



ZSCALER AND GOOGLE SECOPS DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	6
Zscaler Overview	6
Google Overview	6
Audience	6
Software Versions	6
Request for Comments	6
Zscaler and Google Introduction	7
ZIA Overview	7
Google SecOps Overview	8
Google Resources	8
Collect Zscaler logs	9
Overview	9
Prerequisites	9
Set Up HTTPS Push Ingestion Using a Webhook	10
Zscaler Setup Steps	20
Check Google SecOps Dashboard	23
Search for Zscaler Logs in Google SecOps	24
Contextualizing Risk Using Google Cloud and Avalor UVM	26
Enable Programmatic Access to a Google Cloud Tenant	27
Create an Avalor UVM Service Account	27
Configure the Google Cloud Data Connectors	31
Google Cloud Platform—Assets Data Source	31
Google Cloud Platform—Vulnerabilities Data Source	35
Google Cloud Platform—Misconfigurations Data Source	39

Google Workspace—Drive Activity Data Source	43
Google Workspace—Admin Activity Data Source	47
Google Workspace—Login Activity Data Source	50
Google Workspace—Mobile Activity Data Source	53
Google Workspace—OAuth Tokens Activity Data Source	56
Google Workspace—Rules Activity Source	59
Google Workspace—Access Transparency Activity Data Source	62
Google Workspace—Calendar Activity Data Source	65
Google Workspace—Chat Activity Data Source	68
Google Workspace—Chrome Activity Data Source	71
Google Workspace—Context-Aware Access Activity Data Source	74
Google Workspace—Data Studio Activity Data Source	77
Google Workspace—Google Cloud Platform Activity Data Source	80
Google Workspace—Google+ Activity Data Source	83
Google Workspace—Groups Activity Data Source	86
Google Workspace—Keep Activity Data Source	89
Google Workspace—SAML Activity Data Source	92
Google Workspace—Tokens Activity Data Source	95
Google Workspace—User Accounts Activity Data Source	98
Google Workspace—Enterprise Groups Activity Data Source	101
Google Sheets	104
Review and Adjust Data Model Mapping	110
Create a Crown Jewel Label for a Google Cloud Compute Engine VM	110
Review and Adjust Risk Scoring	117

Appendix A: Requesting Zscaler Support 120

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
BYOP	Bring Your Own Project (Google)
CA	Central Authority (Zscaler)
CCP	Certified Cyber Professional
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GKE	Google Kubernetes Engine (Google)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NSS	Nanolog Streaming Service
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SIEM	Security Information and Event Management
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: [ZS](#)) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see [Zscaler's website](#) or follow Zscaler on Twitter @zscaler.

Google Overview

Google (NASDAQ: [GOOGL](#)) is an American multinational corporation and technology company focusing on online advertising, search engine technology, cloud computing, computer software, quantum computing, e-commerce, consumer electronics, and artificial intelligence (AI). Its mission is to organize the world's information and make it universally accessible and useful. It is one of the world's most valuable brands due to its market dominance, data collection, and technological advantages in the field of AI. Google's parent company, Alphabet Inc., is one of the five Big Tech companies, alongside Amazon, Apple, Meta, and Microsoft. To learn more, see [Google's website](#).

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- [Zscaler Resources](#)
- [Google Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers:** Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees:** Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Google Introduction

Overviews of the Zscaler and Google applications are described in this section.



If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Google SecOps Overview

Google Security Operations is a cloud service, built as a specialized layer on top of Google infrastructure, designed for enterprises to privately retain, analyze, and search the large amounts of security and network telemetry they generate.

Google Security Operations normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity. You can use Google Security Operations to detect threats, investigate the scope and cause of those threats, and provide remediation using prebuilt integrations with enterprise workflow, response, and orchestration platforms.

Google SecOps lets you examine the aggregated security information for your enterprise going back for months or longer. Use Google Security Operations to search across all of the domains accessed within your enterprise. You can narrow your search to any specific asset, domain, or IP address to determine if any compromise has taken place.

The Google SecOps platform enables security analysts to analyze and mitigate a security threat throughout its lifecycle by employing the following capabilities:

- **Collection:** Data is ingested into the platform using forwarders, parsers, connectors, and webhooks.
- **Detection:** This data is aggregated, normalized using the Universal Data Model (UDM), and linked to detections and threat intelligence.
- **Investigation:** Threats are investigated through case management, search, collaboration, and context-aware analytics.
- **Response:** Security analysts can respond quickly and provide resolutions using automated playbooks and incident management.

Google Resources

The following table contains links to Google support resources.

Name	Definition
Google SecOps Documentation	Online documentation for Google SecOps.
Google SecOps Support	Online support portal for Google SecOps.

Collect Zscaler logs

This document describes how you can bring Zscaler Internet Access (ZIA) logs into Google SecOps (formerly known as Google Chronicle) using a webhook. This document also lists currently supported Zscaler log types.

For more information on Google SecOps ingestion, refer to the [Google SecOps documentation](#).

Overview

The following deployment architecture diagram shows how Zscaler NSS are configured to send logs to Google SecOps. Each customer deployment might differ from this representation and might be more complex.

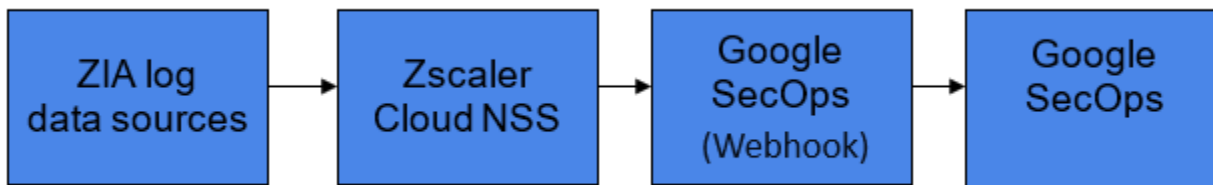


Figure 1. Zscaler and Google SecOps architecture

The architecture diagram shows the following components:

- Data sources: Different types of ZIA logs (Web/Firewall/DNS, etc.).
- Zscaler Cloud NSS: Forwards ZIA logs to Google SecOps via Webhook.
- Google SecOps Webhook: An HTTPS push endpoint to forward the logs to Google SecOps.
- Google SecOps: Retains and analyzes the logs from Zscaler as well as other log sources.

An ingestion label identifies the parser that normalizes raw log data to structured UDM format. As Google SecOps supports different Zscaler technologies, refer to the [parser link](#) and filter on `zscaler` for the full list.

Prerequisites

Make sure the following prerequisites are met:

- Ensure that a [Google Cloud project for Google SecOps](#) is configured and Google SecOps API is enabled for the project.
- [Link a Google SecOps instance](#) to Google Cloud services.
- Ensure that you have access to [Feed management API](#).
- Ensure that the webhook is enabled on your Google SecOps tenant's feed management.
- BYOP API Credential and the webhook API Secret Key are created (detailed steps follow).

Set Up HTTPS Push Ingestion Using a Webhook

You can send Zscaler logs to Google SecOps using an HTTPS webhook. You must first configure a feed with the appropriate log type before configuring an HTTPS webhook to send data.

To set up HTTPS push ingestion using an HTTPS webhook:

1. In the **Google SecOps Feeds** window, click **Add New**.

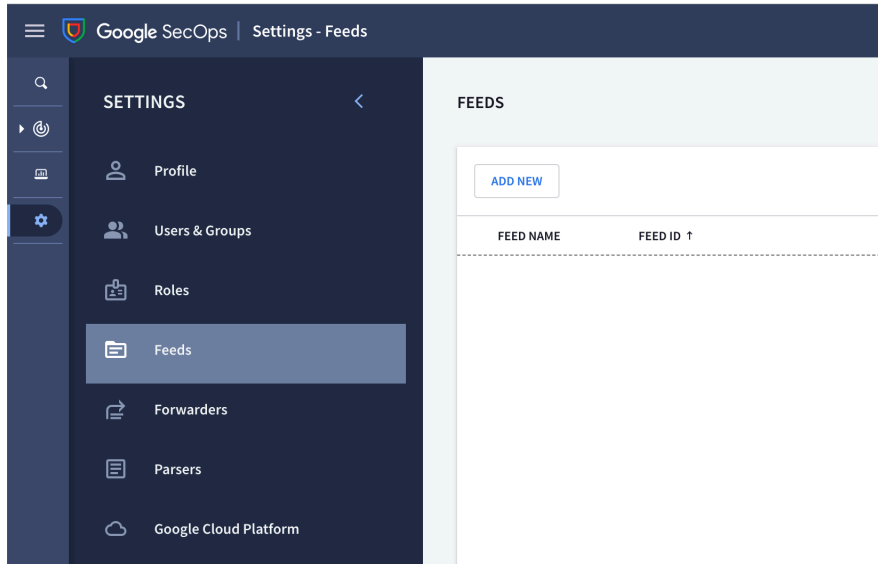


Figure 2. New Feed

2. On the **Add Feed** window, input the following fields:
 - a. **Feed Name:** Enter a name to identify this new feed (e.g., `ZIA_Web`).
 - b. **Source Type:** From the drop-down menu, select **Webhook**.
 - c. **Log Type:** From the drop-down menu, select the correct log type label. See the [parser link](#) for the different ingestion labels. (e.g., **Zscaler** for ZIA Web logs, **Zscaler NGFW** for ZIA Firewall logs, and **Zscaler DNS** for ZIA DNS logs).
 - d. Click **Next**.

ADD FEED

1 Set Properties — 2 Input Parameters — 3 Finalize

To add a feed, select a source type and log type. [Learn more about adding feeds.](#)

FEED NAME *

ZIA_Web

SOURCE TYPE ?

Webhook

LOG TYPE ?

Zscaler

CANCEL PREVIOUS NEXT

Figure 3. Set Properties

3. On the **Input Parameters** window, input the required information:
 - a. **Split Delimiter**: Indicate the delimiter separating the logs to be sent to Google SecOps. Enter `\n` for ZIA logs.
 - b. **Asset Namespace**: (Optional but recommended) Add additional context on the logs.
 - c. **Ingestion Labels**: (Optional but recommended) Add additional context.
 - d. Click **Next**.

ADD FEED

✓ Set Properties — 2 Input Parameters — 3 Finalize

* Required Fields

SPLIT DELIMITER ?
Input: \n

ASSET NAMESPACE ?
Input: Namespace

INGESTION LABELS ?
+ ADD LABEL

Feed Name
ZIA_Web

Source type
Webhook

Log type
Zscaler

CANCEL PREVIOUS NEXT

Figure 4. Input Parameters

4. Confirm your configurations and click **Submit**.

The screenshot shows a web interface for adding a feed. At the top, the title is "ADD FEED". Below it is a progress bar with three steps: "Set Properties" (checked), "Input Parameters" (checked), and "3 Finalize" (active). The main content area lists the following configuration details:

- Feed Name: ZIA_Web
- Source type: Webhook
- Log type: Zscaler
- Split Delimiter: \n
- Asset Namespace:
- Ingestion Labels:

On the right side, there is an information box with a blue 'i' icon. It contains the text "Up next: Generate a secret key and an API key" followed by two bullet points:

- After saving your feed, you'll generate a secret key in the next step
- To generate an API key, go to the Google Cloud Console: [APIs & Services > Credentials](#)

Below the information box is a link: [Learn about authenticating feeds](#)

At the bottom right, there are three buttons: "CANCEL", "PREVIOUS", and "SUBMIT".

Figure 5. Finalize

5. Click **Generate Secret Key** to generate the key.

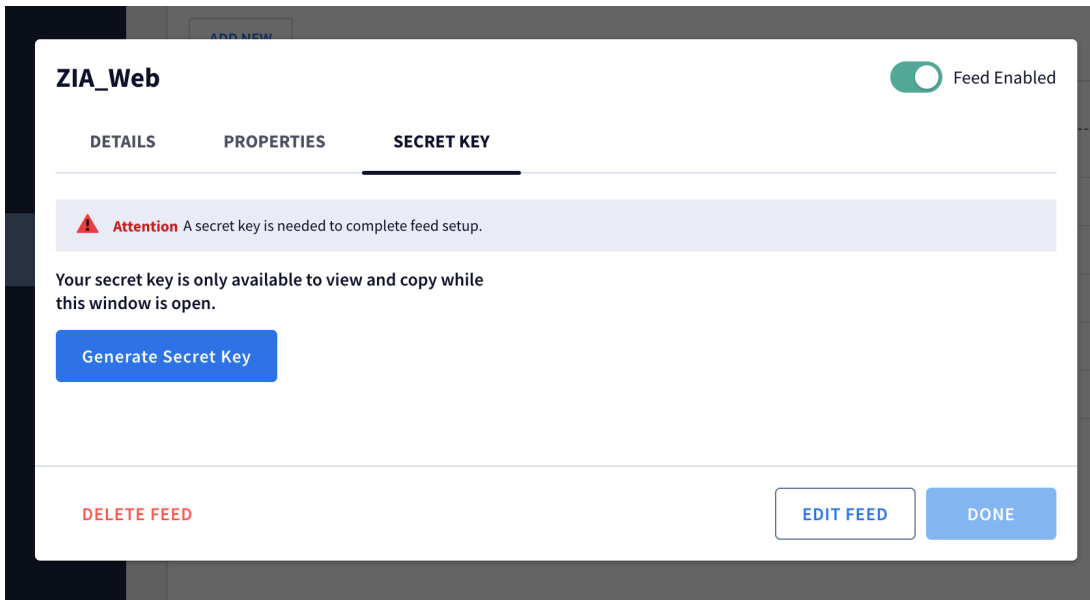


Figure 6. Secret Key

6. Click the **View** icon to reveal the secret key. Select the Secret Key and press **Ctrl+C** to capture the value to share with the Zscaler administrator (see [Zscaler Setup Steps](#)).

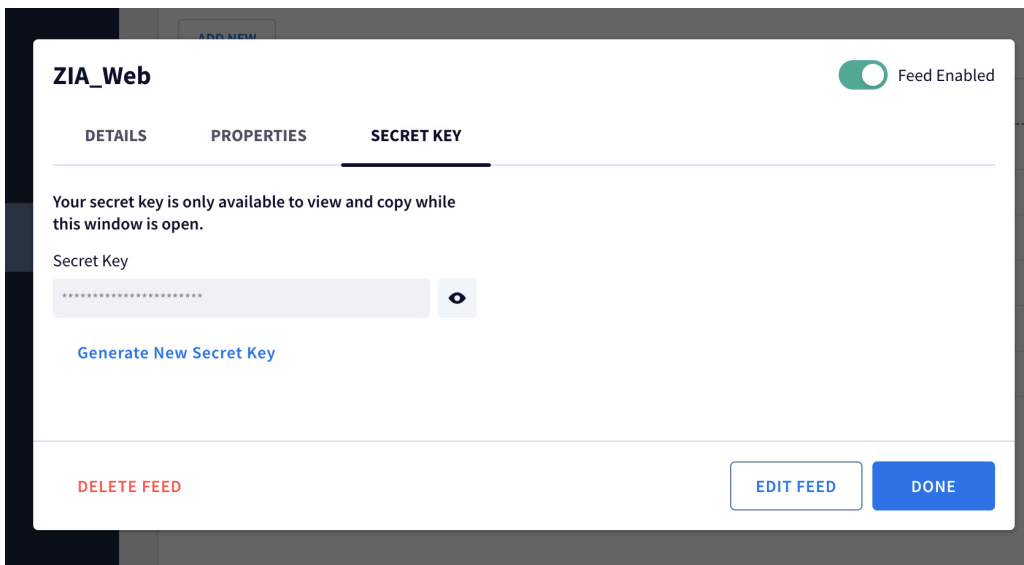


Figure 7. Copy Secret Key

- Copy the **Feed ID** from the **Details** tab.



Do not use the Endpoint information as the API URL on the Zscaler Cloud NSS configuration because it is crafted differently.

ZIA_Web Feed Enabled

DETAILS **PROPERTIES** **SECRET KEY**

Source type: **Webhook** status: **ACTIVE**

Log type: **Zscaler**

Feed ID: 948c1b14-ebcc

Endpoint Information: <https://us-chronicle.googleapis.com/v1alpha/projects/129393218760/locations/us/instances/4b188f9c-5c44-43c6-b572-3aafdf691ba3/feeds/948c1b14-ebcc>

Please Note,
An API key is needed to complete feed setup. To generate an API key, go to the Google Cloud console:

DELETE FEED **EDIT FEED** **DONE**

Figure 8. Details

- Repeat the [Set Up HTTPS Push Ingestion Using a Webhook](#) procedure for other ZIA log types (Firewall and DNS). The result is different feeds, each corresponding to a different ZIA log type, as shown in the following figure.

Google SecOps | Settings - Feeds

FEEDS

[ADD NEW](#)

FEED NAME	FEED ID ↑		STATUS	SOURCE TYPE	LOG TYPE
ZIA_FW	09ba-c5e325		Active	Webhook	Zscaler NGFW
ZIA_DNS	0bc7-3d7c0b		Active	Webhook	Zscaler DNS
ZIA_Web	6db5-ff330		Active	Webhook	Zscaler

Figure 9. Different feeds

9. On your **GCP BYOP** project that is assigned to Google SecOps, create an API key.
 - a. Select your project assigned to the Google SecOps instance from the drop-down menu.

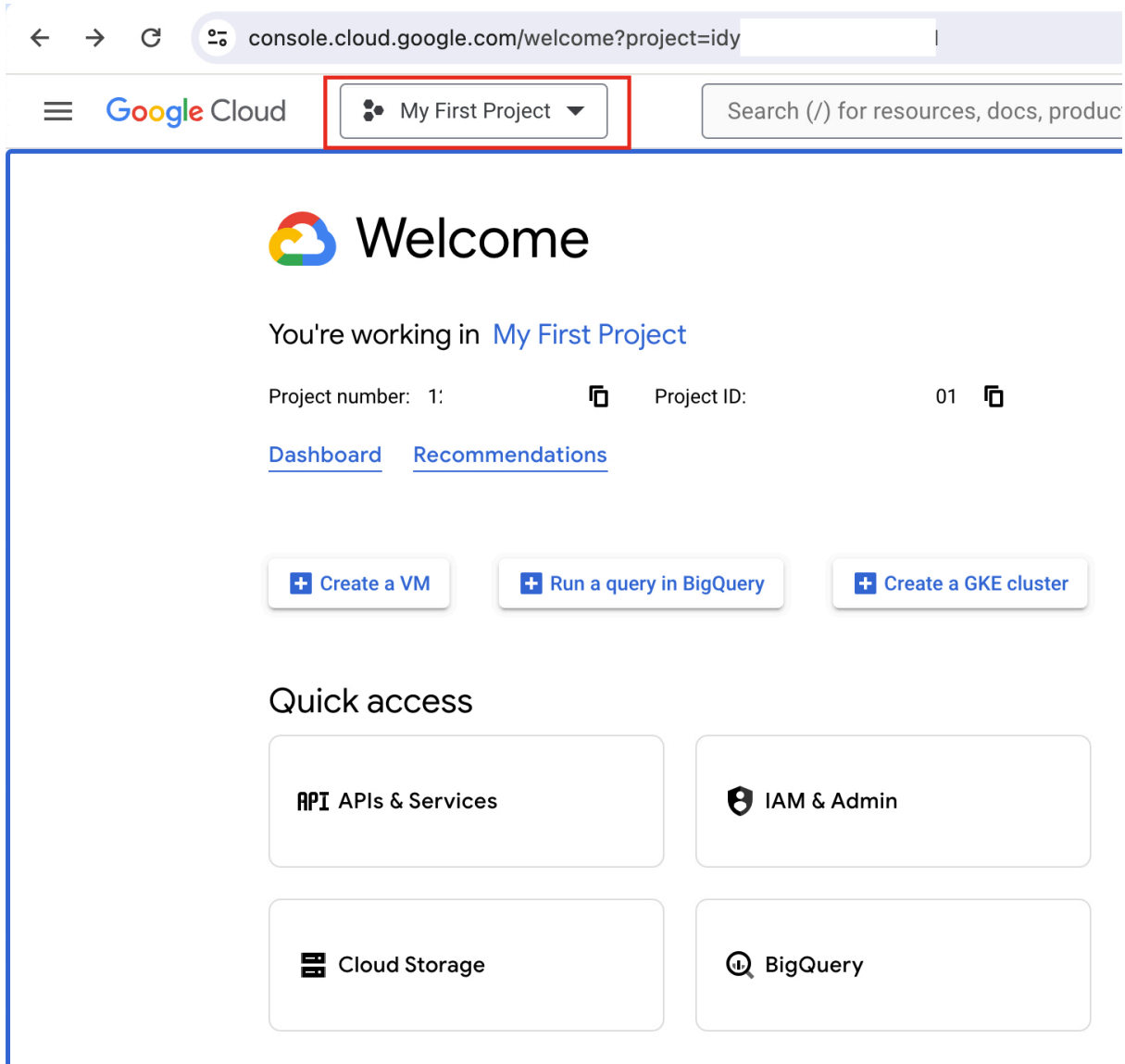


Figure 10. Project

b. Go to **APIs & Services > Credentials**.

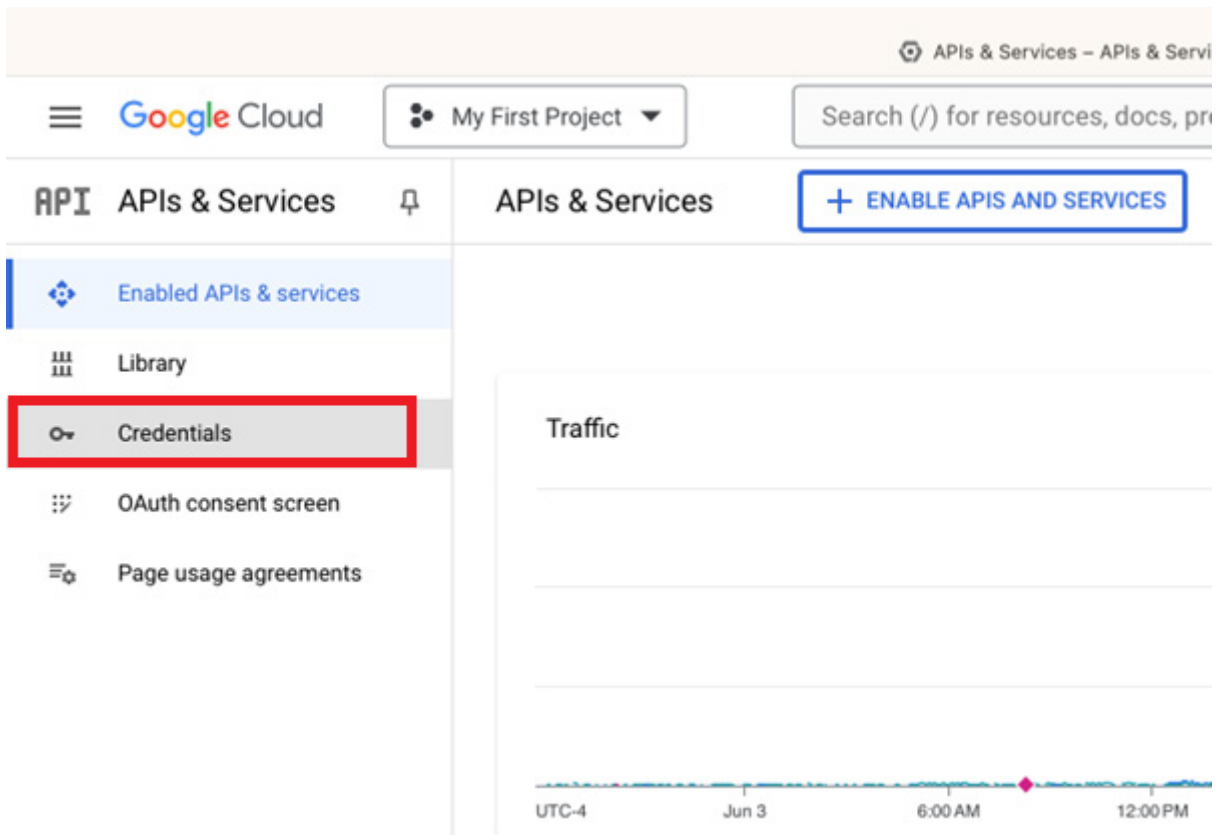


Figure 11. Credentials

- c. Click **+ Create Credentials** and select **API key 1**.

The screenshot shows the Google Cloud API & Services console for a project named 'My First Project'. The 'Credentials' tab is selected, and the '+ CREATE CREDENTIALS' button is highlighted. The 'API Keys' section shows a table with one entry, 'API key 1', which is highlighted with a red box. Below this, a modal window titled 'API key created' is displayed, showing the API key 'AIzaSy...' and providing instructions on how to use it.

API key created

Use this key in your application by passing it with the `key=API_KEY` parameter.

Your API key
AIzaSy...

This key is unrestricted. To prevent unauthorized use, we recommend restricting where and for which APIs it can be used. [Edit API key](#) to add restrictions. [Learn more](#)

CLOSE

Figure 12. Create Credentials

- d. Copy the API key value and click **Close**.
- e. On the generated API key, click the **Actions** icon for further action.
- f. Select **Edit API Key**.

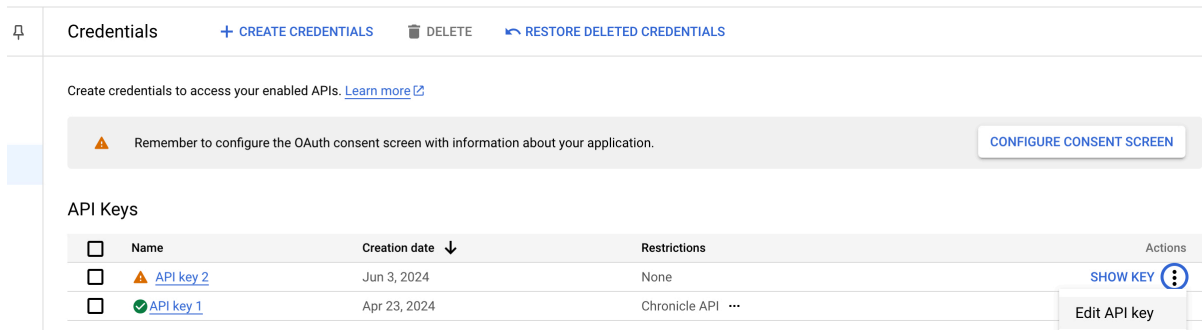


Figure 13. Edit API Key

- g. Under **API restrictions**, select **Restrict key**. Select **Google SecOps API** from the drop-down menu.
- h. Click **OK**.

