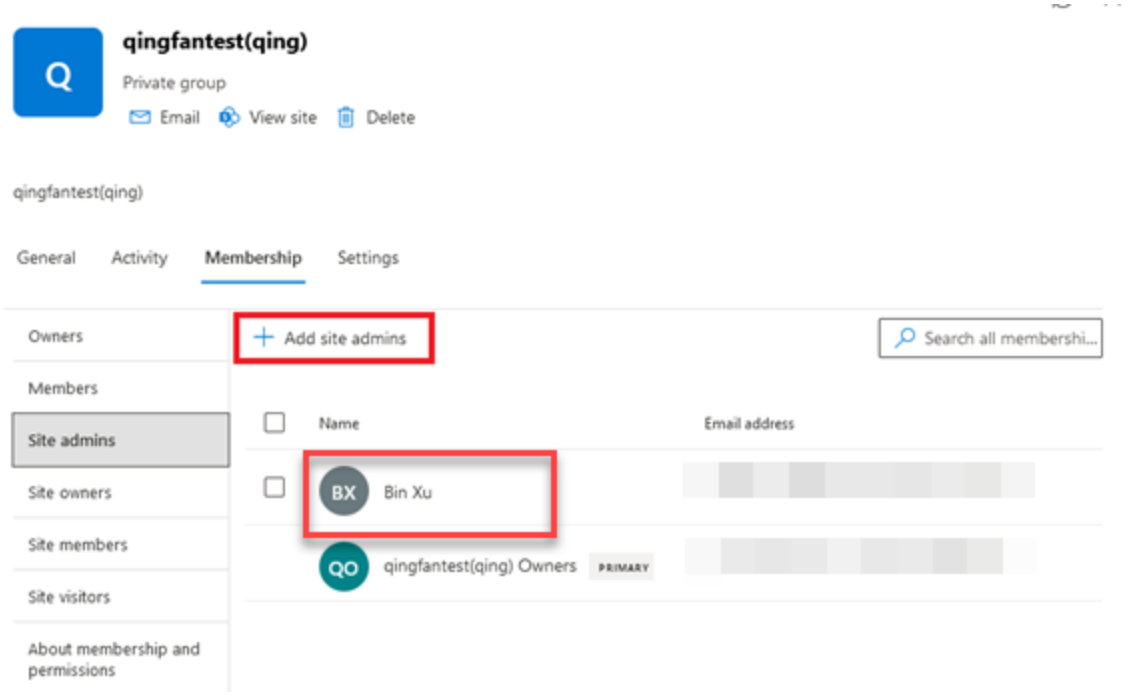
5. In **Active sties**, under **Site name** column, scroll down to look for the targeted site name.



6. Click on the **Site name**, the SharePoint site profile dialog will appear, then click **Membership** tab.



7. Click **+Add site admins** to add the Company Administrator account (the account to be added on FortiCASB) as a new site admin. In this way, FortiCASB will be able to monitor and protect the sharepoint site after the company administrator account is added to FortiCASB.



Note: If you want FortiCASB to monitor and protect other Sharepoint sites of the same domain, repeat **step 6-7** with a different Sharepoint site.

Dropbox Business

OAuth Request error

Please check the user role of the account used to log in to Dropbox Business. This account must have "Team Admin" Permissions.

