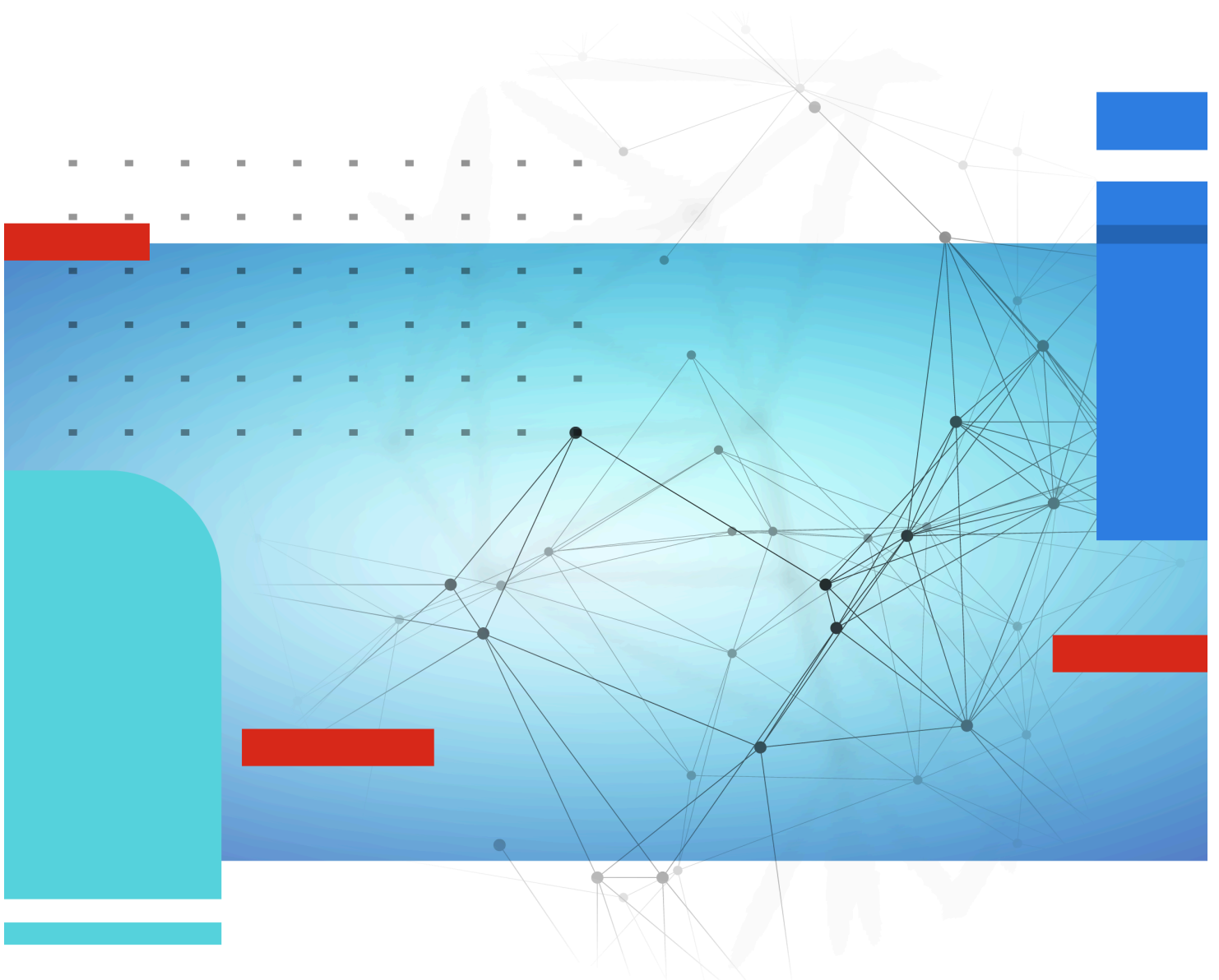




FortiCASB-SSPM Application Connector

Google Workspace Connector



Google Workspace Connector



Category

- IAM

Connection Method

- OAuth
- Service Account

Supported SSOs for connection

- Okta

Data Collected

- Misconfigurations
- 3rd Party Applications
- Tokens
- Identities
- Activities
- Data Posture