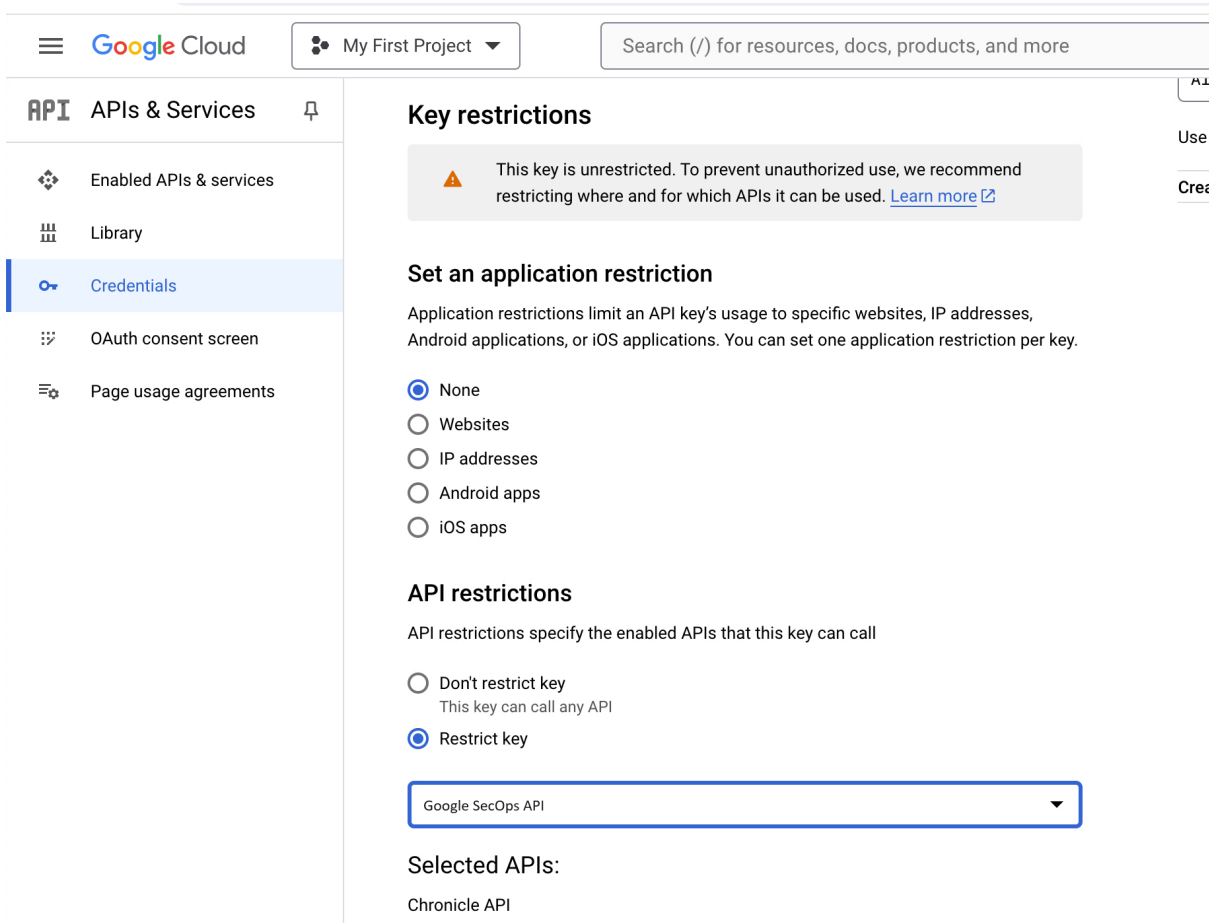


Figure 14. Google SecOps API

10. Share the API key value with the Zscaler administrator (see [Zscaler Setup Steps](#)).

Zscaler Setup Steps

The following demonstrates how to configure ZIA.

1. Configure the Cloud NSS Feed on the ZIA Admin Portal:
 - a. **Feed Name:** Enter or edit the name of the feed. Each feed is a connection between the NSS and your SIEM.
 - b. **NSS Type:** NSS for Web.
 - c. **Status:** Enabled.
 - d. **SIEM Rate:** Unlimited.
 - e. **SIEM Type:** Other.
 - f. **OAuth 2.0 Authentication:** Disabled.
 - g. **JSON Array Notation:** Disabled.
 - h. **Max Batch Size:** 512 KB.
 - i. **API URL:** Should be in the format of:

```
https://<GOOGLE_SECOPS_REGION>-chronicle.googleapis.com/v1alpha/
projects/<GOOGLE_PROJECT_NUMBER>/locations/<LOCATION>/instances/<CUSTOMER_ID>/
feeds/<FEED_ID_THAT_YOU_COPIED_EARLIER>;importPushLogs
```

Where:

- **GOOGLE_SECOPS_REGION:** Region where your Google SecOps instance is hosted (e.g., US).
- **GOOGLE_PROJECT_NUMBER:** BYOP project number (obtain from Settings > Profile as shown in the Google SecOps admin screenshot).
- **LOCATION:** Google SecOps region (e.g., US).
- **CUSTOMER_ID:** Google SecOps customer ID (obtain from Settings > Profile as shown in the Google SecOps admin screenshot).
- **FEED_ID_THAT_YOU_COPIED_EARLIER:** The Feed ID copied from [Set Up HTTPS Push Ingestion Using a Webhook](#).

Sample API URL:

```
https://us-chronicle.googleapis.com/v1alpha/projects/129XXXX760/  
locations/us/instances/4bXXX9c-5c44-XXc6-bXX2-3aaXXXba3/feeds/  
c2XX-c5XX-4b8b-8XX7-dXXX8407:importPushLogs
```

j. **HTTP Headers:**

- **Header 1:** X-goog-api-key
- **Value 1:** API Key generated on GCP BYOP's API Credentials.
- **Header 2:** X-Webhook-Access-Key
- **Value 2:** API secret key generated from the webhook Secret Key.

k. **Log Type:** Web Log.

l. **Feed Output Type:** JSON.

m. **Feed Escape Character:** Leave as default.

n. **Feed Output Format:** Leave at default.

o. **JSON Array Notation:** Disabled.

p. **Timezone:** Your Zscaler organization time zone (e.g., GMT +8).

Figure 15. Edit Cloud NSS Feed

2. Save your settings and test your connectivity. You see a green check mark with the message `Test Connectivity Successful: OK (200)`.

No.	Feed Overview	Log Filter	Feed Output Format	Feed Attributes	Last Connectivity Test
1	FEED NAME Google Web STATUS Enabled API URL https://us-chronicle.googleapis.com/v1alpha/projects/... SIEM TYPE Splunk FEED OUTPUT TYPE JSON LOG TYPE Web Log		15 "sourcetype": "googlesec-web", "event": { "timestamp": "2024-09-10T10:10:10.101Z", "source": "us-chronicle", "destination": "us-chronicle", "severity": "INFO", "message": "Test connectivity successful", "attributes": { "test": "connectivity", "status": "success", "code": 200 } } }	TIME ZONE: GMT MAX BATCH SIZE: 16 KB	Last Validation Successful on 09/10/2024 - 09:10 PM: OK (200)

Figure 16. Test Connectivity

Check Google SecOps Dashboard

The following images show the Google SecOps dashboards.

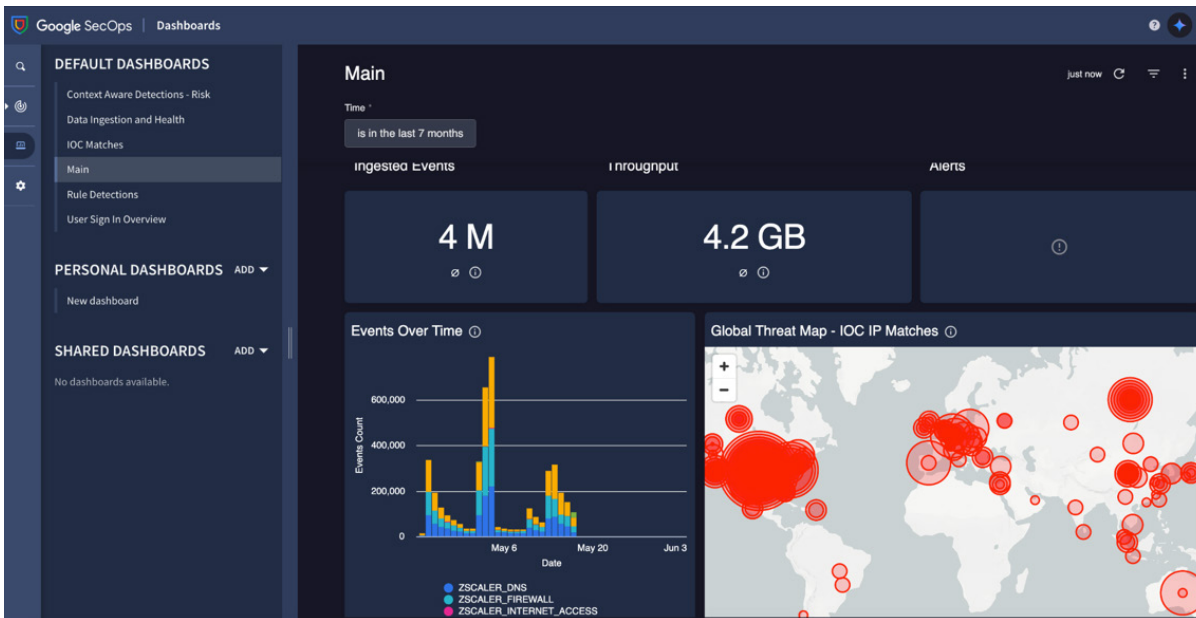


Figure 17. Main Dashboard

The following image is the IOC Matches dashboard.



Figure 18. IOC Matches

Search for Zscaler Logs in Google SecOps

To search for Zscaler logs in the Google SecOps dashboard:

1. Go to the Google SecOps main landing page.

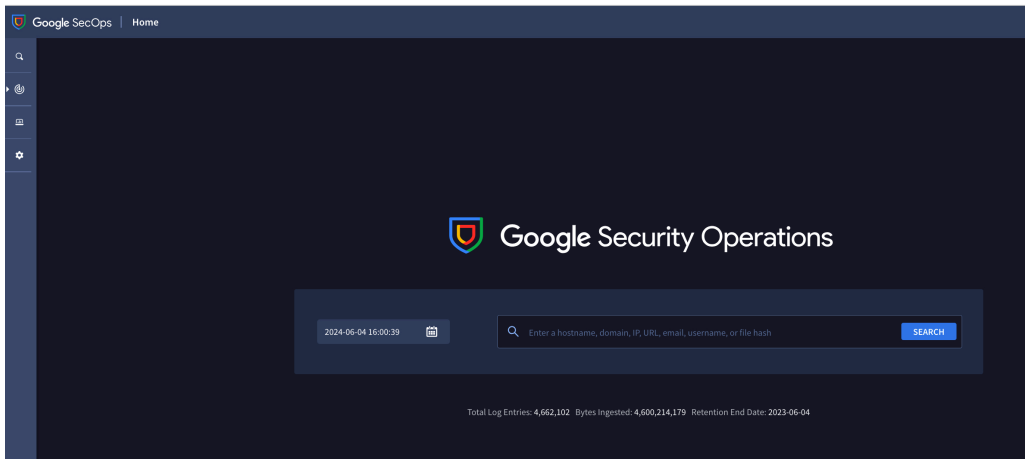


Figure 19. Google SecOps main landing page

2. Search for `zscaler` (with regex setting enabled).

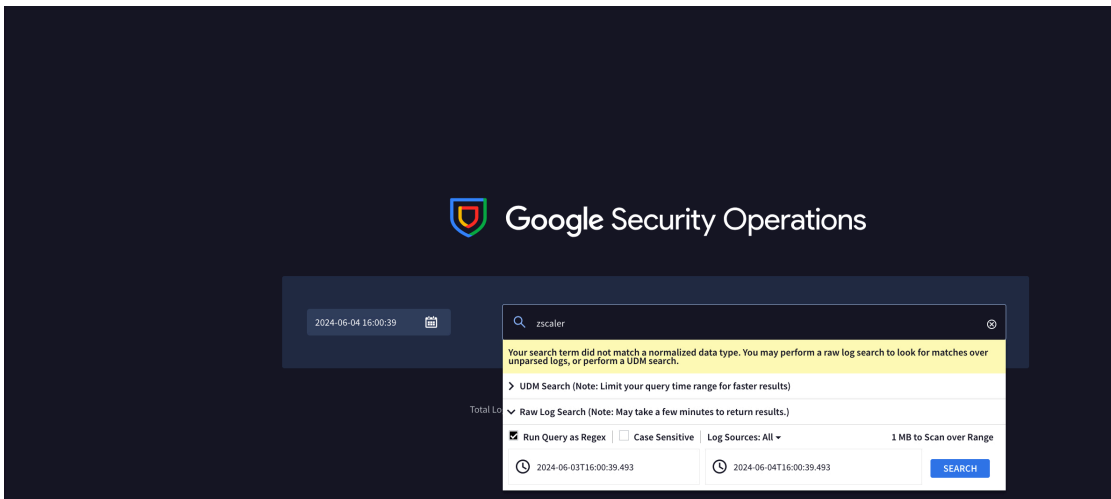


Figure 20. Search for `zscaler`

3. View the search results.

The screenshot displays the Google SecOps Raw Log Search interface. The top section shows the search criteria: "MAY 29, 04:03 PM - JUNE 04, 04:03 PM" and "40 Log Lines (10 Events)". The left sidebar contains a search bar and a list of search results. The main panel shows the details of a selected event, "NETWORK_HTTP", with a timestamp of "2024-05-30 11:15:40". The event details are displayed in a JSON format, showing various fields such as "sourcetype", "event", "datetime", "reason", "event_id", "protocol", "action", "transactionsize", "responsesize", "requestsize", "urlcategory", "serverip", "requestmethod", "referrerurl", "useragent", "product", "location", "clientip", "status", "user", "url", "vendor", "hostname", "clientpublicip", "threatcategory", "threatname", "filetype", "appname", and "paperisk". The right sidebar shows the "UDM Event" details, including "additional.fields", "metadata.base_labels", "metadata.event_timestamp", "metadata.event_type", "metadata.id", "metadata.ingested_timestamp", "metadata.log_type", "metadata.product_name", "metadata.vendor_name", "network.application_protocol", "network.http.method", "network.http.parsed_user_agent.annotation", "network.http.parsed_user_agent.annotation[0].key", "network.http.parsed_user_agent.annotation[0].value", "network.http.parsed_user_agent.annotation[1].key", "network.http.parsed_user_agent.annotation[1].value", "network.http.parsed_user_agent.browser", and "network.http.parsed_user_agent.browser_engine_version".

2024-05-30	EVENT	ASSET IDENTIFIER
11:15:40	NETWORK_CONNECTION r.bing.com	namespace1 > DESKTOP-JSS...
11:15:40	NETWORK_CONNECTION www.bing.com	namespace1 > DESKTOP-JSS...
11:15:40	NETWORK_CONNECTION download.windowsup...	namespace1 > DESKTOP...
11:15:40	NETWORK_CONNECTION login.live.com	namespace1 > DESKTOP-JSS...
11:15:40	NETWORK_CONNECTION api.msn.com	namespace1 > DESKTOP-JSS...
11:15:40	NETWORK_CONNECTION assets.msn.com	namespace1 > DESKTOP-JSS...
11:16:00	NETWORK_CONNECTION r.bing.com	namespace1 > DESKTOP-JSS...
11:16:00	NETWORK_CONNECTION fe2crupdate.microso...	namespace1 > DESKTOP-J...
11:16:00	NETWORK_CONNECTION download.windowsup...	namespace1 > DESKTOP...
2024-06-03	NETWORK_CONNECTION Unknown%20Host	0.0.0.0

```

{
  "sourcetype": "zscaler-ssl-web",
  "event": {
    "datetime": "2024-05-30 10:41:15",
    "reason": "Allowed",
    "event_id": "7374749919595360450",
    "protocol": "HTTPS",
    "action": "Allowed",
    "transactionsize": "16871",
    "responsesize": "11722",
    "requestsize": "5149",
    "urlcategory": "Professional Service
s",
    "serverip": "40.126.35.18",
    "requestmethod": "POST",
    "referrerurl": "None",
    "useragent": "Mozilla/4.0%20(compatibl
e;%20MSIE%206.0;%20Windows%20NT%2010.0;%20
Win64;%20.NET4.0C;%20.NET4.0F;%20IDCRL%202
4.10.0.19045.0.0;%20IDCRL-cfg%2016.000.290
39.9;%20App%20svchost.exe%20%2010.0.19041.
3636;%20c20{DF60E2DF-88AD-4526-AE21-83D130E
F0F68})",
    "product": "NSS",
    "location": "Road%20Warrior",
    "clientip": "10.0.0.3",
    "status": "200",
    "user": "picus_windows_test@bd-siem.co
m",
    "url": "login.live.com/rst2.srf",
    "vendor": "Zscaler",
    "hostname": "login.live.com",
    "clientpublicip": "45.120.106.52",
    "threatcategory": "None",
    "threatname": "None",
    "filetype": "None",
    "appname": "Microsoft Login Services",
    "paperisk": "10",
  }
}

```

Figure 21. Search results

Contextualizing Risk Using Google Cloud and Avalor UVM

Avalor's Data Fabric and Unified Vulnerability Management (UVM) solution integrates, normalizes, and unifies data from various enterprise security and business systems to provide actionable insights, analytics, and operational efficiencies.

Avalor offers a preconfigured connectors for a variety of Google Cloud Platform (GCP) and Google Workspace services including:

- Google Cloud Platform—Assets
- Google Cloud Platform—Vulnerabilities
- Google Cloud Platform—Misconfigurations
- Google Workspace—Drive Activity
- Google Workspace—Admin Activity
- Google Workspace—Login Activity
- Google Workspace—Mobile Activity
- Google Workspace—OAuth Tokens Activity
- Google Workspace—Rules Activity
- Google Workspace—Access Transparency Activity
- Google Workspace—Calendar Activity
- Google Workspace—Chat Activity
- Google Workspace—Chrome Activity
- Google Workspace—Context-Aware access Activity
- Google Workspace—Data Studio Activity
- Google Workspace—Google Cloud Platform Activity
- Google Workspace—Google+ Activity
- Google Workspace—Groups Activity
- Google Workspace—Keep Activity
- Google Workspace—SAML Activity
- Google Workspace—Tokens Activity
- Google Workspace—User Accounts Activity
- Google Workspace—Enterprise Groups Activity
- Google Sheets

The following steps outline how to start ingesting data from these sources, while also (optionally) combining Google Cloud Platform Asset data with Rapid7 Vulnerability information to provide a more contextualized and personalized risk assessment for your organization.

Enable Programmatic Access to a Google Cloud Tenant

The following sections describe enabling access to a Google Cloud tenant

Create an Avalor UVM Service Account

To create an Avalor UVM service account:

1. Go to **APIs & Services**.
2. Click **+ Enable APIs and Services**.

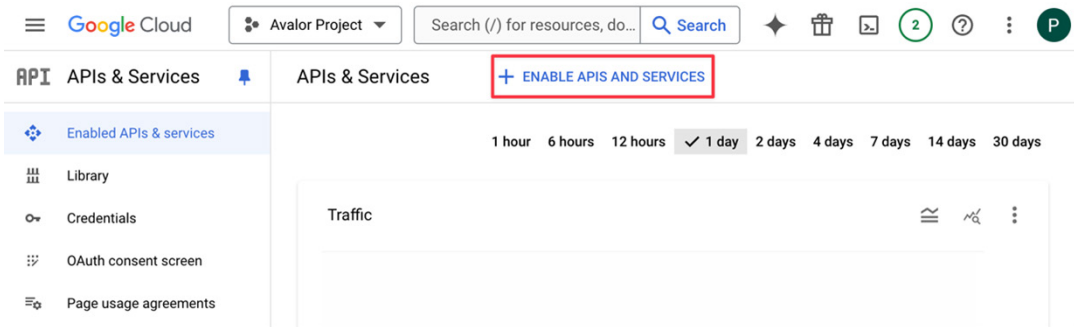


Figure 22. Enable APIs & Services

3. Search for **IAM**.

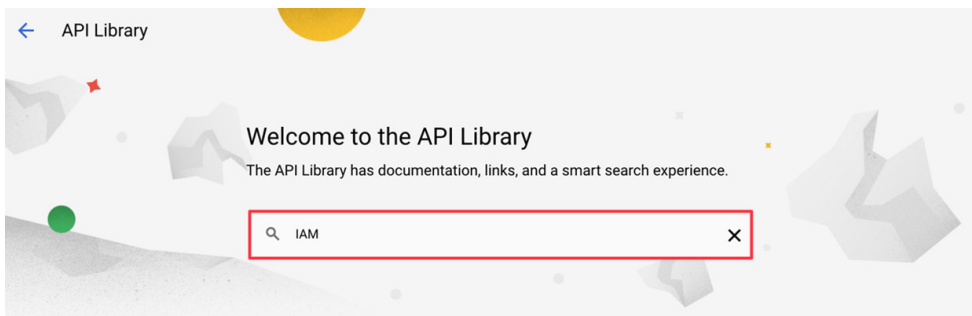


Figure 23. Search for IAM

4. Click **Identity and Access Management (IAM) API**.

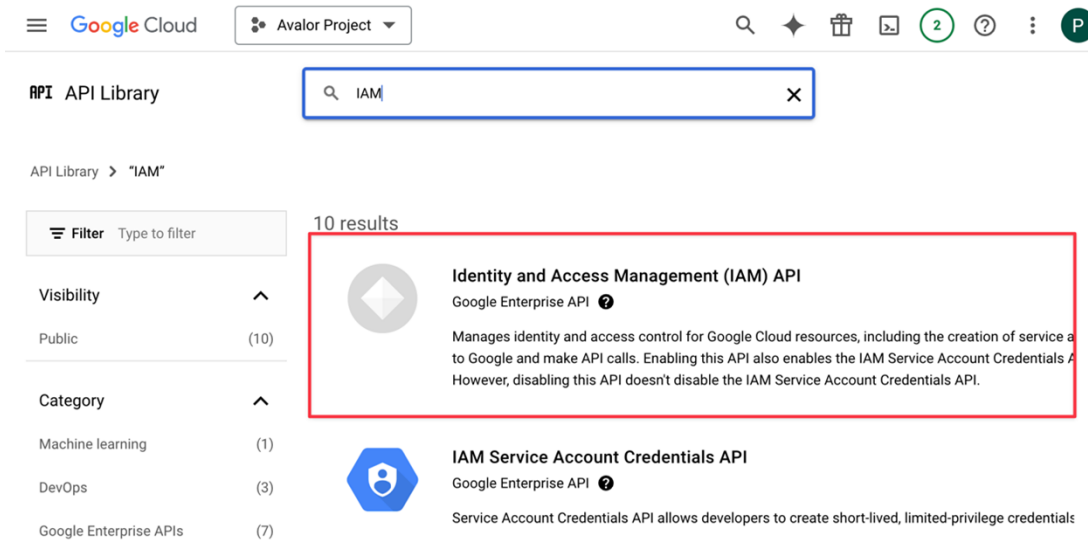


Figure 24. Select Identity and Access Management (IAM) API

5. Click **Enable**.

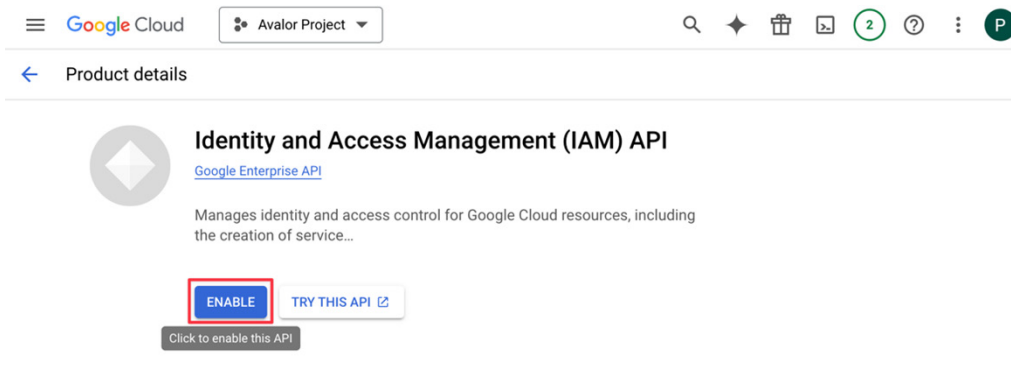


Figure 25. Enable Identity and Access Management (IAM) API

Ensure you have granted admin consent for each permission selected.

6. Under the drop-down menu, select **IAM & Admin > Service Accounts**.

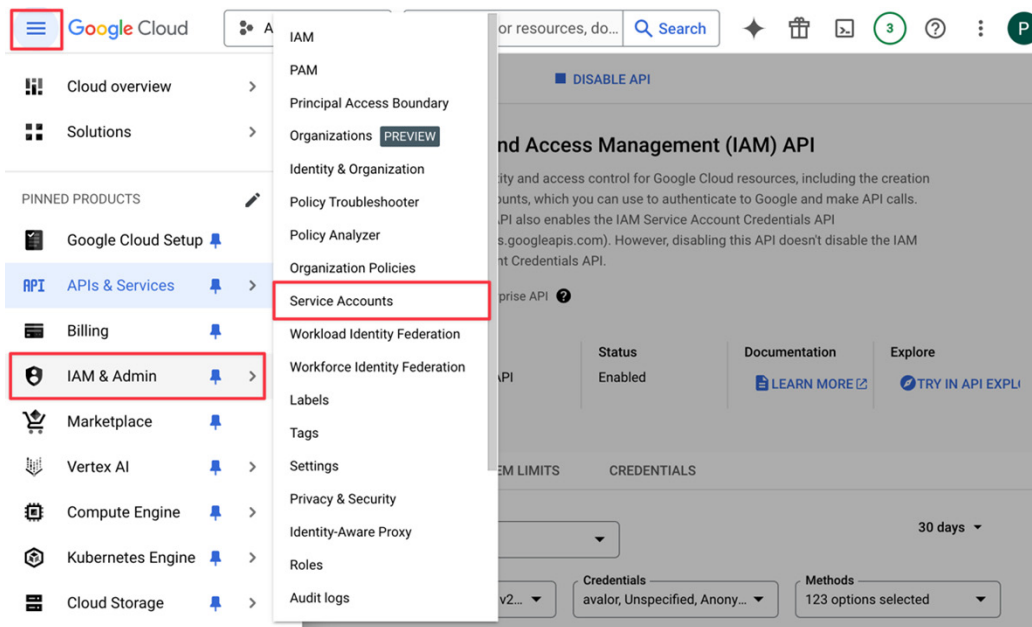


Figure 26. Service Accounts

7. Click **+ Create Service Account**.

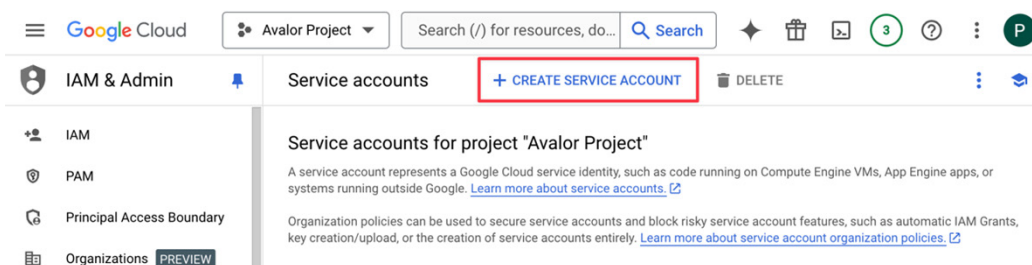


Figure 27. Create Service Accounts

Ensure you have the roles/iam.serviceAccountCreator IAM role before trying to create a Service account.

8. Enter a **Service account name**, then click **Create and Continue** and **Done**.

1 Service account details

Service account name
avalor-demo

Display name for this service account

Service account ID *
avalor-demo

Email address: avalor-demo@avalor-project-436806.iam.gserviceaccount.com

Service account description

Describe what this service account will do

CREATE AND CONTINUE

Figure 28. Service account details

When complete, your Service account is **Enabled**.

Filter Enter property name or value						
<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Actions
<input type="checkbox"/>	avalor-demo@avalor-project-436806.iam.gserviceaccount.com	✓ Enabled	avalor-demo		No keys	⋮

Figure 29. Enabled account

9. Create a Service account key by selecting **Actions > Manage keys**.

Filter Enter property name or value						
<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Actions
<input type="checkbox"/>	avalor-demo@avalor-project-436806.iam.gserviceaccount.com	✓ Enabled	avalor-demo		No	⋮

Manage details
 Manage permissions
Manage keys
 View metrics
 View logs
 Disable
 Delete

Figure 30. Manage keys

Ensure you have deleted the Service account key creation by updating the org-policy via the following command:

```
gcloud org-policies delete iam.disableServiceAccountKeyCreation --organization=<org id>
```

10. Select **Add Key > Create new key**.

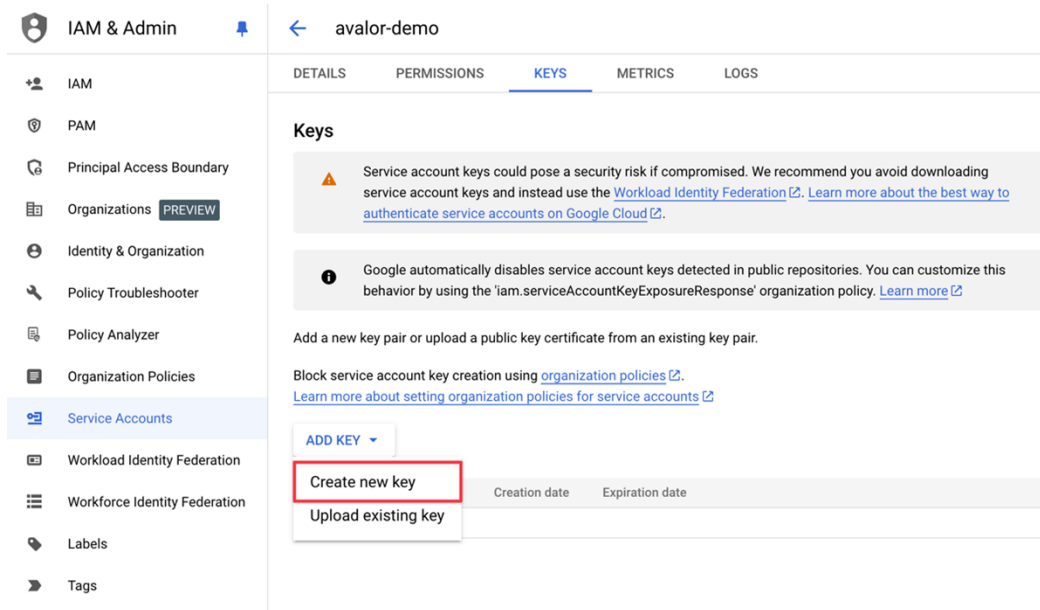


Figure 31. Create new key

11. Select **JSON**.

12. Click **Create**.

Create private key for "avalor-demo"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☒ **JSON**
Recommended

☐ **P12**
For backward compatibility with code using the P12 format

CANCEL

CREATE

Figure 32. JSON

13. Save the downloaded key.

Configure the Google Cloud Data Connectors

The following sections describe configuring the Google Cloud data connectors.