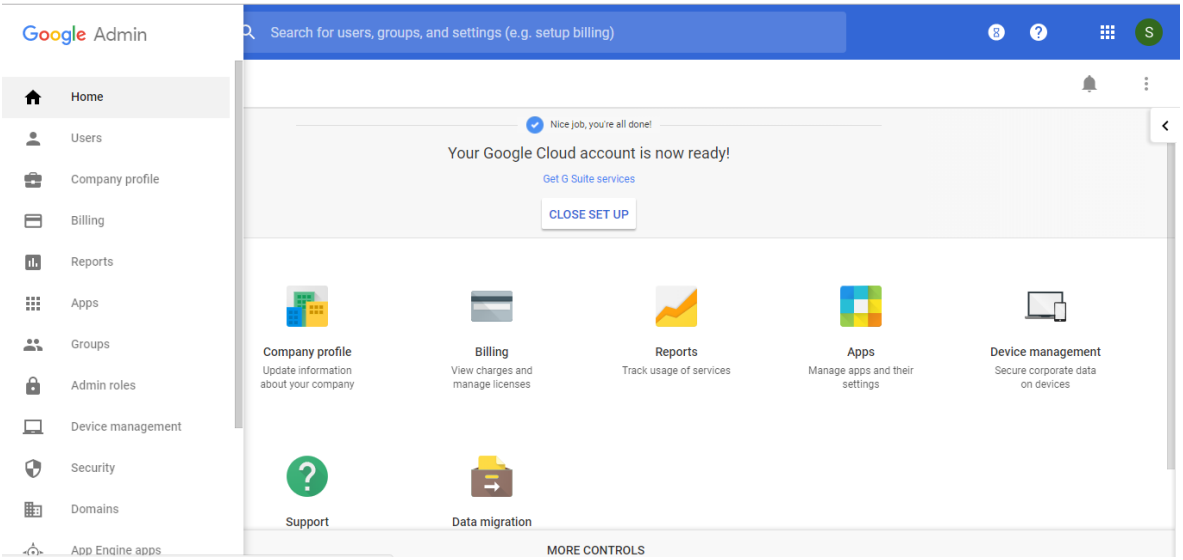
Google Workspace

Google Workspace connection errors

If FortiCASB will not connect to your Google Workspace account, one common reason is because your Google account is not a Super Administrator and does not have the correct permissions.

To check if your Google account is a Super Administrator, go to https://admin.google.com/, and log in with your Google account.

If your interface is the same as the one shown below, you are a Super Administrator.



If you are not a Super Administrator, either ask the Super Administrator to grant you Super Administrator permissions or use the Super Administrator's Google account to link to FortiCASB.

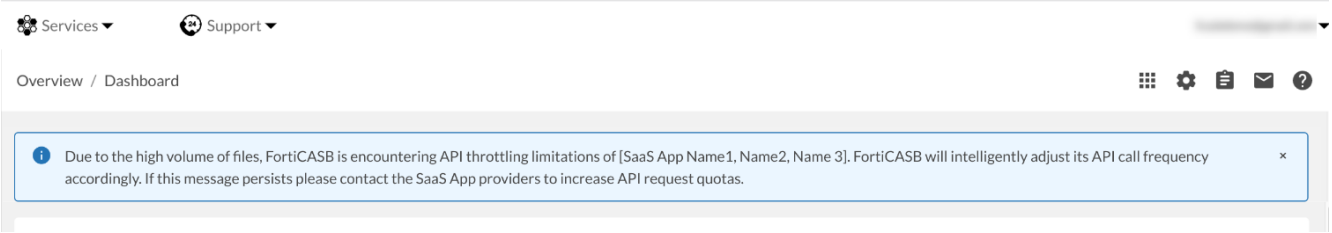
If you're unsure who your administrator is, contact your IT department, help desk, or the manager who gave you the account.

Due to Google requirements, only Google Workspace accounts with a business or enterprise license can use FortiCASB. Google Workspace accounts with a basic license will be unable to use FortiCASB.

API Throttling Limitation Message (All Apps)

For all cloud applications onboard, there is a limitation of the number of files that FortiCASB Data Scan can process at any given time.

When there are too many files uploaded to a cloud application simultaneously, the following API throttling message will appear in **Dashboard** to notify that the number of files have exceeded the number of API requests that FortiCASB can handle.



Solution

Please wait for awhile until FortiCASB adjusts its API calls' frequency or until all API calls have completed.

If the message persists, please reach out to the Cloud Application vendor to increase the API request quotas.

Appendix

Appendix A - Amazon Policy Usage

Communication between AWS and FortiCASB requires granting FortiCASB with permissions to access AWS account resource configuration settings. The method is done through creating custom policy on AWS in JSON format in AWS for .