Supported Actions

- Revoke Permissions to 3rd-party apps

Integration Guide

Intro

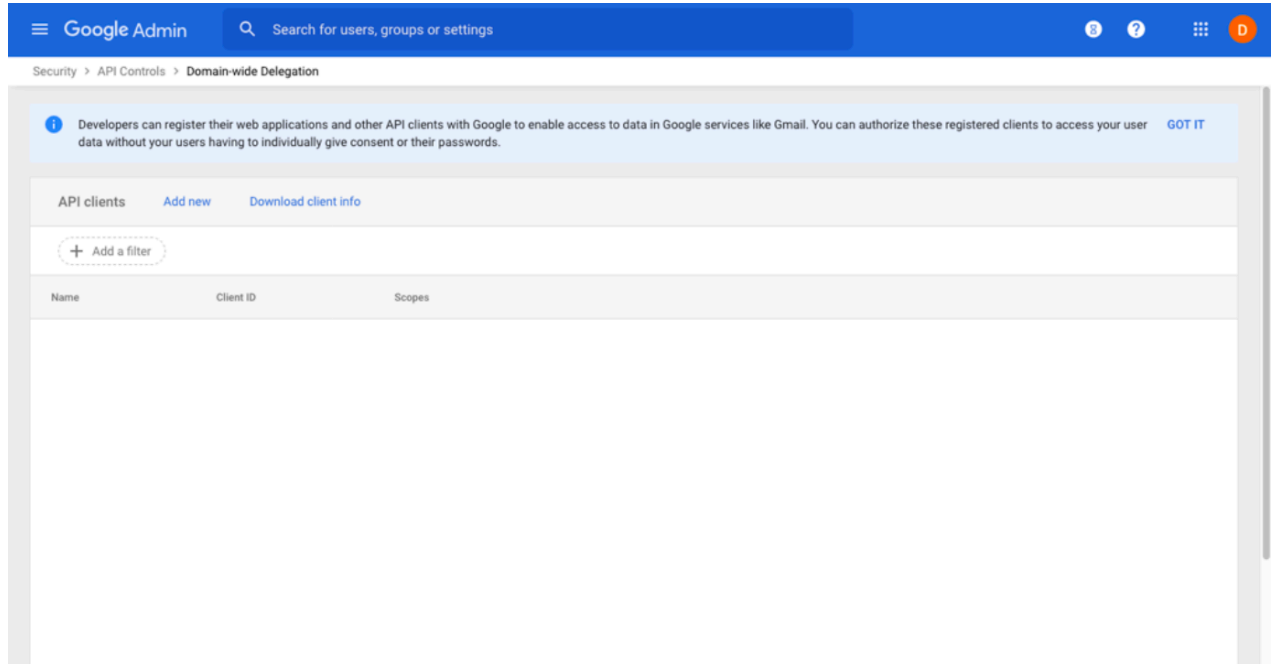
Use this guide to add Google Workspace as a secured SaaS application in FortiCASB-SSPM SaaS Security platform.

This integration guides includes the following parts:

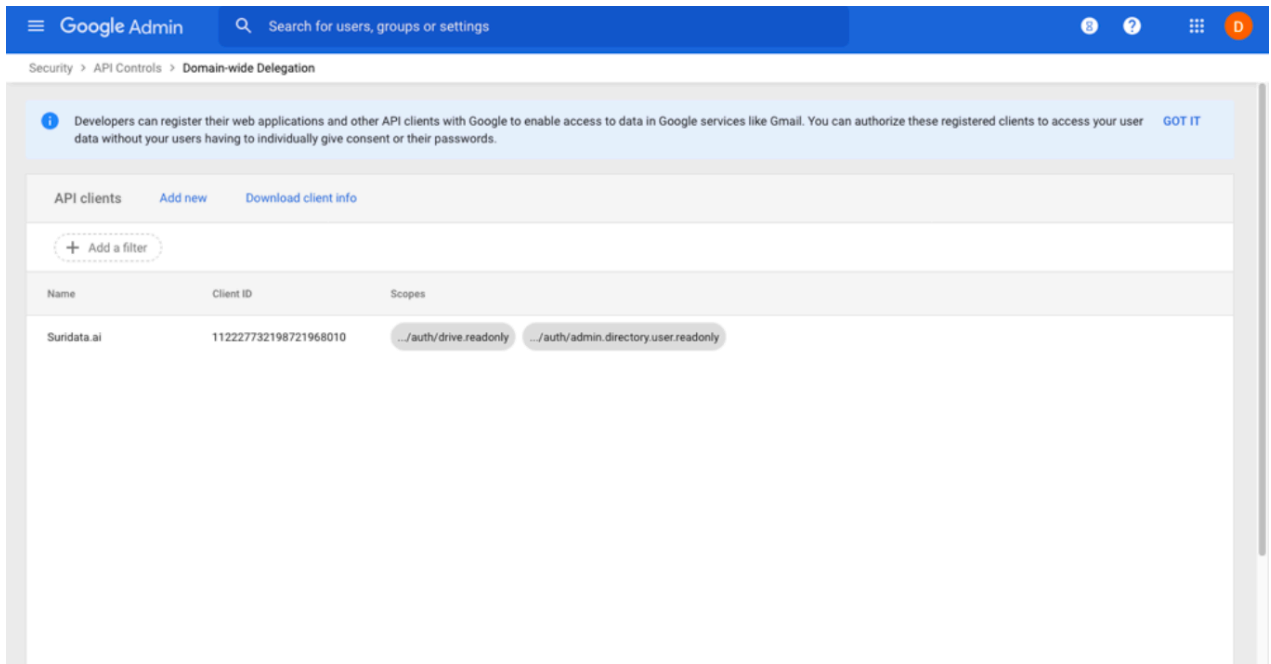
- Setting up domain-wide delegation for Fortinet platform
- Creating a Super admin service account and setting up 2-Step verification
- Adding permissions for Google tokens collection (not mandatory)
- Adding Google Workspace application to the FortiCASB-SSPM platform

Part A: Set up domain-wide delegations for Fortinet platform

1. Sign into your Google Admin console at <https://admin.google.com/>
2. Sign in using an account with Super Administrator privileges
3. From the Admin console home page, go to menu and then security and then API controls
4. Under domain wide delegation, click manage domain wide delegation

