FORTINET

DEFINE • DESIGN • **DEPLOY**

FortiCASB

Deployment Guide

Version 21.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 24, 2022
FortiCASB 21.4 Deployment Guide
00-214-838645-20221024

TABLE OF CONTENTS

Change log

Date	Change Description
2022-09-16	Initial release.
2022-09-30	Added Deployment procedures for Google Workspace on page 16.
2022-10-24	Updated Deployment procedures for Google Workspace on page 16 and subtopics.

Deployment overview

This document is a deployment guide for Fortinet's Cloud Access Security Broker (FortiCASB).

This guide is intended to guide you through basic setup and deployment of a cloud workload on FortiCASB for monitoring user access and day-to-day operations. This guide uses Google Workspace and Microsoft Office 365 as the example cloud workloads or applications to illustrate this process.

FortiCASB's goal is to act as a mediator between the cloud provider and the user to implement preconfigured or customized security policies of the organization on cloud application usage.

FortiCASB offers an API-based approach by obtaining data directly from SaaS cloud applications using REST API queries with OAuth2.0 authentication. Therefore, FortiCASB can essentially perform deep inspection of cloud traffic, providing advanced monitoring, analysis, and reporting providing notifications when suspicious activity is triggered.

Since FortiCASB performs out-of-band communication with SaaS applications, there is no performance impact on user SaaS application traffic.

FortiCASB provides insights on suspicious activity on past and current cloud user activity and relies on the network administrator to review and act upon these insights after they have occurred.

Audience

Cloud security administrators and auditors should find this guide helpful for setting up FortiCASB with cloud workloads.

About this guide

This deployment guide describes steps in deploying one type of cloud application or workload on FortiCASB, namely, Google Workspace and Microsoft Office 365. First evaluate your organization workload to determine whether this deployment guide suits your organization's needs. Reviewing the FortiCASB online help is recommended for deploying other cloud applications or workloads and related configurations.

Product prerequisites

FortiCASB requires users to have active FortiCloud accounts with valid subscriptions. Depending on the Fortinet product subscription you have, your Fortinet subscription may already support a FortiCASB subscription.

FortiCASB supports the following SaaS cloud application platforms:

- AWS S3
- Azure Storage
- Box

- Citrix ShareFile
- Confluence
- Dropbox Business
- Egnyte
- Facebook Workplace
- GitHub
- Google Cloud Storage
- Google Workspace
- Jira
- Microsoft Office 365
- Salesforce
- SAP IAS
- SAP SuccessFactors
- ServiceNow
- Webex Teams
- Zendesk
- Zoom

FortiCASB can simultaneously onboard and provide security monitoring for multiple SaaS applications. This guide has selected the Google Workspace and Office365 workloads as the examples.

For instructions on deploying other SaaS cloud applications, see Add Cloud Application.

Basic setup

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

FortiCASB account permissions can one of the following levels:

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

If you are an administrator, continue to First time setup on page 8.

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 13.

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

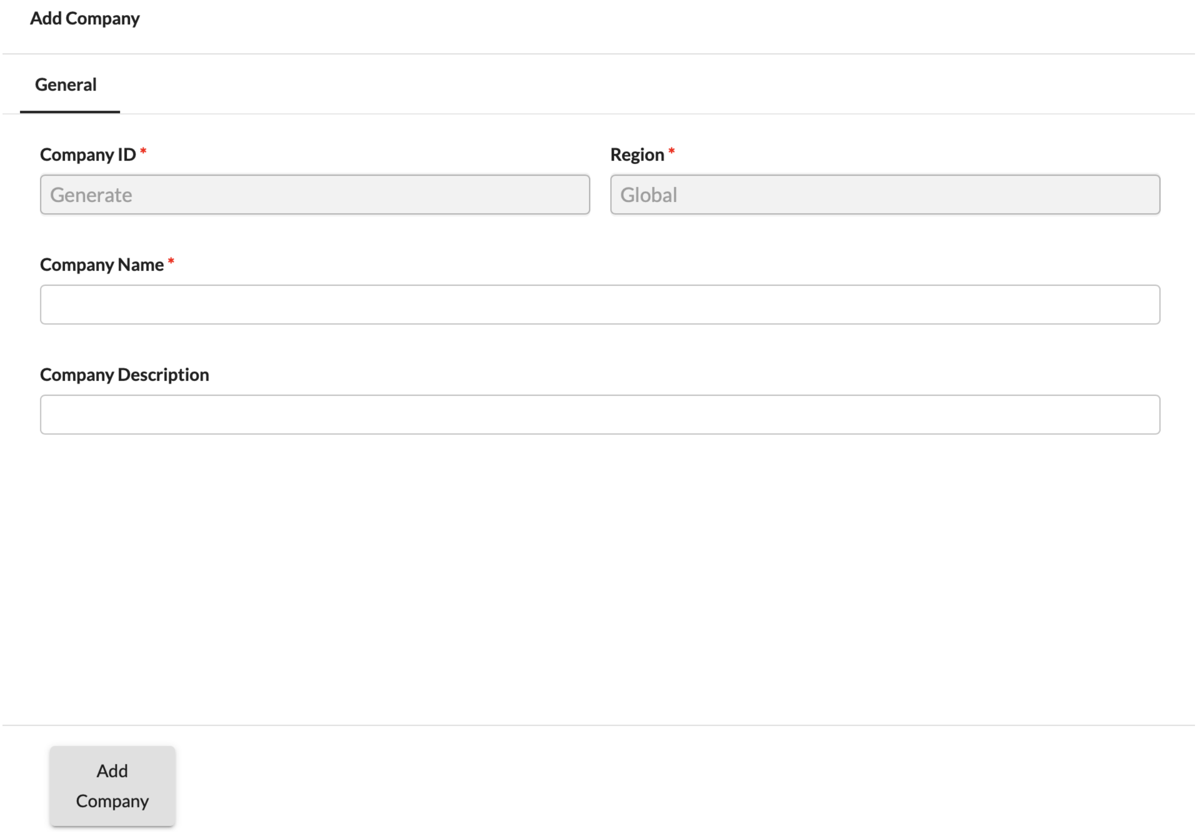
To set up your FortiCASB for the first time, you or your organization must have the following in place:

- Valid FortiCASB license. Contact your primary Fortinet service provider to obtain a license if you do not already have one.
- Administrator with a **primary FortiCloud account** to add your company, business units, and users in FortiCASB.

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

To complete first time setup:

1. Go to https://www.forticasb.com/.
2. Click **Login**. You are 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 the 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.



Add Company

General

Company ID *: Generate

Region *: Global

Company Name *

Company Description

After a company is created, go to Add a business unit on page 9 to create business unit(s).

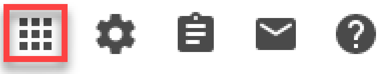
If you have a popup blocker, it blocks the FortiCASB GUI.
Set an exception for the FortiCASB GUI, or open the GUI manually.

Add a business unit

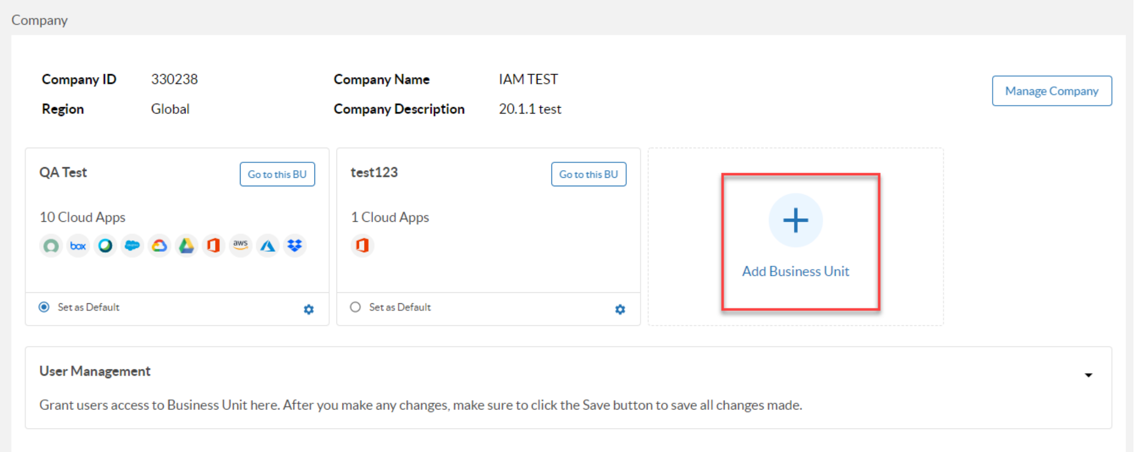
After creating a company, log into FortiCASB to add a business unit.

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.



Company

Company ID 330238 **Company Name** IAM TEST

Region Global **Company Description** 20.1.1 test

Manage Company

QA Test — Go to this BU

10 Cloud Apps

● Set as Default

test123 — Go to this BU

1 Cloud Apps

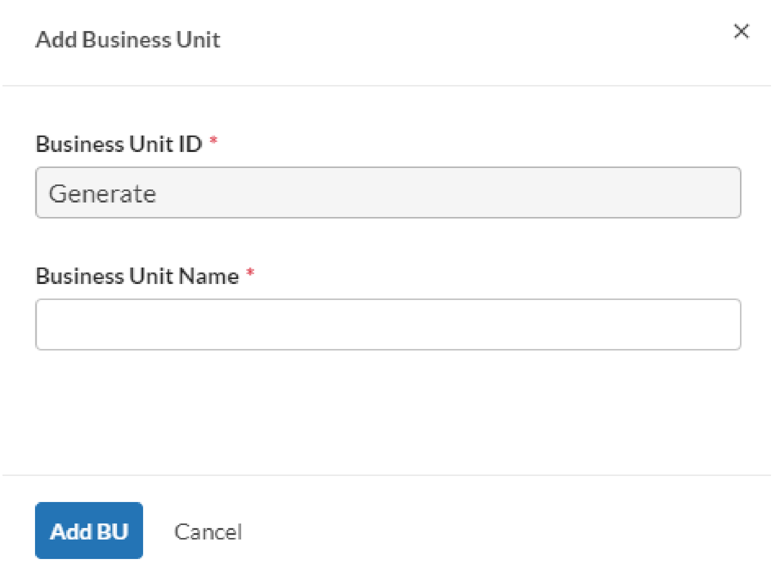
○ Set as Default

+ Add Business Unit

User Management

Grant users access to Business Unit here. After you make any changes, make sure to click the Save button to save all changes made.

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



Add Business Unit

Business Unit ID *

Generate

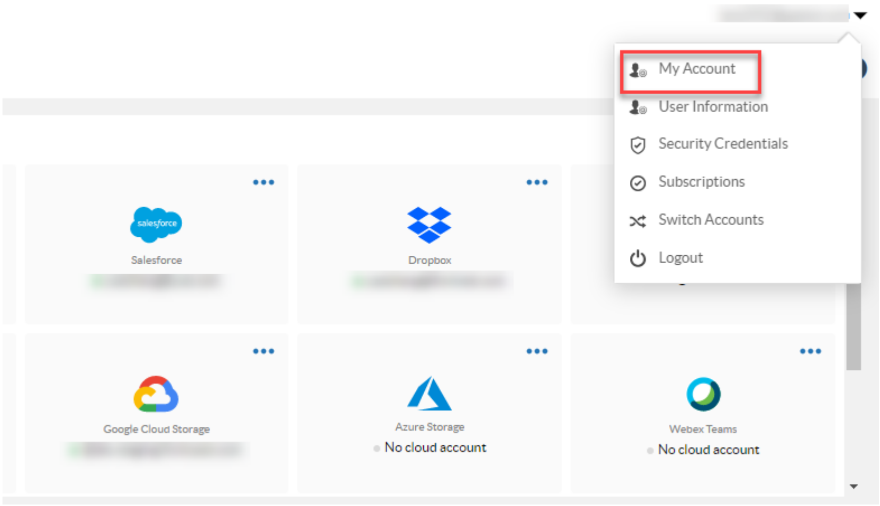
Business Unit Name *

Repeat this process to add additional business units if applicable.

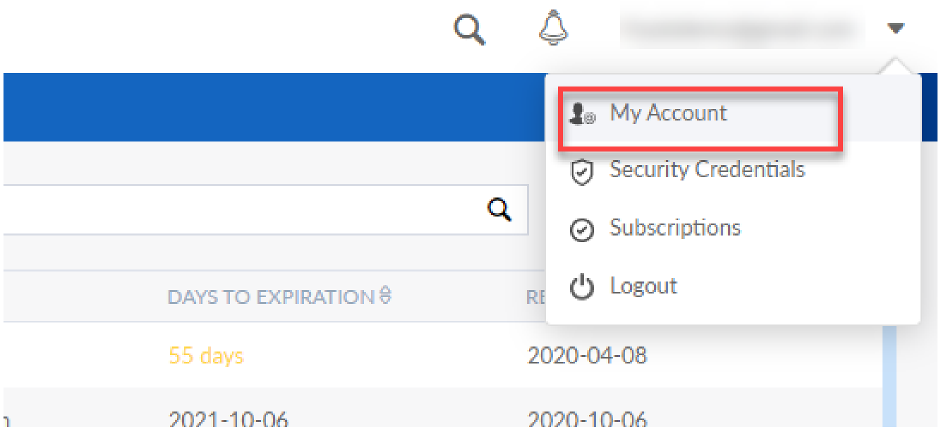
Create a business user

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

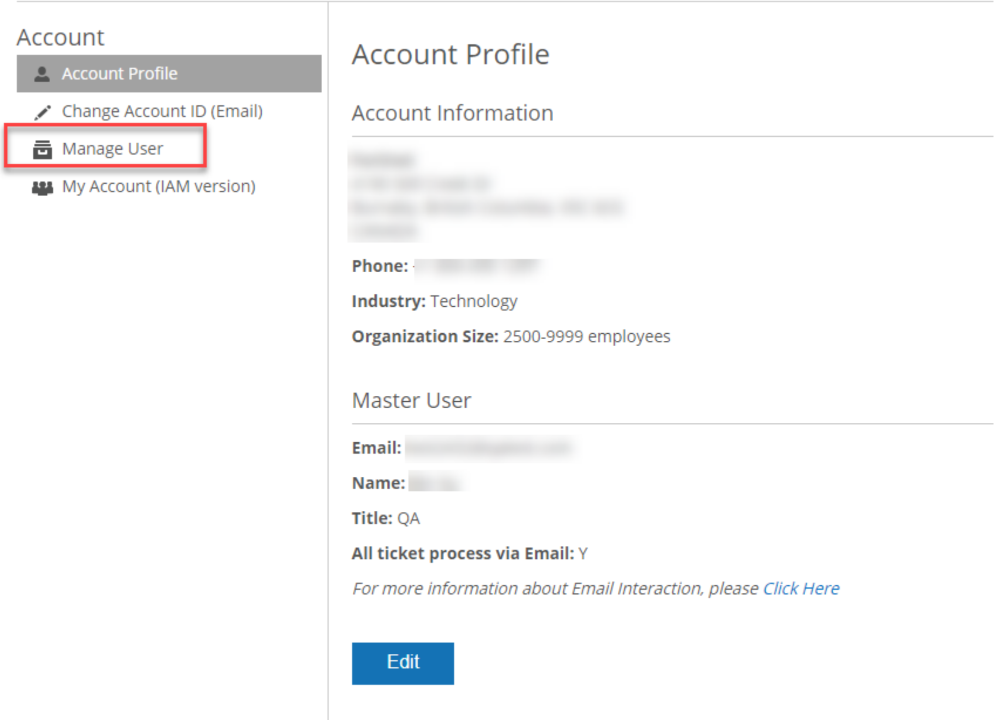
1. Log into FortiCloud: https://support.fortinet.com.
   (Alternatively, you can access FortiCloud after you log into FortiCASB by clicking the account drop down menu button at the right hand side and select **My Account**.)



2. Click on **Account Management** drop down menu and select **My Account**, then you will be re-directed to **FortiCloud**.



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



Account Profile

Account Information

[redacted]

Phone: [redacted]

Industry: Technology

Organization Size: 2500-9999 employees

Master User

Email: [redacted]

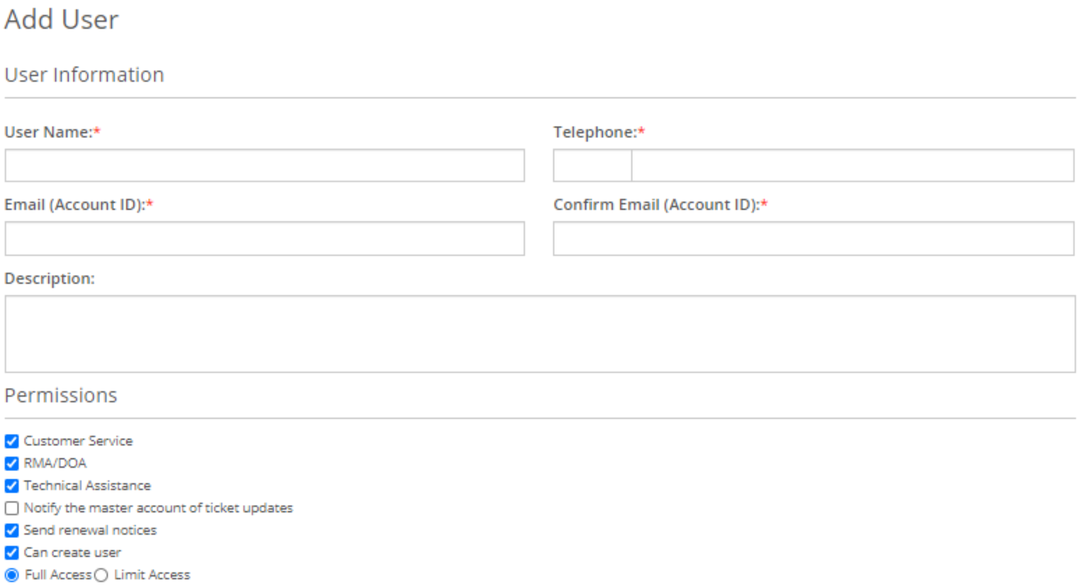
Name: [redacted]

Title: QA

All ticket process via Email: Y

For more information about Email Interaction, please Click Here

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



Add User

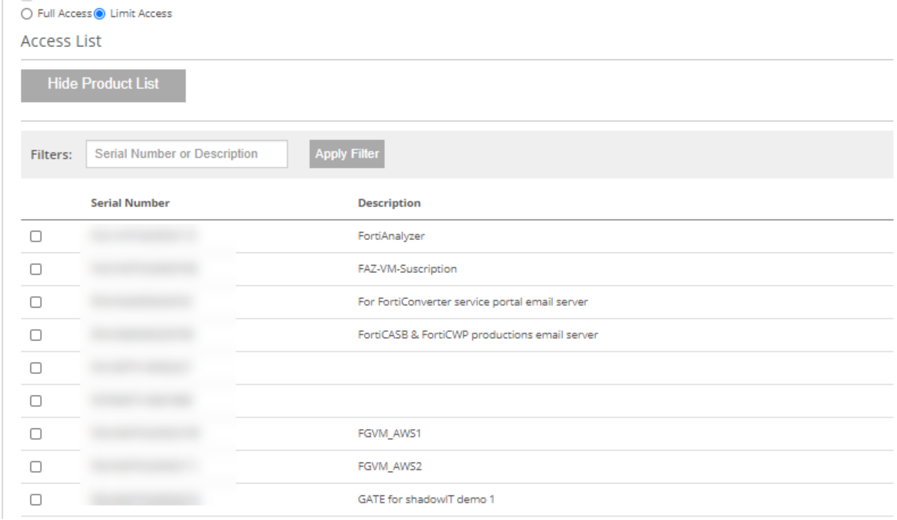
User Information

User Name:*	Telephone:*
Email (Account ID):*	Confirm Email (Account ID):*
Description:	

Permissions

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

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



○ Full Access ● Limit Access

Access List

Filters: Serial Number or Description

	Serial Number	Description
☐	[redacted]	FortiAnalyzer
☐	[redacted]	FAZ-VM-Suscription
☐	[redacted]	For FortiConverter service portal email server
☐	[redacted]	FortiCASB & FortiCWP productions email server
☐	[redacted]	
☐	[redacted]	
☐	[redacted]	FGVM_AWS1
☐	[redacted]	FGVM_AWS2
☐	[redacted]	GATE for shadowIT demo 1

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

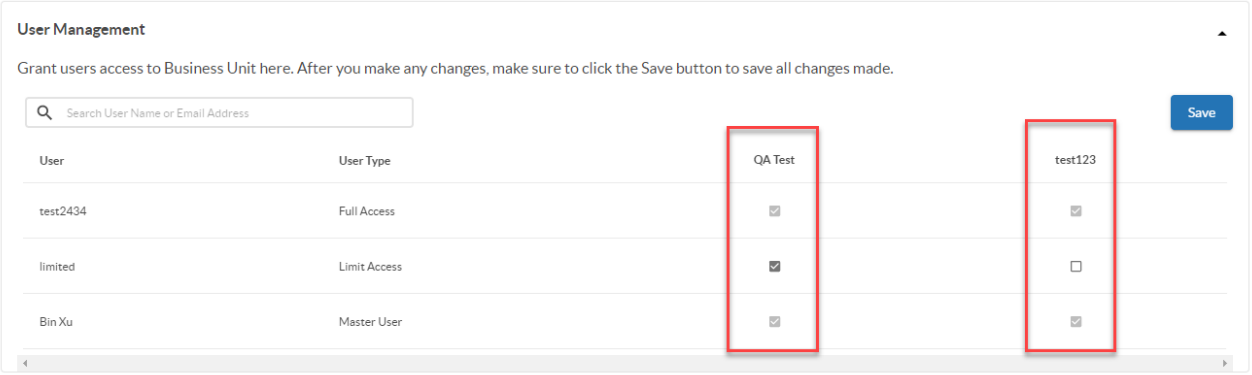
After business user(s) are created, you may assign the new users to the business units through Assign users to a business unit on page 12.

Assign users to a business unit

After you create business users on FortiCloud, they 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: https://www.forticasb.com with your primary FortiCloud account.
2. At the **FortiCASB Dashboard**, click **Company** in 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.



User Management

Grant users access to Business Unit here. After you make any changes, make sure to click the Save button to save all changes made.