Below are lists of the AWS services/policies used and the corresponding reasoning to be used in FortiCASB.

FortiCASB Basic Permission

Service	Policy in JSON Format	Permission Purpose
RDS	"rds:Describe*" "rds:DownloadDBLogFilePortion" "rds:ListTagsForResource"	1. FortiCASB Resource List 2. RDS profile 3. RDS Topology 4. RDS Risk assessment
	"rds:ModifyDBInstance"	1. Allow **autofix** feature of RDS Risk assessment policy "RDS instances should not be publicly accessible".
EFS	"elasticfilesystem:Describe*"	1. FortiCASB Resource List 2. EFS profile 3. EFS Risk assessment
ELB	"elasticloadbalancing:Describe*"	1. FortiCASB Resource List 2. Listener, Load Balancer, Target Group profile 3. ELB Topology 4. ELB Risk assessment
	"elasticloadbalancing:ModifyLoadBalancer Attributes"	1. Allow autofix feature of ELB Risk assessment policy "ELB/ALB deletion protection should be enabled".
Certificate Manager	"acm:List*" "acm:Describe*"	1. FortiCASB Resource List 2. ACM Certificate profile 3. ACM Certificate Risk assessment
CloudFront	"cloudfront:List*" "cloudfront:Get*"	1. FortiCASB Resource List 2. CloudFront profile

		3. CloudFront Risk assessment
	"cloudfront:UpdateDistribution"	1. Allow **autofix** feature of CloudFront Risk assessment policy "CloudFront should use secure ciphers for distribution".
EKS	"eks:ListUpdates" "eks:DescribeUpdate" "eks:DescribeCluster" "eks:ListClusters"	1. FortiCASB Resource List 2. EKS profile 3. EKS Topology
KMS	"kms:List*" "kms:Describe*" "kms:Get*"	1. FortiCASB Resource List 2. KMS Key profile 3. KMS Risk assessment
	"kms:EnableKeyRotation"	1. Allow autofix feature of KMS Risk assessment policy "KMS key rotation should be enabled".
Lambda	"lambda:List*" "lambda:GetPolicy"	1. FortiCASB Resource List 2. Lambda profile 3. Lambda Risk assessment
SQS	"sqs:ReceiveMessage" "sqs:GetQueueUrl" "sqs:GetQueueAttributes" "sqs:ListQueueTags" "sqs:ListQueues" "sqs:ListDeadLetterSourceQueues"	1. FortiCASB Resource List 2. SQS profile 3. SQS Risk assessment
	"sqs:TagQueue" "sqs:UntagQueue" "sqs:ChangeMessageVisibility "sqs:ChangeMessageVisibilityBatch" "sqs:CreateQueue" "sqs:DeleteMessage" "sqs:DeleteMessageBatch" "sqs:DeleteQueue" "sqs:PurgeQueue" "sqs:SendMessage" "sqs:SendMessageBatch" "sqs:SetQueueAttributes"	1. FortiCASB Notification’s integration with AWS SQS service
IAM	"iam:List*" "iam:SimulateCustomPolicy" "iam:GenerateCredentialReport" "iam:Get*"	1. FortiCASB Resource List 2. IAM profile 3. IAM Risk assessment