Google Cloud Platform—Assets Data Source

The Cloud Cloud Platform—Assets data source ingests Google Cloud Asset inventory and associated meta data.

The following sections describe how to configure the Google Cloud Platform—Assets data sources.

Configure the OAuth Scope

1. Enable the Google Cloud Asset API by going to the Google Cloud Console, then selecting **APIs & Services > Library**.
2. Search for **Cloud Asset**, then click **Cloud Asset API**, then click **Enable**.

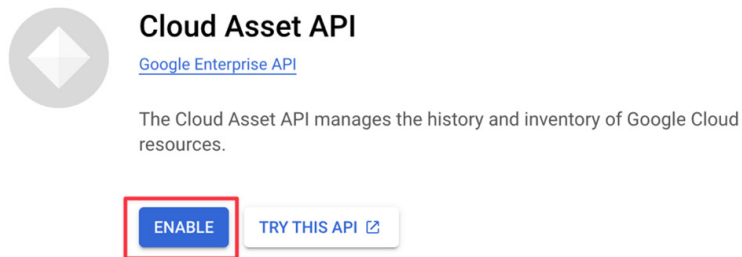


Figure 33. Cloud Asset API

3. Sign in to your Google Cloud Console and go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation** and click **Add new**.

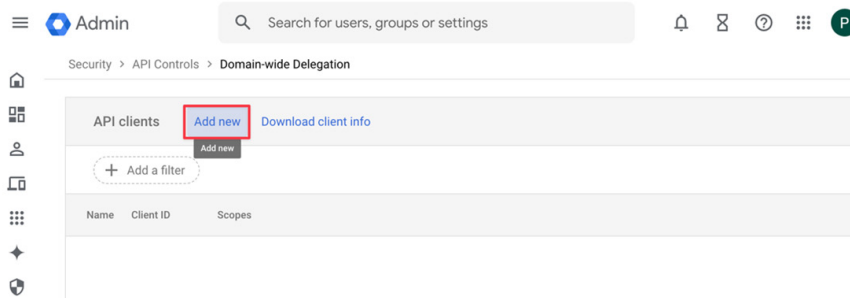


Figure 34. Add new domain-wide delegation

4. Enter the **Client ID** from your downloaded JSON file, input `https://www.googleapis.com/auth/cloud-platform`, and click **Authorize**.

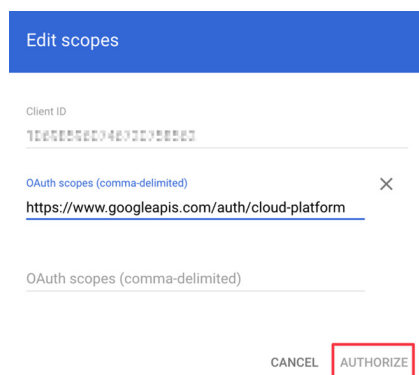


Figure 35. Edit Scope

Configure the IAM Permissions

1. Sign in to your Google Cloud Console.
2. Go to **IAM & Admin** > **IAM**.

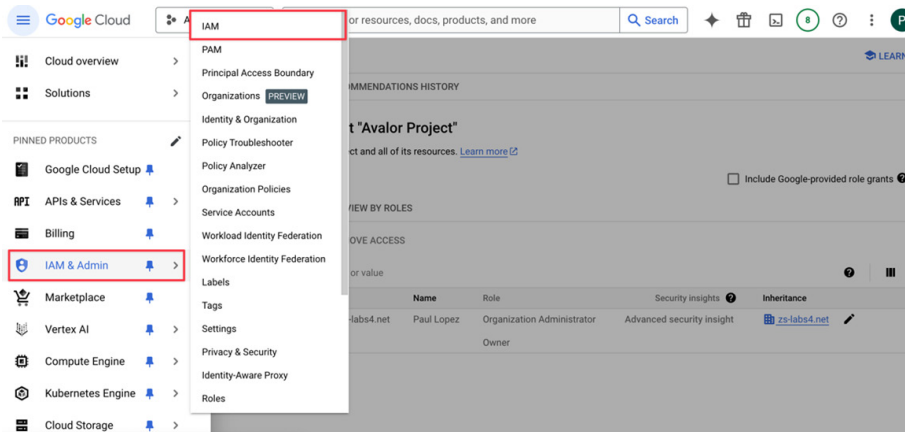


Figure 36. IAM

3. Click **Grant Access**.

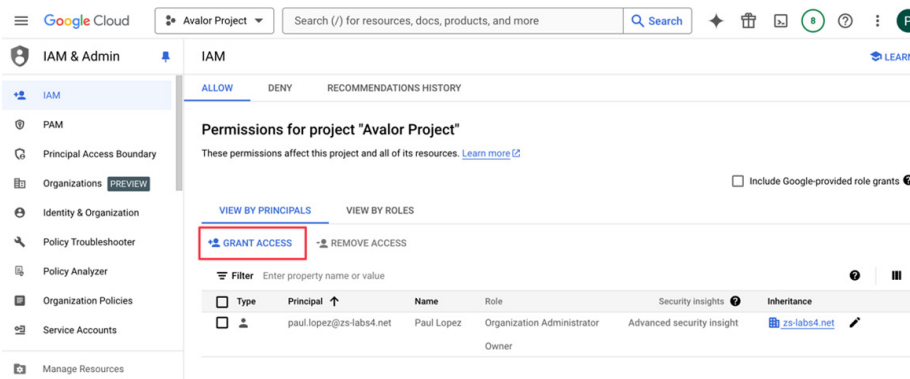


Figure 37. Grant Access

4. Select your Avalor service account under **New principals**, and select **Cloud Asset Viewer** under **Role**.
5. Click **Save**.

Grant access to "Avalor Project"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. [Learn more about IAM conditions](#)

Resource

- Avalor Project

Add principals

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals *

avalor-demo@avalor-project-436806.iam.gserviceaccount.com

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role *

Cloud Asset Viewer

IAM condition (optional)

+ ADD IAM CONDITION

Read only access to cloud assets

SAVE **CANCEL**

Figure 38. Cloud Asset Viewer

Configure the Google Cloud Assets Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

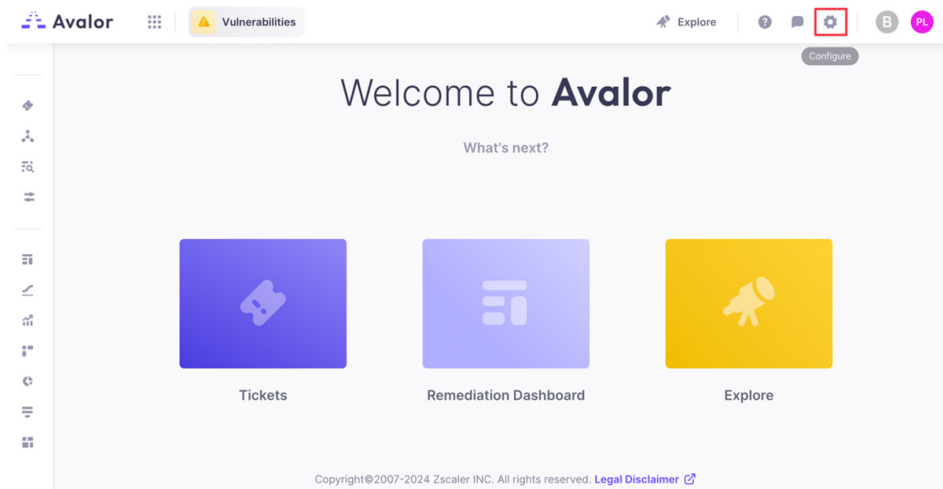


Figure 39. Configure

3. Click **Create**, then search for Google Cloud Platform Assets.

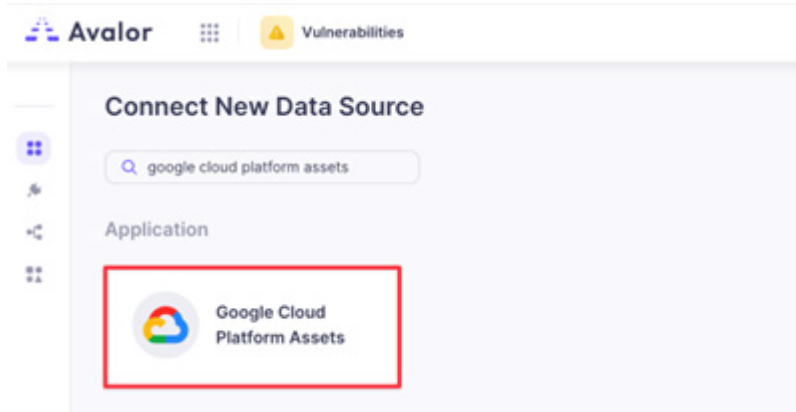


Figure 40. Connect New Data Source

4. Click the **Google Cloud Platform Assets** application.
5. On the **Google Cloud Platform Assets** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Service Account:** Upload the JSON file you downloaded earlier.
 - d. **Pull data only for service account project:** Select if applicable.
 - e. **Filter project with sys prefix:** Select if applicable.
 - f. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - g. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.

- h. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

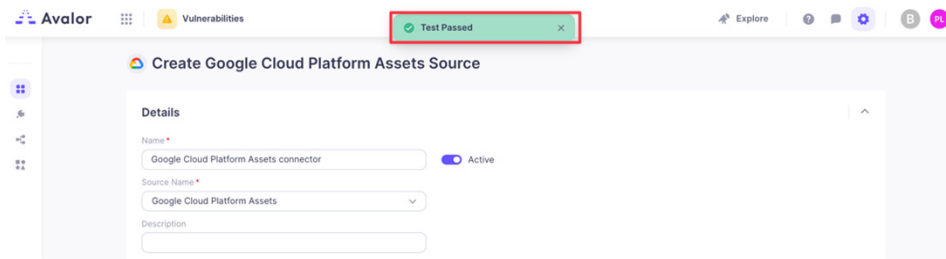


Figure 41. Test Passed

7. Click **Save**.

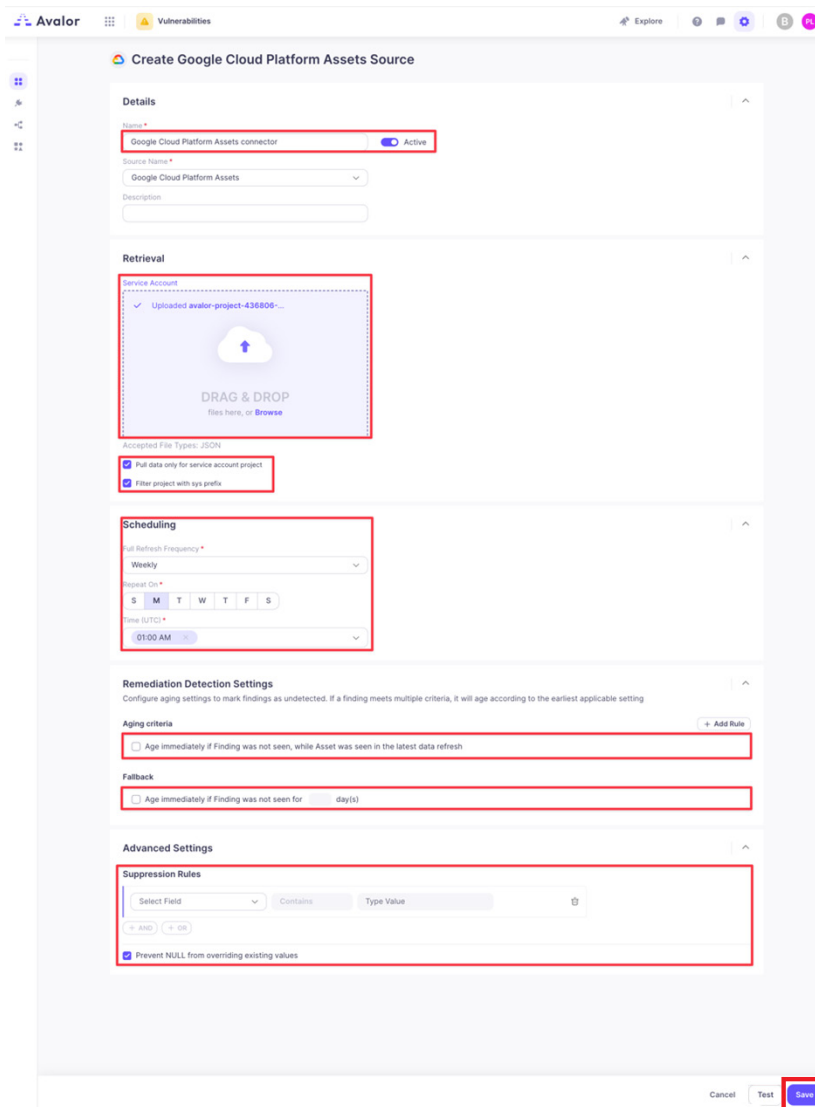


Figure 42. Create Google Cloud Platform Assets Source

Google Cloud Platform–Vulnerabilities Data Source

This data source reads vulnerability information via the Container Analysis API for both the Artifact Registry and with the Advanced Vulnerability Insights (runtime scanning) in GKE.

Artifact Registry and/or Advanced Vulnerability Insights (runtime scanning) in GKE must be enabled in your Google Cloud tenant.

The following sections describe configuring the CCP vulnerability data source.

Configure the OAuth Scope

1. Enable the Google Artifact Registry API by going to the Google Cloud Console, then selecting **APIs & Services > Library**.
2. Search for `Container Analysis API`, then click **Container Analysis API** and **Enable**.

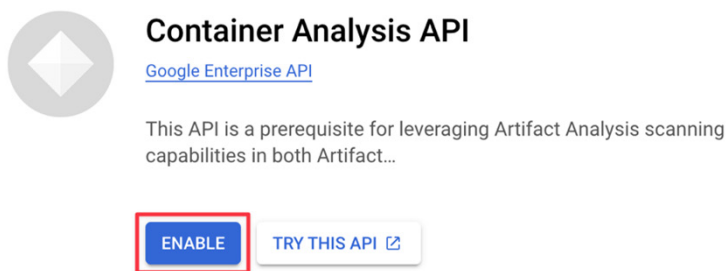


Figure 43. Container Analysis API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

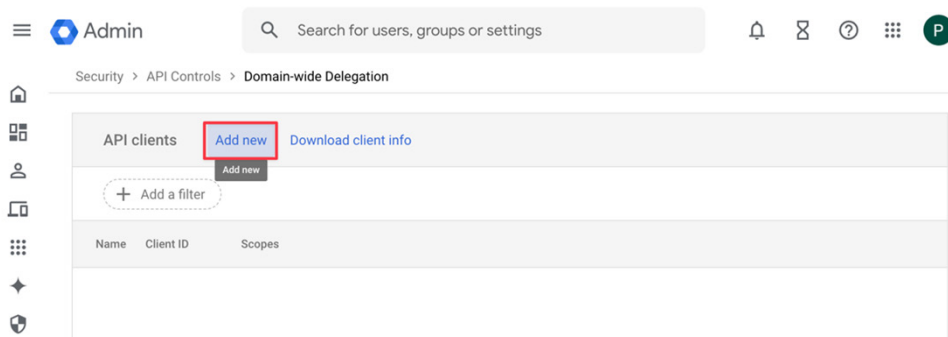


Figure 44. Add new

5. If absent, enter the **Client ID** from your downloaded JSON file, enter `https://www.googleapis.com/auth/cloud-platform` and click **Authorize**.

Configure the IAM Permissions

1. Sign in to your Google Cloud Console.
2. Select **IAM & Admin** > **IAM**.

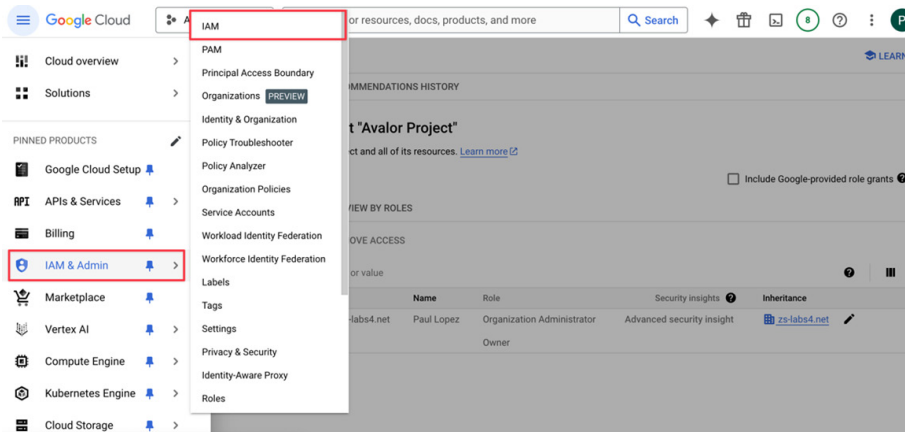


Figure 45. IAM

3. Click **Grant Access**.

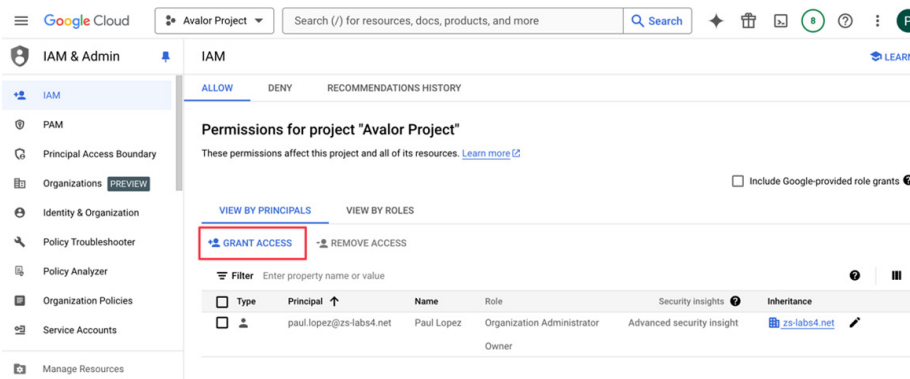


Figure 46. Grant Access

4. Select your Avalor service account under **New principals**, and select **Container Analysis Occurrences Viewer** under **Role**.
5. Click **Save**.

Grant access to "Avalor Project"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. [Learn more about IAM conditions](#)

Resource

• Avalor Project

Add principals

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals *

avalor-demo@avalor-project-436806.iam.gserviceaccount.com

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role *

Container Analysis Occurrences Viewer

Can view Container Analysis Occurrences.

IAM condition (optional)

+ ADD IAM CONDITION

SAVE **CANCEL**

Figure 47. Container Analysis Occurrences Viewer

Configure the Google Cloud Platform Vulnerabilities Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

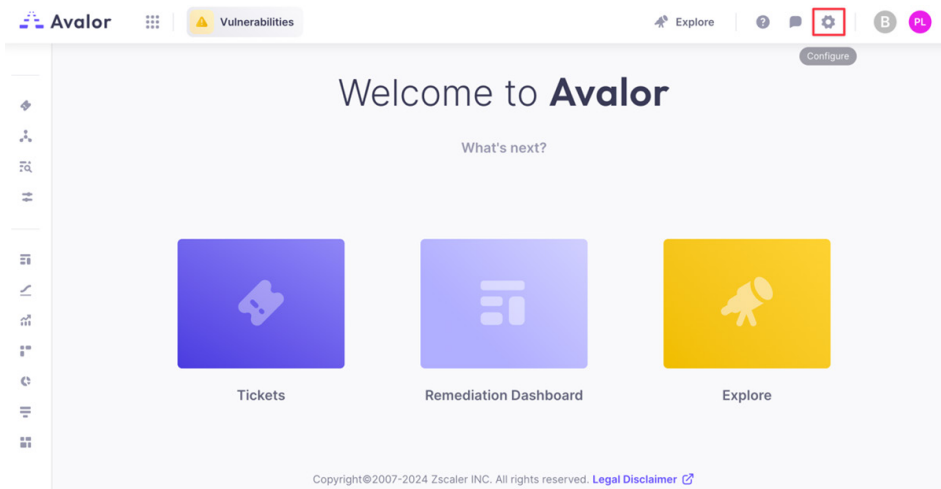


Figure 48. Configure

3. Click **Create**, then search for Google Cloud Platform Vulnerabilities.

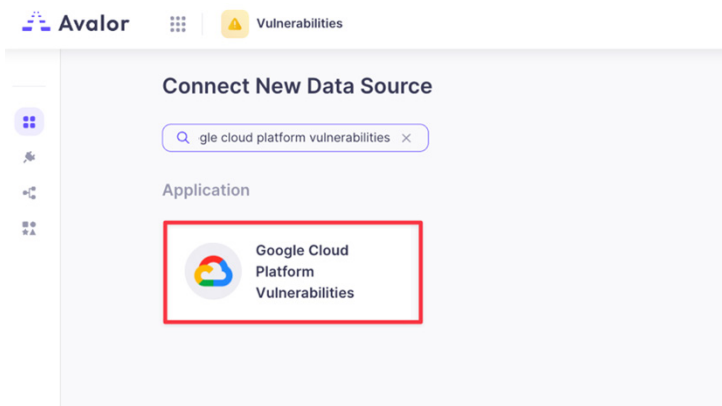


Figure 49. Cloud Platform Vulnerabilities

4. Click the **Google Cloud Platform Vulnerabilities** application.
5. On the **Google Cloud Platform Vulnerabilities** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Service Account:** Upload the JSON file you downloaded earlier.
 - d. **Pull data only for service account project:** Select if applicable.
 - e. **Filter project with sys prefix:** Select if applicable.
 - f. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - g. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.

- h. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
- i. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

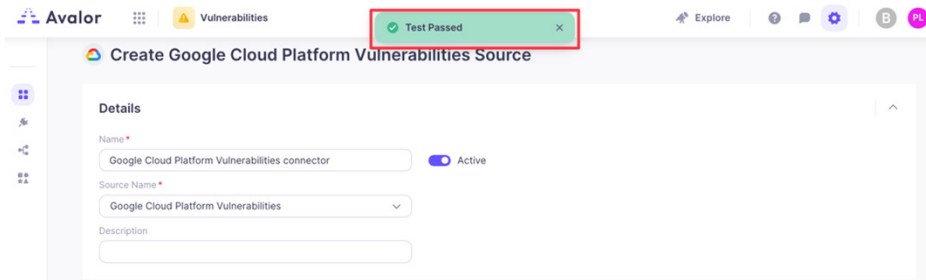


Figure 50. Test Passed

6. Click **Save**.

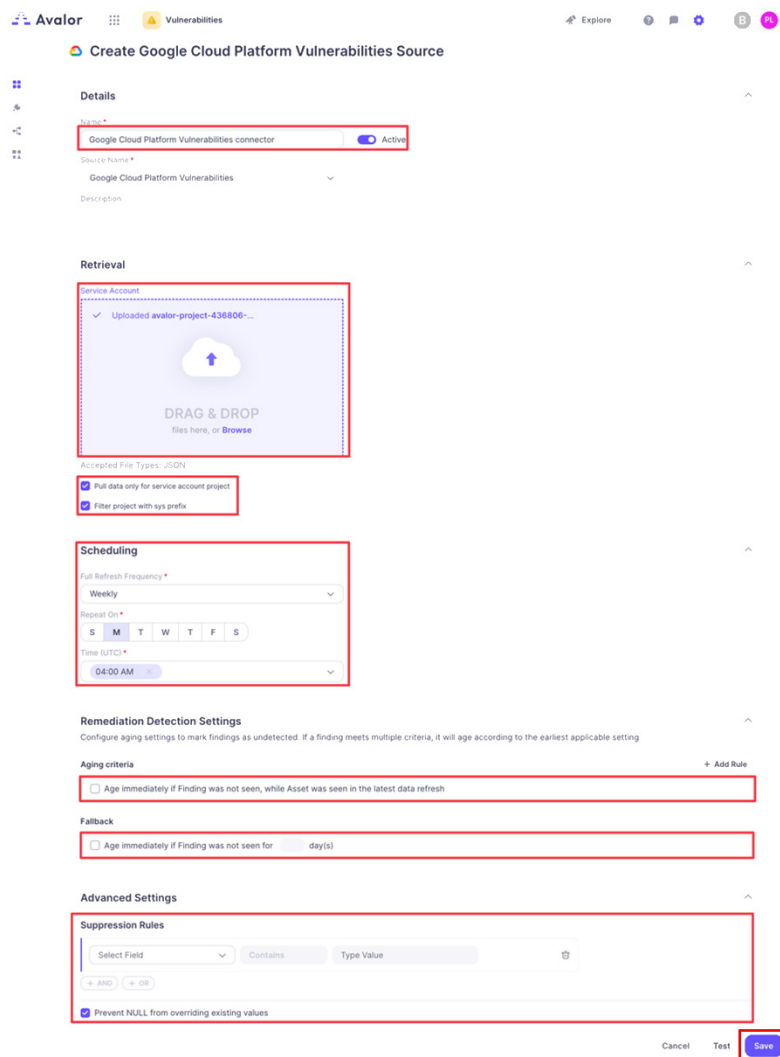


Figure 51. Create Google Cloud Platform Vulnerabilities Source

Google Cloud Platform—Misconfigurations Data Source

This data source reads findings and presents them as misconfiguration information from the Security Command Center API.



Ensure that you enable Security Command Center in your Google Cloud tenant.

The following sections describe how to configure GCP misconfiguration data sources.

Configure the OAuth Scope

1. Sign in to your Google Cloud Console and go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
2. Click **Add new**.

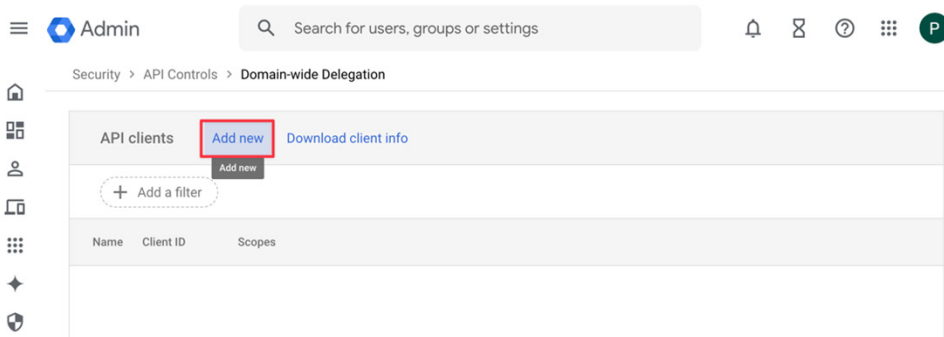


Figure 52. Managed Domain-wide Delegation

3. If absent, enter the **Client ID** from your downloaded JSON file, and enter `https://www.googleapis.com/auth/cloud-platform`.
4. Click **Authorize**.