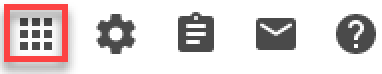
User	User Type	QA Test	test123
test2434	Full Access	☑	☑
limited	Limit Access	☑	□
Bin Xu	Master User	☑	☑

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

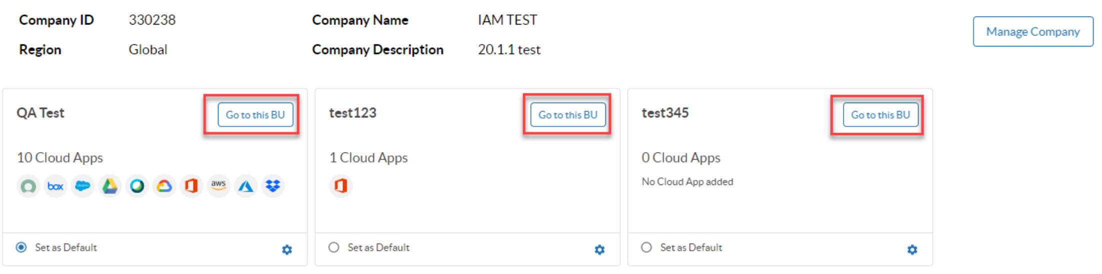
Switch between business units

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 (https://www.forticasb.com), 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**.



Company ID	330238	Company Name	IAM TEST
Region	Global	Company Description	20.1.1 test

QA Test — Go to this BU
10 Cloud Apps
● Set as Default

test123 — Go to this BU
1 Cloud Apps
○ Set as Default

test345 — Go to this BU
0 Cloud Apps
No Cloud App added
○ Set as Default

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.

Deployment plan

The high-level FortiCASB deployment plan seeks to achieve the security goals of monitoring, analyzing, and reporting on suspicious user activity, threats, and policy compliance for SaaS cloud applications using API-based deep inspection.

To deploy the FortiCASB solution, configure the following features in the following order:

1. Provision your FortiCASB instance by adding a company and set the region where to host your FortiCASB instance.
2. Add business units, create business users, and assign users to business units.
3. Add cloud applications to a business unit. This step contains additional steps and varies for each cloud application.
4. Configure policies to trigger alerts.
5. Configure notification settings.
6. Activate alert reports.
7. Activate activity reports.

Post-deployment verification and analysis procedures include using FortiCASB Dashboard, Discovery, Documents, Alerts, and Activity features to verify that FortiCASB is monitoring the configured cloud application and to analyze cloud application data and activity.

Deployment procedures for Google Workspace

In this example, FortiCASB utilizes an 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 utilizes 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.

For instructions on deploying other SaaS cloud applications, see Add Cloud Application.

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 Administrator, see Google Workspace connection errors.

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 three prerequisite steps you need to setup your Google Workspace account before you can add the Google Workspace account on FortiCASB. Please follow the steps below.

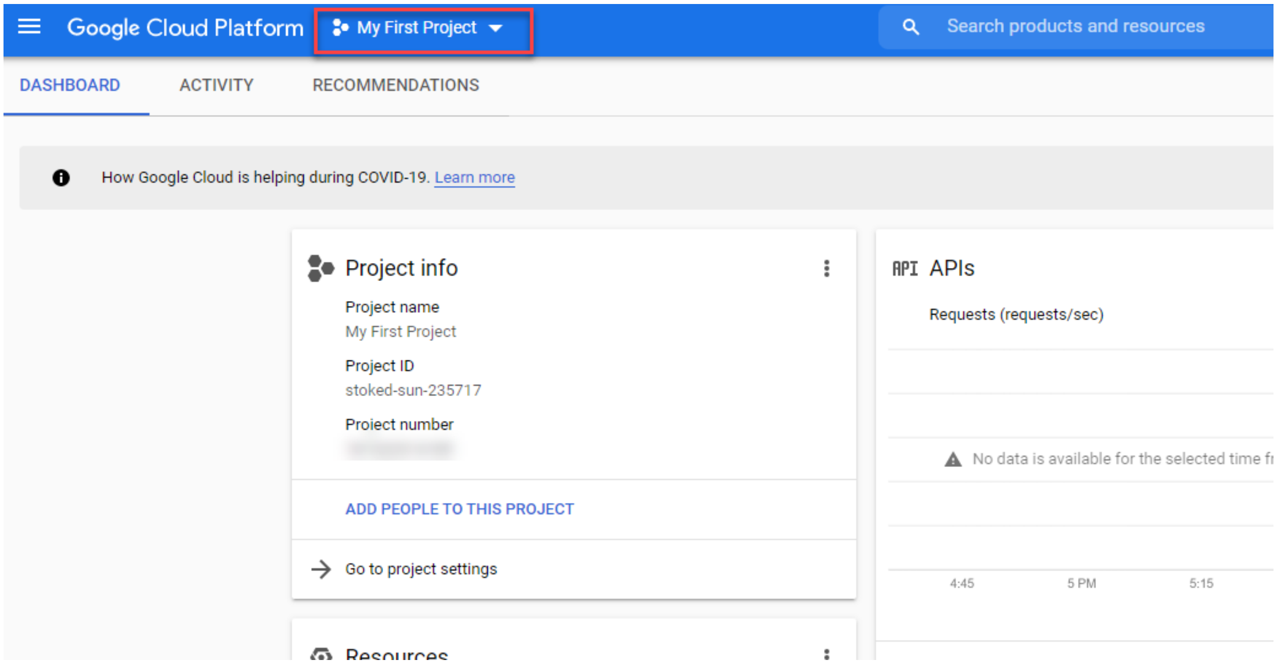
Configure OAuth Consent Screen

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 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**.



How Google Cloud is helping during COVID-19. Learn more

Project info

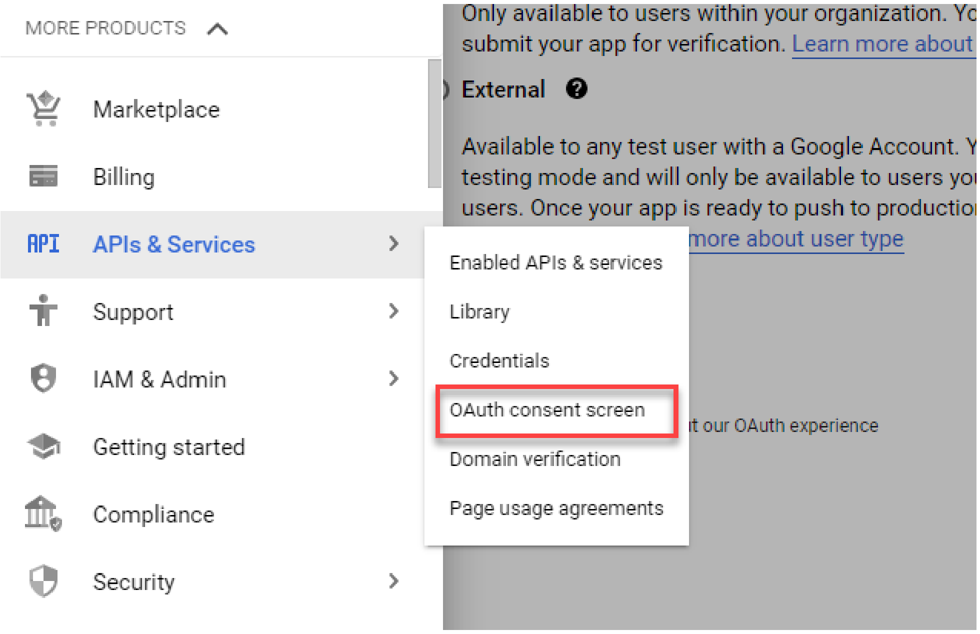
Project name
My First Project

Project ID
stoked-sun-235717

Project number
[redacted]

No data is available for the selected time fr

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



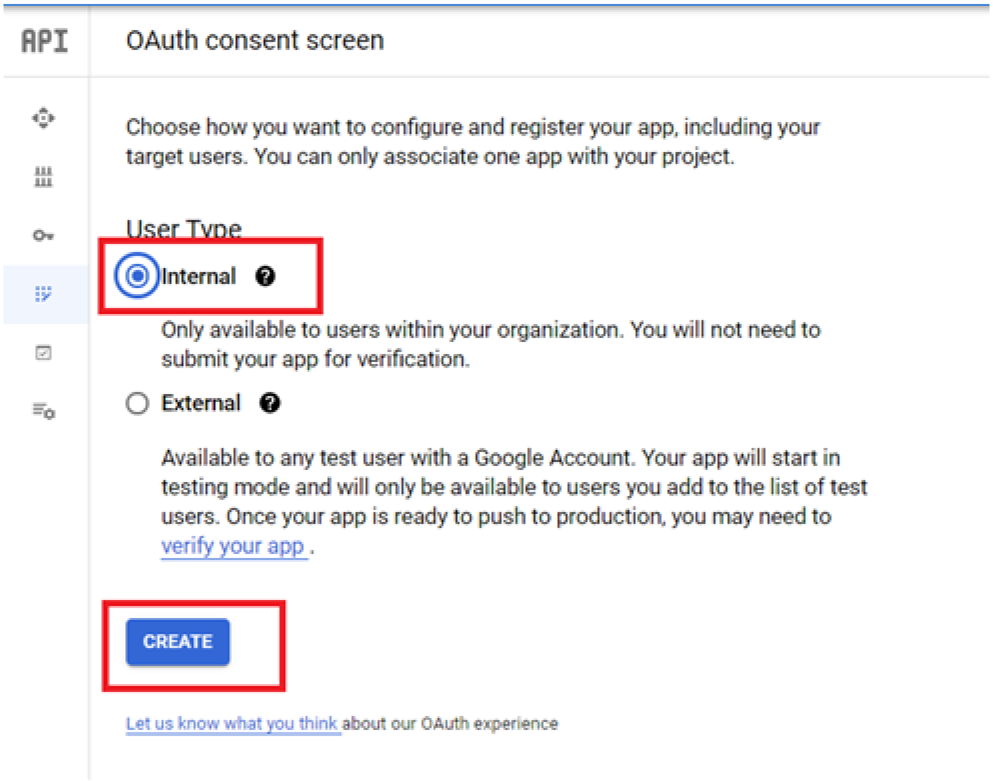
Only available to users within your organization. Yo
submit your app for verification. Learn more about

External

Available to any test user with a Google Account. Y
testing mode and will only be available to users yo
users. Once your app is ready to push to productio
more about user type

t our OAuth experience

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



API

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

● Internal

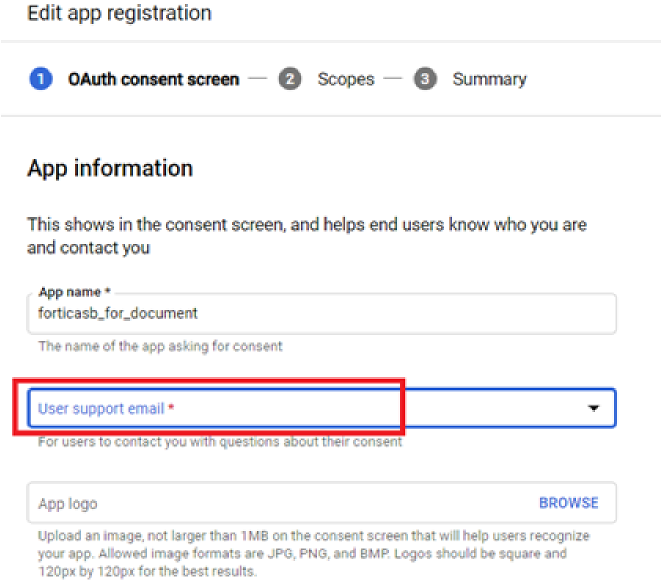
Only available to users within your organization. You will not need to submit your app for verification.

○ External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app .

Let us know what you think about our OAuth experience

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



Edit app registration

App information

This shows in the consent screen, and helps end users know who you are and contact you

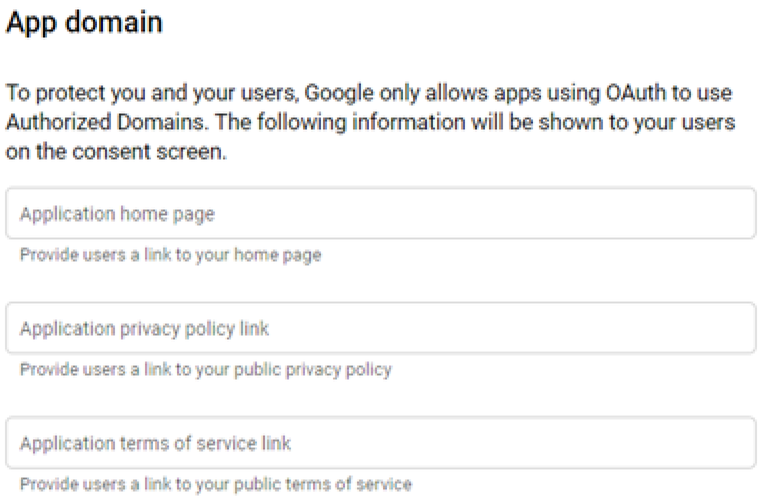
App name *
forticasb_for_document
The name of the app asking for consent

User support email *
For users to contact you with questions about their consent

App logo

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

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



App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

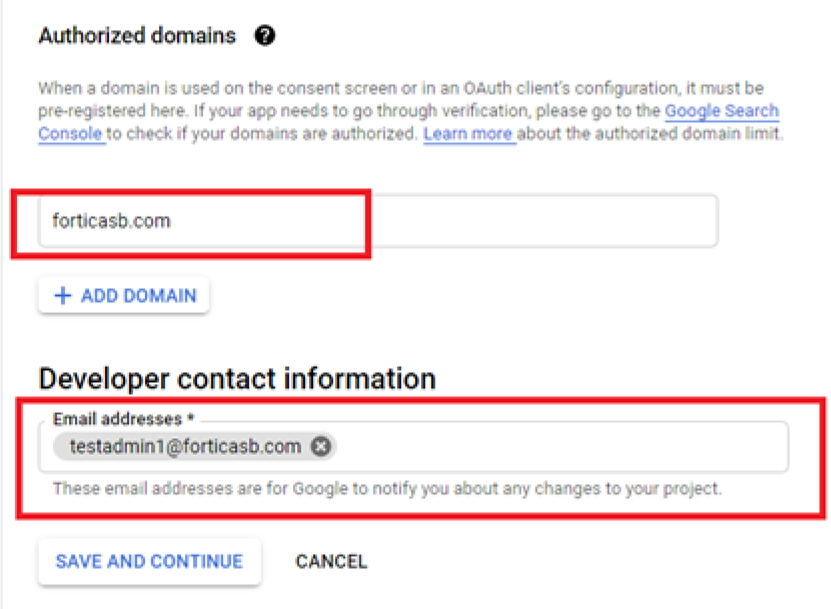
Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

c. Click **+ADD DOMAIN** and enter the domain of this Google Workspace account.
   For example, if the Google Workspace account email address is security_admin@microsoft.com, then the domain is microsoft.com.



Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the Google Search Console to check if your domains are authorized. Learn more about the authorized domain limit.

forticasb.com

Developer contact information

Email addresses *

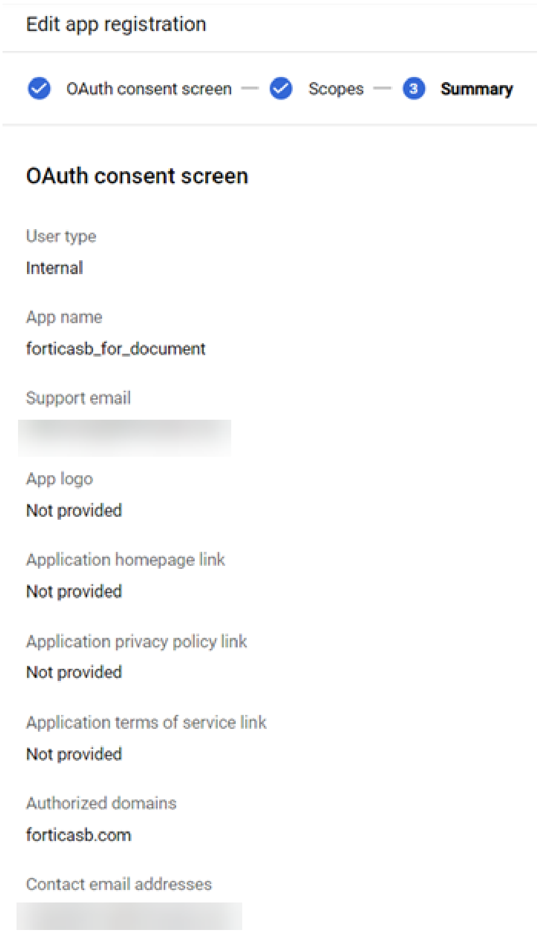
testadmin1@forticasb.com

These email addresses are for Google to notify you about any changes to your project.

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

e. Click **SAVE AND CONTINUE**.

6. In the **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

User type
Internal

App name
forticasb_for_document

Support email
[redacted]

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
[redacted]

Create Google Service Account

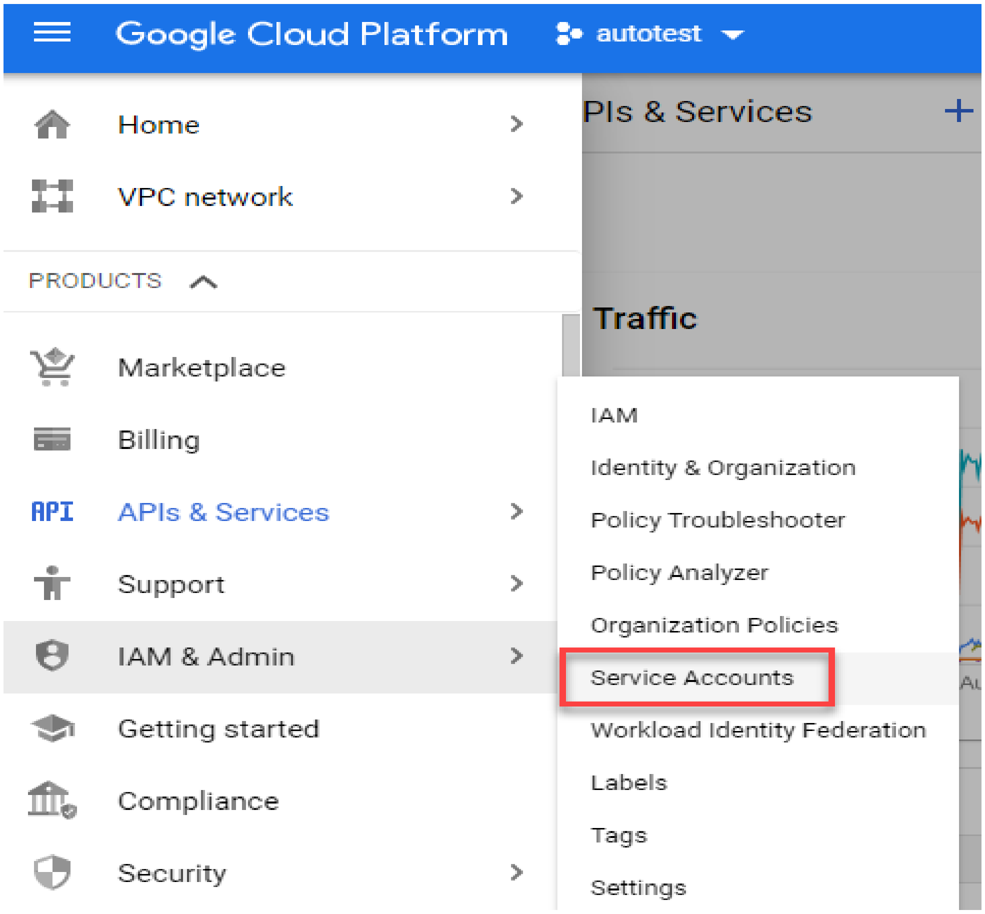
A **service account** created for the Google Workspace account is required to add the account to FortiCASB. The service account needs to be created in the project that has **OAuth Consent Screen** created to activate **Google Workspace Domain-Wide Delegation**. Google Workspace Domain-Wide Delegation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

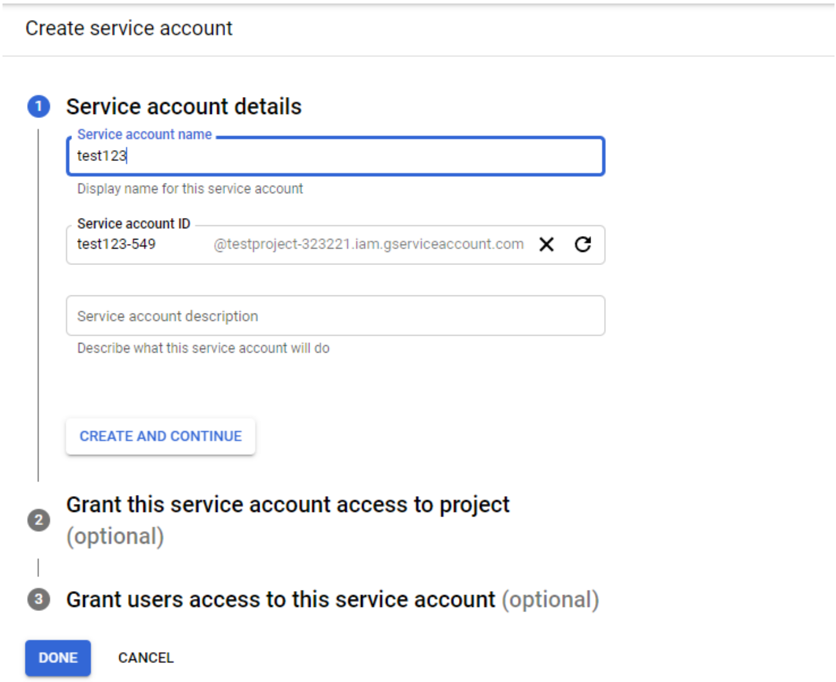
For more information regarding service accounts and domain-wide authority delegation, go to: https://developers.google.com/identity/protocols/OAuth2ServiceAccount#delegatingauthority

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, click **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**.