	"iam:SimulatePrincipalPolicy"	
	"iam:UpdateAccountPasswordPolicy"	1. Allow **autofix** feature of Redshift Risk assessment policy "Password requirements should be enforced".
Redshift	"redshift:Describe*"	1. FortiCASB Resource List 2. Redshift profile 3. Redshift Risk assessment
	"redshift:Describe*" "redshift:ModifyClusterParameterGroup"	1. Allow autofix feature of Redshift Risk assessment policy "Redshift database should use SSL for connections".
Elastic Container Service	"ecs:Describe*" "ecs:List*"	1. FortiCASB Resource List 2. ECS profile 3. ECS Topology
EC2	"ec2:Describe* "ec2:SearchTransitGatewayRoutes "ec2:GetTransitGatewayAttachmentPropagations "ec2:GetTransitGatewayRouteTablePropagations "ec2:GetTransitGatewayRouteTableAssociations"	1. FortiCASB Resource List 2. VPC, Route Table, Subnet, Network ACL, Security Group, Machine Image (AMI), EC2, EBS volume, EBS snapshot profile 3. VPC, Subnet, Network ACL, Security Group, EC2 Topology 4. VPC, Subnet, Security Group, AMI, EC2, EBS Risk assessment
	"ec2:ModifySnapshotAttribute" "ec2:RevokeSecurityGroupEgress "ec2:RevokeSecurityGroupIngress"	1. Allow autofix feature of EBS Risk assessment policy "EBS snapshots should not be publicly accessible". 2. Allow **autofix** feature of Security Group Risk assessment policy "Default Security Group should block all inbound traffic".
CloudWatch Logs	"logs:Get*" "logs:Describe*" "logs:FilterLogEvents"	1. Feature "Traffic" on FortiCASB
Glacier	"glacier:ListVaults" "glacier:GetVaultAccessPolicy"	1. FortiCASB Resource List 2. Glacier profile 3. Glacier Risk assessment
CloudFormation	"cloudformation:ListStack*" "cloudformation:GetTemplate" "cloudformation:DescribeStack*"	1. FortiCASB Resource List 2. CloudFormation profile 3. CloudFormation Risk assessment
S3	"s3:GetBucket*" "s3:GetReplicationConfiguration"	1. FortiCASB Resource List 2. S3 bucket profile

	"s3:GetLifecycleConfiguration" "s3:GetInventoryConfiguration" "s3:ListBucket" "s3:ListBucketMultipartUploads "s3:GetAccountPublicAccessBlock" "s3:ListAllMyBuckets" "s3:GetObjectVersion" "s3:GetObjectVersionTagging" "s3:GetObjectAcl" "s3:GetObjectVersionAcl" "s3:HeadBucket" "s3:ListMultipartUploadParts" "s3:GetObject" "s3:GetAnalyticsConfiguration "s3:GetObjectVersionForReplication" "s3:ListBucketByTags" "s3:ListBucketVersions" "s3:GetAccelerateConfiguration" "s3:GetObjectVersionTorrent" "s3:GetEncryptionConfiguration" "s3:GetObjectTagging" "s3:GetMetricsConfiguration" "s3:GetObjectTorrent"	3. S3 Risk assessment 4. Feature "Buckets" on FortiCASB
	"s3:PutBucketVersioning" "s3:PutBucketAcl" "s3:PutBucketPolicy" "s3:PutObjectAcl" "s3:PutObjectVersionAcl"	1. Allow **autofix** feature of S3 Risk assessment policy "S3 buckets should not be publicly available".
Pinpoint Email /SES	"ses:List*" "ses:Get*"	1. FortiCASB Resource List 2. SES profile 3. SES Risk assessment
CloudTrail	"cloudtrail:GetTrailStatus" "cloudtrail:LookupEvents" "cloudtrail:DescribeTrails" "cloudtrail:ListTags" "cloudtrail:GetEventSelectors"	1. FortiCASB Resource List 2. CloudTrail profile 3. CloudTrail Risk assessment 4. Feature "Activity" on FortiCASB
	"cloudtrail:StartLogging" "cloudtrail:UpdateTrail"	1. Allow **autofix** feature of CloudTrail Risk assessment policy "CloudTrail bucket should not be publicly accessible".