Edit scopes

Client ID

718682562048370358223

OAuth scopes (comma-delimited)

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

OAuth scopes (comma-delimited)

CANCEL AUTHORIZE

Figure 53. Edit scopes

Configure the IAM Permissions

1. Sign in to your Google Cloud Console.
2. Select **IAM & Admin** > **IAM**.

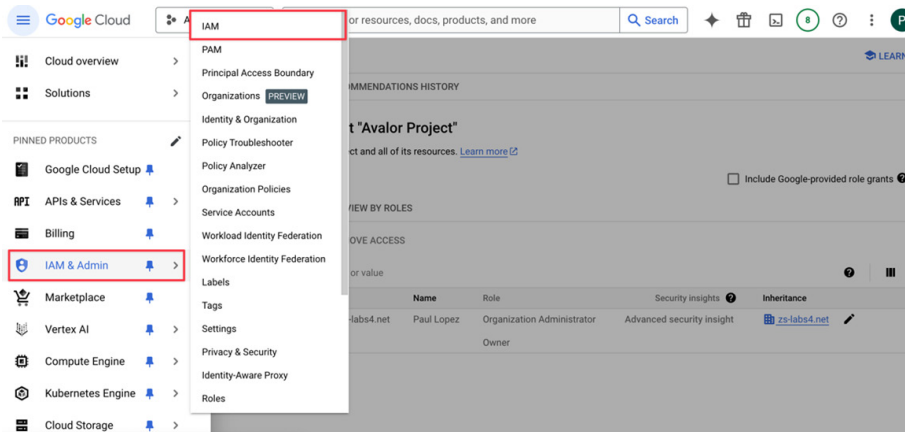


Figure 54. IAM

3. Click **Grant Access**.

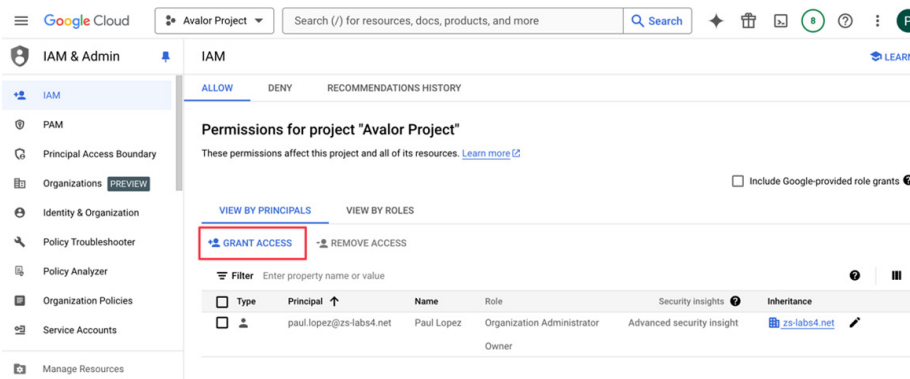


Figure 55. Grant Access

4. Select your Avalor service account under **New principals**, and select **Security Center Admin Viewer** under **Role**.
5. Click **Save**.

Grant access to "Avalor Project"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. [Learn more about IAM conditions](#)

Resource

- Avalor Project

Add principals

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals *

- avalor-demo@avalor-project-436806.iam.gserviceaccount.com

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role *

- Security Center Admin Viewer

IAM condition (optional)

+ ADD IAM CONDITION

SAVE **CANCEL**

Figure 56. Security Center Admin Viewer

Configure the Google Cloud Misconfigurations Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

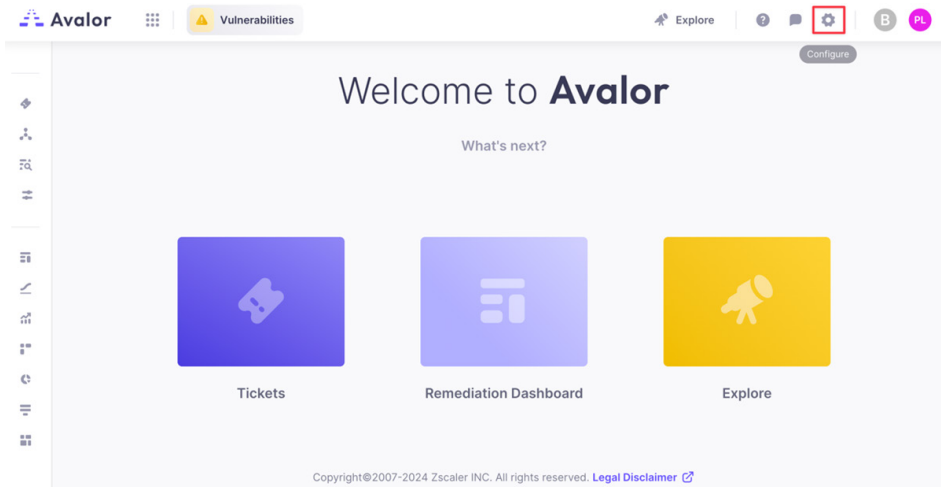


Figure 57. Configure

3. Click **Create**, then search for Google Cloud Platform Misconfigurations.

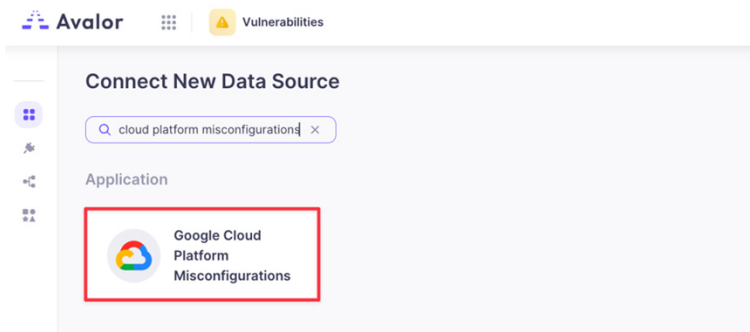


Figure 58. Google Cloud Platform Misconfigurations

4. Click the **Google Cloud Platform Misconfigurations** application.
5. On the **Google Cloud Platform Misconfigurations** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Service Account:** Upload the JSON file you downloaded earlier.
 - d. **Pull data only for service account project:** Select if applicable.
 - e. **Filter project with sys prefix:** Select if applicable.
 - f. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - g. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - h. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

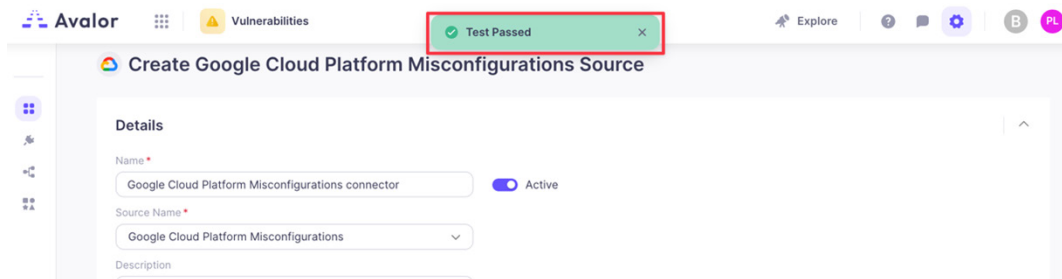


Figure 59. Test Passed

7. Click **Save**.

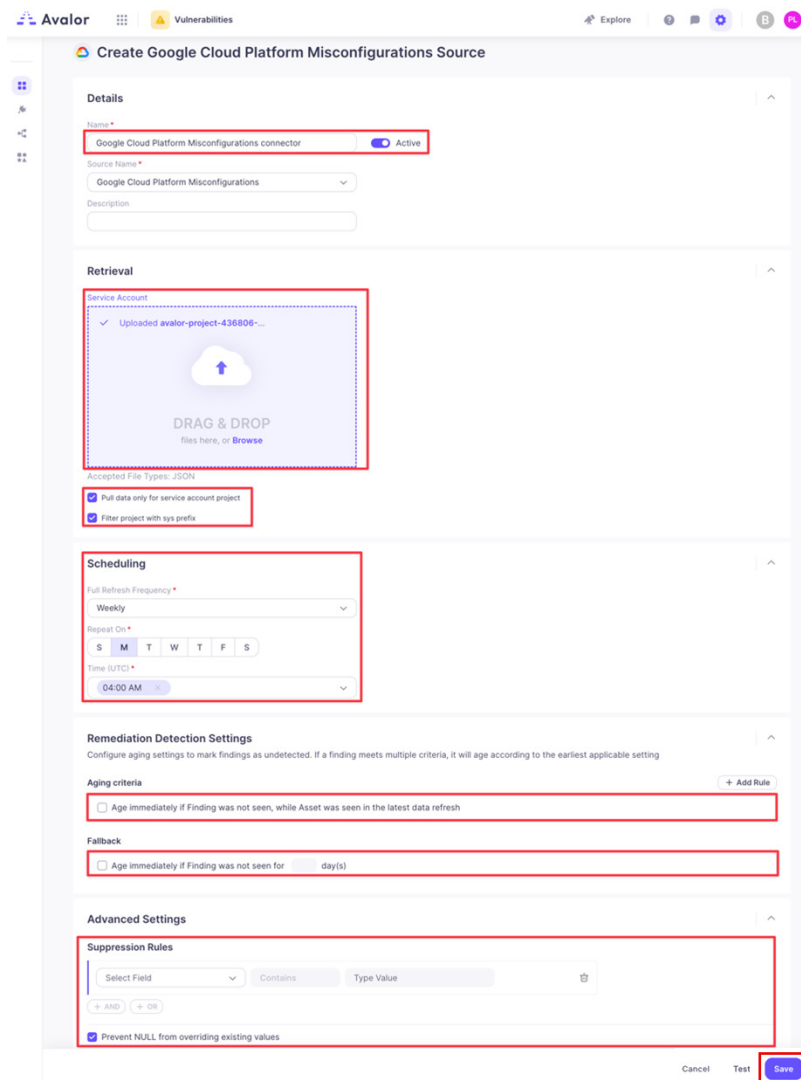


Figure 60. Create Google Cloud Platform Misconfigurations Source

Google Workspace—Drive Activity Data Source

This data source monitors activities related to Google Drive, offering insights into file uploads, downloads, sharing, and other interactions with documents stored in Google Drive via the Google Drive Activity API.

The following sections describe how to configure Google Workspace drive activity data sources.

Configure the OAuth Scope

To enable the Google Drive Activity API:

1. Sign in to your Google Cloud Console.
2. Select **APIs & Services > Library**.
3. Search for Google Drive Activity API.
4. Click **Google Drive Activity API**, then click **Enable**.

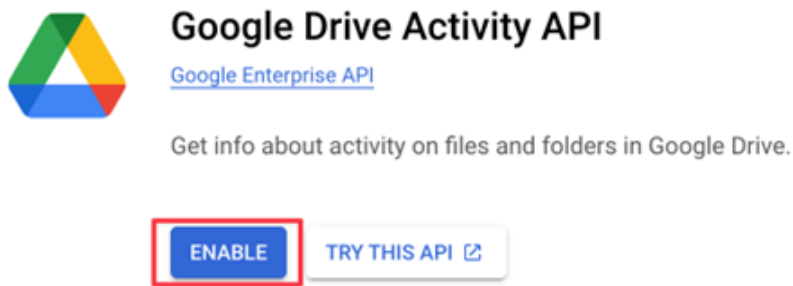


Figure 61. Google Drive Activity API

5. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
6. Click **Add new**.

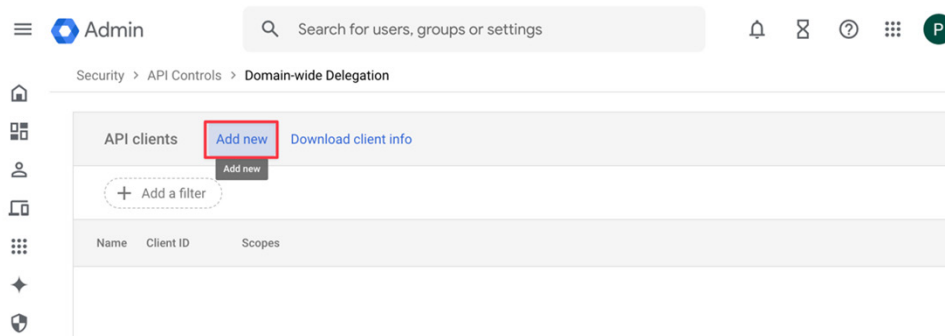


Figure 62. Add new

7. If absent, enter the **Client ID** from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
8. Click **Authorize**.

Add a new client ID

Client ID

106962960-62795092

☐

Overwrite existing client ID

i

OAuth scopes (comma-delimited)

×

https://www.googleapis.com/auth/admin.reports.a

OAuth scopes (comma-delimited)

×

googleapis.com/auth/admin.reports.usage.readonly

CANCEL

AUTHORIZE

Figure 63. Add a new client ID

Configure the Google Workspace—Drive Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

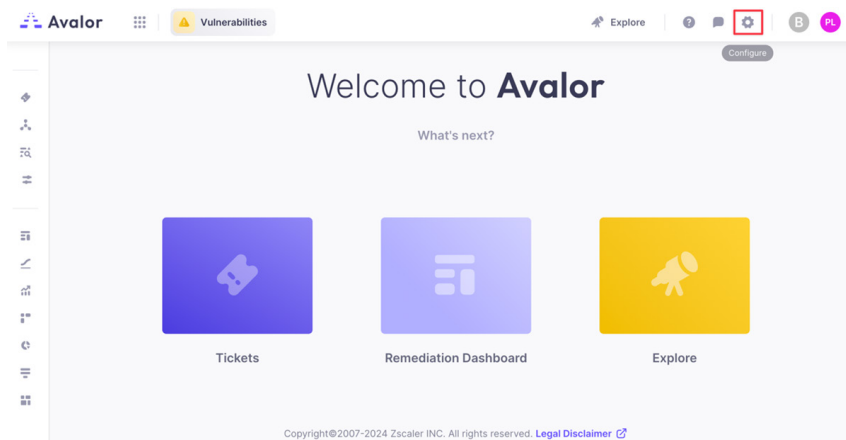



Figure 64. Configure

3. Click **Create**, then search for Google Workspace—Drive Activity.

Connect New Data Source

Q google workspace - drive activity X

Application



Google Workspace
- Drive Activity

Figure 65. Google Workspace - Drive Activity

4. Click the **Google Workspace—Drive Activity** application.
5. On the **Google Workspace—Drive Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

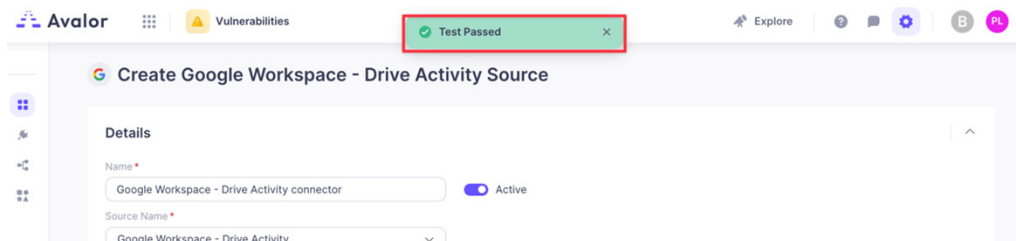


Figure 66. Test Passed

7. Click **Save**.

Create Google Workspace - Drive Activity Source

Details

Name *
Google Workspace - Drive Activity connector Active

Source Name *
Google Workspace - Drive Activity

Description

Retrieval

Credentials JSON *
{ "type": "service_account", "project_id": "avalon-projec..." }

Email *
jason.kim@avalonproject.com

☐ Explode By Events

Scheduling

Full Refresh Frequency *
None

Incremental Refresh Frequency *
Custom

Every *
10 Minutes

Remediation Detection Settings

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

Aging criteria + Add Rule

☐ Age immediately if Finding was not seen, while Asset was seen in the latest data refresh

Fallback

☐ Age immediately if Finding was not seen for day(s)

Advanced Settings

Suppression Rules

Select Field Contains Type Value

+ AND + OR

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 67. Create Google Workspace—Drive Activity Source

Google Workspace—Admin Activity Data Source

This data source provides information about administrative actions taken within the Google Workspace domain, including user management, settings changes, and other administrative tasks via the Admin SDK API.

The following sections describe how to configure a Google Workspace admin activity data source.

Configure the OAuth Scope

This data source reads Admin Activity from the Google Admin SDK API. To enable the Admin SDK API:

1. Sign in to your Google Cloud Console.
2. Select **APIs & Services > Library**.
3. Search for `Admin SDK API`.
4. Click **Admin SDK API**, then click **Enable**.

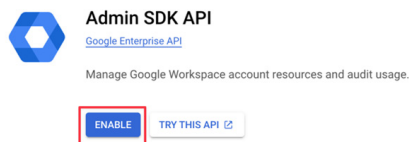


Figure 68. Admin SDK API

5. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
6. Click **Add new**.

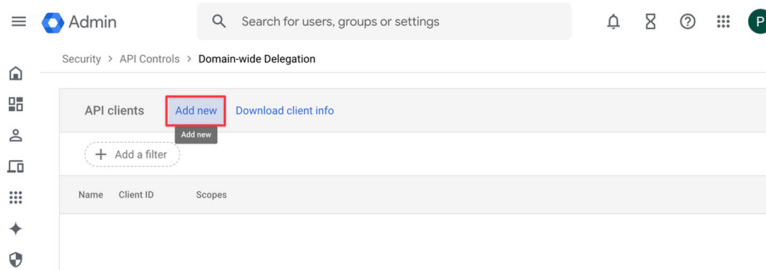


Figure 69. Manage Domain-wide Delegation

7. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
8. Click **Authorize**.

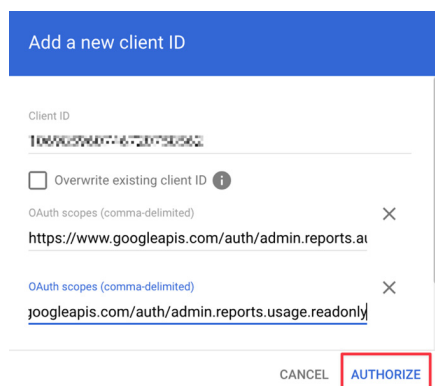


Figure 70. Add a new client ID

Configure the Google Workspace—Admin Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

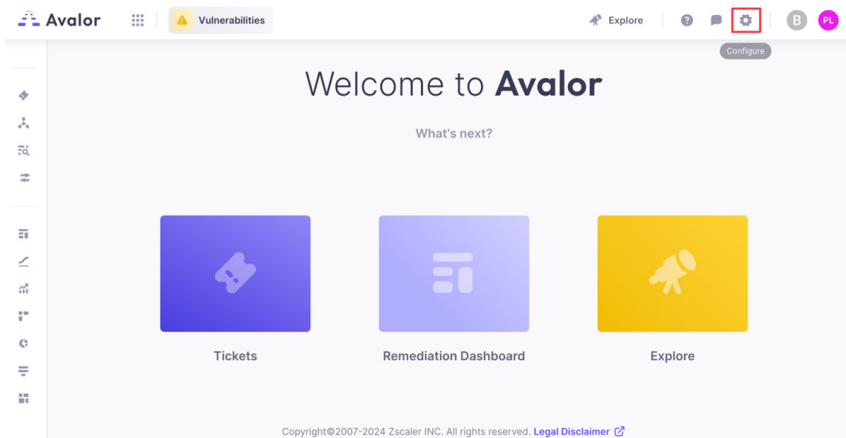


Figure 71. Configure

3. Click **Create**, then search for Google Workspace—Admin Activity.

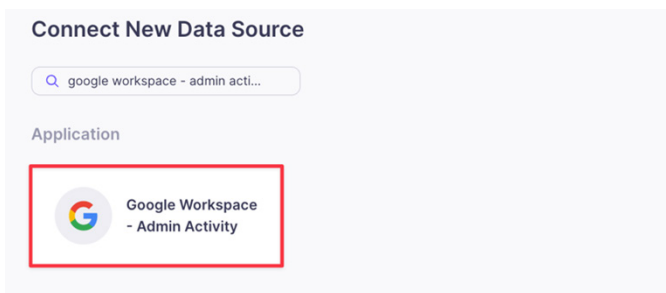


Figure 72. Google Workspace - Admin Activity

4. Click the **Google Workspace—Admin Activity** application.
5. On the **Google Workspace—Admin Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

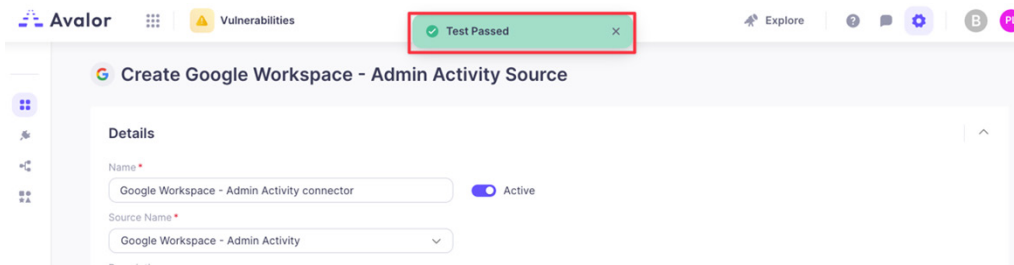


Figure 73. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration form for the 'Create Google Workspace - Admin Activity Source'. The form is divided into several sections:

- Details:** Includes fields for Name (Google Workspace - Admin Activity connector), Source Name (Google Workspace - Admin Activity), and a Description field. The Active toggle is on.
- Retrieval:** Includes a Credentials JSON field with the value { "type": "service_account", "project_id": "avalor-projec...", an Email field, and a Refresh Frequency section with options for Full and Incremental refresh frequencies.
- Scheduling:** Includes a Full Refresh Frequency dropdown set to 'None' and an Incremental Refresh Frequency dropdown set to 'Custom'.
- Remediation Detection Settings:** Includes an Aging criteria section with a checkbox for 'Age immediately if Finding was not seen, while Asset was seen in the latest data refresh' and a Fallback section with a checkbox for 'Age immediately if Finding was not seen for 1 day(s)'.
- Advanced Settings:** Includes a Suppression Rules section with a 'Select Field' dropdown, a 'Contains' button, a 'Type Value' input, and a checkbox for 'Prevent NULL from overriding existing values'.

 At the bottom right of the form, there are three buttons: 'Cancel', 'Test', and 'Save'. The 'Save' button is highlighted with a red box.

Figure 74. Create Google Workspace—Admin Activity Source

Google Workspace—Login Activity Data Source

This data source provides information about user login events, including details like login times, IP addresses, and devices used for authentication via the Admin SDK API.

The following sections describe how to configure a Google Workspace login activity data source.

Configure the OAuth Scope

This data source reads Login Activity from the Google Admin SDK API. To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

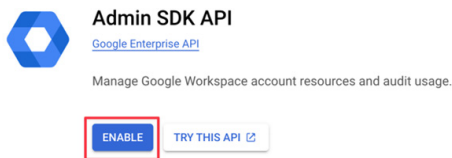


Figure 75. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

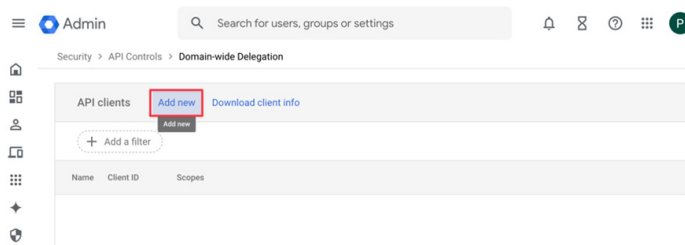


Figure 76. Manage Domain-wide Delegation

5. If absent, enter the **Client ID** from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

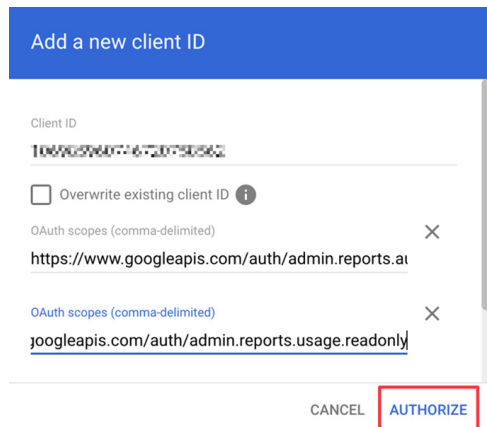


Figure 77. Add a new client ID

Configure the Google Workspace—Login Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

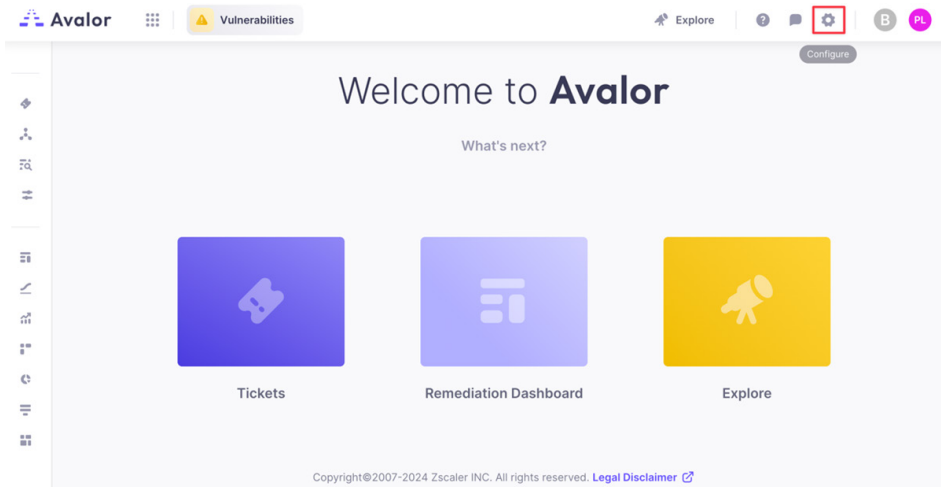


Figure 78. Configure

3. Click **Create**, then search for Google Workspace—Login Activity.

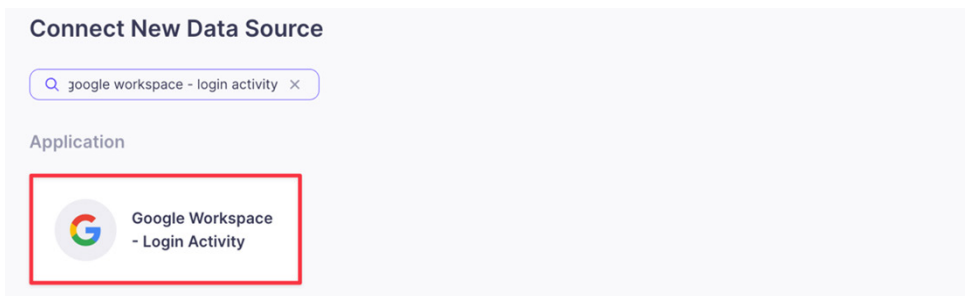


Figure 79. Google Workspace—Login Activity

4. Click the **Google Workspace—Login Activity** application.
5. On the **Google Workspace—Login Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

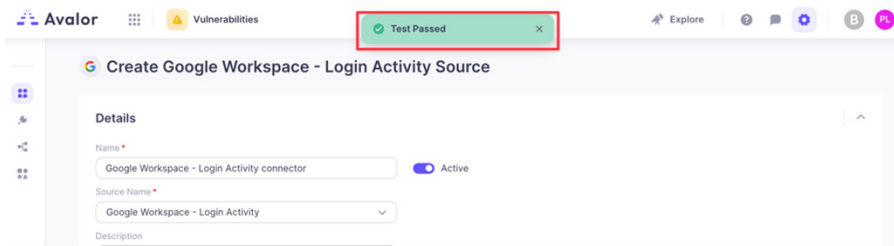


Figure 80. Test Passed

7. Click **Save**.

 This screenshot shows the same configuration page as Figure 80, but with several fields highlighted by red boxes to indicate where to click or enter information:

- Details:** The 'Name' field (Google Workspace - Login Activity connector) and the 'Active' toggle switch.
- Retrieval:** The 'Credentials JSON' field containing a JSON snippet, and the 'Email' field.
- Scheduling:** The 'Full Refresh Frequency' dropdown (set to None), the 'Incremental Refresh Frequency' dropdown (set to Custom), and the 'Every' field (set to 10 minutes).
- Remediation Detection Settings:** The 'Aging criteria' checkbox and the 'Fallback' checkbox.
- Advanced Settings:** The 'Suppression Rules' section, including the 'Select Field' dropdown, the 'Contains' button, the 'Type Value' input, and the 'Prevent NULL from overriding existing values' checkbox.