Create service account

1 Service account details

Service account name: test123

Display name for this service account

Service account ID: test123-549 @testproject-323221.iam.gserviceaccount.com

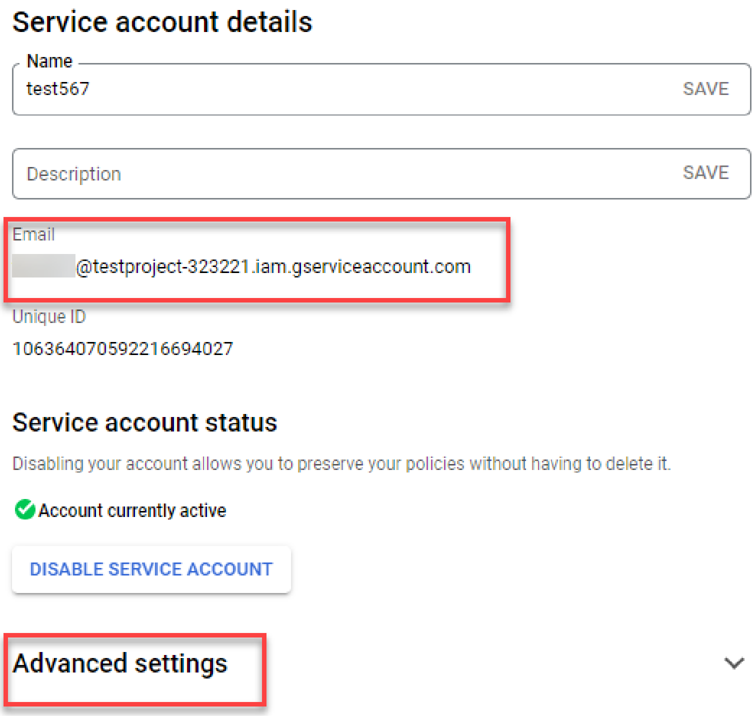
Service account description

Describe what this service account will do

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

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)**.



Service account details

Name: test567

Description

Email

[redacted]@testproject-323221.iam.gserviceaccount.com

Unique ID

106364070592216694027

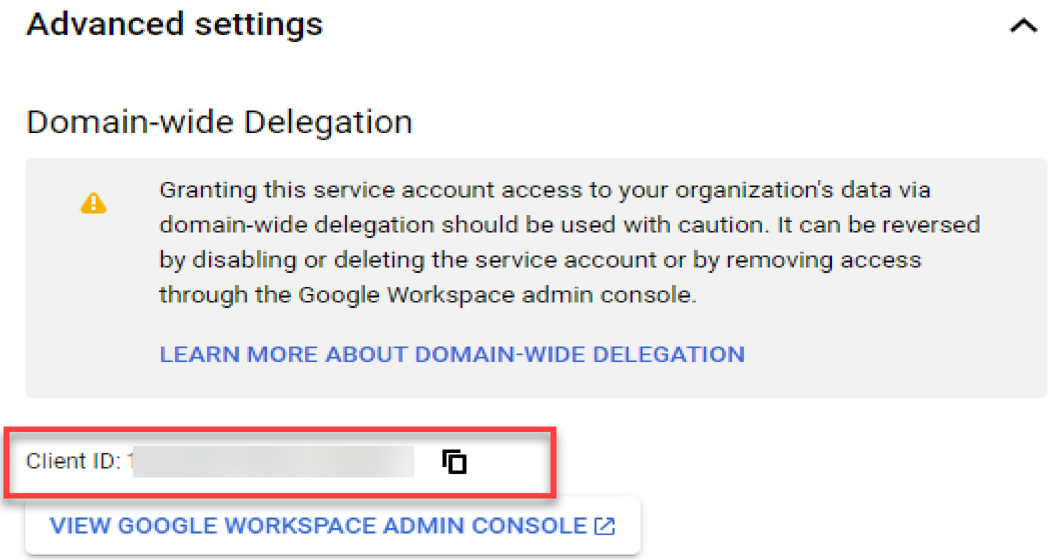
Service account status

Disabling your account allows you to preserve your policies without having to delete it.

✓ Account currently active

Advanced settings

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 24.



Advanced settings

Domain-wide Delegation

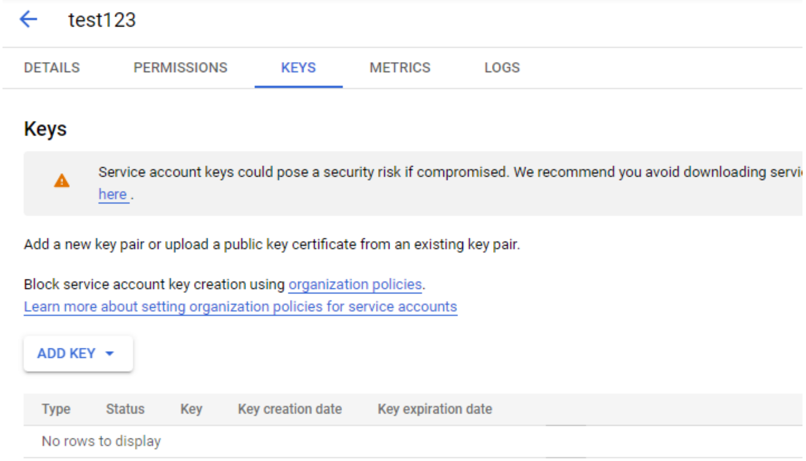
Granting this service account access to your organization's data via domain-wide delegation should be used with caution. It can be reversed by disabling or deleting the service account or by removing access through the Google Workspace admin console.

LEARN MORE ABOUT DOMAIN-WIDE DELEGATION

Client ID: 1[redacted]

VIEW GOOGLE WORKSPACE ADMIN CONSOLE

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.



Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading servi
here .

Add a new key pair or upload a public key certificate from an existing key pair.

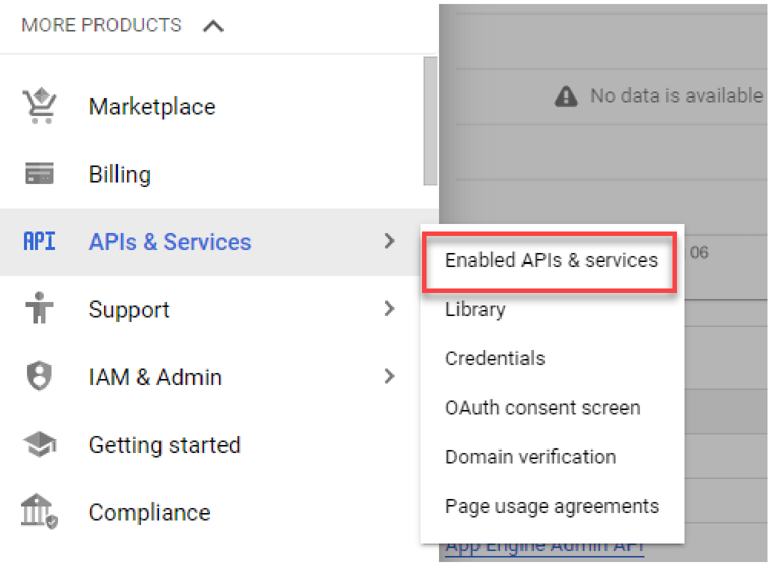
Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

Type	Status	Key	Key creation date	Key expiration date
No rows to display				

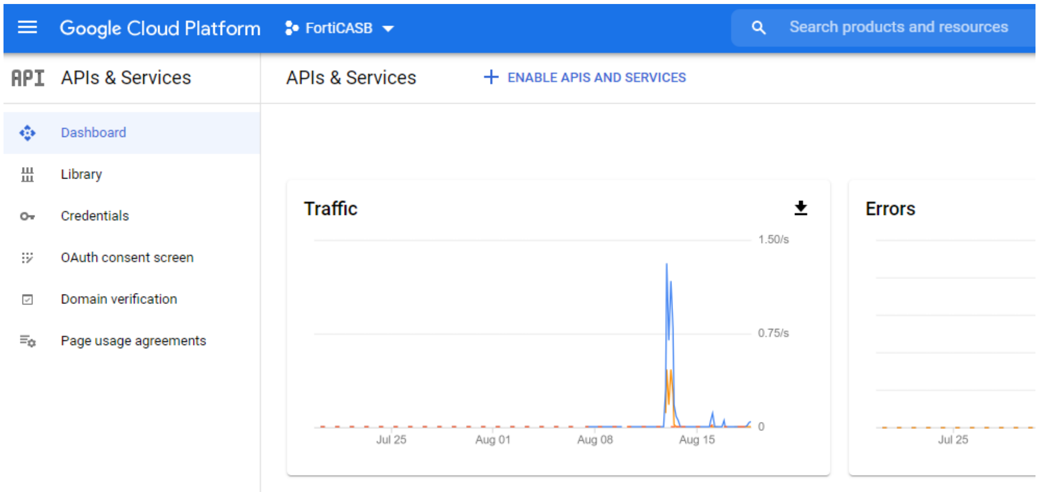
Keep the **Service Account ID** and **P12 private key** later for Google Workspace authentication during installation.
The **Client ID** will be used later in Enable Google Drive API & Authorize Client ID on page 24.

Enable Google Drive API & Authorize Client ID

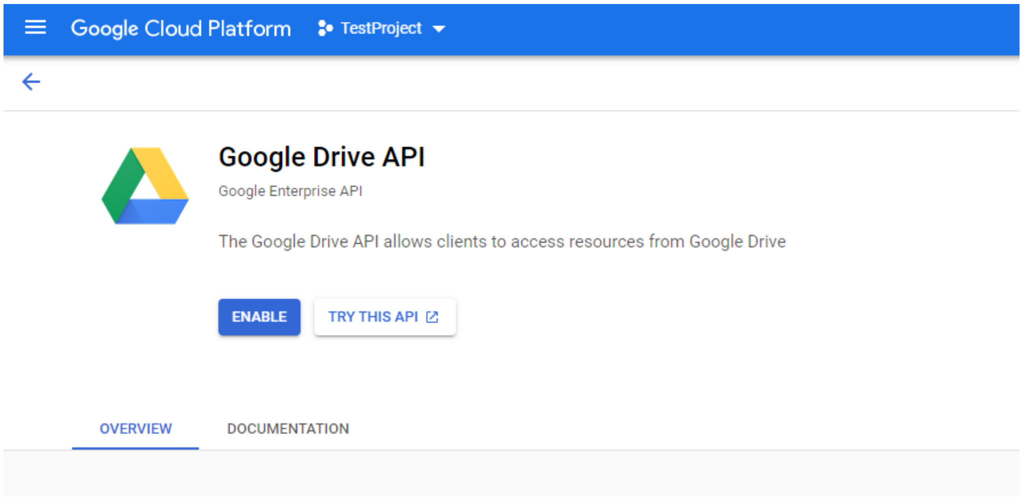
1. In Google Cloud Platform portal, select the same project as where the Service Account was created.
2. Go to **Navigation Menu > APIs & Services > Enabled APIs & services.**



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



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

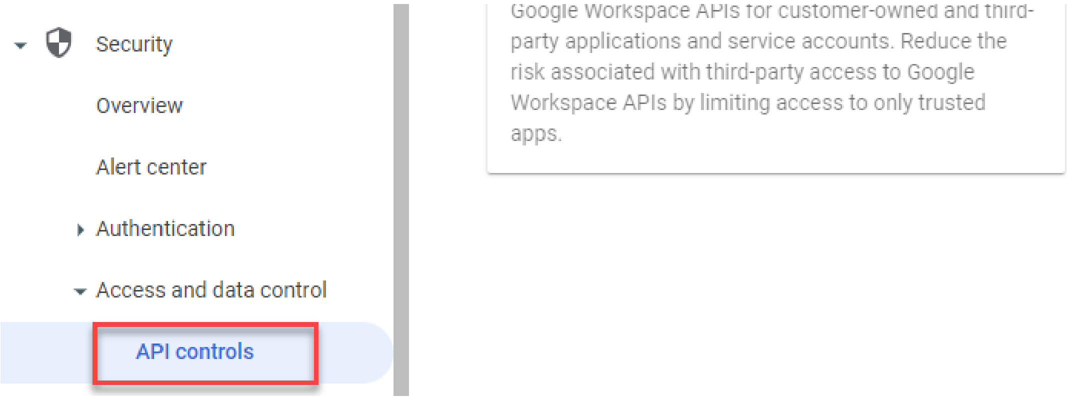


Google Drive API

Google Enterprise API

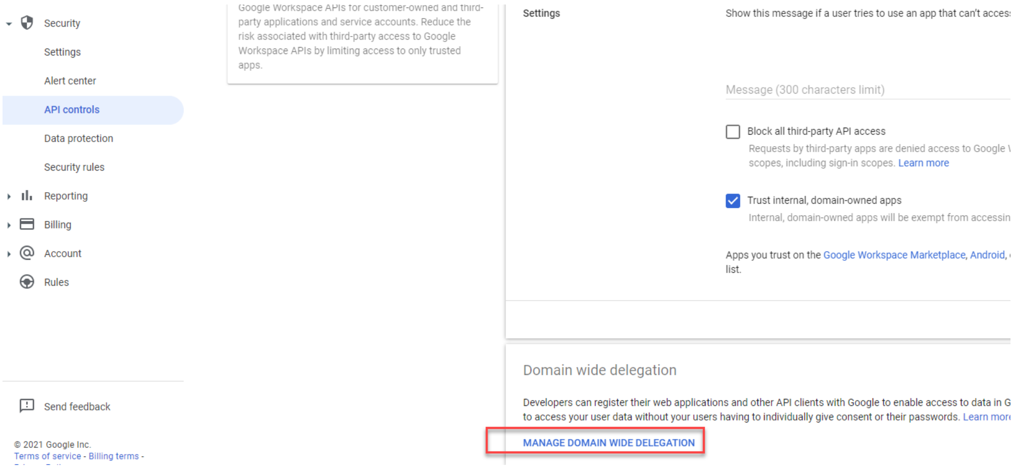
The Google Drive API allows clients to access resources from Google Drive

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



Google Workspace APIs for customer-owned and third-party applications and service accounts. Reduce the risk associated with third-party access to Google Workspace APIs by limiting access to only trusted apps.

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



Google Workspace APIs for customer-owned and third-party applications and service accounts. Reduce the risk associated with third-party access to Google Workspace APIs by limiting access to only trusted apps.

Settings

Show this message if a user tries to use an app that can't acces

Message (300 characters limit)

☐ Block all third-party API access

Requests by third-party apps are denied access to Google \ scopes, including sign-in scopes. Learn more

☑ Trust internal, domain-owned apps

Internal, domain-owned apps will be exempt from accessin

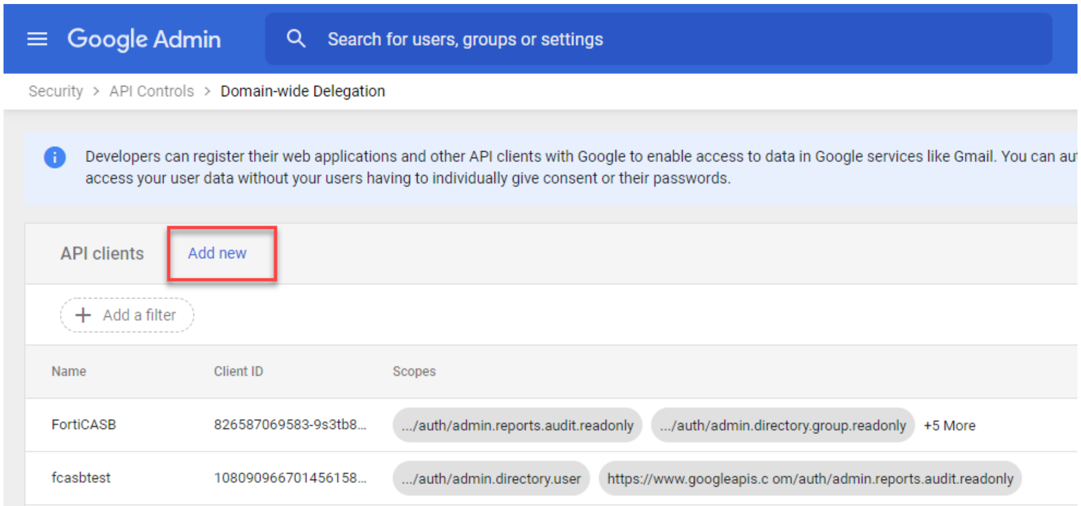
Apps you trust on the Google Workspace Marketplace, Android, list.

Domain wide delegation

Developers can register their web applications and other API clients with Google to enable access to data in G to access your user data without your users having to individually give consent or their passwords. Learn more

© 2021 Google Inc.
Terms of service - Billing terms -

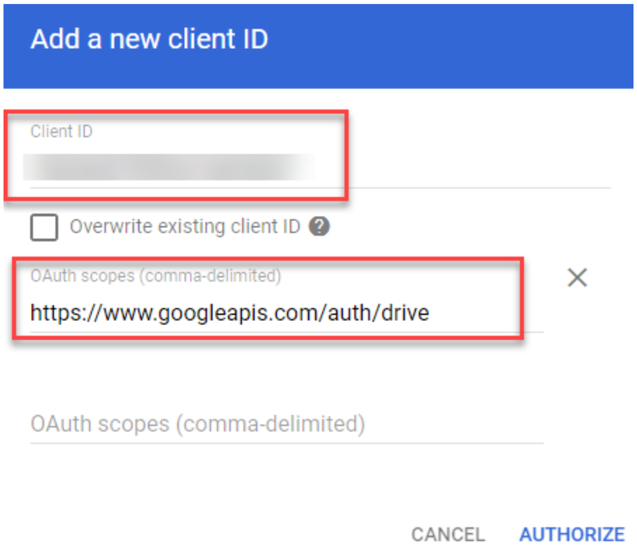
8. Click **Add new** and add the **Client ID** from Create Google Service Account on page 20.


Google Admin
Search for users, groups or settings
Security > API Controls > Domain-wide Delegation
API clients
Add new
+ Add a filter

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can au access your user data without your users having to individually give consent or their passwords.

Name	Client ID	Scopes
FortiCASB	826587069583-9s3tb8...	.../auth/admin.reports.audit.readonly .../auth/admin.directory.group.readonly +5 More
fcasbtest	108090966701456158...	.../auth/admin.directory.user https://www.googleapis.c om/auth/admin.reports.audit.readonly

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



Client ID
[redacted]

□ Overwrite existing client ID

OAuth scopes (comma-delimited)
https://www.googleapis.com/auth/drive

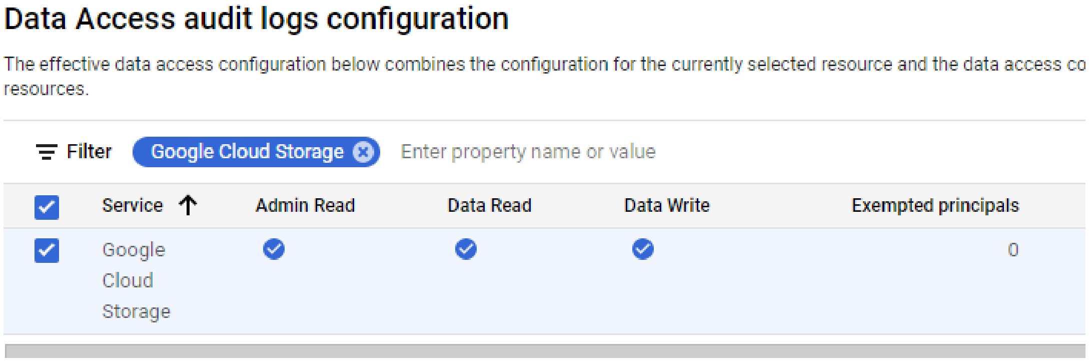
OAuth scopes (comma-delimited)

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. Go to the project to be monitored.
2. Go to **Navigation Menu > IAM & Admin > Audit Logs.**

3. Search for **Google Cloud Storage** from the list of available resources.



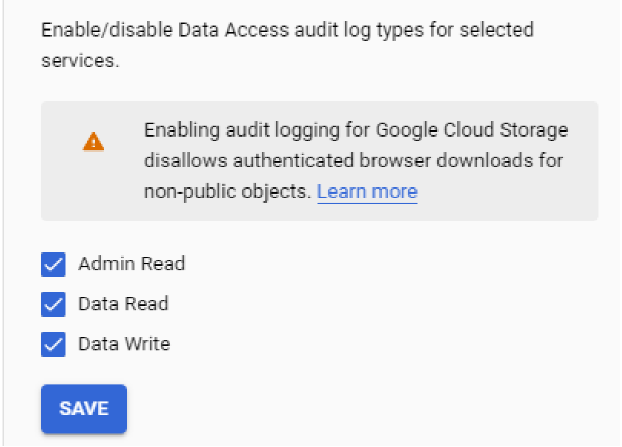
Data Access audit logs configuration

The effective data access configuration below combines the configuration for the currently selected resource and the data access co resources.

Filter Google Cloud Storage ⓧ Enter property name or value

☑	Service ↑	Admin Read	Data Read	Data Write	Exempted principals
☑	Google Cloud Storage	✓	✓	✓	0

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



Enable/disable Data Access audit log types for selected services.

⚠ Enabling audit logging for Google Cloud Storage disallows authenticated browser downloads for non-public objects. Learn more

☑ Admin Read

☑ Data Read

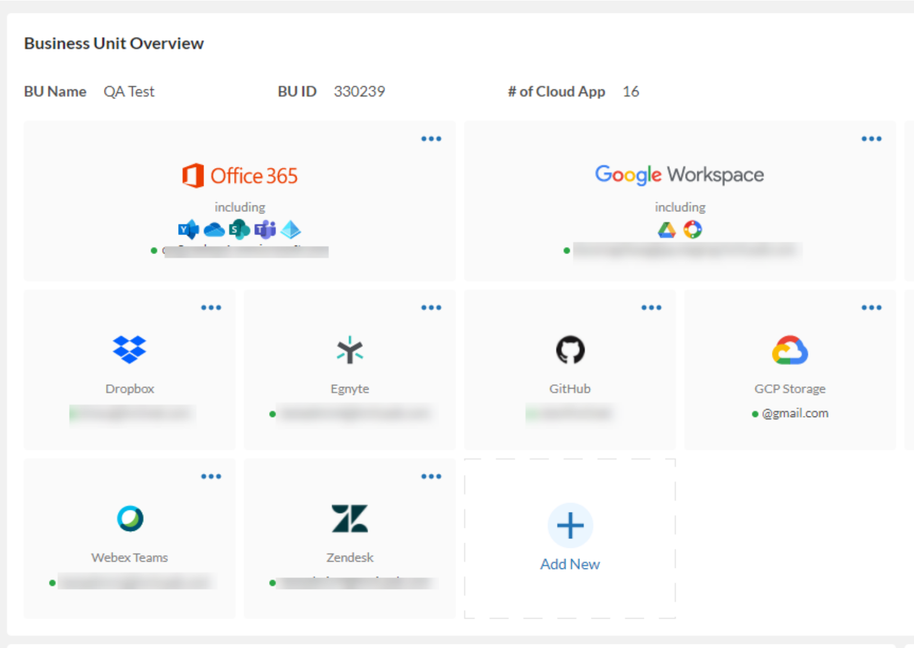
☑ Data Write

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.