Elasticsearch Service	"es:List*" "es:Describe*"	1. FortiCASB Resource List 2. ElasticSearch profile 3. ElasticSearch Risk assessment
Route 53	"route53:ListTrafficPolicyVersions" "route53:GetHealthCheck" "route53:ListHostedZonesByName" "route53:GetHostedZoneCount" "route53:GetHealthCheckLastFailureReason" "route53:ListVPCAssociationAuthorizations" "route53:GetReusableDelegationSetLimit" "route53:ListTagsForResources" "route53:GetAccountLimit" "route53:GetGeoLocation" "route53:GetTrafficPolicy" "route53:ListQueryLoggingConfigs" "route53:GetCheckerIpRanges" "route53:ListGeoLocations" "route53:GetTrafficPolicyInstance" "route53:ListHostedZones" "route53:ListTagsForResource" "route53:ListHealthChecks" "route53:GetHostedZone" "route53:ListResourceRecordSets" "route53:GetHealthCheckCount" "route53:ListReusableDelegationSets" "route53:ListTrafficPolicyInstancesByHostedZone" "route53:GetHostedZoneLimit "route53:ListTrafficPolicyInstances" "route53:GetTrafficPolicyInstanceCount" "route53:GetChange" "route53:ListTrafficPolicies" "route53:GetQueryLoggingConfig" "route53:GetHealthCheckStatus" "route53:GetReusableDelegationSet" "route53:ListTrafficPolicyInstancesByPolicy"	1. FortiCASB Resource List 2. Route53 profile 3. Route53 Risk assessment
SNS	"sns:Get*" "sns:*"	1. FortiCASB Resource List 2. SQS profile 3. SQS Risk assessment
	"sns:*"	1. FortiCASB Notification's integration with AWS SNS service
CloudWatch	"cloudwatch:Describe*"	3. CloudWatch Risk assessment

Appendix B - Normalized Share Types

Introduction

Every cloud application has its own standardized share types for accessing cloud resources. The naming convention of these file sharing types are unique and platform independent.

To provide file sharing insights based on all cloud applications on board, FortiCASB normalized share types are created to standardized the share types among different cloud application platforms. Share types with similar file access permission are grouped together under a FortiCASB normalized share type.

Normalized Share Types and Associated Cloud App Share Types

FortiCASB Normalized Share Types	Cloud Application Share Types	Description	Cloud Application Supported
Editor	File collaborator, Editor, Project Editor, Edit Link Access, etc.	Any user, group, or anyone who can edit the file.	Salesforce, Office 365, Box, Dropbox, Github, Google Workspace, AWS S3, Google Cloud Storage, Egnyte
Viewer	File Viewer, Group Viewer, Project Viwer, View Link Access, etc.	Any user, group, project, who can view the file.	Salesfoce, Office 365, Box, Dropbox, Github, Google Workspace, AWS S3, Google Cloud Storage, Azure, Egnyte
Commenter	User Commenter, Group Commenter, etc.	Anyone who can make a comment on the file.	Google Workspace
Private Access	Private User, Private Team, Private Group	Any private user, group, domain that can access the file privately.	Dropbox, Azure, Egnyte
Others	Previewer, Uploader, Triager, File Recipient	Any non ordinary access to the file include but not limited to file previewer, uploader, recipient, etc.	Salesforce, Box, Google Workspace, Dropbox, Github, WebEx, Egnyte

Data Retention Policy

Data Type	Primary Storage	Secondary Storage	Data Retention with Active License	Retention period after license expired
Company and Business Unit cloud account data	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	Data will not be removed	Data will not be removed
Audit logs, admin logs, and user activities	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	Data will not be removed	Data removed after 90 days
Cloud account activities and alerts	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	1 year	Data removed after 90 days
Cloud account users metadata	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	Data will not be removed	Data removed after 90 days
Cloud file data, documents, e-mail attachments, etc.	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	Data will not be removed	Data removed after 90 days
Cloud accounts OAuth data	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	Data will not be removed	Data removed after 90 days
C-Level, Compliance reports, etc.	Encrypted and stored at AWS RDS and Elasticsearch Database	AWS RDS and Elasticsearch backup snapshots	Data will not be removed	Data removed after 90 days

End User License Agreements

Product License Agreement

The parties to this agreement are you (the end-customer) and Fortinet, Inc. ("Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS “AGREEMENT” OR “EULA”). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET’S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION

UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT, IMMEDIATELY NOTIFY FORTINET LEGAL LEGAL@FORTINET.COM OF REQUESTED EULA CHANGES.