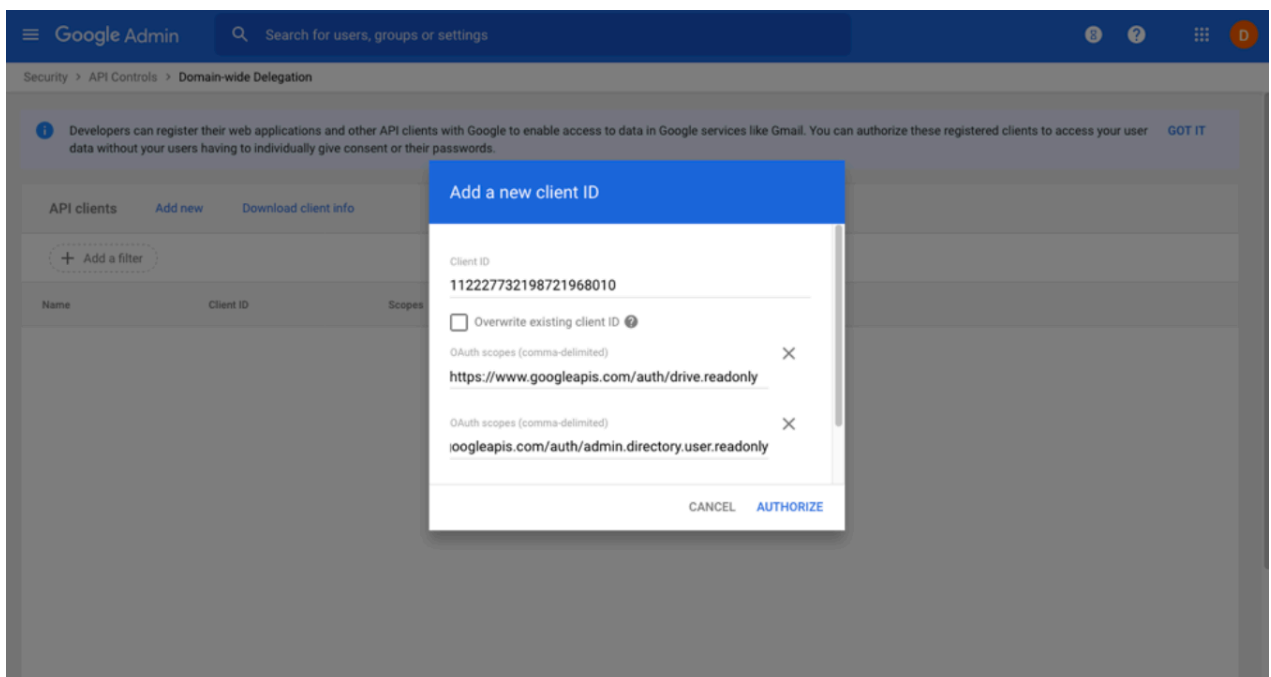


5. On the manage domain wide delegation page, click add new
6. Enter the client ID: 112227732198721968010. In OAuth Scopes, add each scope that the application will have access:
 - o <https://www.googleapis.com/auth/admin.directory.user.readonly>
 - o <https://www.googleapis.com/auth/admin.directory.group.readonly>
 - o <https://www.googleapis.com/auth/admin.directory.orgunit.readonly>
 - o <https://www.googleapis.com/auth/admin.directory.user.security>
 - o <https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly>
 - o <https://www.googleapis.com/auth/admin.reports.audit.readonly>
 - o <https://www.googleapis.com/auth/apps.groups.settings>
 - o <https://www.googleapis.com/auth/cloud-platform>



7. Click “Authorize”

8. The FortiCASB-SSPM app should appear in the admin console



Part B: Create a Super Admin service account and set up 2-Step verification

1. Create a new user and grant a Super Admin role
2. Enroll to 2-Step Verification:
 1. First enroll with a phone number
 2. Once verified add second method using Authenticator app
 3. Press “set up authenticator”

← Authenticator app

Instead of waiting for text messages, get verification codes from an authenticator app. It works even if your phone is offline.

First, download Google Authenticator from the [Google Play Store](#) or the [iOS App Store](#).



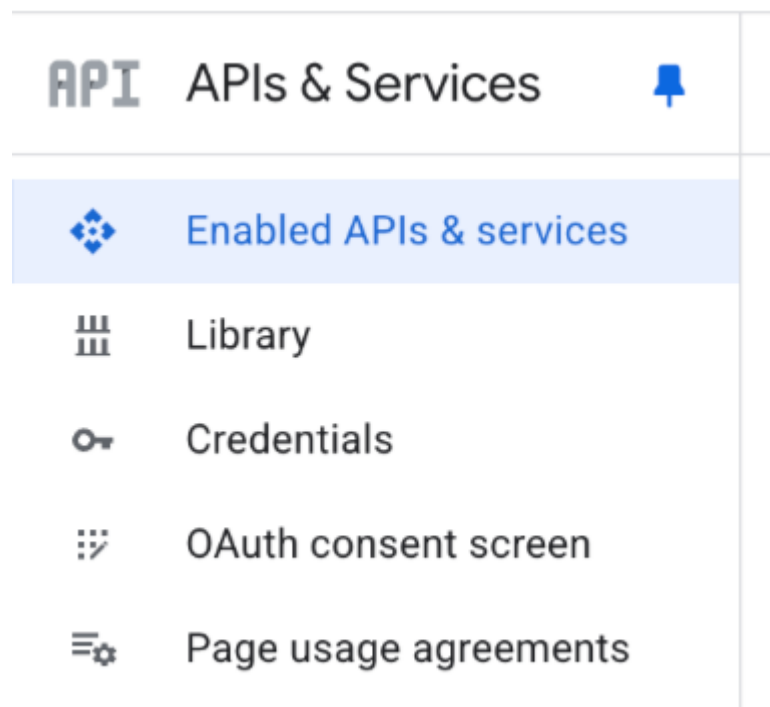
[+ Set up authenticator](#)