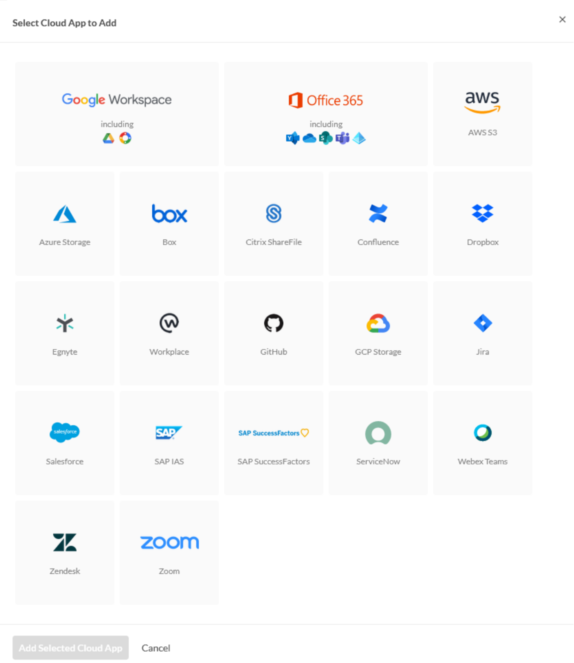
1. Log into FortiCASB with your account.
2. Go to **Overview > Dashboard**, click on **Add New**, select **Google Workspace**, then click **Add Selected Cloud App**.



Business Unit Overview

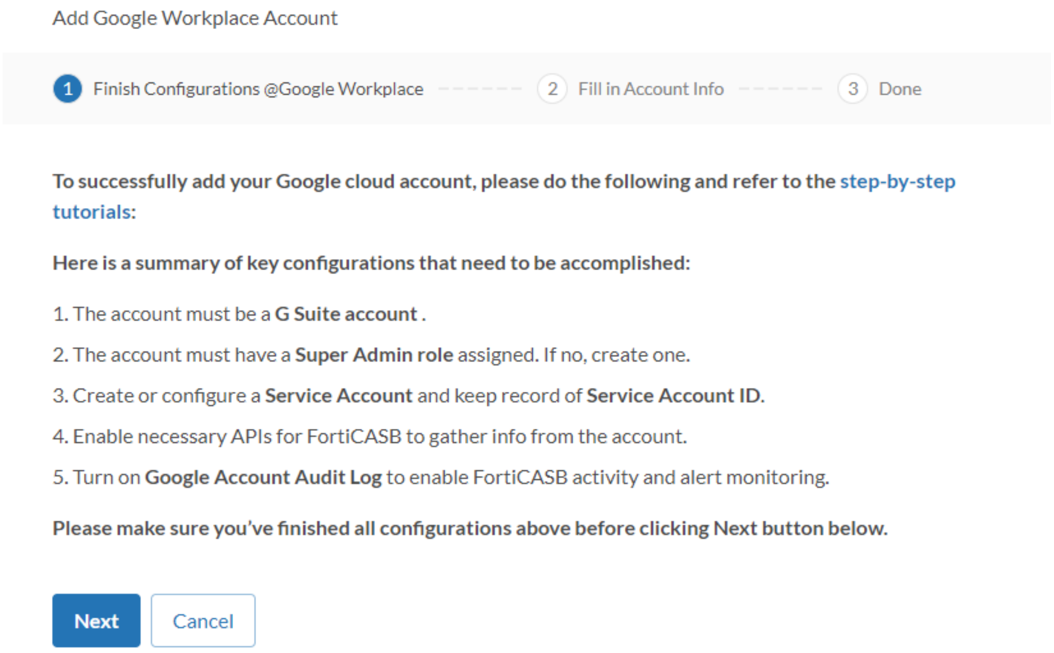
BU Name QA Test BU ID 330239 # of Cloud App 16

- Office 365 including ● [redacted]
- Google Workspace including ● [redacted]
- Dropbox [redacted]
- Egnyte ● [redacted]
- GitHub [redacted]
- GCP Storage ● @gmail.com
- Webex Teams ● [redacted]
- Zendesk ● [redacted]
- Add New



Select Cloud App to Add ×

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


Add Google Workplace Account
1 Finish Configurations @Google Workplace
2 Fill in Account Info
3 Done
Next
Cancel

To successfully add your Google cloud account, please do the following and refer to the step-by-step tutorials:

Here is a summary of key configurations that need to be accomplished:

1. The account must be a **G Suite account** .

2. The account must have a **Super Admin role** assigned. If no, create one.

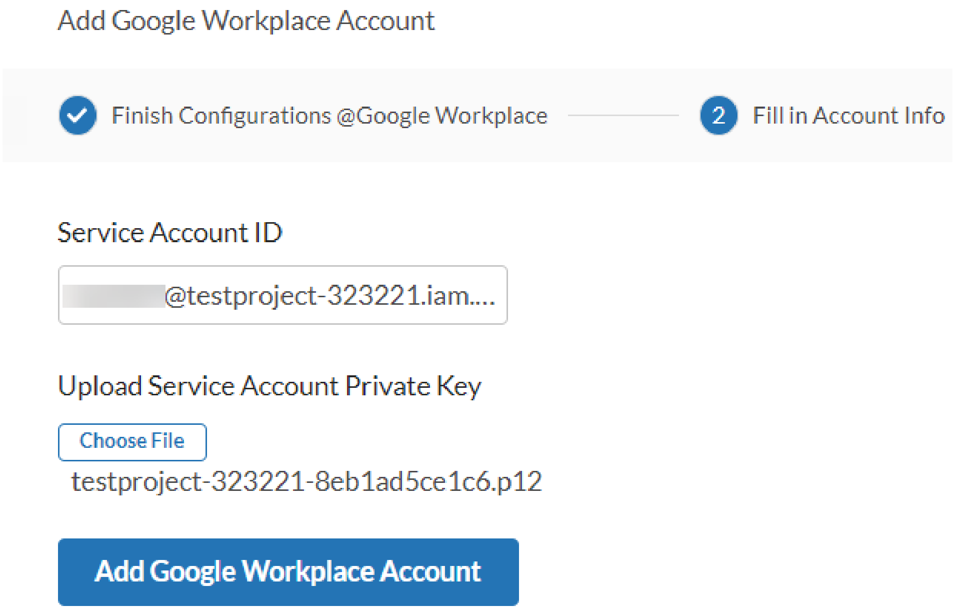
3. Create or configure a **Service Account** and keep record of **Service Account ID**.

4. Enable necessary APIs for FortiCASB to gather info from the account.

5. Turn on **Google Account Audit Log** to enable FortiCASB activity and alert monitoring.

Please make sure you've finished all configurations above before clicking Next button below.

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".


Add Google Workplace Account
Finish Configurations @Google Workplace
2 Fill in Account Info
Choose File
Add Google Workplace Account

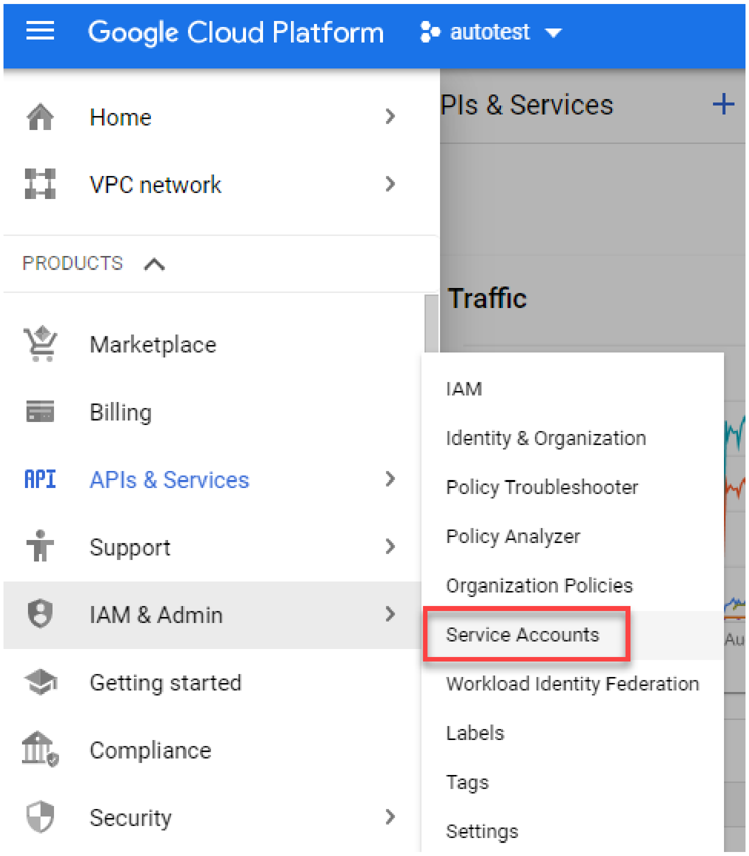
Service Account ID

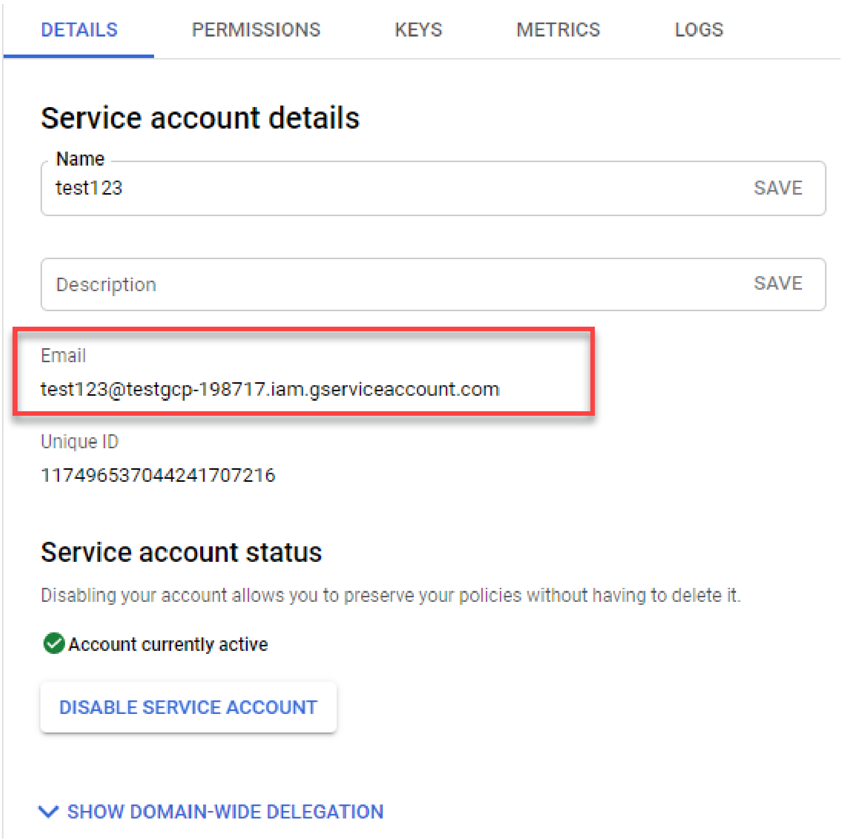
[redacted]@testproject-323221.iam....

Upload Service Account Private Key

testproject-323221-8eb1ad5ce1c6.p12

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





Service account details

Name: test123 SAVE

Description SAVE

Email
test123@testgcp-198717.iam.gserviceaccount.com

Unique ID
117496537044241707216

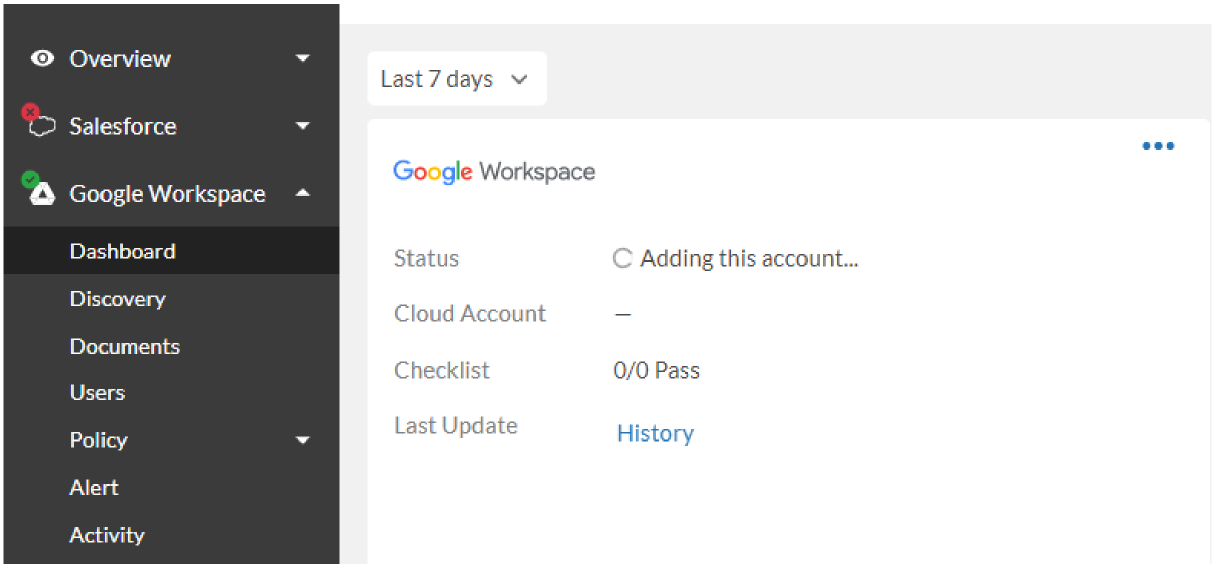
Service account status

Disabling your account allows you to preserve your policies without having to delete it.

✓ Account currently active

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.

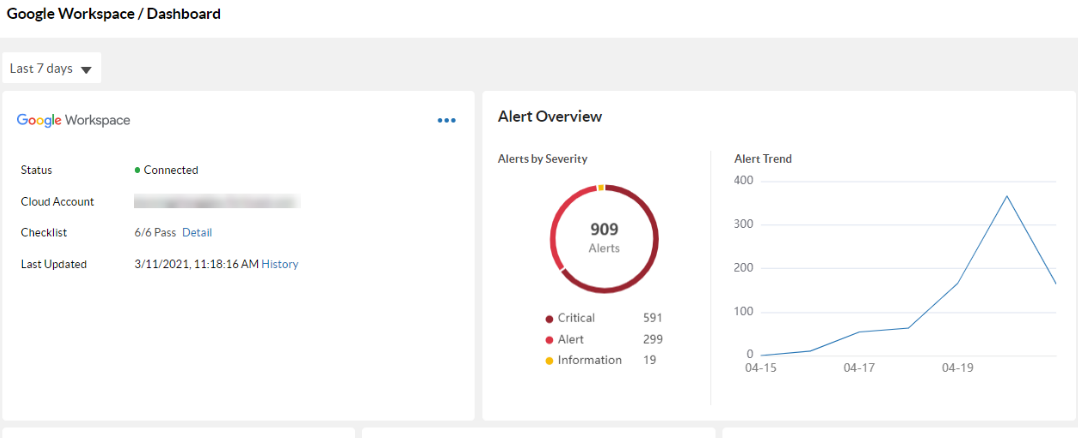


Status: Adding this account...

Cloud Account: –

Checklist: 0/0 Pass

Last Update: History



Status: ● Connected

Cloud Account: [redacted]

Checklist: 6/6 Pass Detail

Last Updated: 3/11/2021, 11:18:16 AM History

● Critical	591
● Alert	299
● Information	19

Deployment procedures for Office 365

This example selects and configures Office 365 to onboard on FortiCASB. FortiCASB offers an API-based approach, pulling data directly from Office 365 via RESTful API. The FortiCASB portal accesses the data collected through API queries with OAuth2.0 authentication. FortiCASB combines these data to monitor and track Office 365 user activities and provide DLP data analysis for files on Office 365.

For instructions on deploying other SaaS cloud applications, see Add Cloud Application.

Microsoft online applications integration

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

Supported Microsoft online applications and details

Microsoft online applications	Monitoring details
Yammer	All chats and shared files
OneDrive	All files shared privately or publicly
SharePoint	Files in Document and "user-created" folders
Teams	All activities, group chats except personal chats, and shared files.
Azure Active Directory	All user activities.

Prerequisites

There are a few prerequisites before adding the Office 365 account on FortiCASB:

1. Office 365 account and license: create Office 365 account with global administrator role.
2. Activate Office 365 account audit log: enable Office 365 audit log to record user activities of the Office 365 account.
3. Add admin to SharePoint site: incorporate protection on Office 365 SharePoint sites by adding the Office 365 account to the site admin.
4. Add Office 365 account: activate site collection by adding the Office 365 account to FortiCASB.

Office 365 account and license

You may use an existing Office 365 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 an Office 365 license, review Determine the Office 365 license type on page 33 to determine the type of Office 365 license you have.

License requirement

Ensure that your Office 365 account license plan includes Active Directory (AD) integration. FortiCASB requires AD support for most of its features. The following Office 365 licenses support AD integration:

- Office 365 Business
- Office 365 Business Essentials
- Office 365 Business Premium
- Office 365 ProPlus
- Office 365 Enterprise E1
- Office 365 Enterprise E3
- Office 365 Enterprise E5
- Office 365 Enterprise K1

Ensure that the role you use to add the Office 365 account on FortiCASB is global administrator. You may also have the Azure AD Premium P2 license (optional).

Without the Azure AD Premium P2 license, FortiCASB's Discovery feature cannot see user entitlements. This does not affect any other FortiCASB functions. User entitlements is a feature on FortiCASB that lets you see the roles and permissions that each user is entitled with. For information on how to obtain the Azure AD Premium P2 license, see Sign up for Azure Active Directory Premium editions.

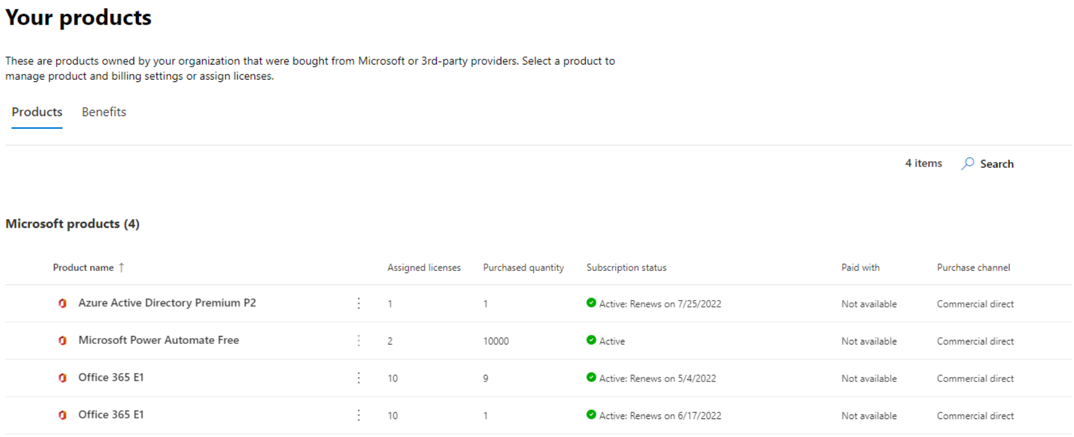
You must also set up the Azure AD Privileged Identity Management application. For more information, see What is Azure AD Privileged Identity Management?.

Determine the Office 365 license type

To determine the Office 365 license type that you have:

1. Log into your Office 365 account.
2. Click the **Apps** button located in the top-left corner of your Office 365 home screen.
3. Select **Admin**. You are redirected to the Microsoft 365 admin center.
4. On the navigation pane, go to **Billing > Your Products**. It displays your Office 365 license, along with your Azure

Active Directory Premium P2 license, if you purchased it.



Your products

These are products owned by your organization that were bought from Microsoft or 3rd-party providers. Select a product to manage product and billing settings or assign licenses.

Products Benefits

4 items Search

Microsoft products (4)

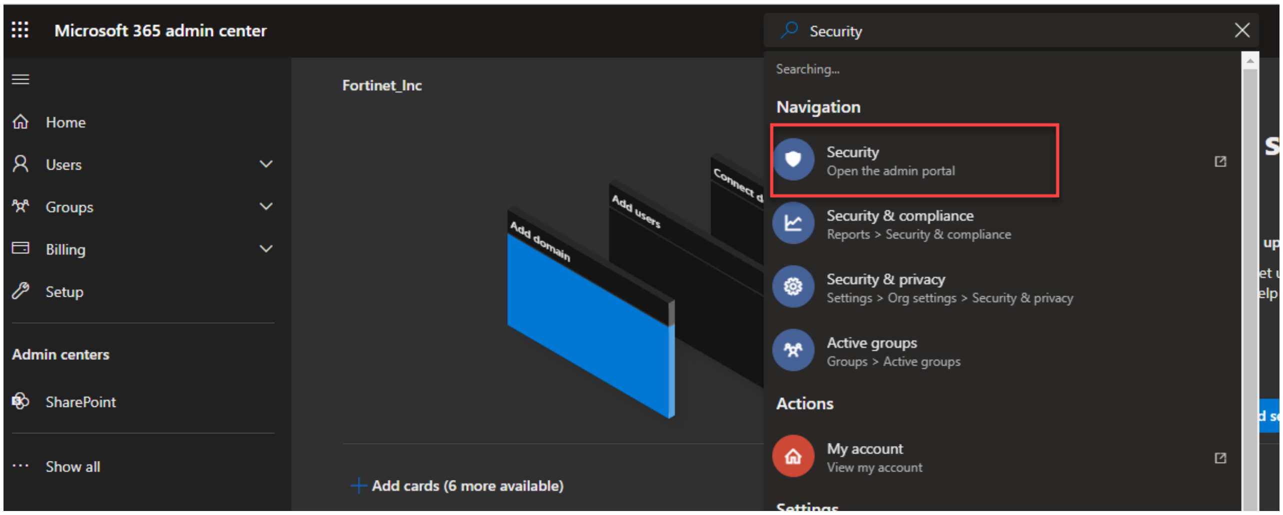
Product name ↑	Assigned licenses	Purchased quantity	Subscription status	Paid with	Purchase channel
Azure Active Directory Premium P2	1	1	✓ Active: Renews on 7/25/2022	Not available	Commercial direct
Microsoft Power Automate Free	2	10000	✓ Active	Not available	Commercial direct
Office 365 E1	10	9	✓ Active: Renews on 5/4/2022	Not available	Commercial direct
Office 365 E1	10	1	✓ Active: Renews on 6/17/2022	Not available	Commercial direct

Activate the Office 365 account audit log

You must activate the Office 365 audit log to record user and admin activities. This allows FortiCASB to monitor the Office 365 account's activities. It may take several hours after you enable the audit log before FortiCASB receives the audit logs from your Office 365 account.