1. License Grant.

This is a license agreement between you and Fortinet, not a sales agreement. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet’s Products which is discussed in detail in section 15 below, and the term “Software” includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non- transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms, in the event of termination, or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if (a) agreed by Fortinet in writing, (b) you are authorized by Fortinet in writing to provide managed service provider services (“MSSP”) to your end-customers, and (c) you pay for an MSSP license, then you may use the Software and/or Software embedded in Fortinet Hardware to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation (including license term restrictions), and solely on the Fortinet appliance, or, in the case of blades, CPUs, platform, devices or databases, on the single blade, CPU, platform, device or database on which Fortinet installed the Software, or, for stand-alone Software, solely on a single computer running a validly-licensed copy of the operating system for which the Software was designed unless and except set forth in the published documentation otherwise. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs, platforms, devices or databases are licensed per blade, solely for one blade and not for multiple blades that may be installed in a chassis, per CPU, per platform, per device, or per database basis, up to the blade, CPU, platform, device, database number defined in the license and as applicable and in accordance with the documentation. The Software is "in use" on any appliances, blades, CPUs, platforms, devices, or

databases when it is loaded into temporary memory (i.e. RAM), accessed, downloaded, installed, or used on an appliance, blade, CPU, platform, device, or database. You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

2. Limitation on Use.

You are prohibited from and may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to: (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner (except as expressly permitted for MSSP partners); (c) transfer assign or sublicense right to any other person or entity (except as provided in section 5): (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers; (e) use the Software to determine, or disclose the results of, any benchmarking or performance measurements; (f) interfere with a platform for use of the Software; (g) use the Software on a device not owned and controlled by you; (h) use automated means to access online portions of the platform for the Software; (i) use the Software for third- party training, commercial time-sharing or service bureau use or (except as expressly set forth in this Agreement) use the Software to provide services to third parties, (j) share non-public features or content of the software with any third party; (k) access the software in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the software, or to copy any ideas, features, functions or graphics of the software; or, (l) engage in web scraping or data scraping on or related to the software, including without limitation, collection of information through any software that simulates human activity or any bot or web crawler.

3. Proprietary Rights.

All rights (including copyrights, trade secret, patent and other intellectual property rights), title, interest in and to the Software and any Product, and any copy thereof remain with Fortinet. You acknowledge that no title or other intellectual property rights in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific limited license as expressly set forth in section 1 (“License Grant”) above. You expressly agree and acknowledge that Fortinet owns, retains, and shall retain all intellectual property rights in and to, and you have no intellectual property rights in and to, the Products and the Software other than the License Grant. You agree to keep confidential all Fortinet confidential information and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

The term of the license is the shorter of (a) the term as set forth in the ordering documents, other Fortinet documentation, or per Fortinet practices or policies (such as with evaluation or beta licenses or subscription or other term licenses) and (b) for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement or for other reasons as stated in Fortinet’s other documentation. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet.

5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (i) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products and Services, you are not authorized to sell Product(s), Software or Services, but, regardless, by selling Product(s), Software or Services, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receive a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way. Fortinet's license, warranty, and support is only available for Products that you purchased directly from an authorized Fortinet channel partner. Products not purchased from an authorized Fortinet channel partner are not eligible, will not be supported, and may be blocked from registration.

6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website, https://support.fortinet.com, or such other website as provided by Fortinet, or for which the warranty otherwise starts according to Fortinet's policies, and any support is only valid for products properly purchased through authorized distributors and resellers. The warranty periods discussed below will start according to Fortinet's policies posted at http://www.fortinet.com/aboutus/legal.html or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end

user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products. Fortinet warrants that the hardware portion of the Products ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): (a) a three hundred sixty-five (365) day limited warranty for the Hardware products; (b) for FortiAP, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware; (c) for FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de- installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an

identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that Software as initially shipped by Fortinet will substantially conform to Fortinet's then-current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non- conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term “functional

specifications” means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCUSSED ABOVE DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTITOKEN WHICH HAS A 365 DAY WARRANTY FROM THE DATE OF SHIPMENT FROM FORTINET’S FACILITIES, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE, AND FORTINET DISLAIMS LIABILITY REGARDING YOUR WEB BROWSER’S REQUIREMENTS OR ANY THIRD PARTY DEVICE OR APPLIANCE USED TO OPERATE THE SOFTWARE.