 At the bottom right, the 'Save' button is highlighted with a red box.

Figure 81. Create Google Workspace—Login Activity

Google Workspace—Mobile Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe configuring a Google Workspace mobile activity data source.

Configure the OAuth Scope

To enable the Admin SD API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

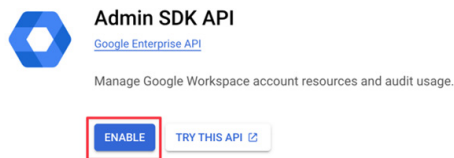


Figure 82. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

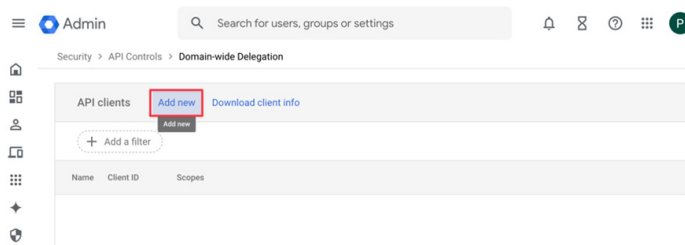


Figure 83. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

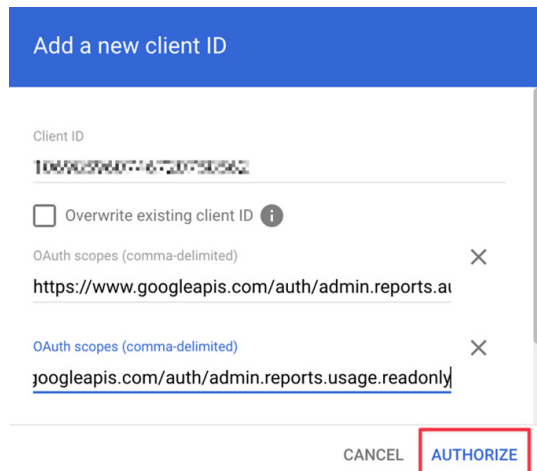


Figure 84. Add a new client ID

Configure the Google Workspace—Mobile Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

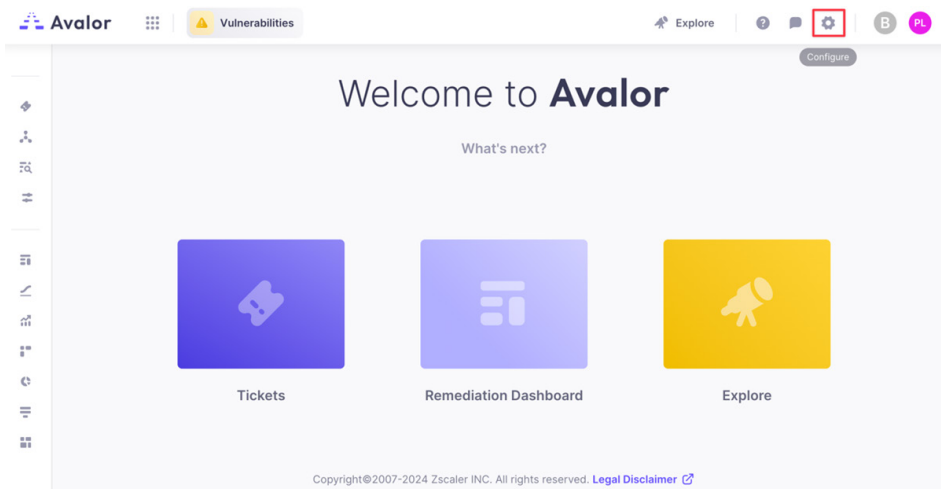


Figure 85. Configure

3. Click **Create**, then search for Google Workspace—Mobile Activity.

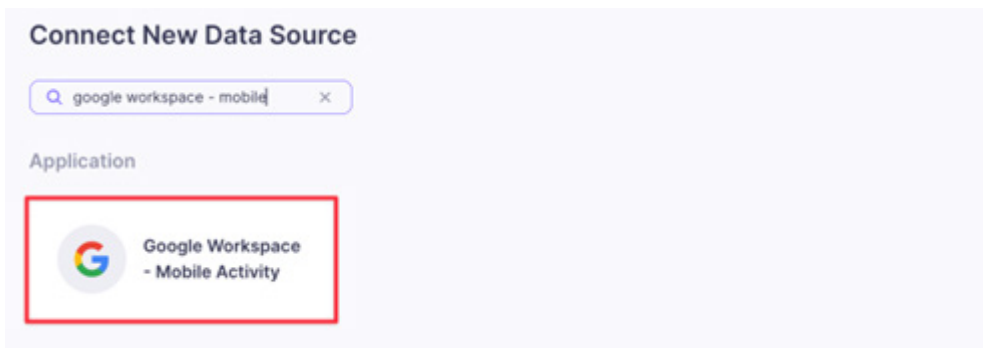


Figure 86. Google Workspace—Mobile Activity

4. Click the **Google Workspace—Mobile Activity** application.
5. On the **Google Workspace—Mobile Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

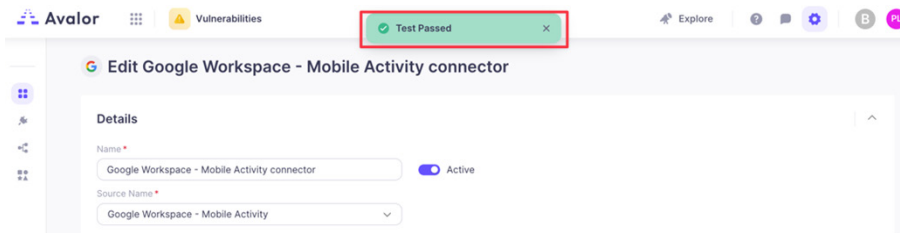


Figure 87. Test Passed

7. Click **Save**.

Figure 88. Create Google Workspace—Mobile Activity Source

Google Workspace—OAuth Tokens Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe configuring a Google Workspace OAuth tokens activity data source.

Configure the OAuth Scope

To enable the Admin SD API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

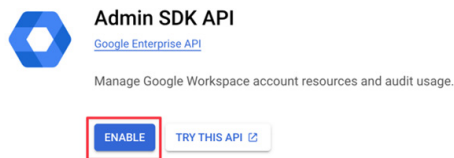


Figure 89. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

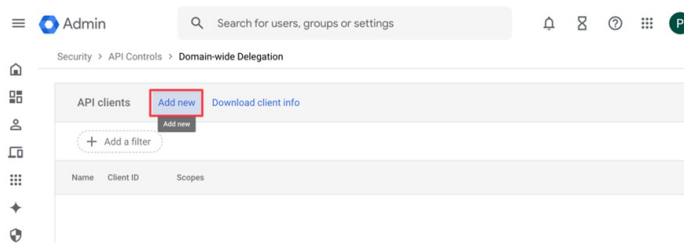


Figure 90. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

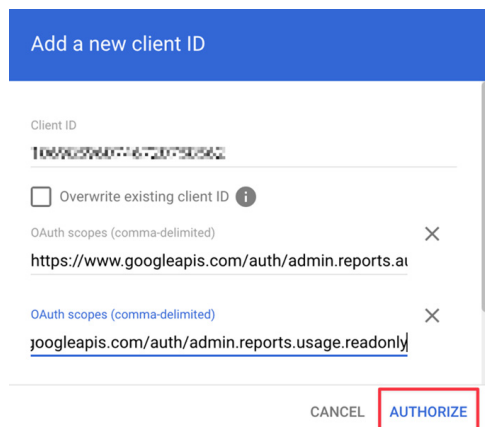


Figure 91. Add a new client ID

Configure the Google Workspace—OAuth Tokens Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

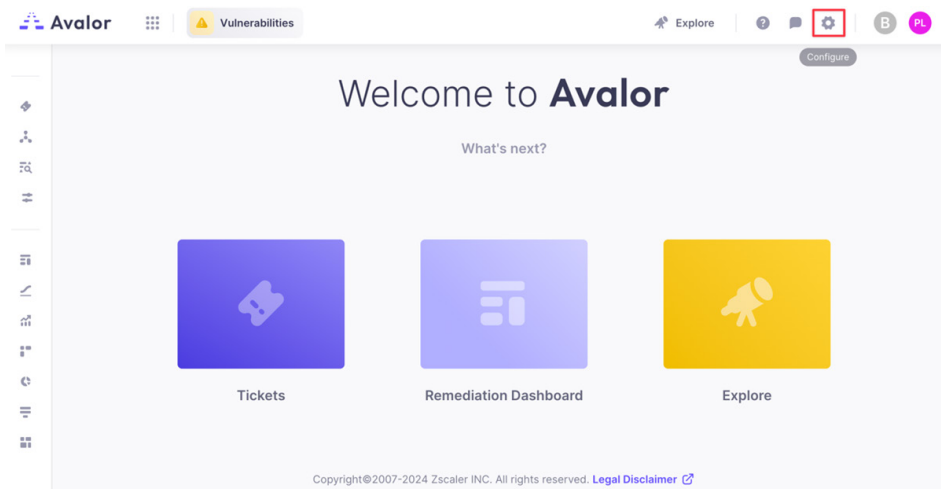


Figure 92. Configure

3. Click **Create**, then search for Google Workspace—OAuth Tokens Activity.

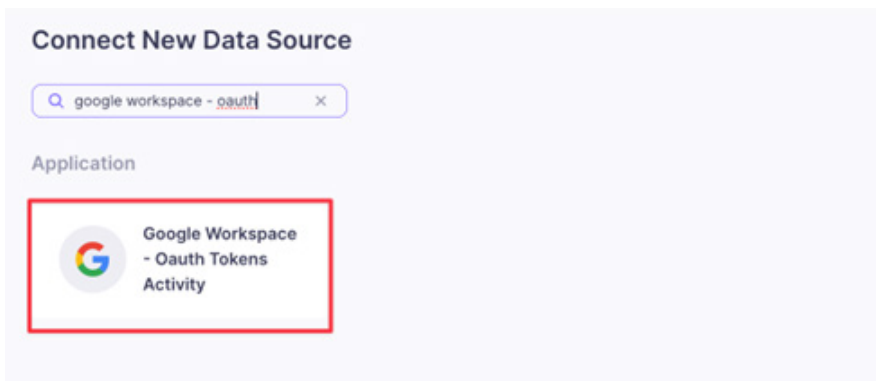


Figure 93. Google Workspace—OAuth Tokens Activity

4. Click the **Google Workspace—OAuth Tokens Activity** application.
5. On the **Google Workspace—OAuth Tokens Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

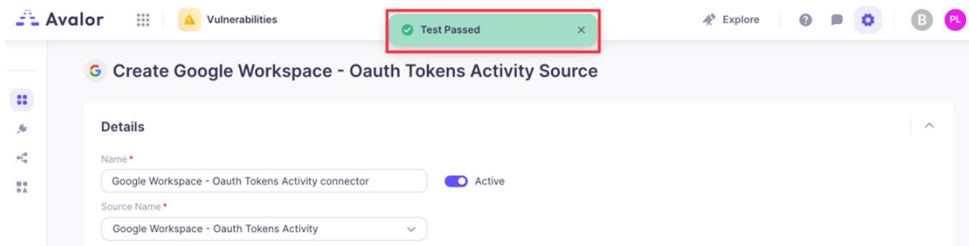


Figure 94. Test Passed

7. Click **Save**.

This screenshot shows the full configuration page for the 'Create Google Workspace - OAuth Tokens Activity Source'. The 'Details' section includes the name, an 'Active' toggle, and source name. The 'Retrieval' section contains the 'Credentials JSON' field with a sample JSON snippet, an 'Email' field, and a 'Description' field. The 'Scheduling' section has dropdowns for 'Full Refresh Frequency' (set to 'None') and 'Incremental Refresh Frequency' (set to 'Custom'), along with an 'Every' field set to '10' minutes. The 'Remediation Detection Settings' section includes 'Aging criteria' and 'Fallback' options, both with checkboxes. The 'Advanced Settings' section features a 'Suppression Rules' table with columns for 'Select Field', 'Contains', and 'Type Value', and a checkbox for 'Prevent NULL from overriding existing values'. At the bottom right, there are 'Cancel', 'Test', and 'Save' buttons, with the 'Save' button highlighted by a red box.

Figure 95. Create Google Workspace—OAuth Tokens Activity Source

Google Workspace—Rules Activity Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe configuring a Google Workspace rules activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

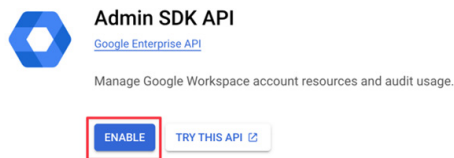


Figure 96. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

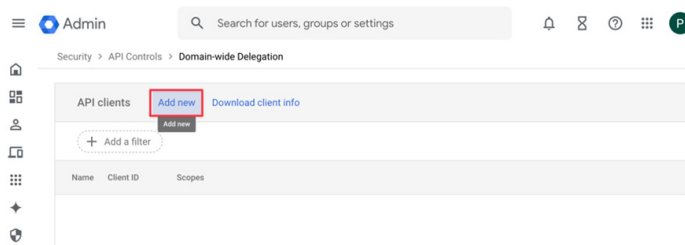


Figure 97. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

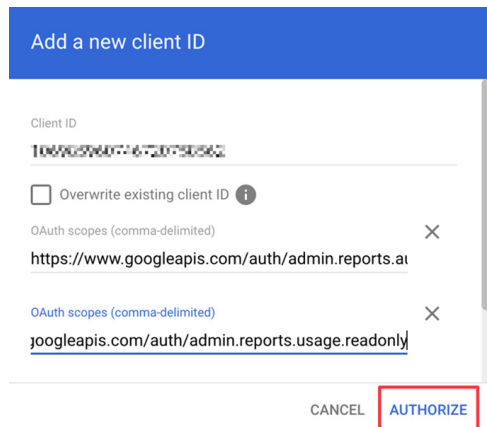


Figure 98. Add a new client ID

Configure the Google Workspace—Rules Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

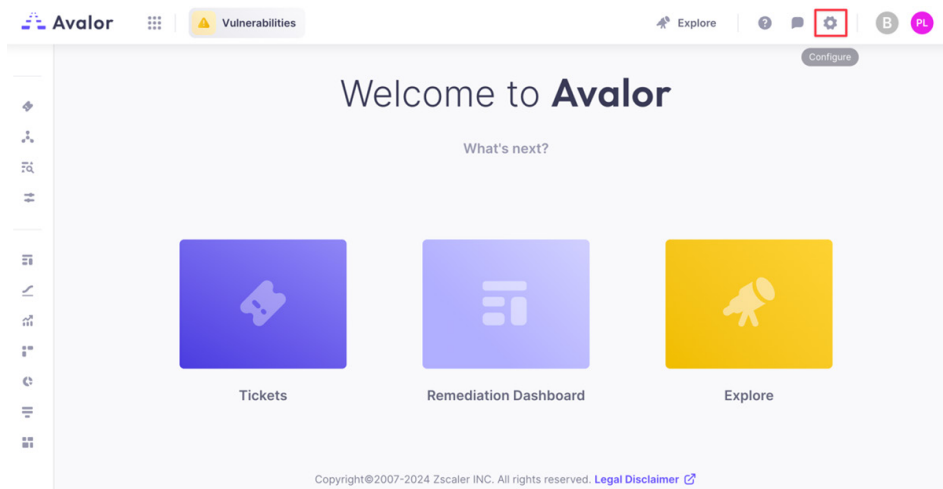


Figure 99. Configure

3. Click **Create**, then search for Google Workspace—Rules Activity.

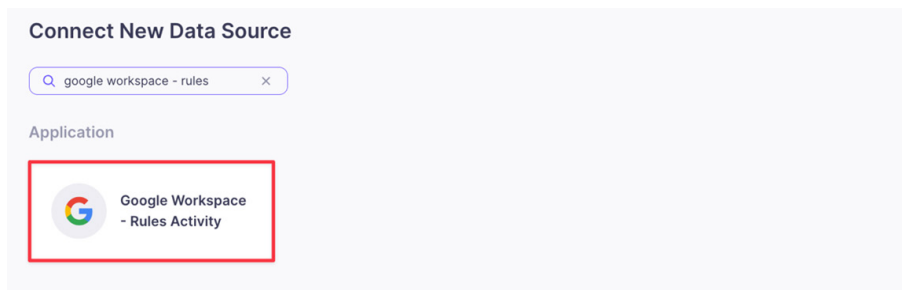


Figure 100. Google Workspace—Rules Activity

4. Click the **Google Workspace—Rules Activity** application.
5. On the **Google Workspace—Rules Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

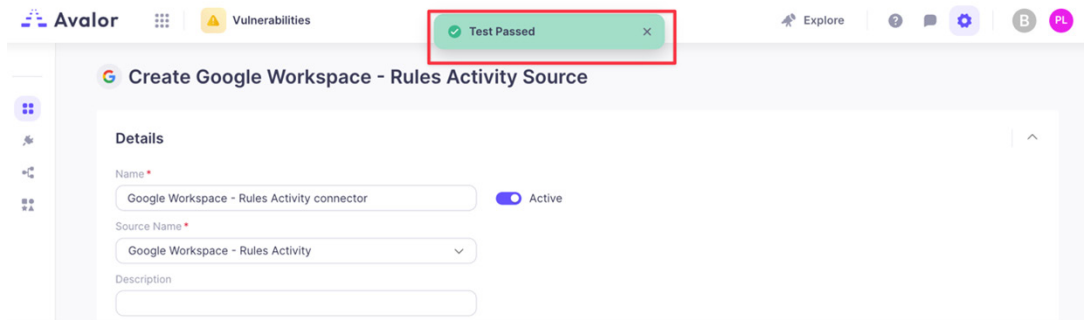


Figure 101. Test Passed

7. Click **Save**.

 This screenshot shows the full 'Create Google Workspace - Rules Activity Source' form. The sections are:

- Details:** Name (Google Workspace - Rules Activity connector), Source Name (Google Workspace - Rules Activity), and Description (empty). The 'Active' toggle is on.
- Retrieval:** Credentials JSON ({"type": "service_account", "project_id": "avalor-projec..."}), Email (p8: aqph2g 8k-8h4 n: 448).
- Scheduling:** Full Refresh Frequency (None), Incremental Refresh Frequency (Custom), Every (10 Minutes).
- Remediation Detection Settings:** Aging criteria (Age immediately if Finding was not seen, while Asset was seen in the latest data refresh), Fallback (Age immediately if Finding was not seen for 1 day(s)).
- Advanced Settings:** Suppression Rules (Select Field, Contains, Type Value, Prevent NULL from overriding existing values checked).

 At the bottom right, there are 'Cancel', 'Test', and 'Save' buttons.

Figure 102. Create Google Workspace—Rules Activity Source

Google Workspace—Access Transparency Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace access transparency activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

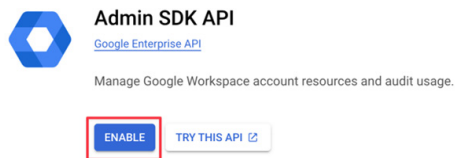


Figure 103. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

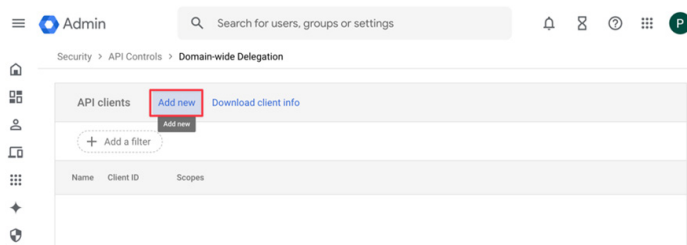


Figure 104. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

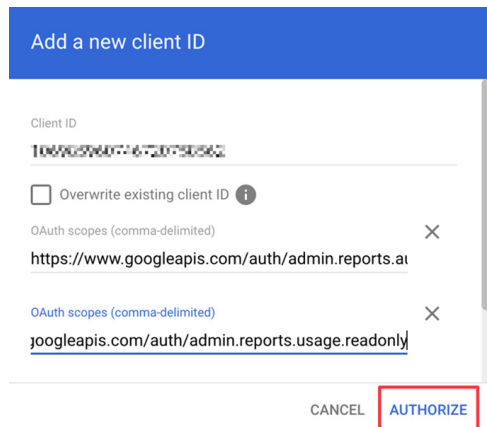


Figure 105. Add a new client ID

Configure the Google Workspace—Access Transparency Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

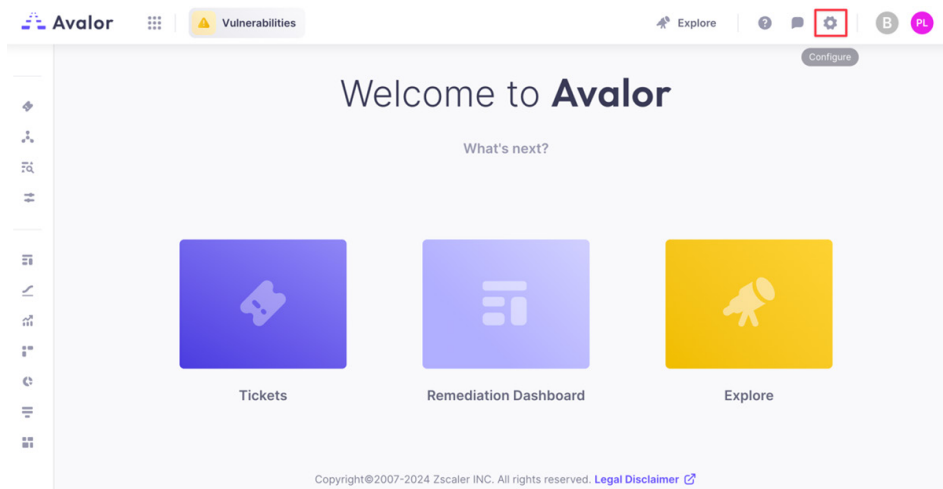


Figure 106. Configure

3. Click **Create**, then search for Google Workspace - Access Transparency Activity.

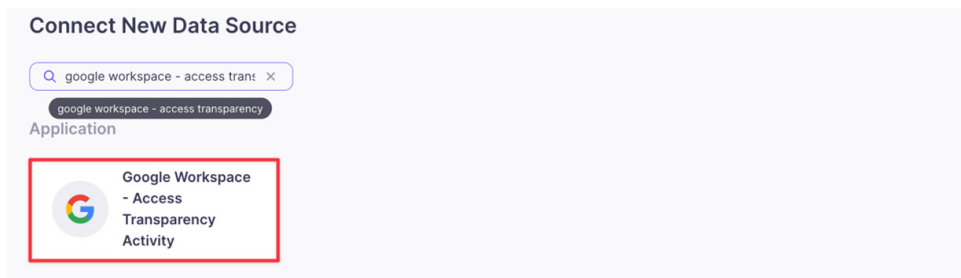


Figure 107. Google Workspace—Access Transparency Activity

4. Click the **Google Workspace—Access Transparency Activity** application.
5. On the **Google Workspace—Access Transparency Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

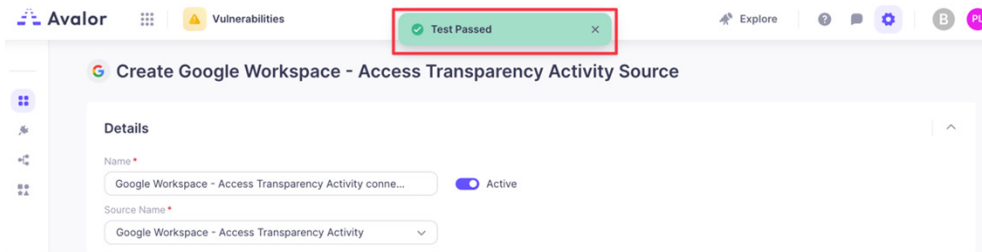


Figure 108. Test Passed

7. Click **Save**.

 A screenshot of the 'Create Google Workspace - Access Transparency Activity Source' configuration page. The page is divided into several sections:

- Details:** The 'Name' field is highlighted with a red box. The 'Active' toggle switch is also highlighted.
- Retrieval:** The 'Credentials JSON' field is highlighted with a red box, containing a JSON snippet: `{ "type": "service_account", "project_id": "avalor-projec..." }`. The 'Email' field is also highlighted with a red box, containing a service account email address.
- Scheduling:** The 'Full Refresh Frequency' dropdown is set to 'None' and is highlighted with a red box. The 'Incremental Refresh Frequency' dropdown is set to 'Custom' and is also highlighted with a red box. The 'Every' field is set to '10' minutes.
- Remediation Detection Settings:** The 'Aging criteria' section has a checkbox 'Age immediately if Finding was not seen, while Asset was seen in the latest data refresh' which is highlighted with a red box. The 'Fallback' section has a checkbox 'Age immediately if Finding was not seen for' followed by a text field 'day(s)' which is also highlighted with a red box.
- Advanced Settings:** The 'Suppression Rules' section is highlighted with a red box. It shows a rule configuration with 'Select Field' and 'Contains' operators. Below the rule configuration, the checkbox 'Prevent NULL from overriding existing values' is checked.

 At the bottom right of the page, there are three buttons: 'Cancel', 'Test', and 'Save'. The 'Save' button is highlighted with a red box.