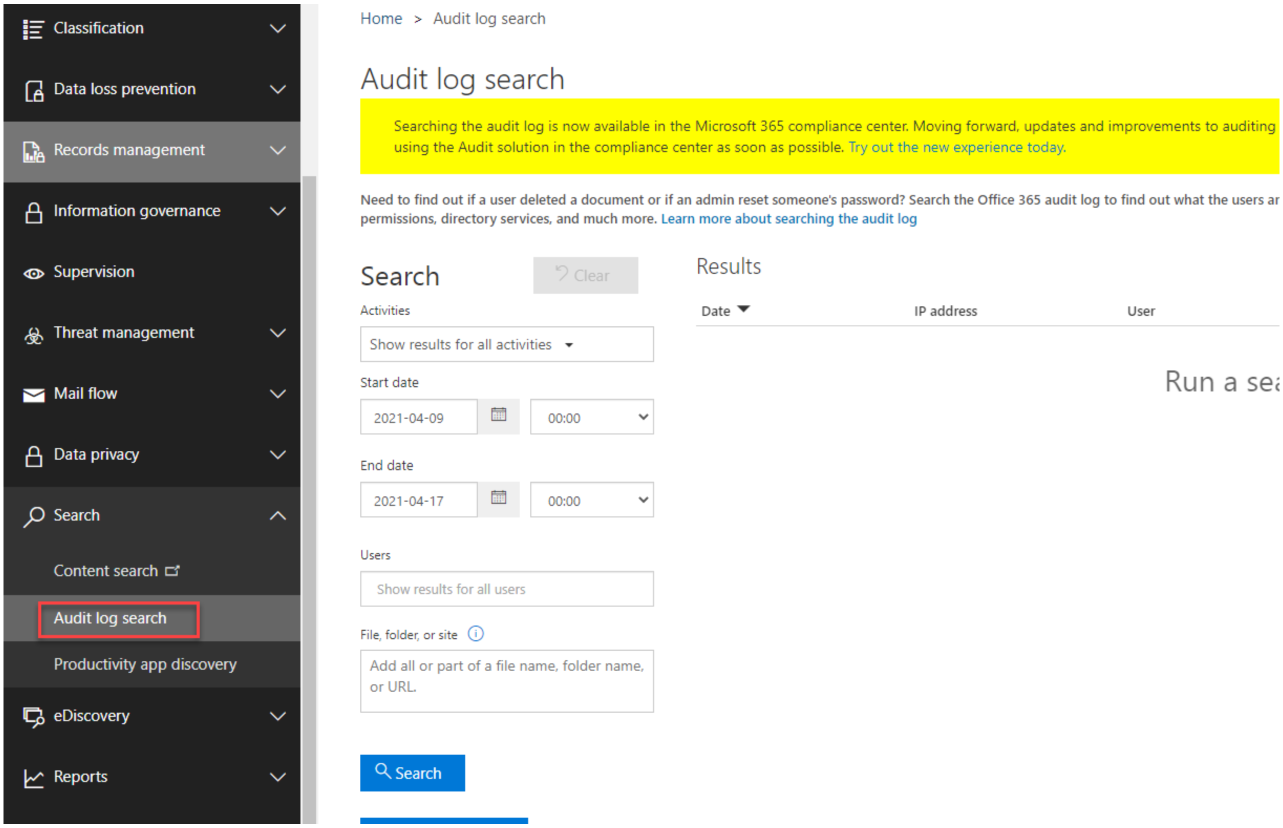
To activate the Office 365 account audit log:

1. Log in to your Office 365 account as the admin user.
2. Click the Office 365 menu option ⋮⋮⋮ and select the **Admin** portal to be redirected to the Microsoft 365 admin center.



3. In the top search bar, search for and select **Security**. This redirects you to the Office 365 Security & Compliance page.

4. Scroll to go to **Search > Audit log search**.



Audit log search

Searching the audit log is now available in the Microsoft 365 compliance center. Moving forward, updates and improvements to auditing using the Audit solution in the compliance center as soon as possible. Try out the new experience today.

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users ar permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: Show results for all activities

Start date: 2021-04-09 00:00

End date: 2021-04-17 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

5. Click **Turn on auditing**. If you do not see this option, the organization has already enabled it. If you are a new tenant, allow 24 hours for auditing to become available.
6. After enabling auditing, allow 24 hours for it to become available.

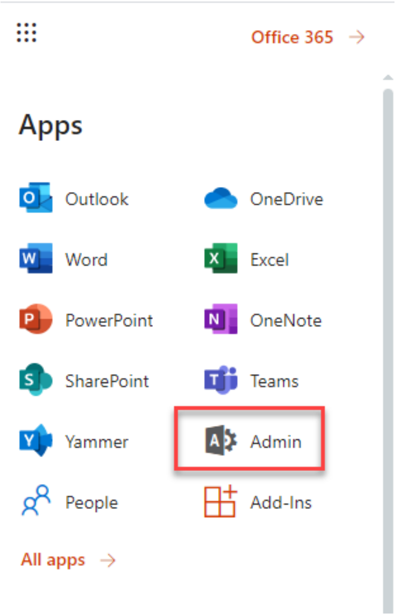
You can now activate site collection by adding the Office 365 account to FortiCASB.

⚠ If you see an error when adding Office 365 to FortiCASB, you may need to wait to enable auditing on the Office 365 portal.

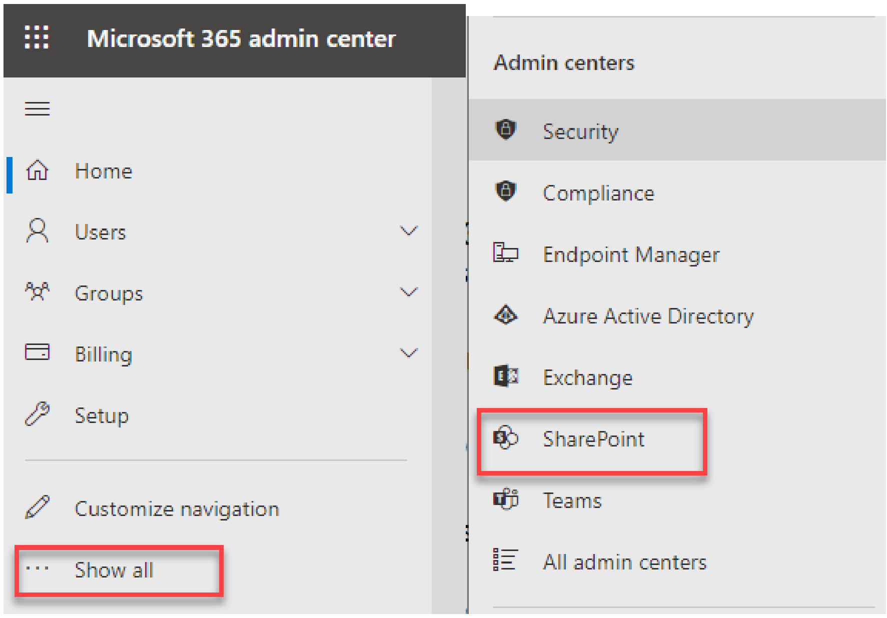
Add an administrator to a SharePoint site

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.

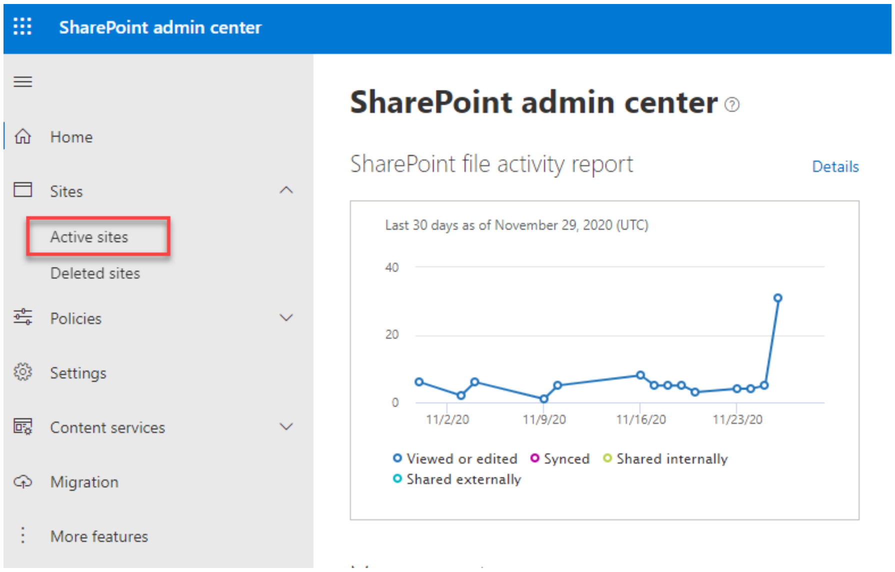
1. Log into Office 365 (https://office.com) with your admin account to be added to FortiCASB.
2. Click on App Launcher button ⠿ at the top left corner, and select **Admin**.



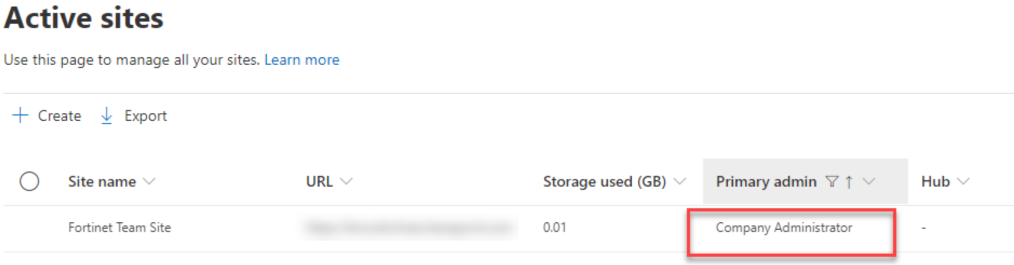
3. In **Microsoft 365 admin center** left navigation menu, click on **Show all** to show other options. Scroll down to **Admin Centers** and click **SharePoint** to enter **SharePoint admin center**.



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".

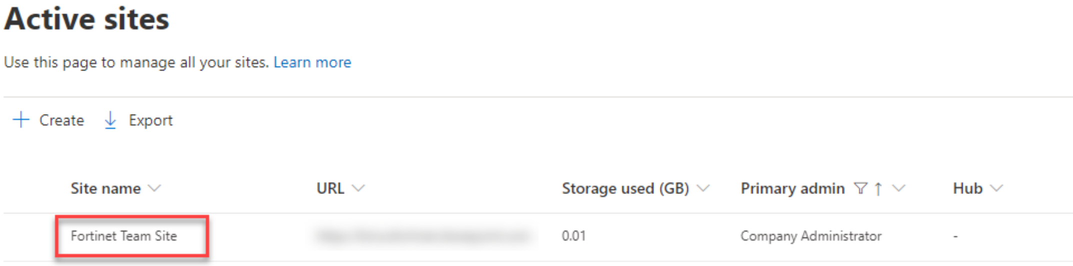


Active sites

Use this page to manage all your sites. Learn more

○	Site name	URL	Storage used (GB)	Primary admin	Hub
	Fortinet Team Site	[redacted]	0.01	Company Administrator	-

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

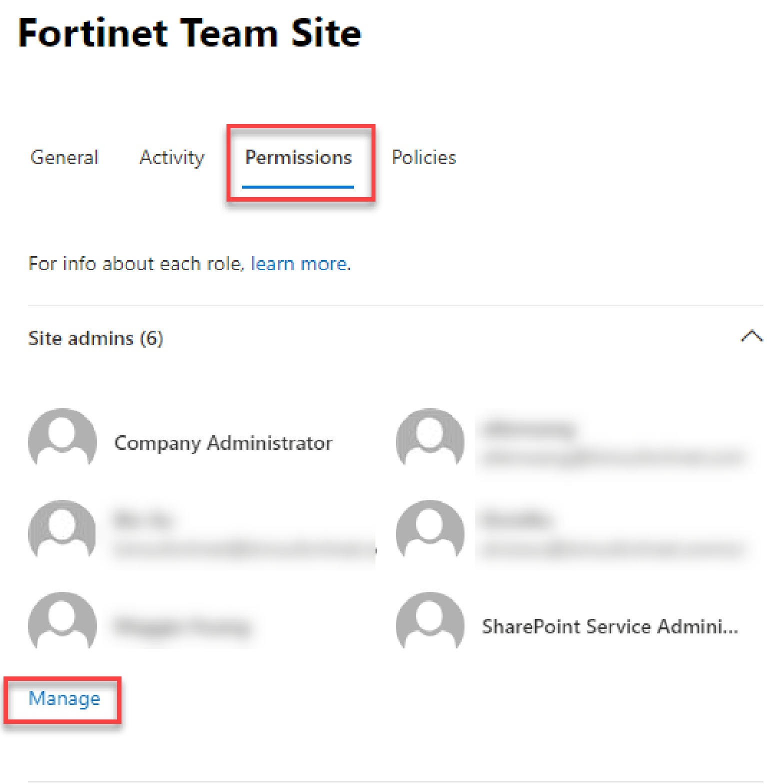


Active sites

Use this page to manage all your sites. Learn more

Site name	URL	Storage used (GB)	Primary admin	Hub
Fortinet Team Site	[redacted]	0.01	Company Administrator	-

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



Fortinet Team Site

For info about each role, learn more.

Site admins (6)

Company Administrator

[redacted]

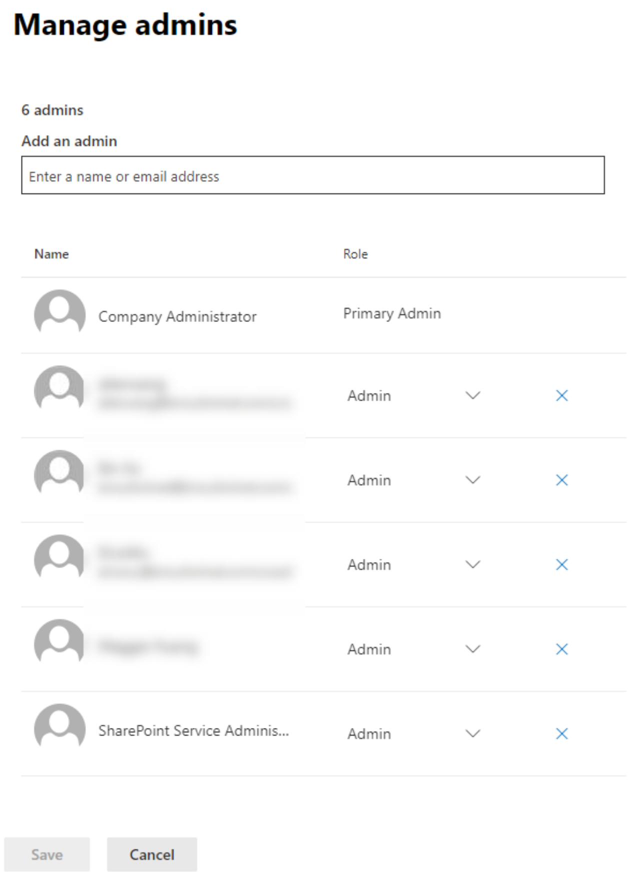
[redacted]

[redacted]

[redacted]

SharePoint Service Admini...

8. Check if your account is one of the site admins. If not, click **Manage** to add your account to the Manage admins, then click **Save**. In this way, FortiCASB will be able to monitor and protect the sharepoint site after your admin account is added to FortiCASB.



Manage admins

6 admins

Add an admin

Enter a name or email address

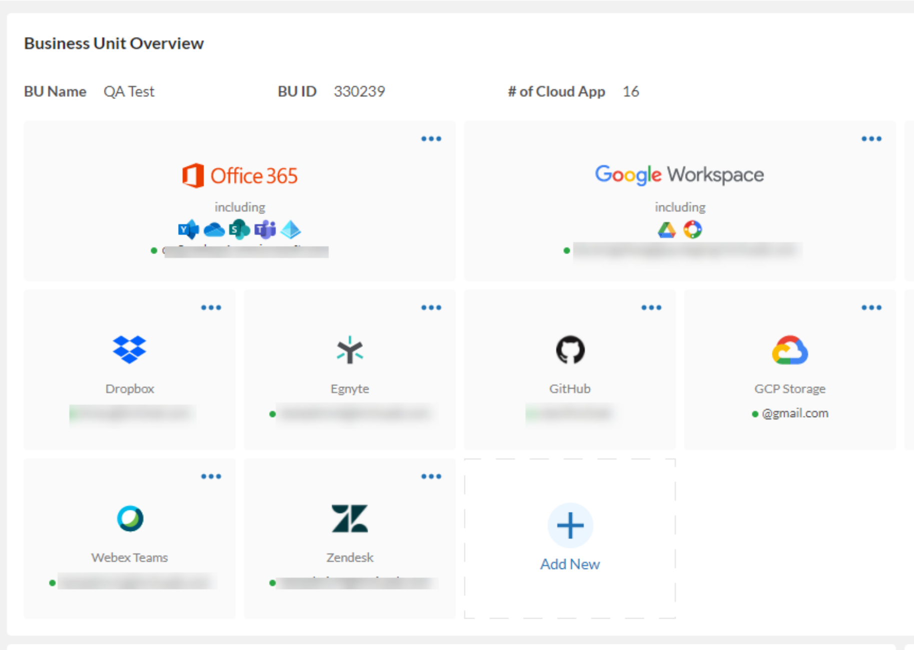
Name	Role
Company Administrator	Primary Admin
[redacted]	Admin
[redacted]	Admin
[redacted]	Admin
[redacted]	Admin
SharePoint Service Adminis...	Admin

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

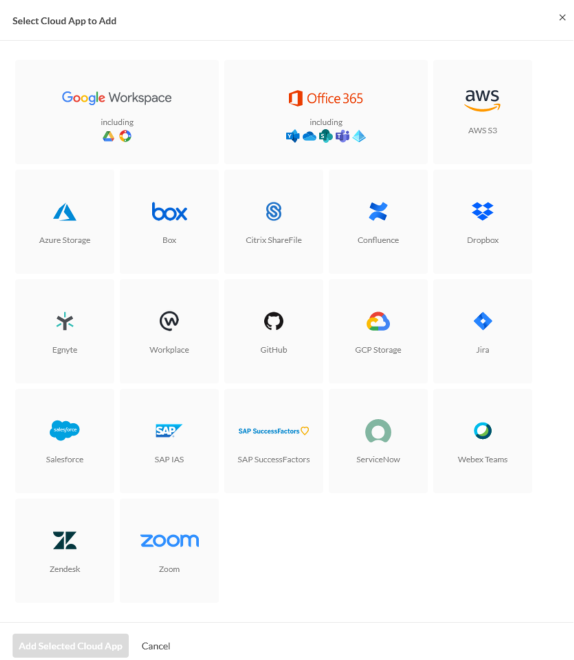
After all the Office 365 configurations are completed from previous sections, follow these steps to add your Office 365 account on FortiCASB.

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**.



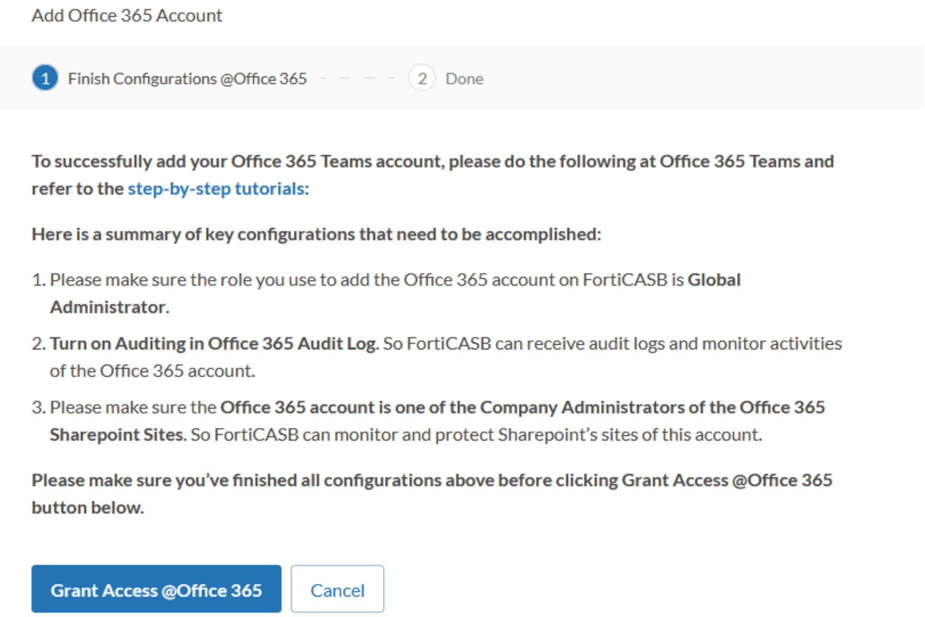
Business Unit Overview

BU Name QA Test BU ID 330239 # of Cloud App 16



Select Cloud App to Add

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



Add Office 365 Account

To successfully add your Office 365 Teams account, please do the following at Office 365 Teams and refer to the step-by-step tutorials:

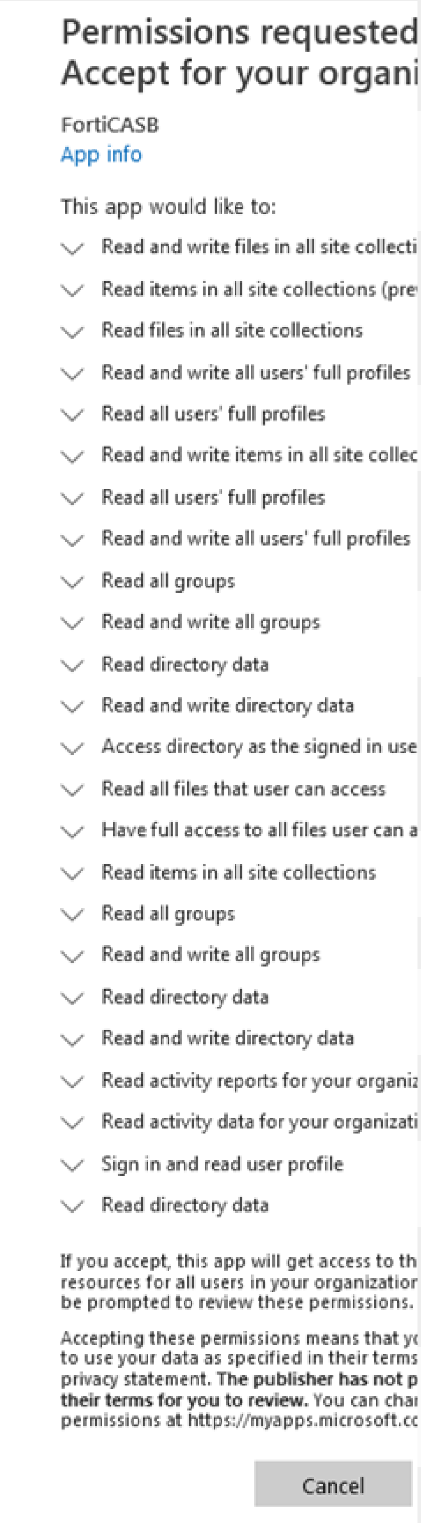
Here is a summary of key configurations that need to be accomplished:

1. Please make sure the role you use to add the Office 365 account on FortiCASB is **Global Administrator**.
2. **Turn on Auditing in Office 365 Audit Log.** So FortiCASB can receive audit logs and monitor activities of the Office 365 account.
3. Please make sure the **Office 365 account is one of the Company Administrators of the Office 365 Sharepoint Sites.** So FortiCASB can monitor and protect Sharepoint's sites of this account.