The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee; or (e) is procured from a non- authorized reseller or non-authorized distributor. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided “as-is” without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user’s use of evaluation or beta Software or Product is limited to thirty

(30) days from original shipment unless otherwise agreed in writing by Fortinet. For clarity, notwithstanding anything to the contrary, all sales are final and no provision in this EULA entitles you to return Products, other than as expressly set forth herein.

8. Governing Law.

Any disputes arising out of this Agreement or Fortinet’s limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet’s limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable, and agree that any controversy or claim arising out of or relating to this Agreement shall be determined in the federal and state courts located in Santa Clara County, California, as applicable.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE- INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS, AT FORTINET’S SOLE AND ABSOLUTE DISCRETION: REPAIR, REPLACEMENT, OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE; PROVIDED, HOWEVER, IN NO EVENT SHALL ANY END-CUSTOMER REMEDIES UNDER THIS EULA AND ANY SUPPORT AGREEMENT EXCEED THE AMOUNT PAID TO FORTINET FOR THE SPECIFIC APPLICABLE DEFECTIVE OR NON-CONFORMING PRODUCT AT ISSUE.

10. Compliance with Laws, including Import/Export Laws and FCPA.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see https://www.bis.doc.gov. Fortinet assumes no responsibility or liability for your failure to obtain any necessary import and export approvals and licenses, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation.

You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by

regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you hereby agree that, for any orders that you place with Fortinet whereby any legal or regulatory requirements may apply to Fortinet such as requirements related to the International Traffic in Arms Regulations, or Buy American Act, or the Trade Agreements Act: you are responsible to ensure the Purchase Order submitted to Fortinet by you and/or any partners clearly states the specific requirement in writing, or otherwise Fortinet is not bound by any such requirements. You represent that you understand, and you hereby agree to comply with, all applicable laws including but not limited to the U.S. Foreign Corrupt Practices Act . You represent that you hereby agree that you and your employees have not accepted, and will not accept, anything of value, including money, meals, entertainment, paid-for travel, beta, testing, evaluation, donation or free Products and/or related services, or anything else of value, in exchange for Fortinet maintaining current business or for new business opportunities. You represent and warrant to Fortinet that you and your employees, consultants, agents and representatives will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. You agree you and your employees will be responsible to comply in full with all laws and policies applicable to any and all dealings with Fortinet in general and its distributors, resellers and partners.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 (“Transfer”) above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agreement to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet’s General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions. Notwithstanding anything to the contrary, this EULA constitutes the entire agreement between Fortinet and its end-customers and supersedes any and all prior representations or conflicting provisions, such as limitations of liability, warranties, or otherwise in any and all purported end customer agreements, whether entered into now or in the future. In the event of a conflict between this EULA and another agreement, this EULA shall prevail unless the conflicting agreement expressly states that it replaces this EULA, expressly referring to this EULA, and is agreed to in writing by authorized representatives of the parties (which, in the case of Fortinet, is Fortinet’s General Counsel).

14. Privacy.

You agree to Fortinet’s collection, use, disclosure, protection and transfer of your information, as set forth in the Fortinet privacy policy on the Fortinet web site (http://www.fortinet.com/about-us/privacy.html), including (a) Fortinet’s use of the Customer information to send information regarding Fortinet products and services; and (b) Fortinet’s disclosure of your information to provide assistance to law enforcement, governmental agencies and other authorities or to allow Fortinet to protect its Customers’ and/or end users’ rights.

15. Open Source Software.

Fortinet’s products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public

License, Version 2, of June 1991 (“GPL”) or GNU Lesser General Public License, Version 2.1, of February 1999 (“LGPL”) or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify any Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete

machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US $25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. To receive the modified software modules, you must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules “AS-IS” without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may obtained by contacting Fortinet’s Legal Department at legal@fortinet.com.