Figure 109. Create Google Workspace—Access Transparency Activity Source

Google Workspace—Calendar Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace calendar activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

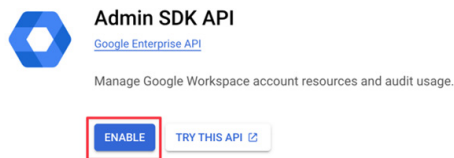


Figure 110. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

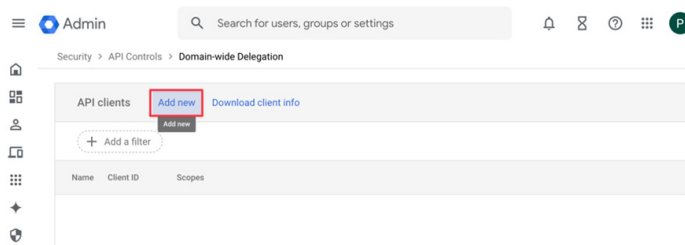


Figure 111. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

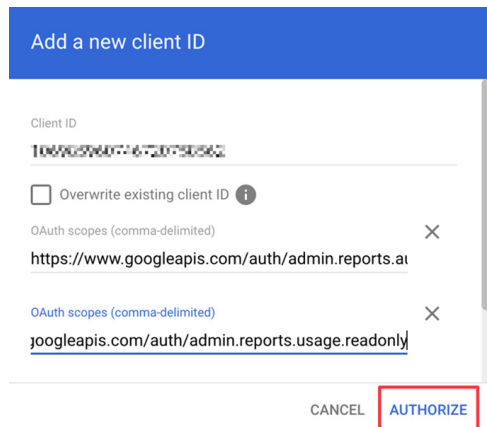


Figure 112. Add a new client ID

Configure the Google Workspace—Calendar Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

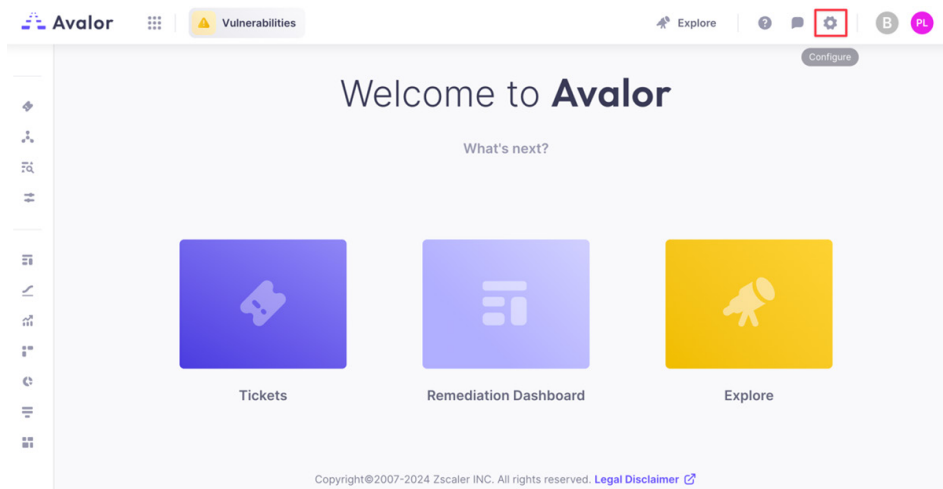


Figure 113. Configure

3. Click **Create**, then search for Google Workspace - Calendar Activity.

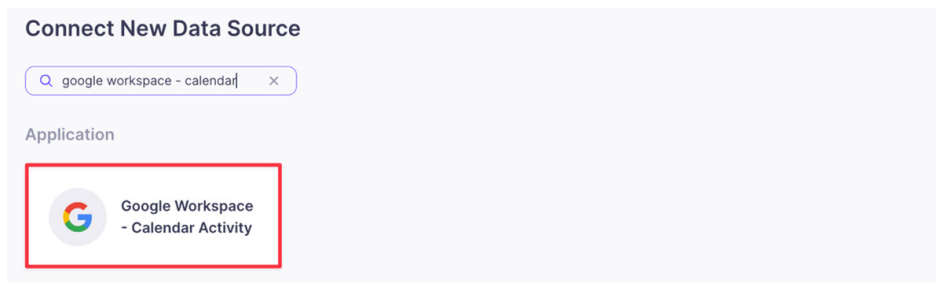


Figure 114. Google Workspace—Calendar Activity

4. Click the **Google Workspace—Calendar Activity** application.
5. On the **Google Workspace—Calendar Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

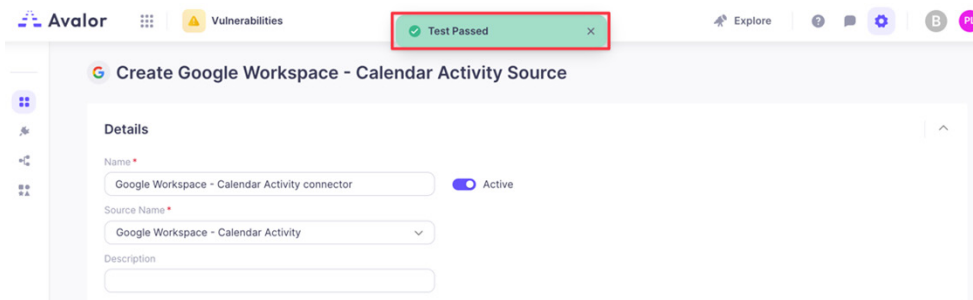


Figure 115. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the 'Create Google Workspace - Calendar Activity Source'. The 'Details' section is at the top, with 'Name' set to 'Google Workspace - Calendar Activity connector' and 'Active' toggle on. Below this is the 'Retrieval' section, where 'Credentials (JSON)' is set to a JSON object: { "type": "service_account", "project_id": "avalor-projec...", and 'Email' is set to '51-4...@...'. The 'Scheduling' section has 'Full Refresh Frequency' set to 'None' and 'Incremental Refresh Frequency' set to 'Custom' with 'Every' set to '10' minutes. The 'Remediation Detection Settings' section includes 'Aging criteria' (unchecked) and 'Fallback' (unchecked). The 'Advanced Settings' section shows 'Suppression Rules' with a rule 'Select Field' containing 'Type Value' and a checkbox 'Prevent NULL from overriding existing values' which is checked. At the bottom right, there are 'Cancel', 'Test', and 'Save' buttons, with 'Save' highlighted.

Figure 116. Create Google Workspace—Calendar Activity Source

Google Workspace—Chat Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace chat activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

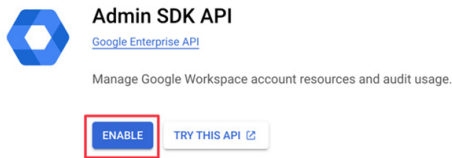


Figure 117. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

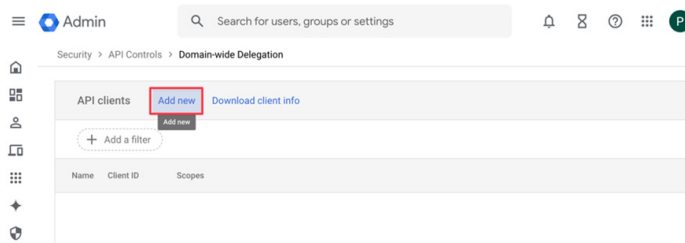


Figure 118. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

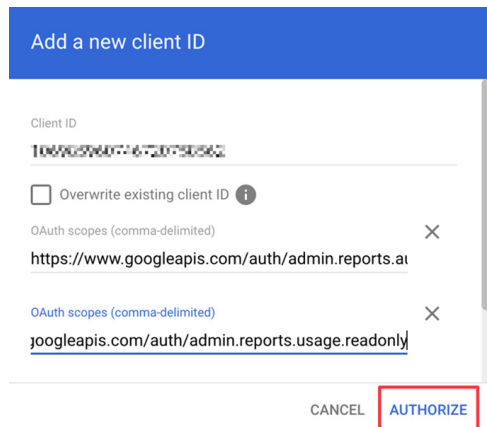


Figure 119. Add a new client ID

Configure the Google Workspace—Chat Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

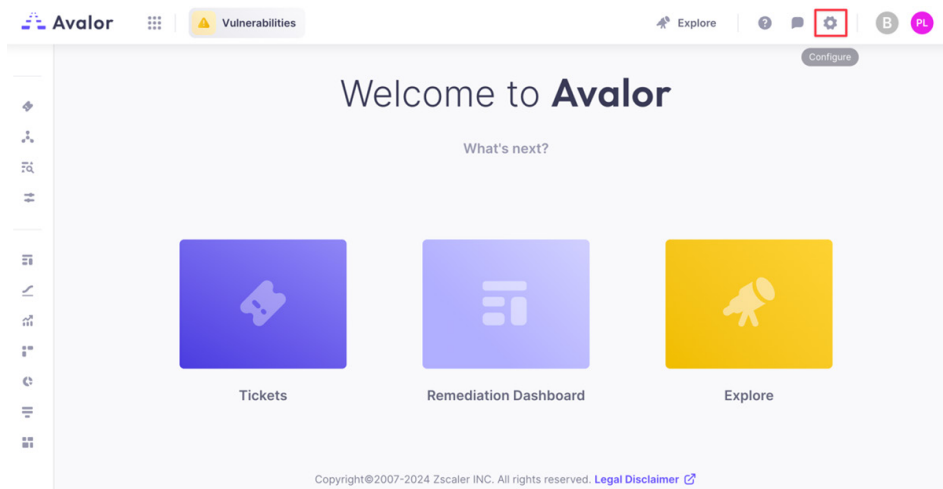


Figure 120. Configure

3. Click **Create**, then search for Google Workspace—Chat Activity.

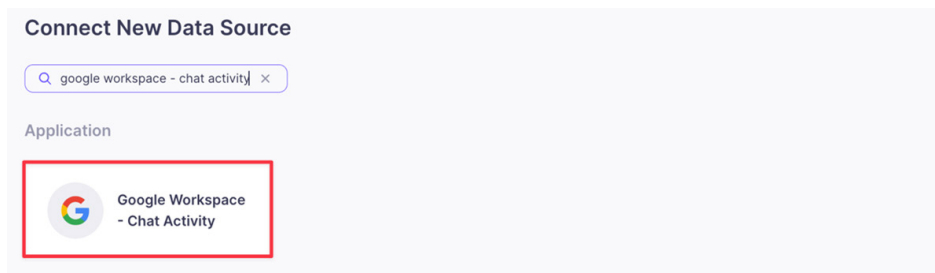


Figure 121. Google Workspace—Chat Activity

4. Click the **Google Workspace—Chat Activity** application.
5. On the **Google Workspace—Chat Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

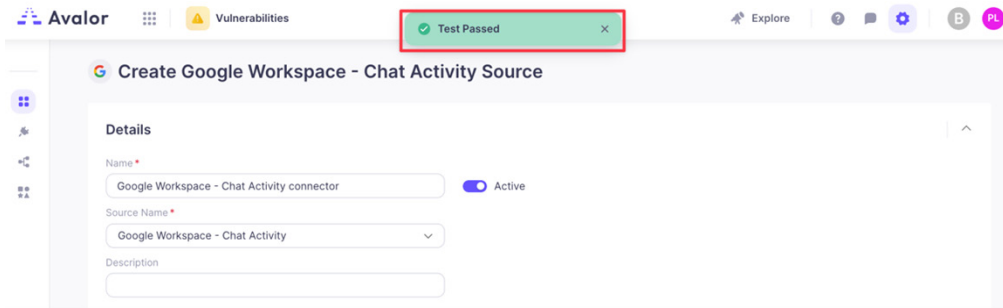


Figure 122. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the 'Create Google Workspace - Chat Activity Source'.
 - **Details:** 'Name' is 'Google Workspace - Chat Activity connector', 'Active' is checked, 'Source Name' is 'Google Workspace - Chat Activity', and 'Description' is empty.
 - **Retrieval:** 'Credentials JSON' contains a service account key snippet, and 'Email' is the corresponding service account email.
 - **Scheduling:** 'Full Refresh Frequency' is 'None', 'Incremental Refresh Frequency' is 'Custom', and 'Every' is set to '10 Minutes'.
 - **Remediation Detection Settings:** Under 'Aging criteria', the checkbox 'Age immediately if Finding was not seen, while Asset was seen in the latest data refresh' is checked. Under 'Fallback', the checkbox 'Age immediately if Finding was not seen for' is checked with a 'day(s)' input field.
 - **Advanced Settings:** Under 'Suppression Rules', a rule is defined with 'Select Field' as the condition, 'Contains' as the operator, and 'Type Value' as the value. The checkbox 'Prevent NULL from overriding existing values' is checked.
 At the bottom right, there are 'Cancel', 'Test', and 'Save' buttons, with 'Save' highlighted in red.

Figure 123. Create Google Workspace—Chat Activity Source

Google Workspace—Chrome Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace Chrome activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

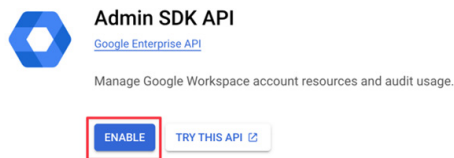


Figure 124. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

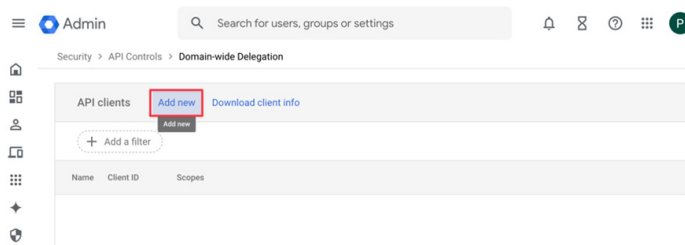


Figure 125. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

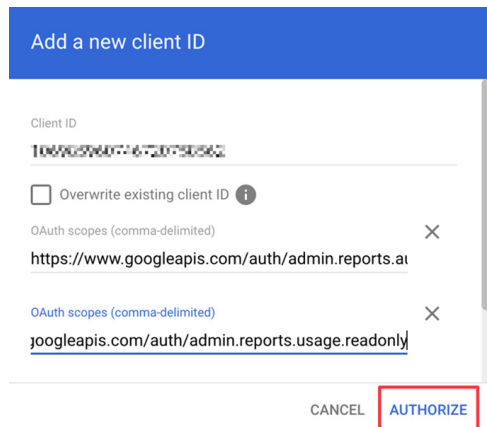


Figure 126. Add a new client ID

Configure the Google Workspace—Chrome Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

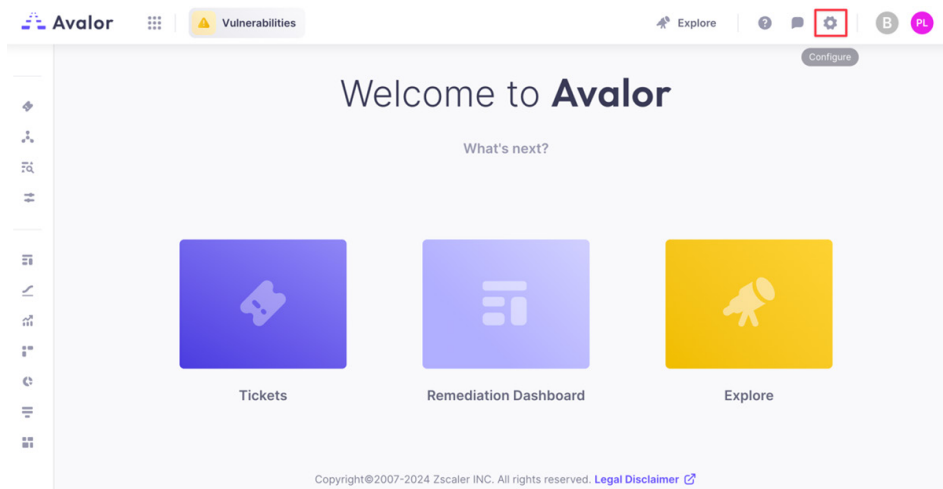


Figure 127. Configure

3. Click **Create**, then search for Google Workspace - Chrome Activity.

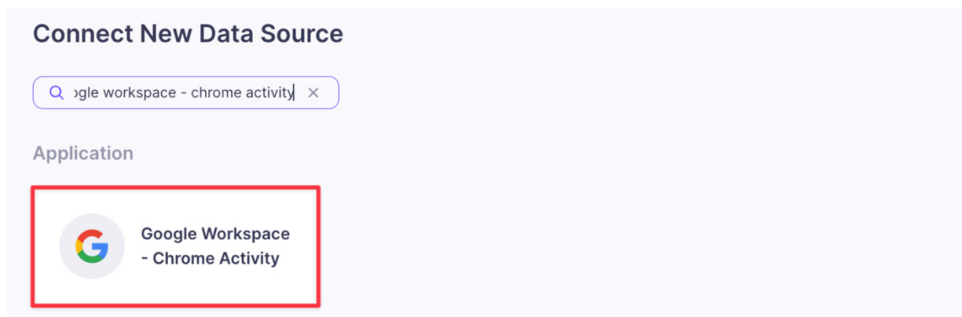


Figure 128. Google Workspace—Chrome Activity

4. Click the **Google Workspace—Chrome Activity** application.
5. On the **Google Workspace—Chrome Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

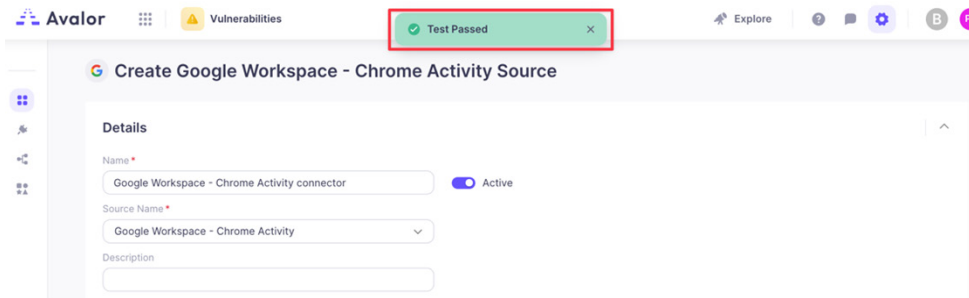


Figure 129. Test Passed

7. Click **Save**.

Create Google Workspace - Chrome Activity Source

Details

Name *
Google Workspace - Chrome Activity connector Active

Source Name *
Google Workspace - Chrome Activity

Description

Retrieval

Credentials JSON *
{ "type": "service_account", "project_id": "avalor-projec..."

Email *
[redacted]

Scheduling

Full Refresh Frequency *
None

Incremental Refresh Frequency *
Custom

Every *
10 Minutes

Remediation Detection Settings

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

Aging criteria + Add Rule
☐ Age immediately if Finding was not seen, while Asset was seen in the latest data refresh

Fallback
☐ Age immediately if Finding was not seen for day(s)

Advanced Settings

Suppression Rules

Select Field Contains Type Value

+ AND + OR

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 130. Create Google Workspace—Chrome Activity Source

Google Workspace—Context-Aware Access Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace context-aware access activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

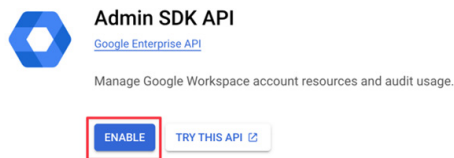


Figure 131. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

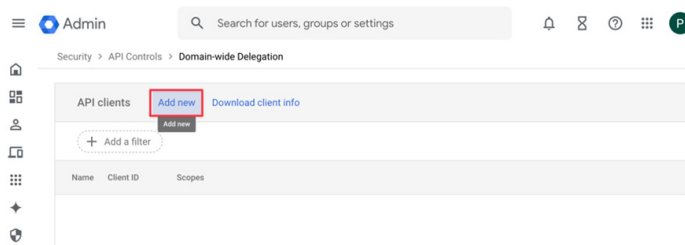


Figure 132. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

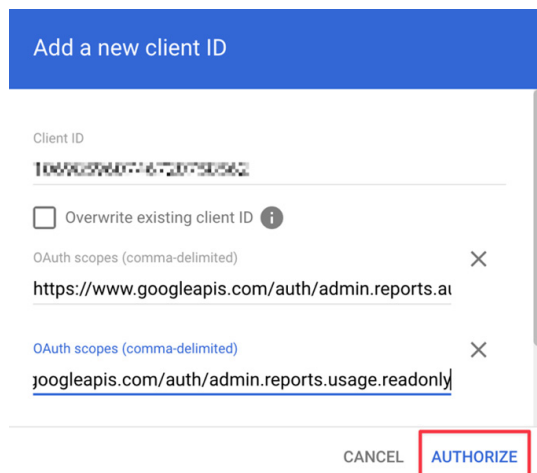


Figure 133. Add a new client ID

Configure the Google Workspace—Context-Aware Access Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

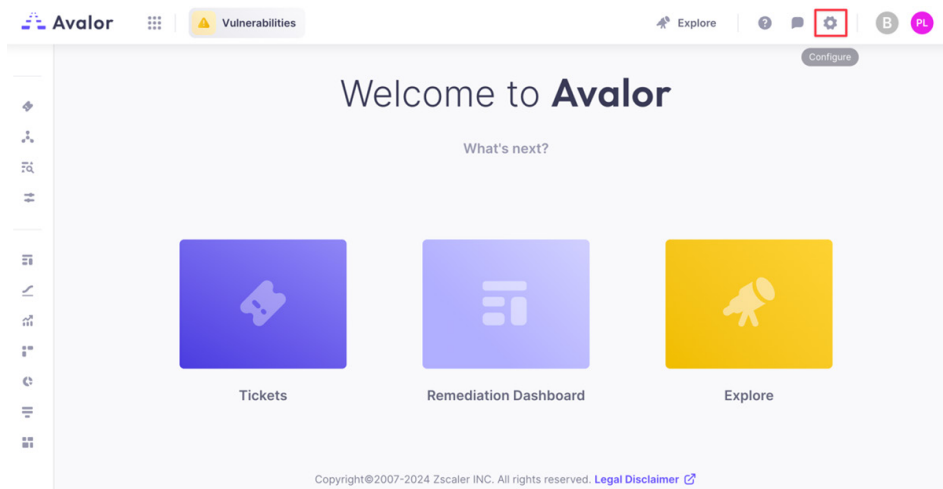


Figure 134. Configure

3. Click **Create**, then search for Google Workspace—Context-Aware Access Activity.

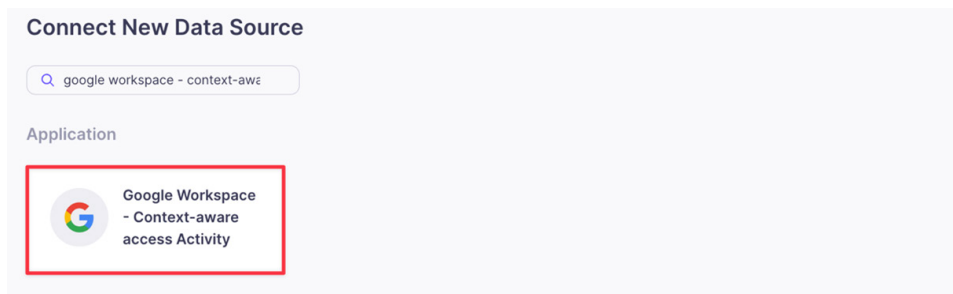


Figure 135. Google Workspace—Context-Aware Access Activity

4. Click the **Google Workspace—Context-Aware Access Activity** application.
5. On the **Google Workspace—Context-Aware Access Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

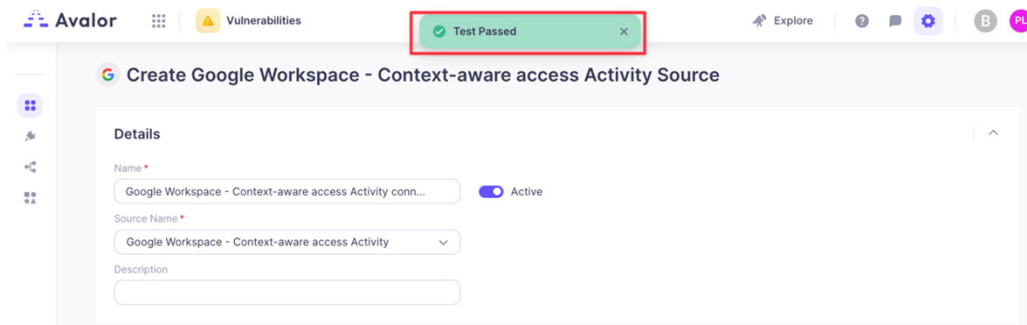


Figure 136. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the "Create Google Workspace - Context-aware access Activity Source". Several fields are highlighted with red boxes:

- Details:** The Name field, the Active toggle switch, and the Source Name dropdown.
- Retrieval:** The Credentials JSON field containing {"type": "service_account", "project_id": "avalor-projec..."} and the Email field containing [REDACTED].
- Scheduling:** The Full Refresh Frequency dropdown (set to None), the Incremental Refresh Frequency dropdown (set to Custom), and the Every field (set to 10 Minutes).
- Remediation Detection Settings:** The Aging criteria checkbox (unchecked) and the Fallback checkbox (unchecked).
- Advanced Settings:** The Suppression Rules section, which includes a table with columns for Select Field, Contains, and Type Value, and a checkbox for "Prevent NULL from overriding existing values" which is checked.

 At the bottom right, the "Save" button is highlighted with a red box.

Figure 137. Create Google Workspace—Context-Aware Access Activity Source

Google Workspace—Data Studio Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace data studio activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

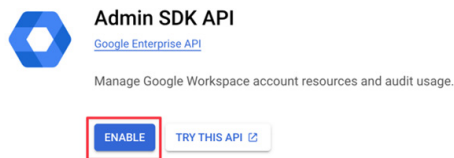


Figure 138. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

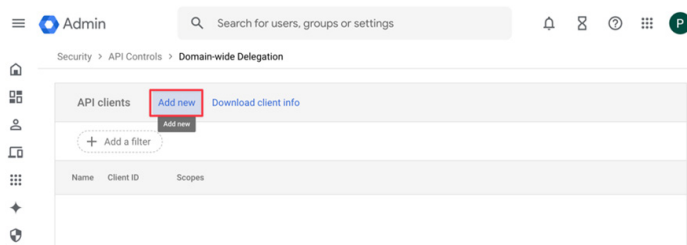


Figure 139. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

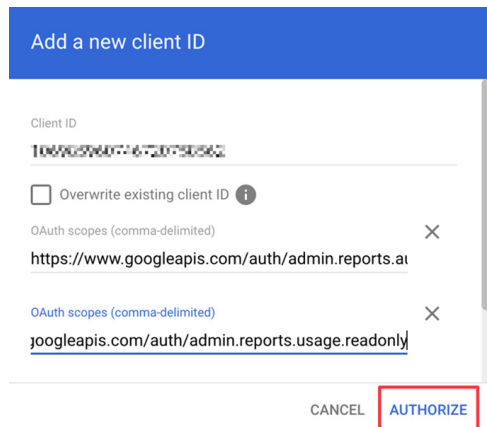


Figure 140. Add a new client ID

Configure the Google Workspace—Data Studio Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

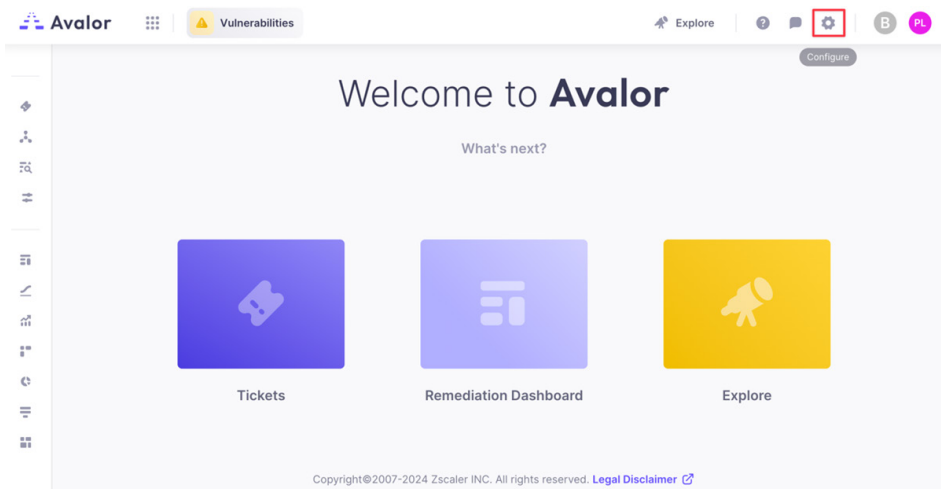


Figure 141. Configure

3. Click **Create**, then search for Google Workspace—Data Studio Activity.

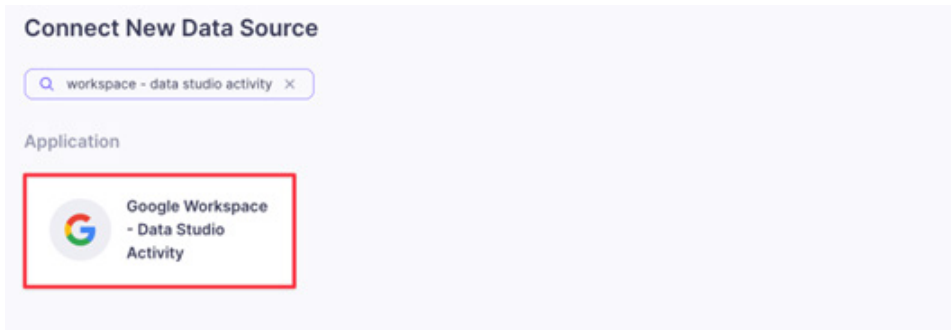


Figure 142. Google Workspace—Data Studio Activity

4. Click the **Google Workspace—Data Studio Activity** application.
5. On the **Google Workspace—Data Studio Activity** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

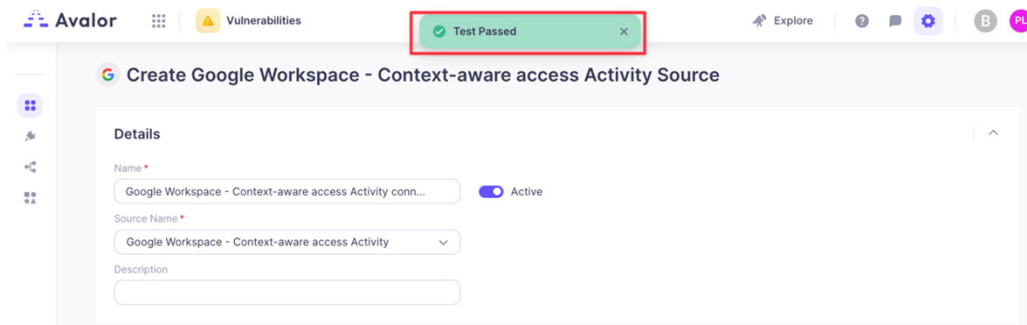


Figure 143. Test Passed

7. Click **Save**.

 This screenshot shows the "Create Google Workspace - Data Studio Activity Source" configuration page. Several fields are highlighted with red boxes:

- Details:** The "Name" field is set to "Google Workspace - Data Studio Activity connector" and the "Active" toggle is turned on.
- Retrieval:** The "Credentials JSON" field contains a JSON snippet: `{ "type": "service_account", "project_id": "avalor-projec..." }`. The "Email" field contains `project-ops@ca-studio.com`.
- Scheduling:** The "Full Refresh Frequency" is set to "None", and the "Incremental Refresh Frequency" is set to "Custom". The "Every" field is set to "10" minutes.
- Remediation Detection Settings:** Under "Aging criteria", the checkbox "Age immediately if Finding was not seen, while Asset was seen in the latest data refresh" is checked. Under "Fallback", the checkbox "Age immediately if Finding was not seen for" is checked with a value of "day(s)".
- Advanced Settings:** Under "Suppression Rules", a rule is defined with "Select Field" containing "Contains" and "Type Value". The checkbox "Prevent NULL from overriding existing values" is checked.