Please make sure you've finished all configurations above before clicking Grant Access @Office 365 button below.

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

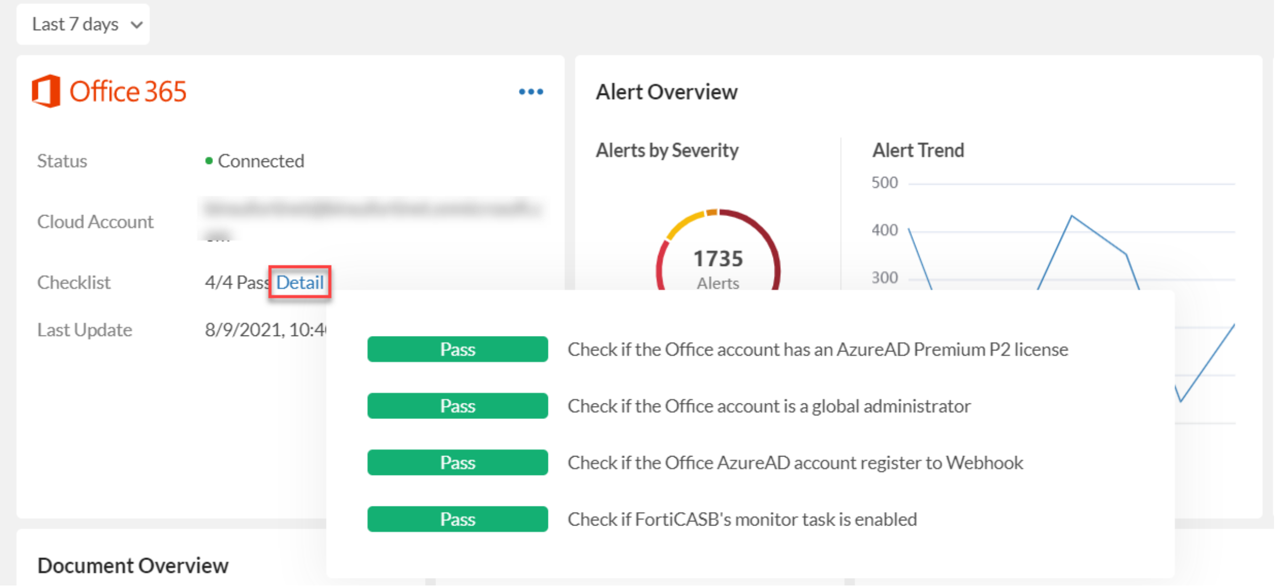
4. After logging in, Office 365 will prompt you to accept FortiCASB access.
   Note: FortiCASB does not request all but only partial permissions from the global administrator user. Below is a list of permissions requested by FortiCASB.

 Permissions requested Accept for your organi FortiCASB App info This app would like to: Read and write files in all site collecti Read items in all site collections (pre 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 collec Read all users' full profiles Read and write 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 use Read all files that user can access Have full access to all files user can a Read items in all site collections Read all groups Read and write all groups Read directory data Read and write directory data Read activity reports for your organiz Read activity data for your organizati Sign in and read user profile Read directory data If you accept, this app will get access to th resources for all users in your organizatior be prompted to review these permissions. Accepting these permissions means that yo to use your data as specified in their terms privacy statement. **The publisher has not p their terms for you to review.** You can chai permissions at https://myapps.microsoft.cc Cancel	**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

5. 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 added.



Last 7 days

Office 365

Status	● Connected
Cloud Account	[redacted]
Checklist	4/4 Pass Detail
Last Update	8/9/2021, 10:4

Pass	Check if the Office account has an AzureAD Premium P2 license
Pass	Check if the Office account is a global administrator
Pass	Check if the Office AzureAD account register to Webhook
Pass	Check if FortiCASB's monitor task is enabled

Deployment procedures common for all cloud applications

The following deployment procedures are common for all deployments, regardless of the cloud application configured (Google Workspace, Office 365, and so on).

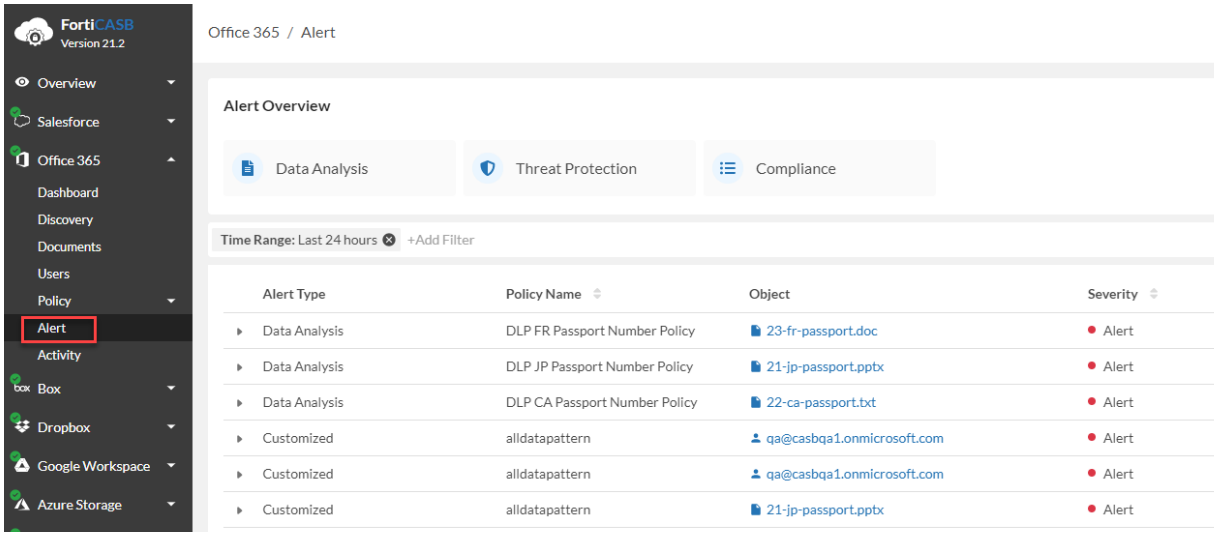
Configure policy to trigger alert

FortiCASB generates an alert when suspicious activities trigger a policy. There are three policy types:

Type	Pertains to...
Data analysis	Data types stored in the cloud application
Threat protection	Suspicious user activity
Compliance	Specific regulations, such as HIPAA, PCI, and SOX

You must enable a policy to trigger an alert.

To view alerts of each cloud application, click on a cloud application drop down menu and click on **Alert**.



Office 365 / Alert

Alert Overview

Data Analysis | Threat Protection | Compliance

Time Range: Last 24 hours +Add Filter

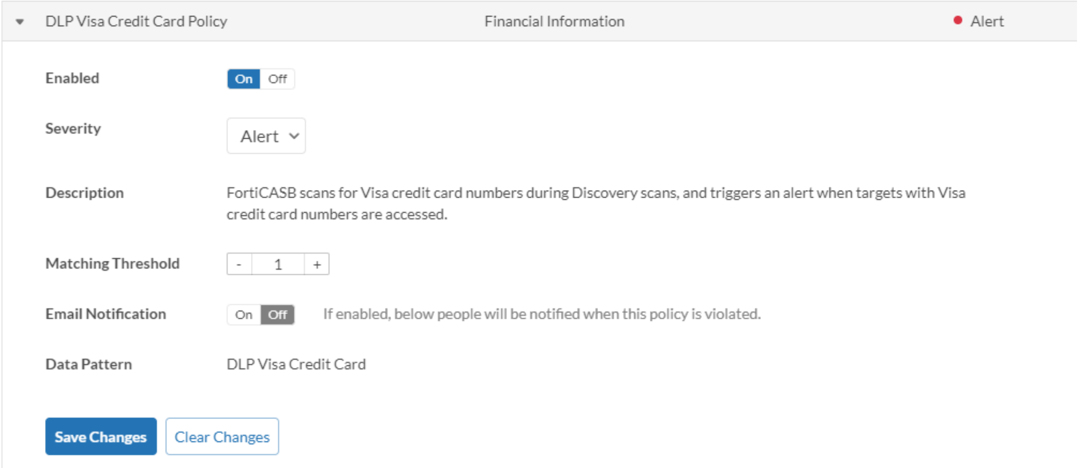
Alert Type	Policy Name	Object	Severity
Data Analysis	DLP FR Passport Number Policy	23-fr-passport.doc	● Alert
Data Analysis	DLP JP Passport Number Policy	21-jp-passport.pptx	● Alert
Data Analysis	DLP CA Passport Number Policy	22-ca-passport.txt	● Alert
Customized	alldatapattern	qa@casbqa1.onmicrosoft.com	● Alert
Customized	alldatapattern	qa@casbqa1.onmicrosoft.com	● Alert
Customized	alldatapattern	21-jp-passport.pptx	● Alert

Policy configuration example

A data loss prevention (DLP) Visa credit card policy identifies Visa credit card numbers accessed through the cloud account activity. When the number of Visa credit card numbers accessed in any activity incident reaches the preconfigured threshold, an alert is triggered.

To configure a DLP Visa credit card 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 **Data Analysis**.
3. Locate **DLP Visa Credit Card Policy** and click on the right arrow key **>** button to expand the policy.
4. Click **On** in **Enabled** to enable the policy.. The default is always turned on.



DLP Visa Credit Card Policy   Financial Information   ● Alert

Enabled: On | Off

Severity: Alert

Description: FortiCASB scans for Visa credit card numbers during Discovery scans, and triggers an alert when targets with Visa credit card numbers are accessed.

Matching Threshold: - 1 +

Email Notification: On | Off   If enabled, below people will be notified when this policy is violated.

Data Pattern: DLP Visa Credit Card

5. Click on **Severity level** drop down menu to select the severity level (**Critical, Alert, Warning, Information**).
6. In **Matching Threshold**, enter the threshold of the number of credit card numbers to be detected in an activity incident for an alert to be generated.
   For example, a matching threshold of 2 will trigger an alert when two or more credit card numbers are detected in the cloud account activity.
7. Click **Save Changes** to save and update the configuration.

After the policy is enabled and configured, when cloud account activity detects access of visa credit card numbers reaches the preconfigured matching threshold, an alert will be triggered. For more details, please refer to Configure policy to trigger alert on page 44.

Configure notification settings

When an alert is triggered, a notification is sent to users as defined in notification settings.

To configure notification settings:

1. Go to **Notification Setting** in the top right corner.
2. In the **Email Receivers** field, enter the desired email addresses. Click **Save**.
3. On the **Report** tab, add the users to receive notifications for report generation.

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.

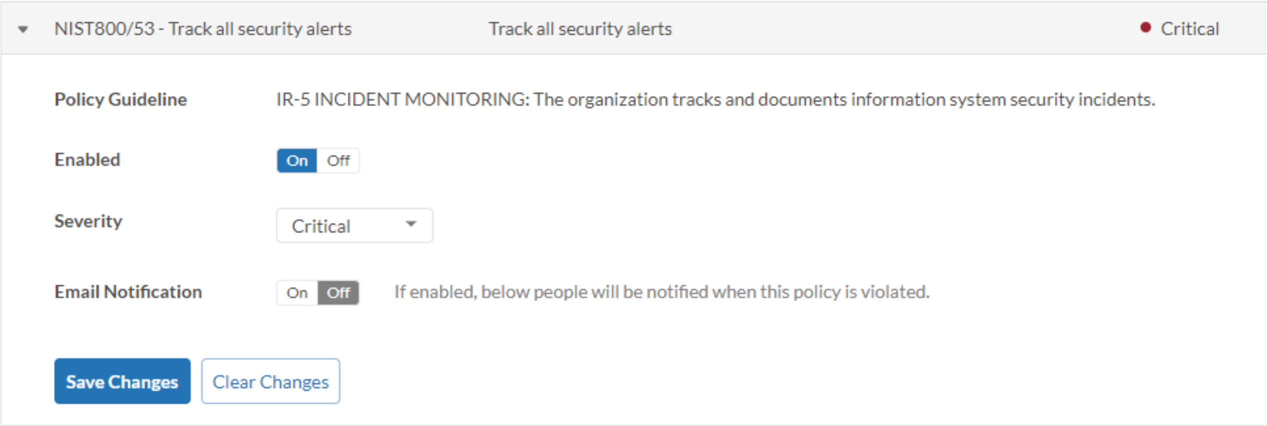
To enable Alert Report to export all daily security alerts, please enable any of the Compliance policies below to activate the feature:

- **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**.



▾ NIST800/53 - Track all security alerts   Track all security alerts   ● Critical

Policy Guideline: IR-5 INCIDENT MONITORING: The organization tracks and documents information system security incidents.

Enabled: [✓ On] Off

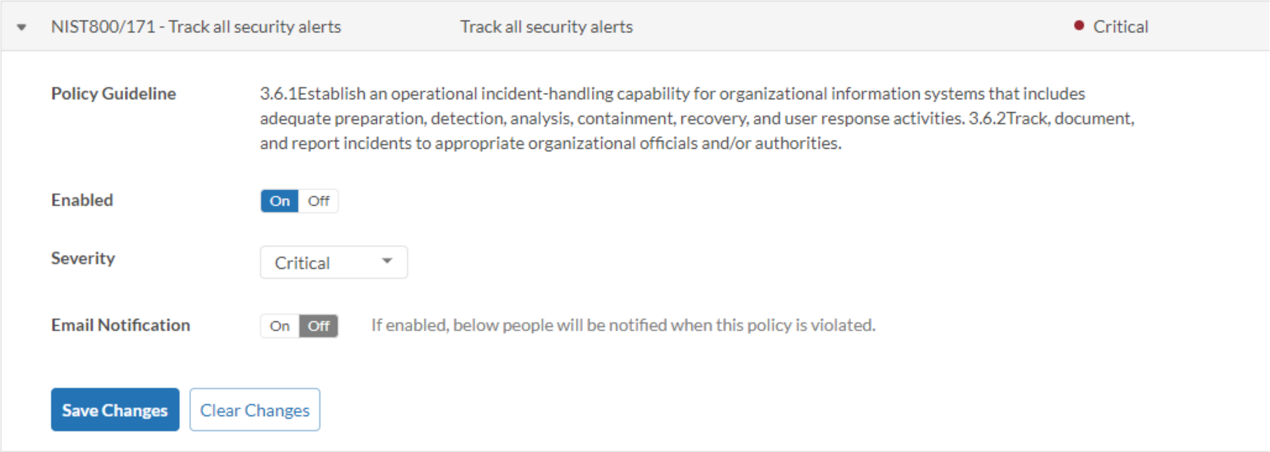
Severity: Critical

Email Notification: On [✓ Off]   If enabled, below people will be notified when this policy is violated.

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**.



NIST800/171 - Track all security alerts — Track all security alerts — ● Critical

Policy Guideline: 3.6.1Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2Track, document, and report incidents to appropriate organizational officials and/or authorities.

Enabled: On Off

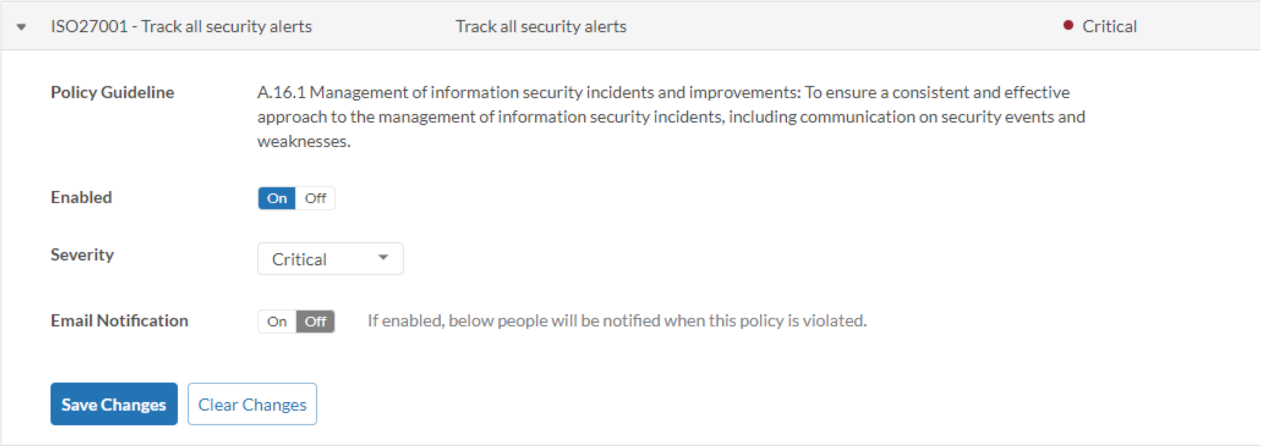
Severity: Critical

Email Notification: On Off — If enabled, below people will be notified when this policy is violated.

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**.



ISO27001 - Track all security alerts — Track all security alerts — ● Critical

Policy Guideline: A.16.1 Management of information security incidents and improvements: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Enabled: On Off

Severity: Critical

Email Notification: On Off — If enabled, below people will be notified when this policy is violated.

4. Enable the policy by clicking the **On** button.

Activate Activity Report

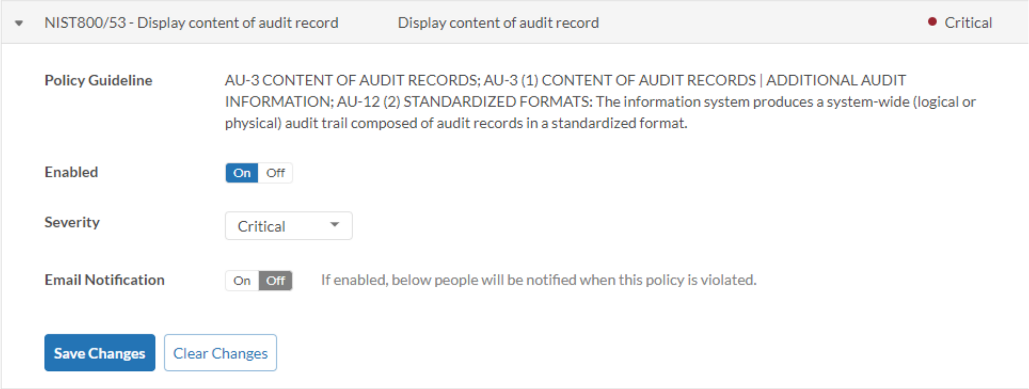
Activity Report keeps track of all daily cloud account activities and lets you download daily activity report. At the end of each month, all daily activity reports will be consolidated into one monthly report for download.

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**.



▾ NIST800/53 - Display content of audit record   Display content of audit record   ● Critical

Policy Guideline   AU-3 CONTENT OF AUDIT RECORDS; AU-3 (1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION; AU-12 (2) STANDARDIZED FORMATS: The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Enabled   [✓ On] Off

Severity   Critical

Email Notification   On [✓ Off]   If enabled, below people will be notified when this policy is violated.

4. Enable the policy by clicking the **On** button.

Post-deployment verification and analysis procedures

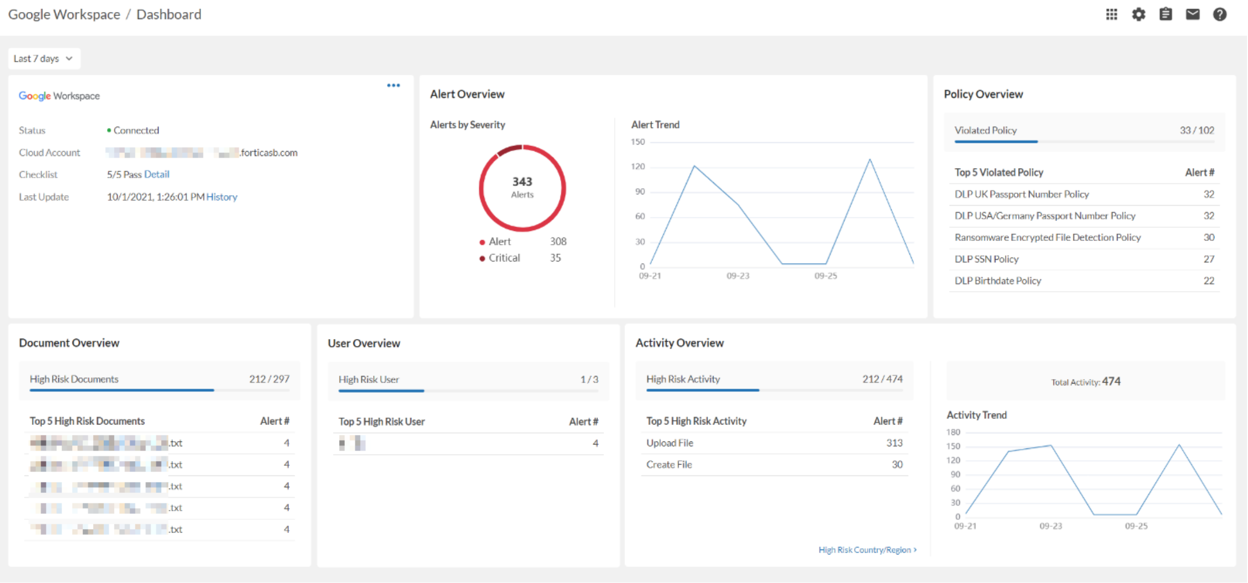
This section describes the post-deployment procedures that an administrator can use to verify FortiCASB has been properly configured to monitor the selected cloud application.