4. Click on "Can't scan it?"
5. Copy the code (this is the OTP Secret) in section 2 and click next
3. Continue to Add Google Workspace (on the following parts)

Part C: Adding permissions for Google tokens collection

Step 1- enabling the APIs

1. Login to console.cloud.google.com
2. Select required project or projects
3. Navigae on the menu to APIs & Services
4. Enable API Keys API and Identity and Access Management (IAM) API



☰ Filter Filter

Name

[Google Drive API](#)

[Gmail API](#)

[Admin SDK API](#)

[Groups Settings API](#)

[API Keys API](#)

[Identity and Access Management \(IAM\) API](#)

[Cloud Resource Manager API](#)

[Cloud Logging API](#)

[Drive Labels API](#)

[Access Context Manager API](#)

[BigQuery API](#)

[BigQuery Storage API](#)

[Cloud Datastore API](#)

[Cloud Monitoring API](#)

Step 2- grant permissions

1. In the project selection, change to organization level
2. In menu navigate to IAM & Admin, then IAM
3. Click Grant Access
4. As principal enter the email of the service-account
5. In assigned roles select API Keys Viewer

Part D: Add Google Workspace to the platform

1. Navigate to the App Store → Click on Google Workspace



Google Workspace

Google Workspace



Note: Before you authorize make sure you complete the following steps:

- Sign in to your "[Domain-wide Delegation](#)" on [Google Admin console](#) using your google account with super administrator privileges.
- Add a new client ID with the following details:

Client ID: **112227732198721968010**

OAuth Scopes:

[https://www.googleapis.com/auth/
admin.directory.user.readonly](https://www.googleapis.com/auth/admin.directory.user.readonly)

[https://www.googleapis.com/auth/
admin.directory.group.readonly](https://www.googleapis.com/auth/admin.directory.group.readonly)

[https://www.googleapis.com/auth/
admin.directory.orgunit.readonly](https://www.googleapis.com/auth/admin.directory.orgunit.readonly)

[https://www.googleapis.com/auth/
admin.directory.user.security](https://www.googleapis.com/auth/admin.directory.user.security)

[https://www.googleapis.com/auth/
admin.directory.rolemanagement.readonly](https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly)

[https://www.googleapis.com/auth/
admin.reports.audit.readonly](https://www.googleapis.com/auth/admin.reports.audit.readonly)

<https://www.googleapis.com/auth/apps.groups.settings>

<https://www.googleapis.com/auth/cloud-platform>

 [Create External Link](#)

[Connect](#)

2. Click "Connect"

3. Sign in using a google account with super administrator privileges

Sign in

to continue to **Suridata**

[Forgot email?](#)

To continue, Google will share your name, email address, language preference, and profile picture with Suridata.

[Create account](#)

[Next](#)

English (United States) ▼

[Help](#)

[Privacy](#)

[Terms](#)

4. The Google authentication window will disappear once login is complete, and a username and password screen will appear
5. Enter the service account Username, Password and OTP Secret from previous section and press SHOW PASSCODE



Google Workspace

Google Workspace



Select a shared account

Shared Accounts *

 shiran@test1.com via Azure

Use an application account

SSO Provider

No SSO Provider

Username *

Password *

OTP Secret

Generate

Save as Shared Account

Used as IDP

[Create External Link](#)

Back

Next

6. Copy the Time-based one-time password

7. Paste the authentication code into the browser in the Authentication Code input field and click Submit.

If you are prompted with a Google Login Challenge due to suspicious activity, and SSO is enabled, enter the Google Login Challenge OTP in the next step to bypass MFA



Google Workspace

Google Workspace

 [Create External Link](#)

8. Remove the 2-Step verification phone method

9. Return to the connection page and complete the process by clicking "Connect".

That's it! You're all set.

Your SaaS security is our priority!

The FortiCASB-SSPM team

FORTINET[®]