 At the bottom right, the "Save" button is highlighted in red.

Figure 144. Create Google Workspace—Data Studio Activity Source

Google Workspace—Google Cloud Platform Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Cloud platform activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

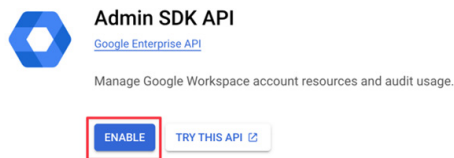


Figure 145. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

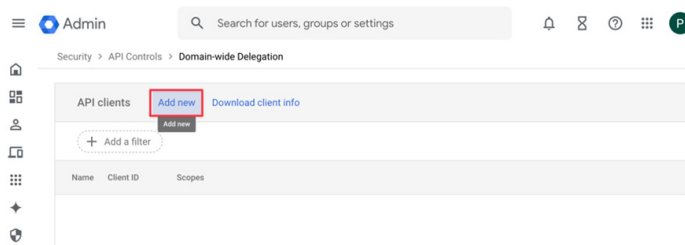


Figure 146. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

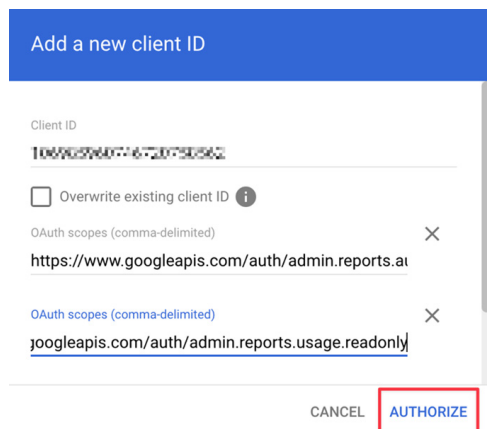


Figure 147. Add a new client ID

Configure the Google Workspace—Google Cloud Platform Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

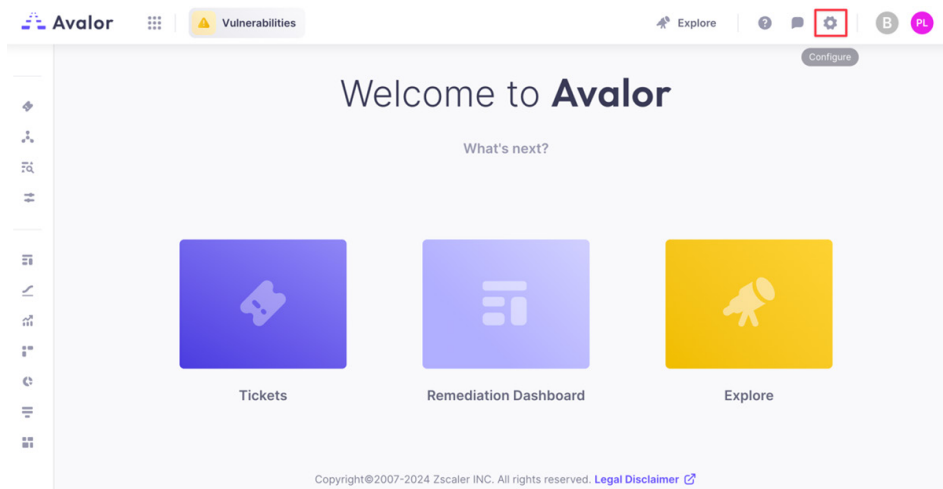


Figure 148. Configure

3. Click **Create**, then search for Google Workspace—Google Cloud Platform Activity.

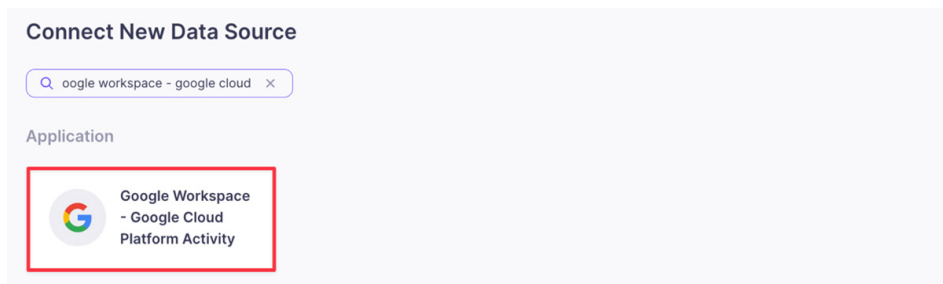


Figure 149. Google Workspace—Google Cloud Platform Activity

4. Click the **Google Workspace—Google Cloud Platform Activity** application.
5. On the **Google Workspace—Google Cloud Platform Activity** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

Google Workspace—Google+ Activity Data Source

This data source monitors activities related to Google+ via the Google Admin SDK API. The following sections describe how to configure a Google+ activity data source.



Google+ is discontinued.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for **Admin SDK API**, then click **Admin SDK API** and **Enable**.

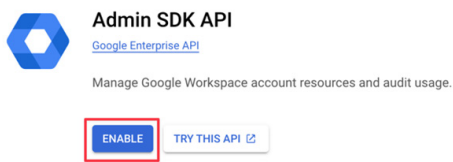


Figure 152. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

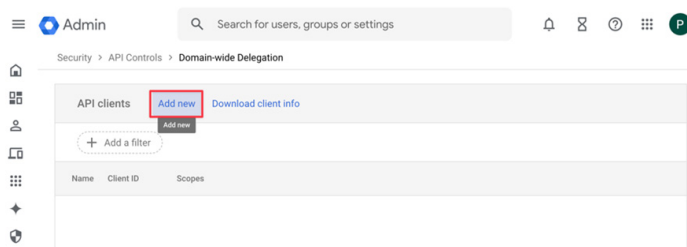


Figure 153. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`.
6. Click **Authorize**.

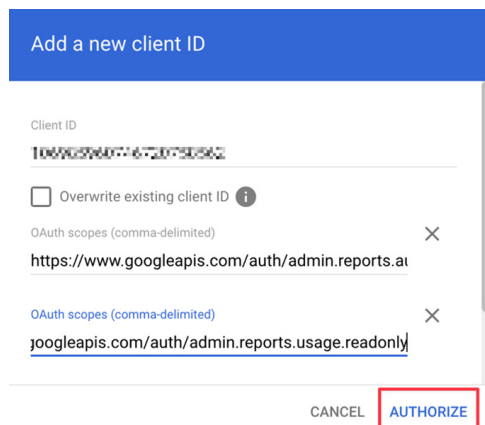


Figure 154. Add a new client ID

Configure the Google Workspace—Google+ Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

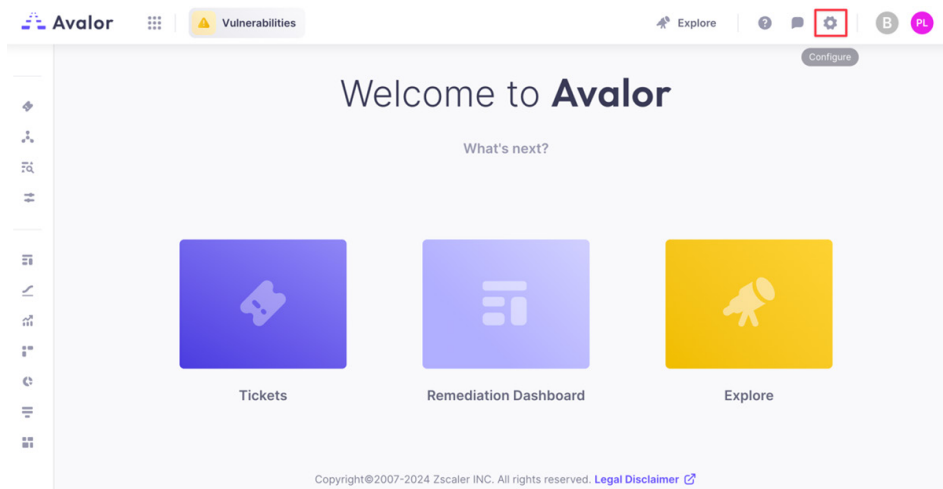


Figure 155. Configure

3. Click **Create**, then search for Google Workspace—Google+ Activity.

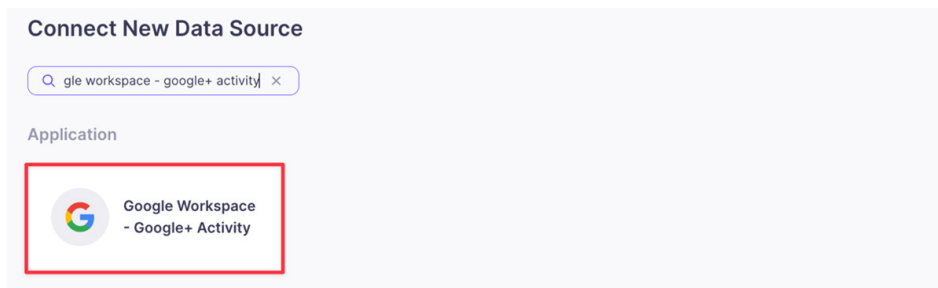


Figure 156. Google Workspace—Google+ Activity

4. Click the **Google Workspace—Google+ Activity** application.
5. On the **Google Workspace—Google+ Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

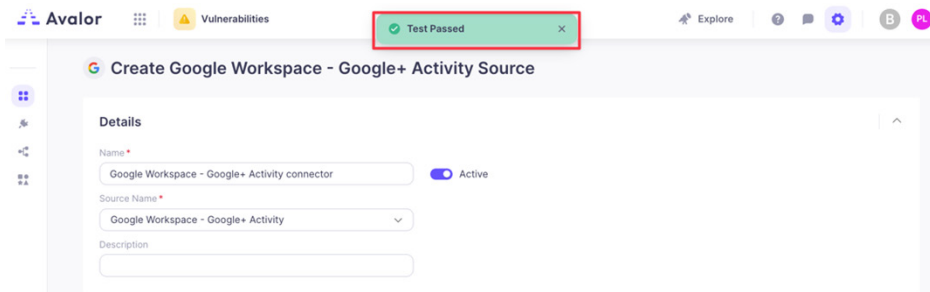


Figure 157. Test Passed

7. Click **Save**.

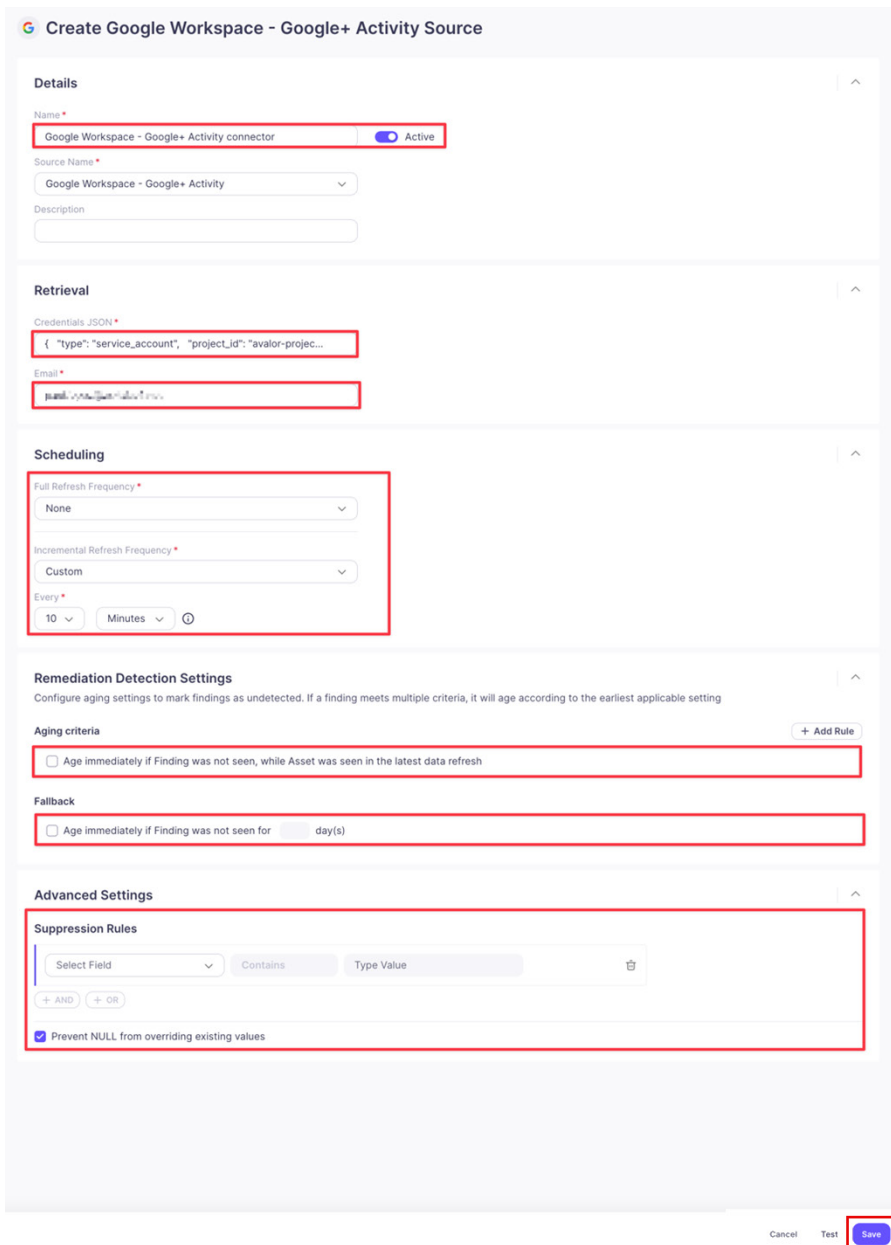


Figure 158. Create Google Workspace—Google+ Activity Source

Google Workspace—Groups Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace groups activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

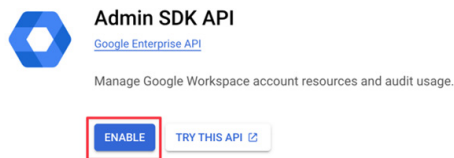


Figure 159. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

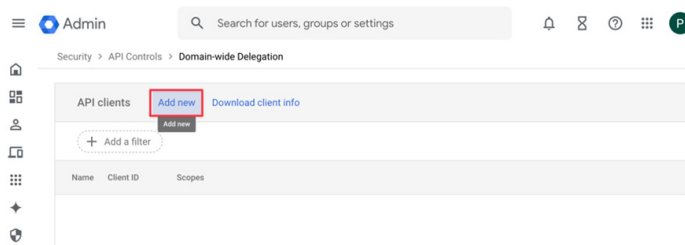


Figure 160. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

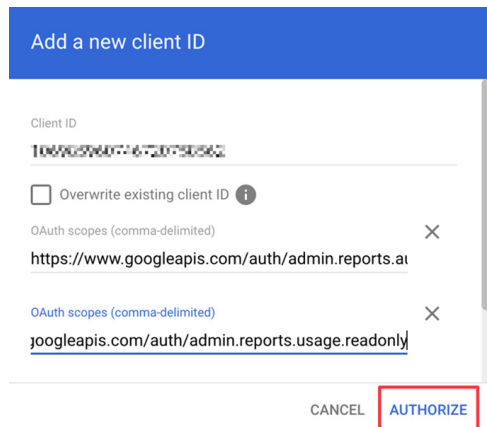


Figure 161. Add a new client ID

Configure the Google Workspace—Groups Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

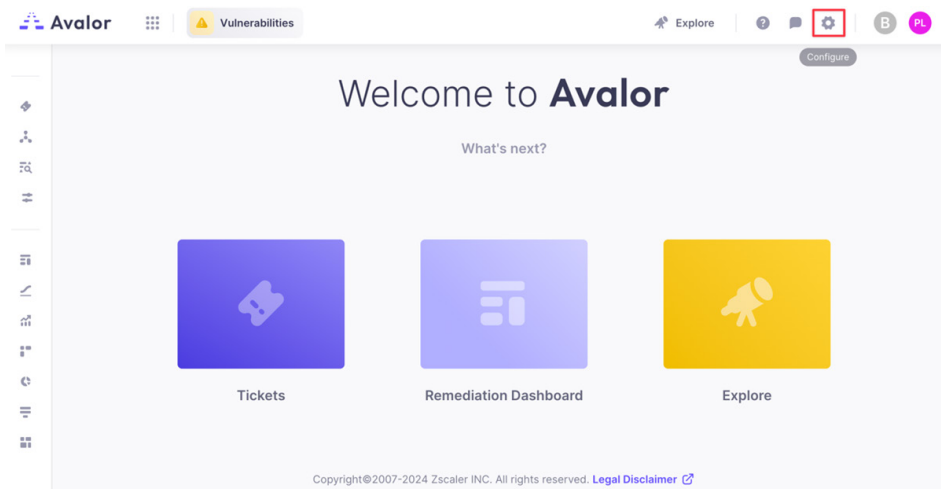


Figure 162. Configure

3. Click Create, then search for Google Workspace—Groups Activity.

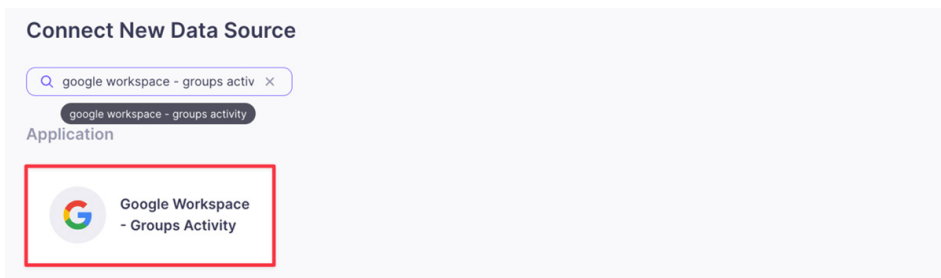


Figure 163. Google Workspace—Groups Activity

4. Click the Google Workspace—Groups Activity application.
5. On the Google Workspace—Groups Activity page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

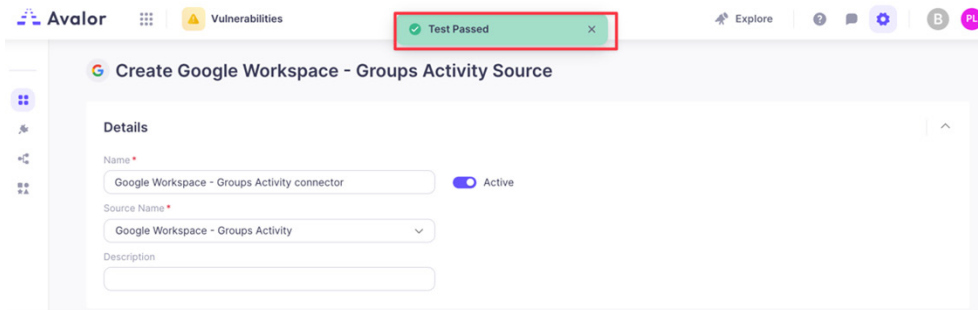


Figure 164. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the 'Create Google Workspace - Groups Activity Source'.

- Details:** Name is 'Google Workspace - Groups Activity connector' (highlighted), Source Name is 'Google Workspace - Groups Activity', and the 'Active' toggle is on.
- Retrieval:** Credentials JSON is '{ "type": "service_account", "project_id": "avalor-projec..." }' (highlighted), and Email is '...' (highlighted).
- Scheduling:** Full Refresh Frequency is 'None', Incremental Refresh Frequency is 'Custom', and the 'Every' field is set to '10' minutes.
- Remediation Detection Settings:** Under 'Aging criteria', the checkbox 'Age immediately if Finding was not seen, while Asset was seen in the latest data refresh' is checked (highlighted). Under 'Fallback', the checkbox 'Age immediately if Finding was not seen for' is checked with a value of '1' day(s) (highlighted).
- Advanced Settings:** Under 'Suppression Rules', the checkbox 'Prevent NULL from overriding existing values' is checked (highlighted).

 At the bottom right, there are buttons for 'Cancel', 'Test', and 'Save' (highlighted).

Figure 165. Create Google Workspace—Groups Activity Source

Google Workspace—Keep Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace keep activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

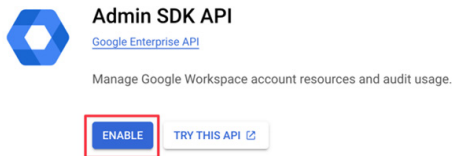


Figure 166. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

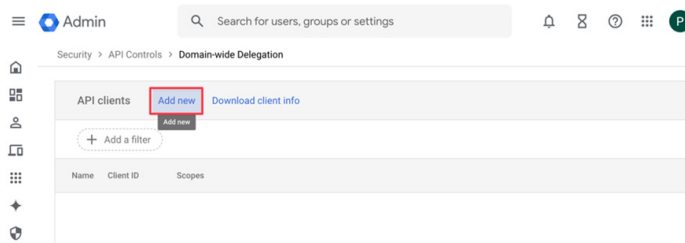


Figure 167. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

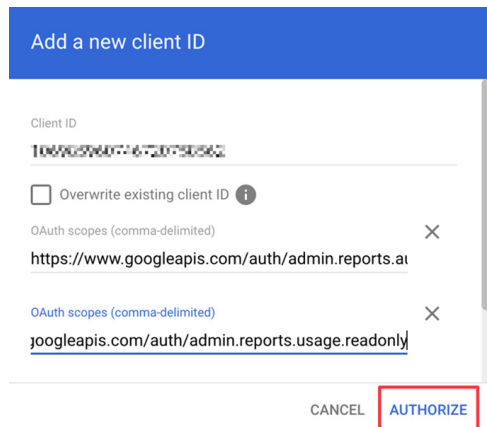


Figure 168. Add a new client ID

Configure the Google Workspace—Keep Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

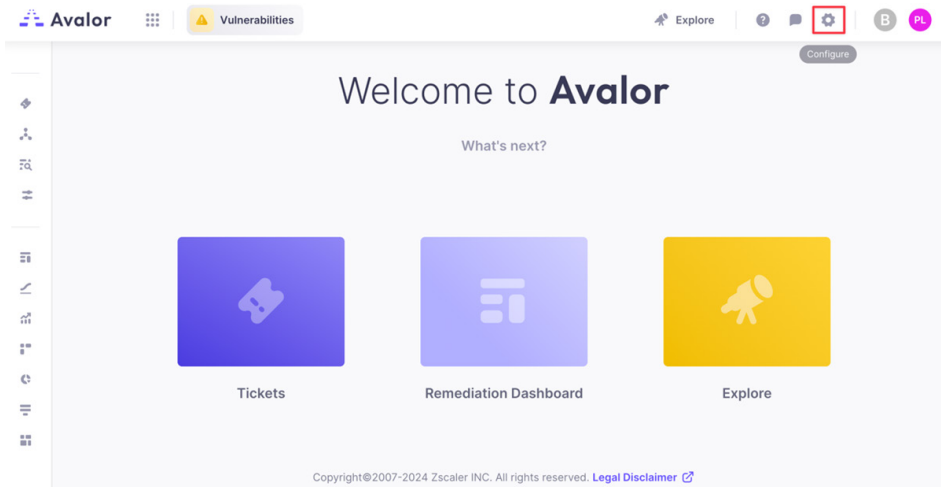


Figure 169. Configure

3. Click **Create**, then search for Google Workspace—Keep Activity.

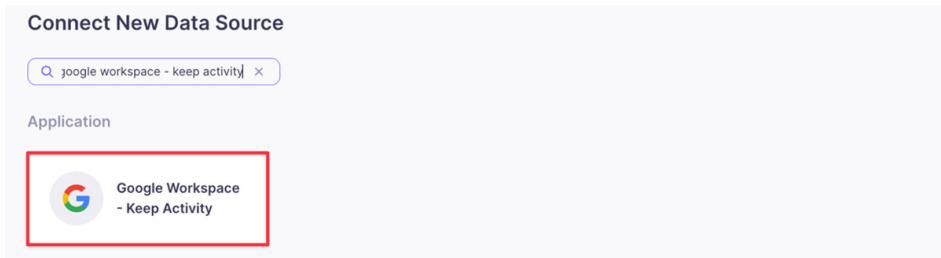


Figure 170. Google Workspace—Keep Activity

4. Click the **Google Workspace—Keep Activity** application.
5. On the **Google Workspace—Keep Activity** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

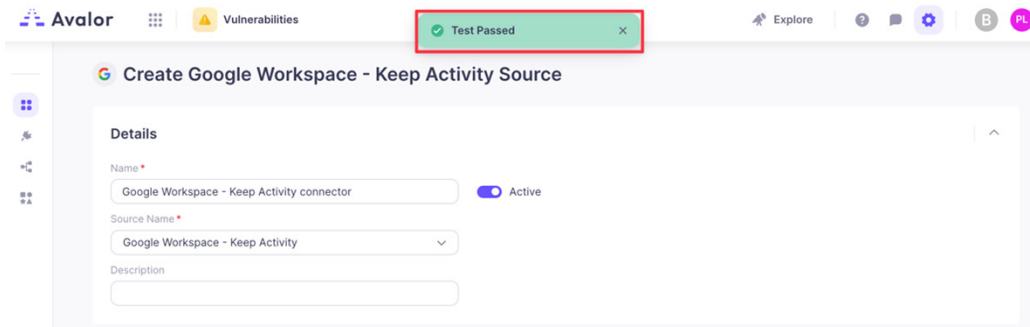


Figure 171. Test Passed

7. Click **Save**.

This screenshot shows the same configuration page as Figure 171, but with several fields highlighted in red boxes to indicate where user input is required. The highlighted areas include:

- The "Name" field and the "Active" toggle switch.
- The "Source Name" dropdown menu.
- The "Credentials JSON" field, containing a JSON object: `{ "type": "service_account", "project_id": "avalor-projec..." }`.
- The "Email" field, containing a service account email address.
- The "Scheduling" section, which includes:
 - "Full Refresh Frequency" set to "None".
 - "Incremental Refresh Frequency" set to "Custom".
 - "Every" set to "10" and "Minutes" selected.
- The "Remediation Detection Settings" section, which includes:
 - A checkbox for "Age immediately if Finding was not seen, while Asset was seen in the latest data refresh".
 - A checkbox for "Age immediately if Finding was not seen for" followed by a "day(s)" input field.
- The "Advanced Settings" section, specifically the "Suppression Rules" area, which includes:
 - A rule configuration with "Select Field", "Contains", and "Type Value" options.
 - A checkbox for "Prevent NULL from overriding existing values".

 At the bottom right of the form, the "Save" button is highlighted in a red box.