After deployment, it is recommended that an administrator continuously use these procedures to analyze cloud application data and activity.

Dashboard

FortiCASB presents an overview of the cloud application and visually summarizes key usage statistics including alerts by severity, top five violations, or high-risk entries depending on category, and trends over different time periods. The Dashboard page presents this overview and acts as the starting point for visibility into the cloud application.

For example, the Dashboard page for Google Workspace is as follows:



Google Workspace / Dashboard

Last 7 days

Google Workspace

Status	● Connected
Cloud Account	[redacted].forticasb.com
Checklist	5/5 Pass Detail
Last Update	10/1/2021, 1:26:01 PM History

Alert Overview

Alerts by Severity

343 Alerts

● Alert	308
● Critical	35

Alert Trend

Policy Overview

Violated Policy 33 / 102

Top 5 Violated Policy	Alert #
DLP UK Passport Number Policy	32
DLP USA/Germany Passport Number Policy	32
Ransomware Encrypted File Detection Policy	30
DLP SSN Policy	27
DLP Birthdate Policy	22

Document Overview

High Risk Documents 212 / 297

Top 5 High Risk Documents	Alert #
[redacted].txt	4
[redacted].txt	4
[redacted].txt	4
[redacted].txt	4
[redacted].txt	4

User Overview

High Risk User 1 / 3

Top 5 High Risk User	Alert #
[redacted]	4

Activity Overview

High Risk Activity 212 / 474

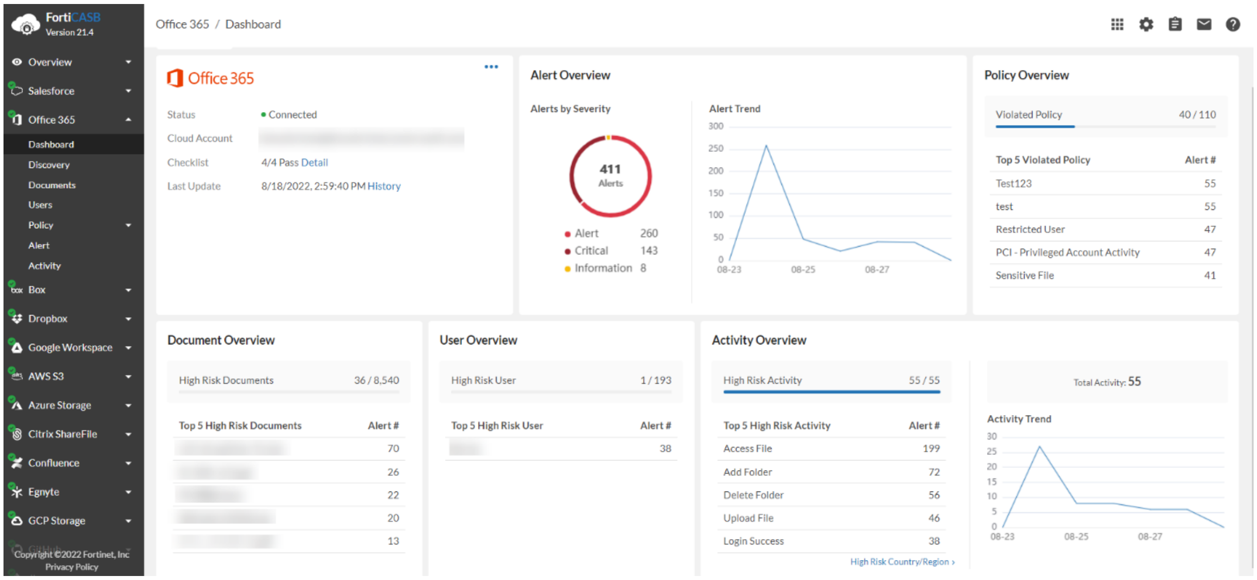
Top 5 High Risk Activity	Alert #
Upload File	313
Create File	30

High Risk Country/Region ›

Total Activity: 474

Activity Trend

For example, the Dashboard page for Office 365 is as follows:



Status ● Connected

Cloud Account [redacted]

Checklist 4/4 Pass Detail

Last Update 8/18/2022, 2:59:40 PM History

● Alert	260
● Critical	143
● Information	8

Violated Policy 40 / 110

Top 5 Violated Policy	Alert #
Test123	55
test	55
Restricted User	47
PCI - Privileged Account Activity	47
Sensitive File	41

High Risk Documents 36 / 8,540

Top 5 High Risk Documents	Alert #
[redacted]	70
[redacted]	26
[redacted]	22
[redacted]	20
[redacted]	13

High Risk User 1 / 193

Top 5 High Risk User	Alert #
[redacted]	38

High Risk Activity 55 / 55

Total Activity: 55

Top 5 High Risk Activity	Alert #
Access File	199
Add Folder	72
Delete Folder	56
Upload File	46
Login Success	38

Discovery

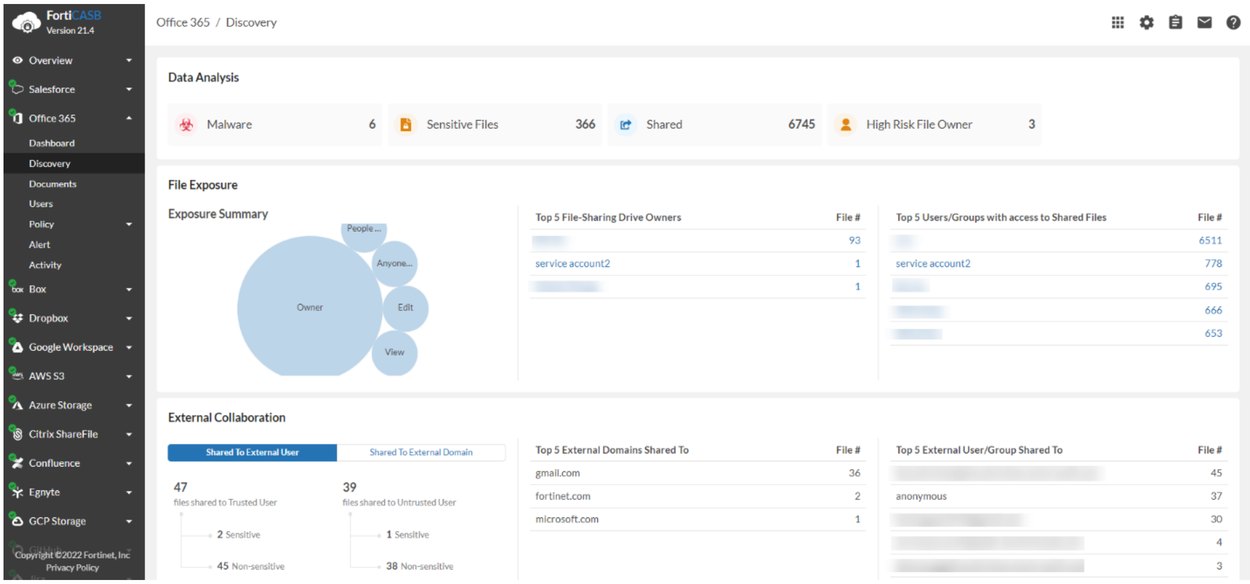
FortiCASB classifies data as data at rest or traffic data. **Data at rest** is data uploaded onto the cloud application before it has been linked with FortiCASB, while **traffic data** is any data uploaded after FortiCASB has started monitoring the cloud application.

You can run scans on the data in your cloud platforms to determine their contents. Depending on the policies you set, FortiCASB classifies the data as **sensitive** or **non-sensitive data**. This can be seen in the **Discovery** page of each cloud application.

The **Discovery** page shows basic information about the data in your cloud application, as well as information about the users with access to your data.

If you do not run a manual scan, FortiCASB will scan files on individual basis whenever a user access the file.

For example, the **Discovery** page for Office 365 is as follows:



Data Analysis

Malware	6
Sensitive Files	366
Shared	6745
High Risk File Owner	3

File Exposure

Exposure Summary

Top 5 File-Sharing Drive Owners	File #
[redacted]	93
service account2	1
[redacted]	1

Top 5 Users/Groups with access to Shared Files	File #
[redacted]	6511
service account2	778
[redacted]	695
[redacted]	666
[redacted]	653

External Collaboration

47
files shared to Trusted User
2 Sensitive
45 Non-sensitive

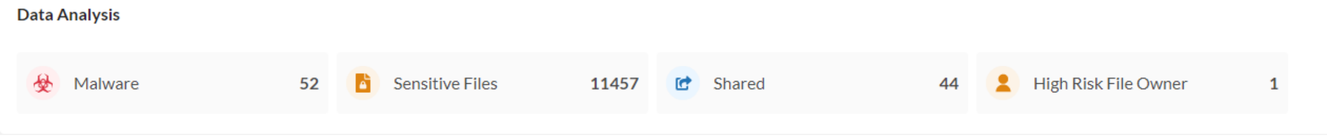
39
files shared to Untrusted User
1 Sensitive
38 Non-sensitive

Top 5 External Domains Shared To	File #
gmail.com	36
fortinet.com	2
microsoft.com	1

Top 5 External User/Group Shared To	File #
[redacted]	45
anonymous	37
[redacted]	30
[redacted]	4
[redacted]	3

Data Analysis

Data Analysis gives an overview of sensitive data in your cloud application.



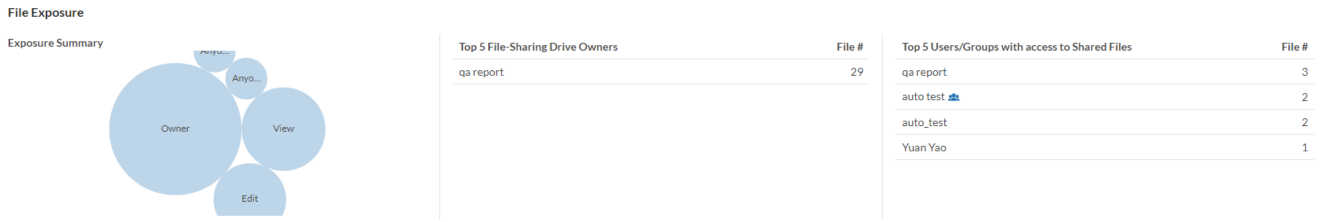
Data Analysis

Malware	52
Sensitive Files	11457
Shared	44
High Risk File Owner	1

File Type	Description
Sensitive Files	Shows the number of files on your cloud application with sensitive information.
High Risk File Owners	Shows how many users own files with sensitive information.
Shared Files	Shows the number of shared files.
Malware Files	Shows the number of files with malware scan results.

File Exposure

File Exposure gives an overview of shared files on your cloud application.



File Exposure

Exposure Summary

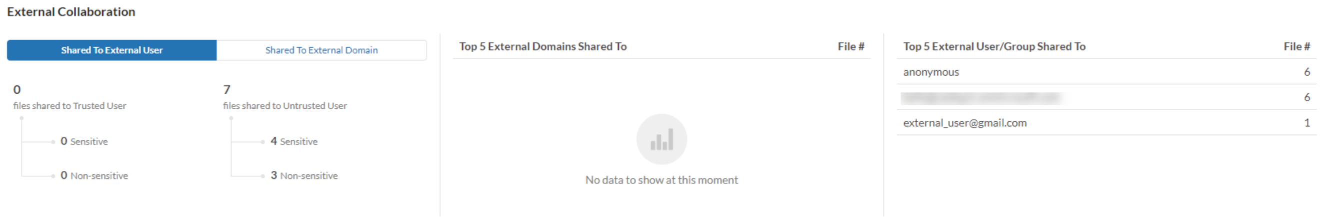
Top 5 File-Sharing Drive Owners	File #
qa report	29

Top 5 Users/Groups with access to Shared Files	File #
qa report	3
auto test	2
auto_test	2
Yuan Yao	1

Topic	Description
Exposure Summary	Gives a summary of the file exposure. Click to filter the list.
Top File-Sharing Owners	Shows the owners sharing the most files.
Top Users/Groups with access to Shared Files	Shows the users or groups with access to the most files.

External Collaboration

External Collaboration highlights the file shared to the external user/group.



External Collaboration

0
files shared to Trusted User
0 Sensitive
0 Non-sensitive

7
files shared to Untrusted User
4 Sensitive
3 Non-sensitive

Top 5 External Domains Shared To	File #

No data to show at this moment

Top 5 External User/Group Shared To	File #
anonymous	6
[redacted]	6
external_user@gmail.com	1

Topic	Description
External Summary	Gives a summary of the external files.
Top External Domains	Shows external domains which are shared the most files.
Top External Users	Shows external users which are shared the most files.

Documents

The Documents page shows all the files FortiCASB currently monitors. The infographic gives an overview of the files categorized by **File Type**, **Data Analysis**, and **Share Type**.

When the cloud application is first added to FortiCASB, files are pulled from the cloud application account to Documents page. Thereafter, FortiCASB automatically updates the Documents page when users attempt to access files on the cloud application account.

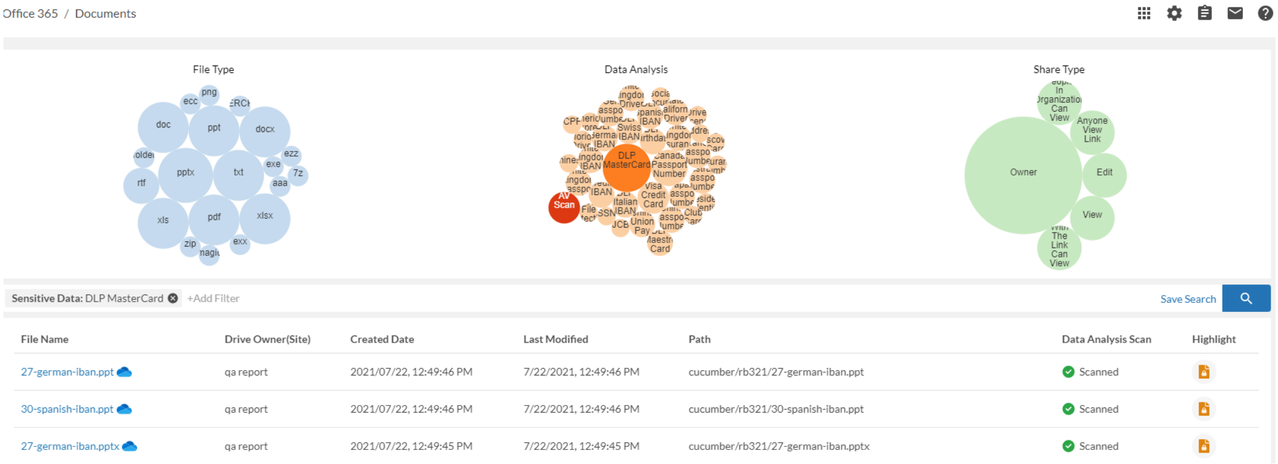
Document Filter on page 53

Microsoft Online Application Integration (Office 365 Only) on page 54

Document Filter

Click on the infographic bubbles to filter documents by **File Type**, **Data Analysis**, or **Share Type**. Data Analysis filters files through DLP scan, the results are categorized by the type of DLP search.

For example, click on the bubble, "DLP Master Card" filter will only show files with Master Card numbers.



Sensitive Data: DLP MasterCard ⊗ +Add Filter

Save Search

File Name	Drive Owner(Site)	Created Date	Last Modified	Path	Data Analysis Scan	Highlight
27-german-iban.ppt ☁	qa report	2021/07/22, 12:49:46 PM	7/22/2021, 12:49:46 PM	cucumber/rb321/27-german-iban.ppt	✓ Scanned	🔒
30-spanish-iban.ppt ☁	qa report	2021/07/22, 12:49:46 PM	7/22/2021, 12:49:46 PM	cucumber/rb321/30-spanish-iban.ppt	✓ Scanned	🔒
27-german-iban.pptx ☁	qa report	2021/07/22, 12:49:45 PM	7/22/2021, 12:49:45 PM	cucumber/rb321/27-german-iban.pptx	✓ Scanned	🔒

Click on one of the file will show all the relevant info related to the file. It has credit card number, master card numb

Highlight

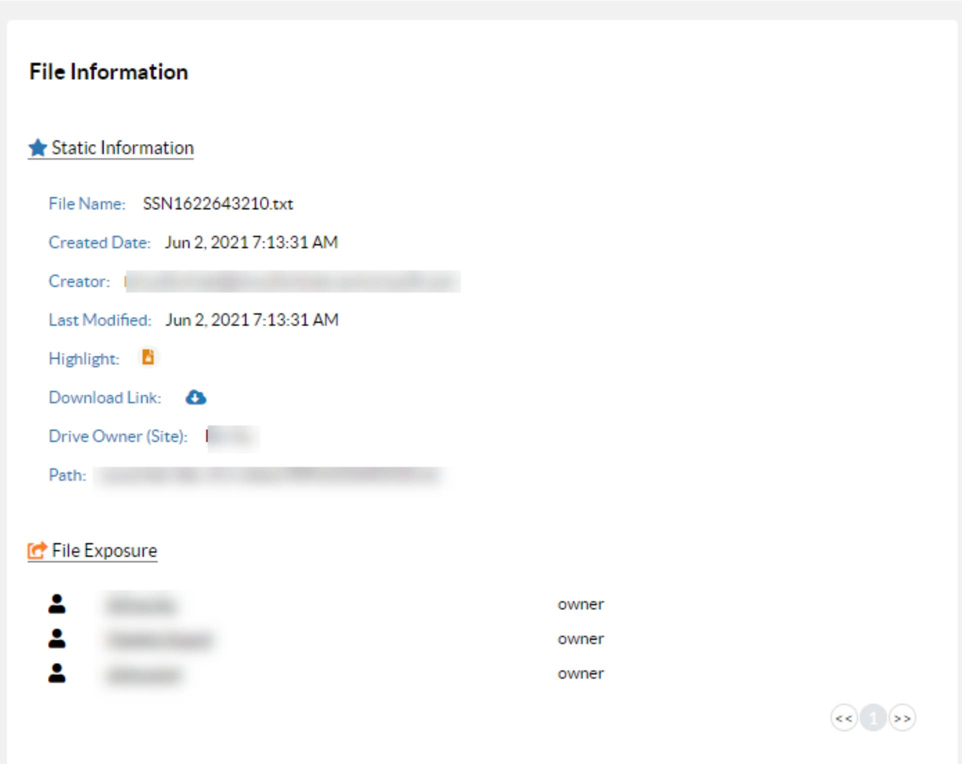
The highlight icon displays specific document type, below is correlated file type with description.

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.

Action

In **Action** column, Click ↗ to view **detail** information on the file.

In the file information page. you can view and **download** the file by clicking ☁.



File Information

★ Static Information

File Name: SSN1622643210.txt

Created Date: Jun 2, 2021 7:13:31 AM

Creator: [redacted]

Last Modified: Jun 2, 2021 7:13:31 AM

Highlight:

Download Link:

Drive Owner (Site): [redacted]

Path: [redacted]

File Exposure

[redacted]	owner
[redacted]	owner
[redacted]	owner

Microsoft Online Application Integration (Office 365 Only)

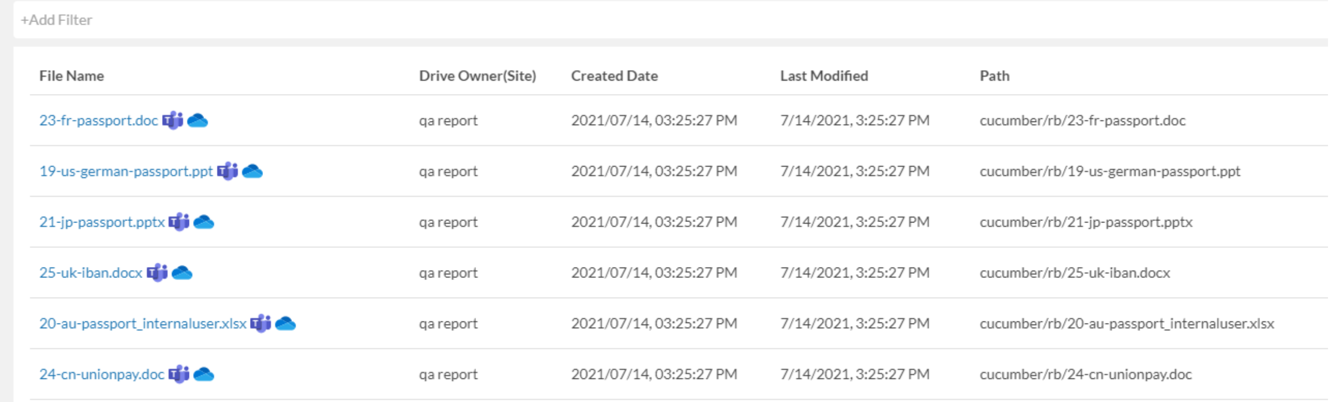
The Microsoft online application integration monitors **Microsoft Yammer, Microsoft One Drive, Microsoft Sharepoint**, and **Microsoft Teams**.

In **FortiCASB > Office 365 > Documents**, all shared files from Microsoft Online Application are shown with corresponding logos.

Microsoft Online Application 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.



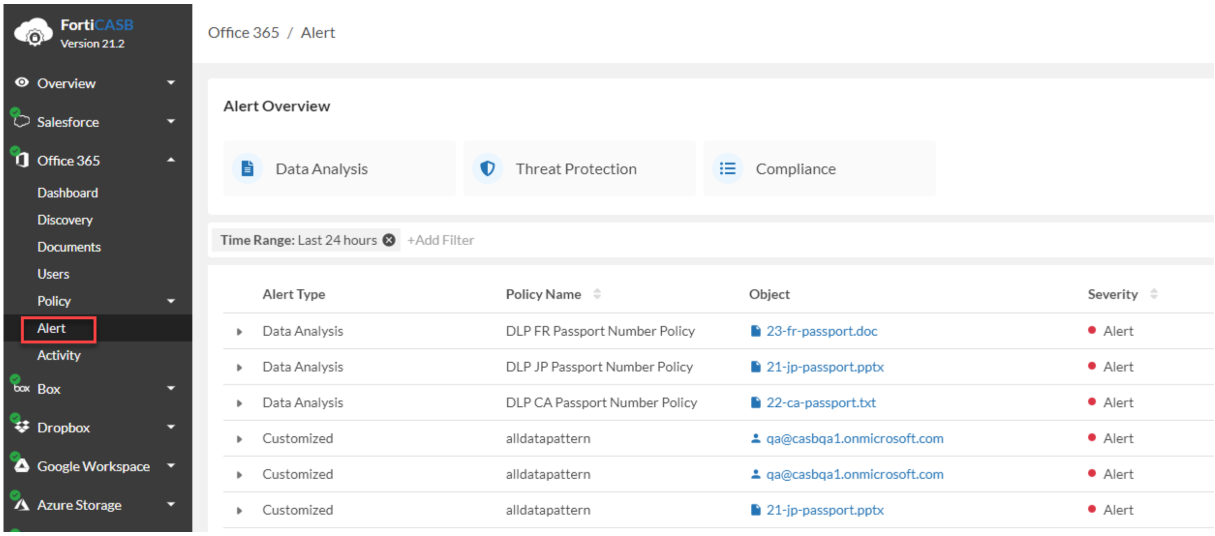
File Name	Drive Owner(Site)	Created Date	Last Modified	Path
23-fr-passport.doc	qa report	2021/07/14, 03:25:27 PM	7/14/2021, 3:25:27 PM	cucumber/rb/23-fr-passport.doc
19-us-german-passport.ppt	qa report	2021/07/14, 03:25:27 PM	7/14/2021, 3:25:27 PM	cucumber/rb/19-us-german-passport.ppt
21-jp-passport.pptx	qa report	2021/07/14, 03:25:27 PM	7/14/2021, 3:25:27 PM	cucumber/rb/21-jp-passport.pptx
25-uk-iban.docx	qa report	2021/07/14, 03:25:27 PM	7/14/2021, 3:25:27 PM	cucumber/rb/25-uk-iban.docx
20-au-passport_internaluser.xlsx	qa report	2021/07/14, 03:25:27 PM	7/14/2021, 3:25:27 PM	cucumber/rb/20-au-passport_internaluser.xlsx
24-cn-unionpay.doc	qa report	2021/07/14, 03:25:27 PM	7/14/2021, 3:25:27 PM	cucumber/rb/24-cn-unionpay.doc

Alert

FortiCASB sends you alerts when any of the **enabled** policy is triggered by user activity.

- DLP 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.

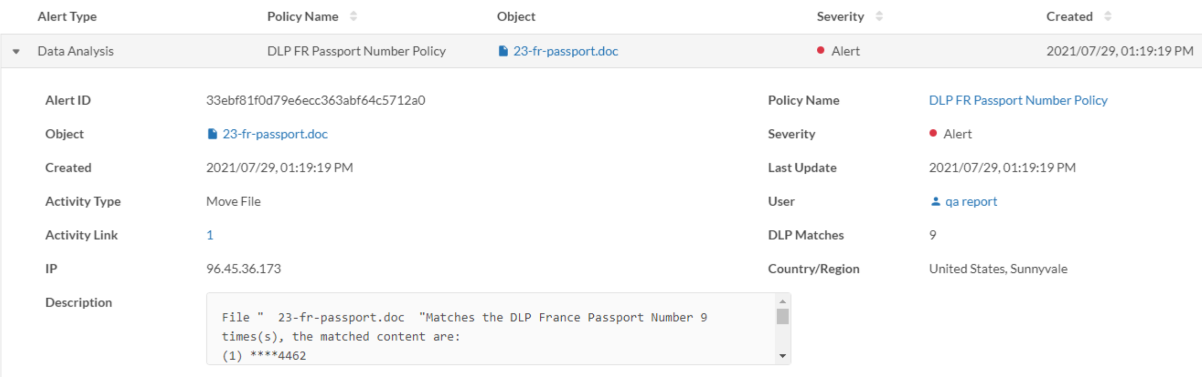
To view alerts of each cloud application, click on a cloud application drop down menu and click on **Alert**.



Alert Type	Policy Name	Object	Severity
Data Analysis	DLP FR Passport Number Policy	23-fr-passport.doc	● Alert
Data Analysis	DLP JP Passport Number Policy	21-jp-passport.pptx	● Alert
Data Analysis	DLP CA Passport Number Policy	22-ca-passport.txt	● Alert
Customized	alldatapattern	qa@casbqa1.onmicrosoft.com	● Alert
Customized	alldatapattern	qa@casbqa1.onmicrosoft.com	● Alert
Customized	alldatapattern	21-jp-passport.pptx	● 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.



Alert Type	Policy Name	Object	Severity	Created
Data Analysis	DLP FR Passport Number Policy	23-fr-passport.doc	● Alert	2021/07/29, 01:19:19 PM

Alert ID	33ebf81f0d79e6ecc363abf64c5712a0	Policy Name	DLP FR Passport Number Policy
Object	23-fr-passport.doc	Severity	● Alert
Created	2021/07/29, 01:19:19 PM	Last Update	2021/07/29, 01:19:19 PM
Activity Type	Move File	User	qa report
Activity Link	1	DLP Matches	9
IP	96.45.36.173	Country/Region	United States, Sunnyvale

Description

```
File "  23-fr-passport.doc  "Matches the DLP France Passport Number 9
times(s), the matched content are:
(1) ****4462
```

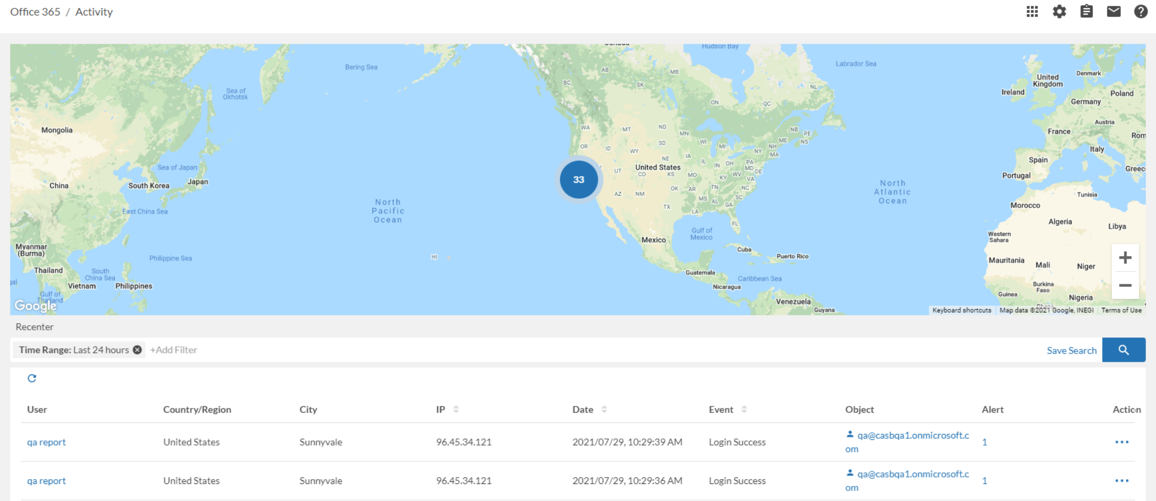
To enable a policy to trigger alert, please refer to Policy Configuration.

Daily alerts can be compiled into Alert reports for export, please see Activate Alert Report on page 46.

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.



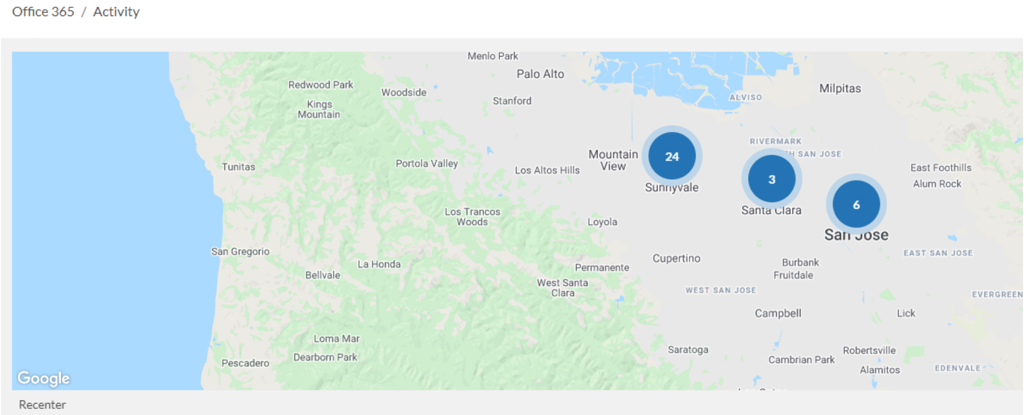
Office 365 / Activity

Time Range: Last 24 hours +Add Filter

User	Country/Region	City	IP	Date	Event	Object	Alert	Action
qa report	United States	Sunnyvale	96.45.34.121	2021/07/29, 10:29:39 AM	Login Success	qa@casbqa1.onmicrosoft.com	1	•••
qa report	United States	Sunnyvale	96.45.34.121	2021/07/29, 10:29:36 AM	Login Success	qa@casbqa1.onmicrosoft.com	1	•••

Activity Map options

- **Activity**—Click on an activity bubble on the map to bring up an activities at that specific location.



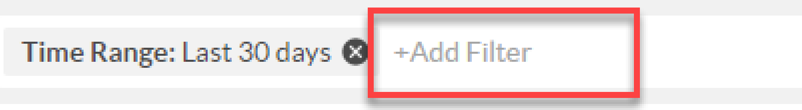
Office 365 / Activity

Recenter

- **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.
- **Clear Map**—Click the **Clear Map** button to clear the map of activity indicators.

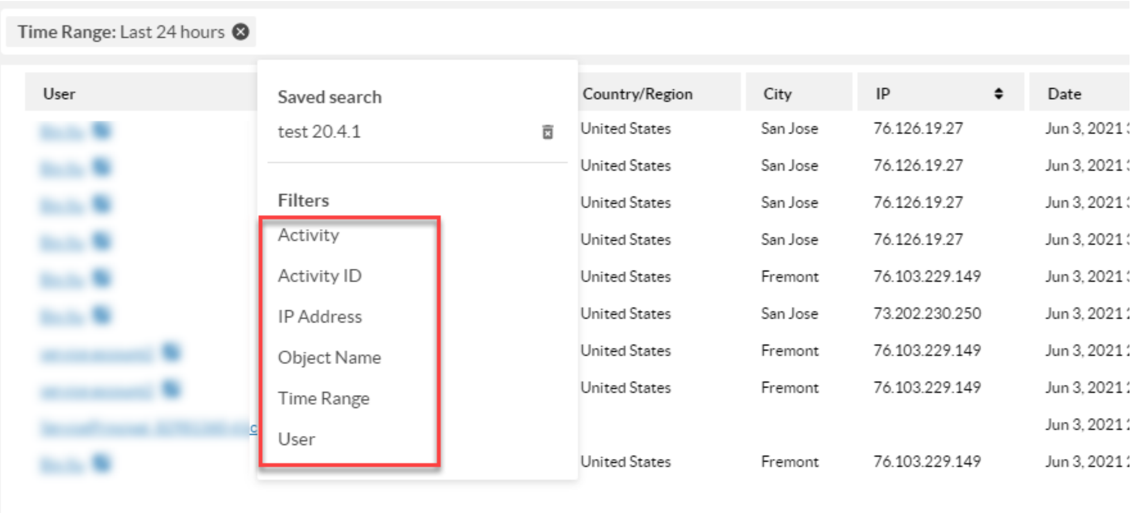
Activity Filter Example

1. Click on **+Add Filter** drop down menu.



Time Range: Last 30 days ⊗ +Add Filter

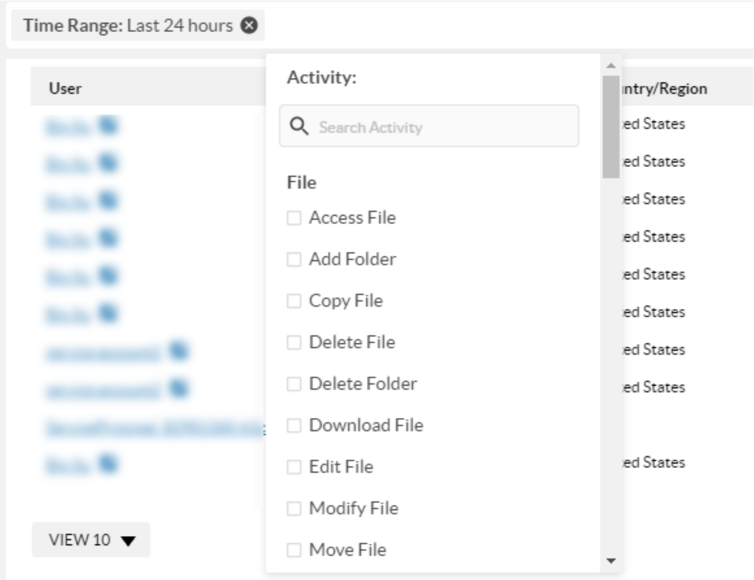
2. Select a filter type, "Activity".



Time Range: Last 24 hours ⊗

User	Country/Region	City	IP	Date
[redacted]	United States	San Jose	76.126.19.27	Jun 3, 2021
[redacted]	United States	San Jose	76.126.19.27	Jun 3, 2021
[redacted]	United States	San Jose	76.126.19.27	Jun 3, 2021
[redacted]	United States	San Jose	76.126.19.27	Jun 3, 2021
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021
[redacted]	United States	San Jose	73.202.230.250	Jun 3, 2021
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021
[redacted]				Jun 3, 2021
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021

3. Then scroll down to select a type of activity, "Access File".



Time Range: Last 24 hours ⊗

Activity:

Search Activity

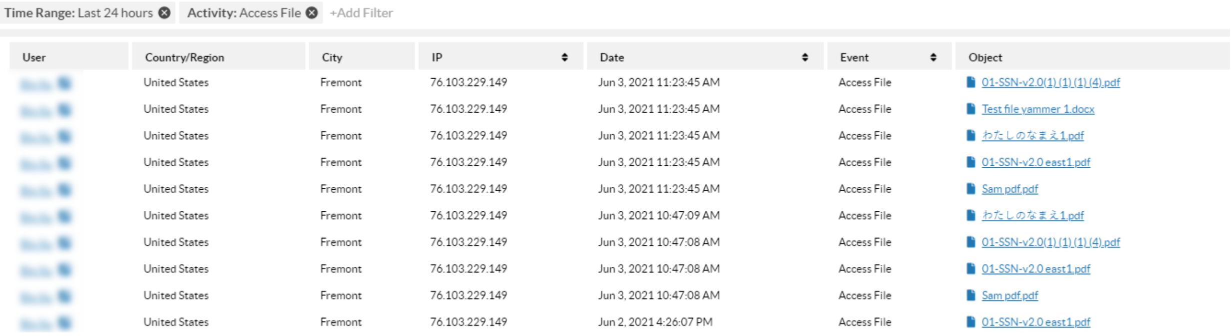
File

- □ Access File
- □ Add Folder
- □ Copy File
- □ Delete File
- □ Delete Folder
- □ Download File
- □ Edit File
- □ Modify File
- □ Move File

User	ntry/Region
[redacted]	ed States
[redacted]	ed States
[redacted]	ed States
[redacted]	ed States
[redacted]	ed States
[redacted]	ed States
[redacted]	ed States
[redacted]	ed States
[redacted]	
[redacted]	ed States

VIEW 10 ▼

4. Then click Search button to update the search with the filter, only "Access File" activities will be shown in the time range.



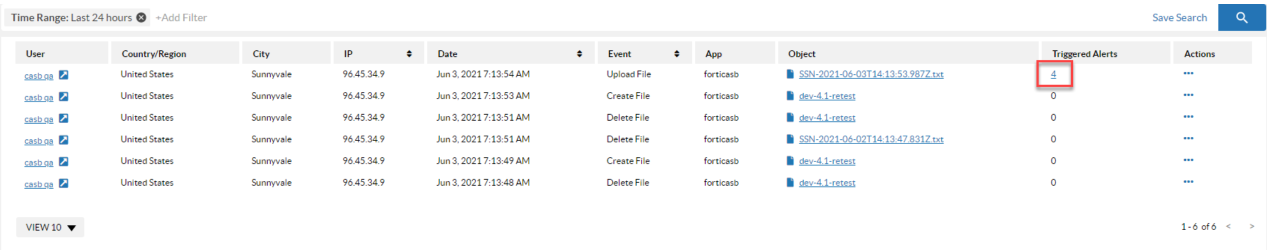
Time Range: Last 24 hours ⊗ Activity: Access File ⊗ +Add Filter

User	Country/Region	City	IP	Date	Event	Object
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 11:23:45 AM	Access File	01-SSN-v2.0(1) (1) (1) (4).pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 11:23:45 AM	Access File	Test file yammer 1.docx
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 11:23:45 AM	Access File	わたしのなまえ1.pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 11:23:45 AM	Access File	01-SSN-v2.0 east1.pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 11:23:45 AM	Access File	Sam pdf.pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 10:47:09 AM	Access File	わたしのなまえ1.pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 10:47:08 AM	Access File	01-SSN-v2.0(1) (1) (1) (4).pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 10:47:08 AM	Access File	01-SSN-v2.0 east1.pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 3, 2021 10:47:08 AM	Access File	Sam pdf.pdf
[redacted]	United States	Fremont	76.103.229.149	Jun 2, 2021 4:26:07 PM	Access File	01-SSN-v2.0 east1.pdf

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**.



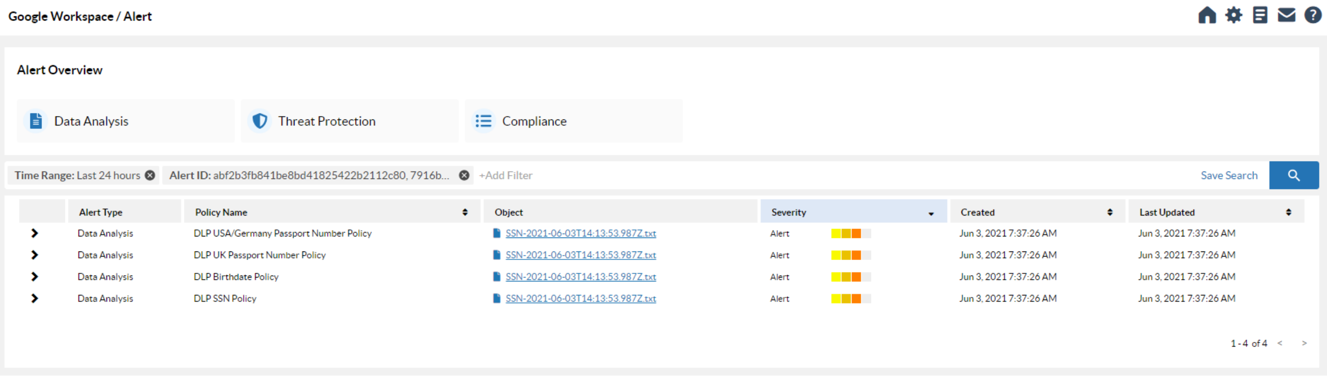
Time Range: Last 24 hours ⊗ +Add Filter Save Search

User	Country/Region	City	IP	Date	Event	App	Object	Triggered Alerts	Actions
casb qa	United States	Sunnyvale	96.45.34.9	Jun 3, 2021 7:13:54 AM	Upload File	forticasb	SSN-2021-06-03T14:13:53.987Z.txt	4	•••
casb qa	United States	Sunnyvale	96.45.34.9	Jun 3, 2021 7:13:53 AM	Create File	forticasb	dev-4.1-retest	0	•••
casb qa	United States	Sunnyvale	96.45.34.9	Jun 3, 2021 7:13:51 AM	Delete File	forticasb	dev-4.1-retest	0	•••
casb qa	United States	Sunnyvale	96.45.34.9	Jun 3, 2021 7:13:51 AM	Delete File	forticasb	SSN-2021-06-02T14:13:47.831Z.txt	0	•••
casb qa	United States	Sunnyvale	96.45.34.9	Jun 3, 2021 7:13:49 AM	Create File	forticasb	dev-4.1-retest	0	•••
casb qa	United States	Sunnyvale	96.45.34.9	Jun 3, 2021 7:13:48 AM	Delete File	forticasb	dev-4.1-retest	0	•••

VIEW 10 ▼ 1-6 of 6 < >

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.



	Alert Type	Policy Name	Object	Severity	Created	Last Updated
›	Data Analysis	DLP USA/Germany Passport Number Policy	SSN-2021-06-03T14:13:53.987Z.txt	Alert	Jun 3, 2021 7:37:26 AM	Jun 3, 2021 7:37:26 AM
›	Data Analysis	DLP UK Passport Number Policy	SSN-2021-06-03T14:13:53.987Z.txt	Alert	Jun 3, 2021 7:37:26 AM	Jun 3, 2021 7:37:26 AM
›	Data Analysis	DLP Birthdate Policy	SSN-2021-06-03T14:13:53.987Z.txt	Alert	Jun 3, 2021 7:37:26 AM	Jun 3, 2021 7:37:26 AM
›	Data Analysis	DLP SSN Policy	SSN-2021-06-03T14:13:53.987Z.txt	Alert	Jun 3, 2021 7:37:26 AM	Jun 3, 2021 7:37:26 AM

Daily cloud account activities will be compiled into Activity reports for export, please see Activity Report.

Appendix A - Documentation references

FortiCASB Online Help

www.fortinet.com