Figure 172. Create Google Workspace—Keep Activity Source

Google Workspace—SAML Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace SAML activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

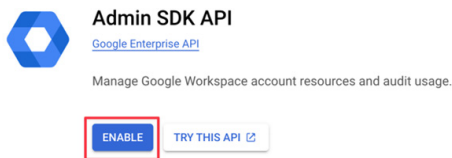


Figure 173. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

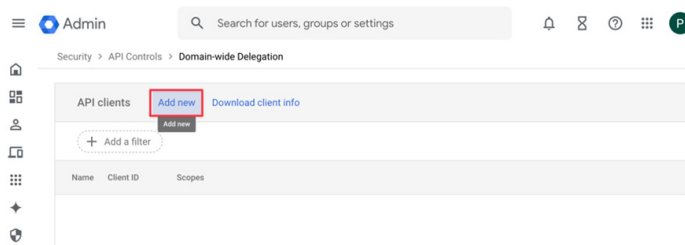


Figure 174. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

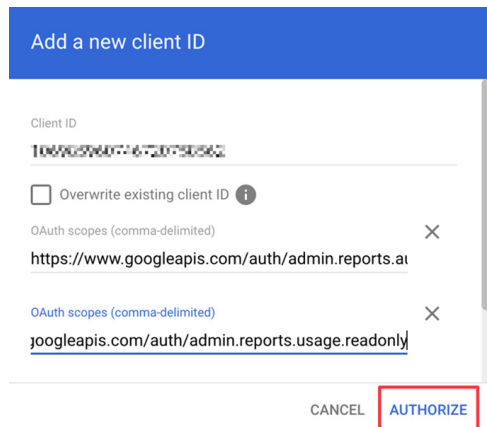


Figure 175. Add a new client ID

Configure the Google Workspace—SAML Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

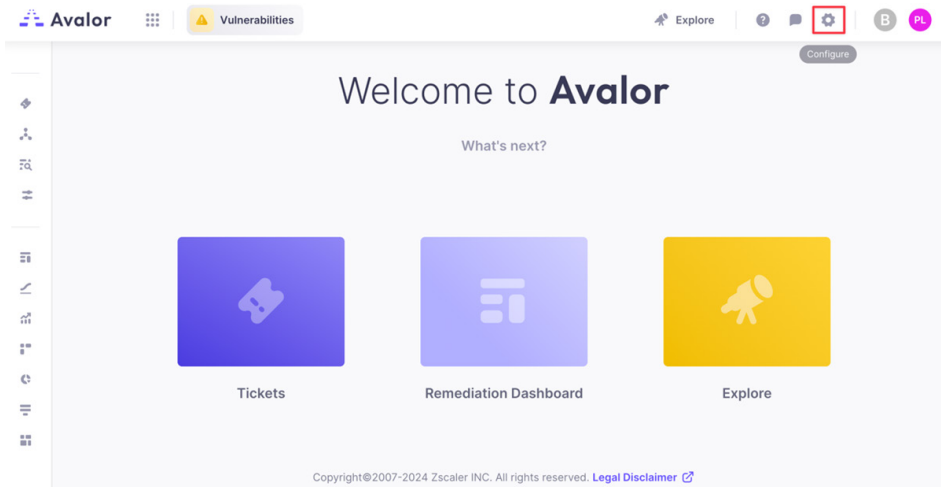


Figure 176. Configure

3. Click **Create**, then search for Google Workspace—SAML Activity.

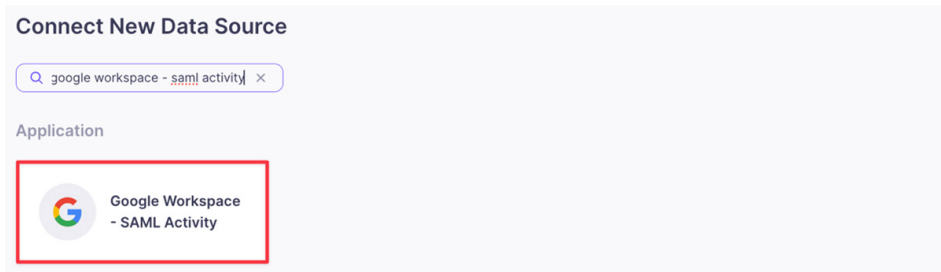


Figure 177. Google Workspace—SAML Activity

4. Click the **Google Workspace—SAML Activity** application.
5. On the **Google Workspace—SAML Activity** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

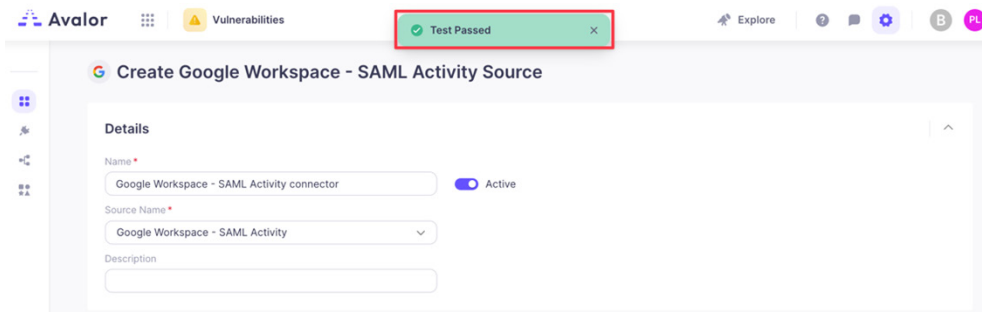


Figure 178. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the 'Create Google Workspace - SAML Activity Source'.
 - **Details:** Name is 'Google Workspace - SAML Activity connector', Source Name is 'Google Workspace - SAML Activity', and the 'Active' toggle is on.
 - **Retrieval:** Credentials JSON is '{ "type": "service_account", "project_id": "avalor-projec..." }' and Email is '101...@101...'.
 - **Scheduling:** Full Refresh Frequency is 'None', Incremental Refresh Frequency is 'Custom', and it's set to 'Every 10 Minutes'.
 - **Remediation Detection Settings:** Includes 'Aging criteria' and 'Fallback' sections with checkboxes for immediate aging.
 - **Advanced Settings:** Includes 'Suppression Rules' with a rule 'Select Field' containing 'Type Value' and a checked option 'Prevent NULL from overriding existing values'.
 At the bottom right, there are 'Cancel', 'Test', and 'Save' buttons, with 'Save' highlighted by a red box.

Figure 179. Create Google Workspaces—SAML Activity Source

Google Workspace—Tokens Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace tokens activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

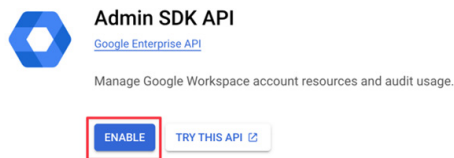


Figure 180. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

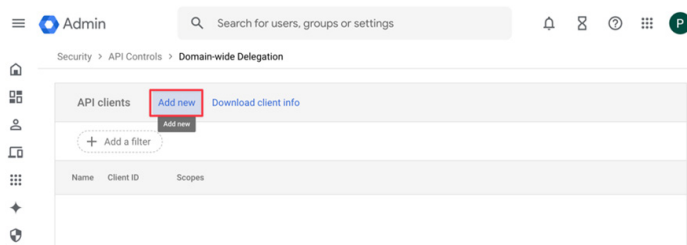


Figure 181. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

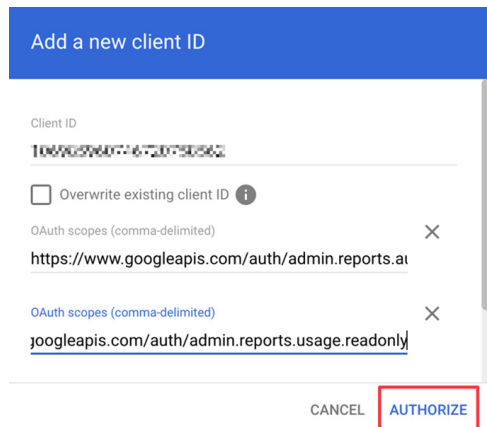


Figure 182. Add a new client ID

Configure the Google Workspace—Tokens Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

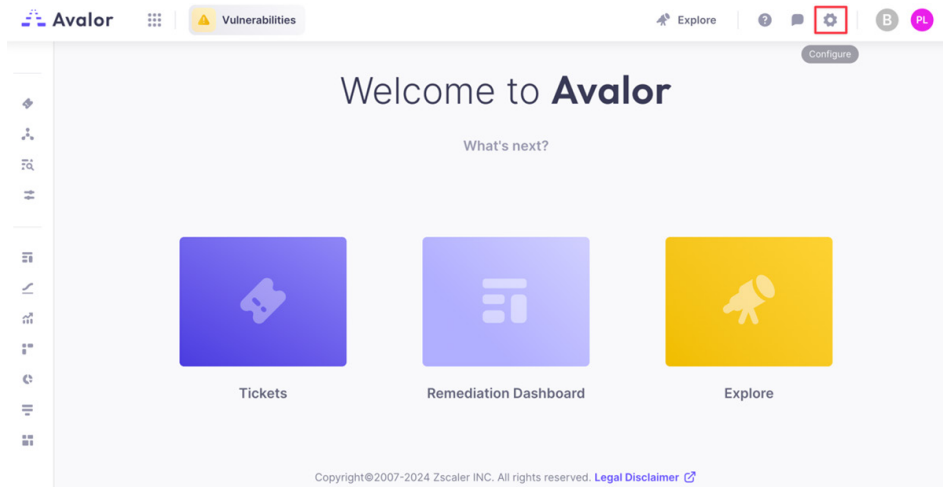


Figure 183. Configure

3. Click **Create**, then search for Google Workspace—Tokens Activity.

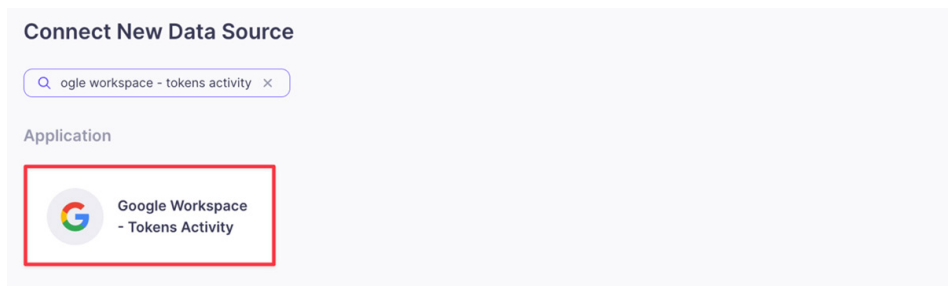


Figure 184. Google Workspace—Tokens Activity

4. Click the **Google Workspace—Tokens Activity** application.
5. On the **Google Workspace—Tokens Activity** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

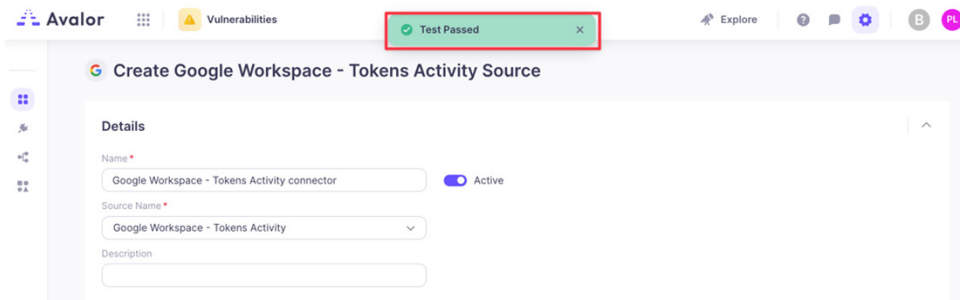


Figure 185. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the 'Create Google Workspace - Tokens Activity Source'. Several fields are highlighted with red boxes:

- Details:** The 'Name' field (Google Workspace - Tokens Activity connector) and the 'Active' toggle.
- Retrieval:** The 'Credentials JSON' field containing a service account key and the 'Email' field.
- Scheduling:** The 'Full Refresh Frequency' (set to None), 'Incremental Refresh Frequency' (set to Custom), and the 'Every' interval (set to 10 minutes).
- Remediation Detection Settings:** The 'Aging criteria' checkbox and the 'Fallback' checkbox.
- Advanced Settings:** The 'Suppression Rules' section, including the 'Select Field' dropdown, the 'Contains' operator, and the 'Prevent NULL from overriding existing values' checkbox.

 At the bottom right, the 'Save' button is highlighted in red.

Figure 186. Create Google Workspace—Tokens Activity Source

Google Workspace—User Accounts Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace user accounts activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

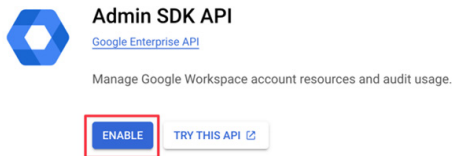


Figure 187. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

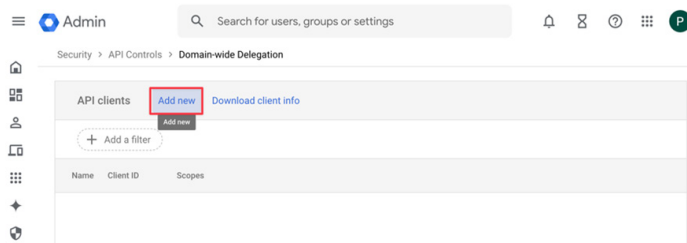


Figure 188. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

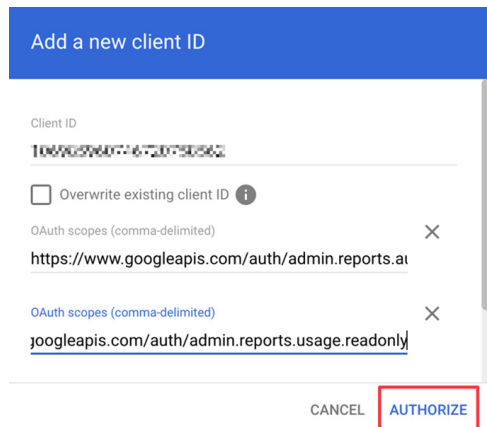


Figure 189. Add a new client ID

Configure the Google Workspace—User Accounts Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

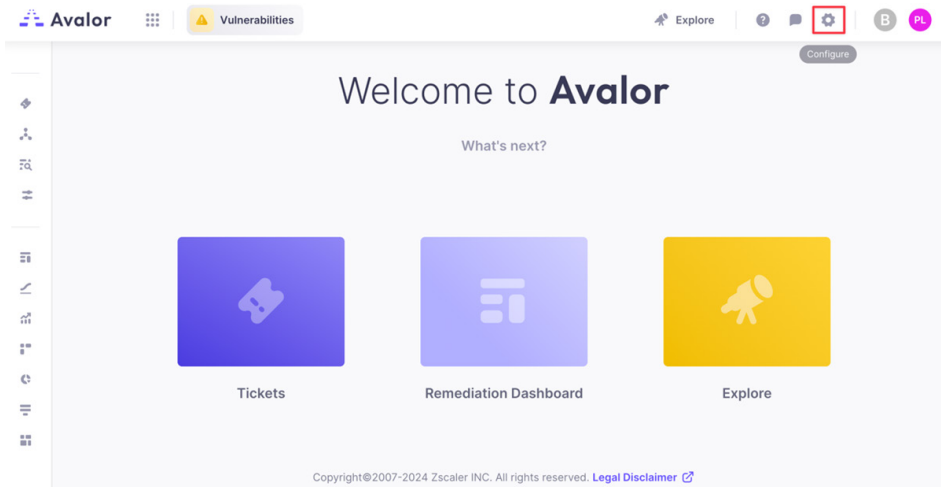


Figure 190. Configure

3. Click **Create**, then search for Google Workspace - User Accounts Activity.

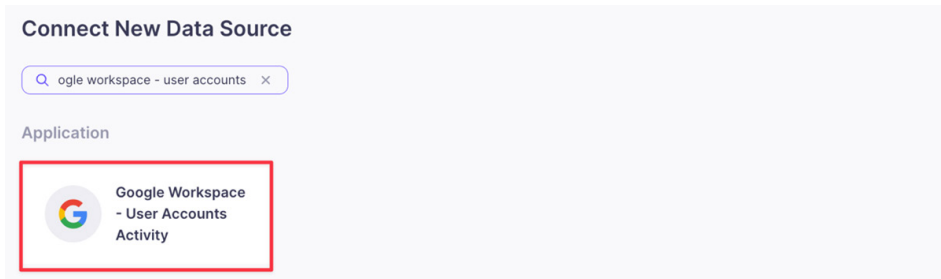


Figure 191. Google Workspace—User Accounts Activity

4. Click the **Google Workspace—User Accounts Activity** application.
5. On the **Google Workspace—User Accounts Activity** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

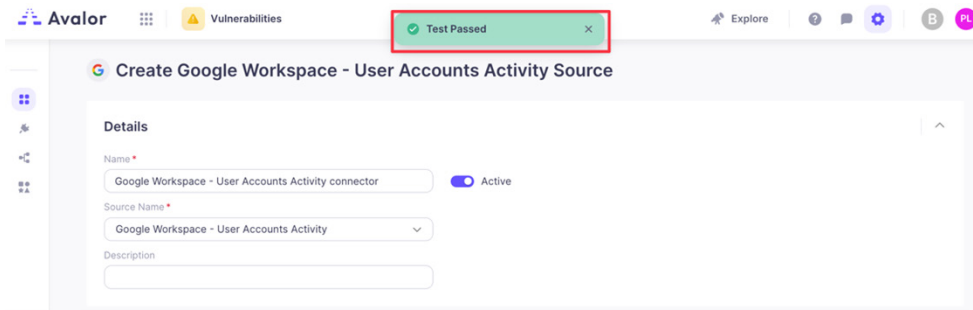


Figure 192. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the 'Create Google Workspace - User Accounts Activity Source'. The 'Details' section is at the top, followed by 'Retrieval' (with JSON credentials and email highlighted), 'Scheduling' (with refresh frequencies and interval highlighted), 'Remediation Detection Settings' (with aging criteria and fallback rules highlighted), and 'Advanced Settings' (with suppression rules highlighted). At the bottom right, the 'Save' button is highlighted.

Figure 193. Create Google Workspace—User Accounts Activity Source

Google Workspace—Enterprise Groups Activity Data Source

This data source tracks mobile device usage within the Google Workspace domain, including information about device types, operating systems, and user activities on mobile devices from the Google Admin SDK API.

The following sections describe how to configure a Google Workspace enterprise group activity data source.

Configure the OAuth Scope

To enable the Admin SDK API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for `Admin SDK API`, then click **Admin SDK API** and **Enable**.

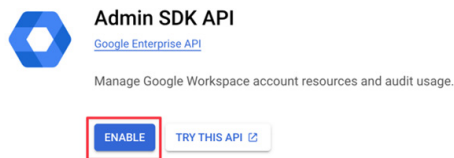


Figure 194. Admin SDK API

3. Go to **Security > Access and data control > API Controls > Manage Domain-wide Delegation**.
4. Click **Add new**.

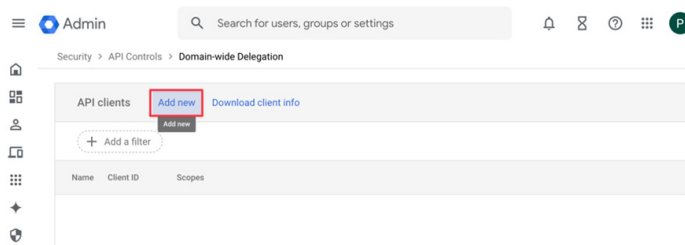


Figure 195. Manage Domain-wide Delegation

5. If absent, enter the Client ID from your downloaded JSON file, and enter both:
 - `https://www.googleapis.com/auth/admin.reports.audit.readonly`
 - `https://www.googleapis.com/auth/admin.reports.usage.readonly`
6. Click **Authorize**.

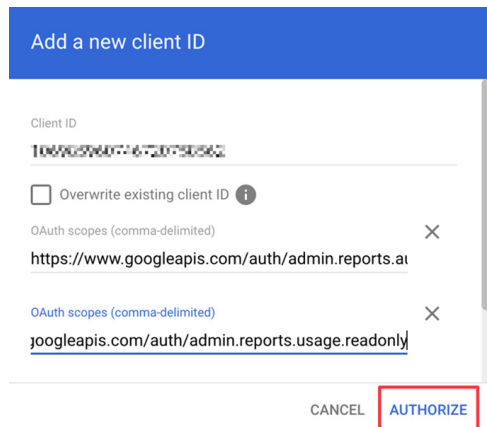


Figure 196. Add a new client ID

Configure the Google Workspace—Enterprise Groups Activity Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

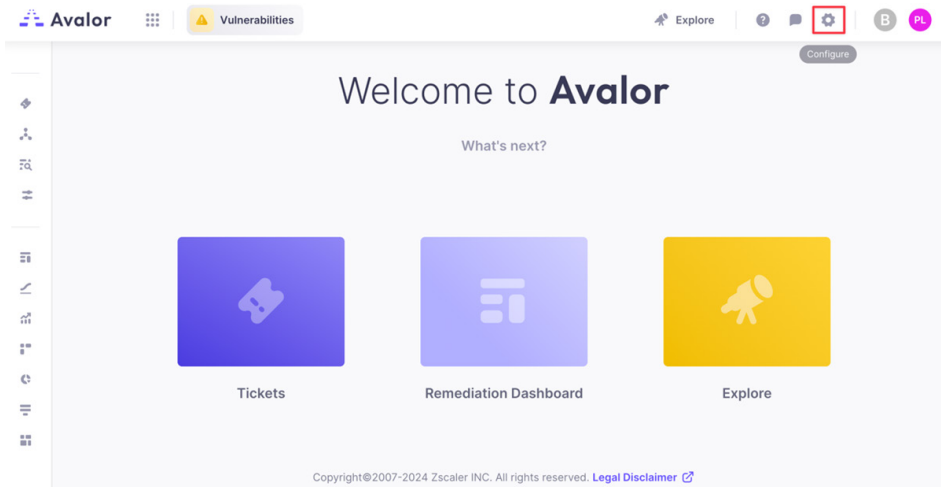


Figure 197. Configure

3. Click **Create**, then search for Google Workspace—Enterprise Groups Activity.

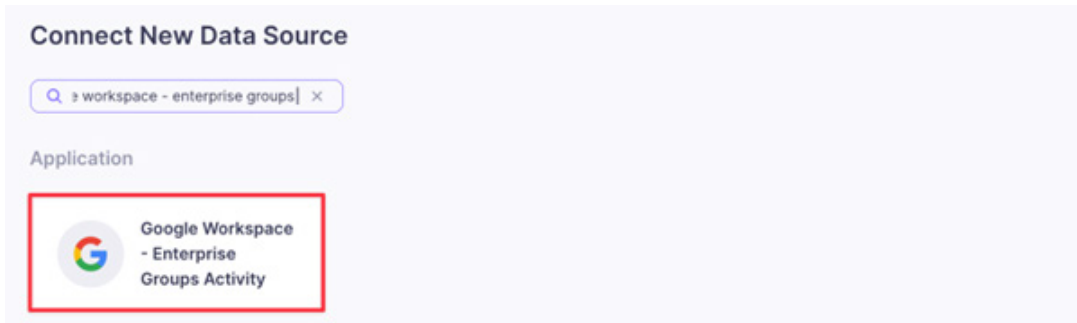


Figure 198. Google Workspace—Enterprise Groups Activity

4. Click the **Google Workspace—Enterprise Groups Activity** application.
5. On the **Google Workspace—Enterprise Groups Activity** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Credentials JSON:** Copy the contents of the JSON file you downloaded earlier.
 - d. **Email:** Enter the email address of the account used to create the Service Account.
 - e. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).

6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

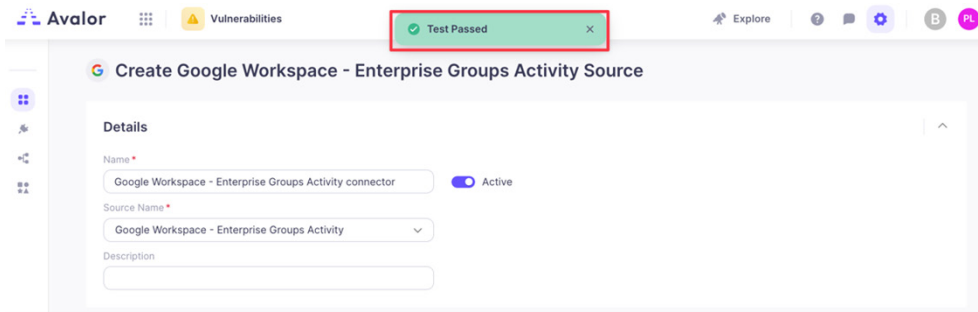


Figure 199. Test Passed

7. Click **Save**.

 This screenshot shows the full configuration page for the "Create Google Workspace - Enterprise Groups Activity Source". Several fields are highlighted with red rectangles:

- Details:** The "Name" field and the "Active" toggle switch.
- Retrieval:** The "Credentials JSON" field containing a JSON snippet and the "Email" field.
- Scheduling:** The "Full Refresh Frequency" dropdown (set to "None"), the "Incremental Refresh Frequency" dropdown (set to "Custom"), and the "Every" field (set to "10 Minutes").
- Remediation Detection Settings:** The "Aging criteria" checkbox and the "Fallback" checkbox.
- Advanced Settings:** The "Suppression Rules" section, which includes a rule configuration area and a checked checkbox for "Prevent NULL from overriding existing values".

 At the bottom right of the page, the "Save" button is highlighted with a red rectangle.

Figure 200. Create Google Workspaces—Enterprise Groups Activity Source

Google Sheets

This connector ingests data from a Google Sheet to simplify bulk data import. When importing data, the first row is treated as headings for any other data in the sheet, and you should create the sheet with this in mind.

In the following example, Asset, Crown Jewel, IP Address, and Description are used as headings for the rest of the data.

	A	B	C	D
1	Asset	Crown Jewel	IP Address	Description
2	test1.domain.com	TRUE	192.168.0.1	First Server
3	test2.domain.com	FALSE	192.168.0.2	Second Server
4	test3.domain.com	TRUE	192.168.0.3	Third Server
5				
6				

Figure 201. Google Sheet example

This connector does not use a GCP Service Account.

Configure the OAuth Client

This data source ingests data from a Google Sheets using the Google Sheets v4 API.

To enable the Google Sheets API:

1. Sign in to your Google Cloud Console, then select **APIs & Services > Library**.
2. Search for Google Sheets API, then click **Google Sheets API** and **Enable**.

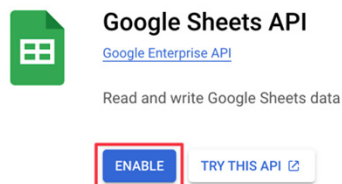


Figure 202. Google Sheets API

3. Go to **APIs & Services > Credentials**.
4. Click **+ Create Credentials**, then **OAuth client ID**.

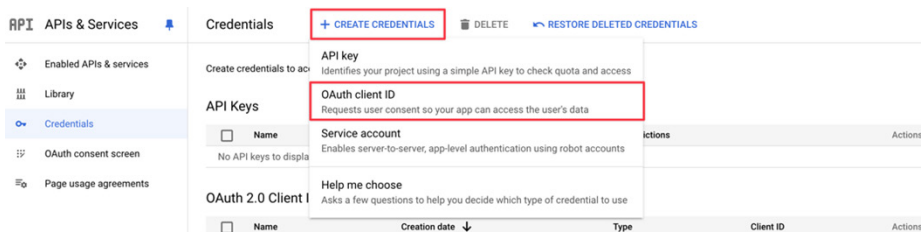


Figure 203. OAuth client ID

5. On the **Create OAuth Client ID** page, complete the following:
 - a. **Application type**: Select **Web application** from the drop-down menu.
 - b. **Name**: Enter a name (i.e., avalor-demo-client)
 - c. **Authorized redirect URIs**: Enter `https://developers.google.com/oauthplayground`.

6. Click **Create**.

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
avalor-demo-client

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins **?**

For use with requests from a browser

+ ADD URI

Authorized redirect URIs **?**

For use with requests from a web server

URIs 1 *
<https://developers.google.com/oauthplayground>

+ ADD URI

Note: It may take 5 minutes to a few hours for settings to take effect

CREATE

CANCEL

Figure 204. Create OAuth client ID

7. Copy the **Client ID** and **Client secret**.

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Client ID	284097262002- [REDACTED]
Client secret	[REDACTED]
Creation date	November 15, 2024 at 11:47:55 AM GMT+11
Status	Enabled

DOWNLOAD JSON

OK

Figure 205. OAuth client created

Generate a Refresh Token

1. Go to <https://developers.google.com/oauthplayground/>.
2. Click the **Cog Wheel** icon and complete the following:
 - a. Select the checkbox for **Use your own OAuth credentials**.
 - b. Input your **OAuth Client ID**.
 - c. Input your **OAuth Client Secret**.

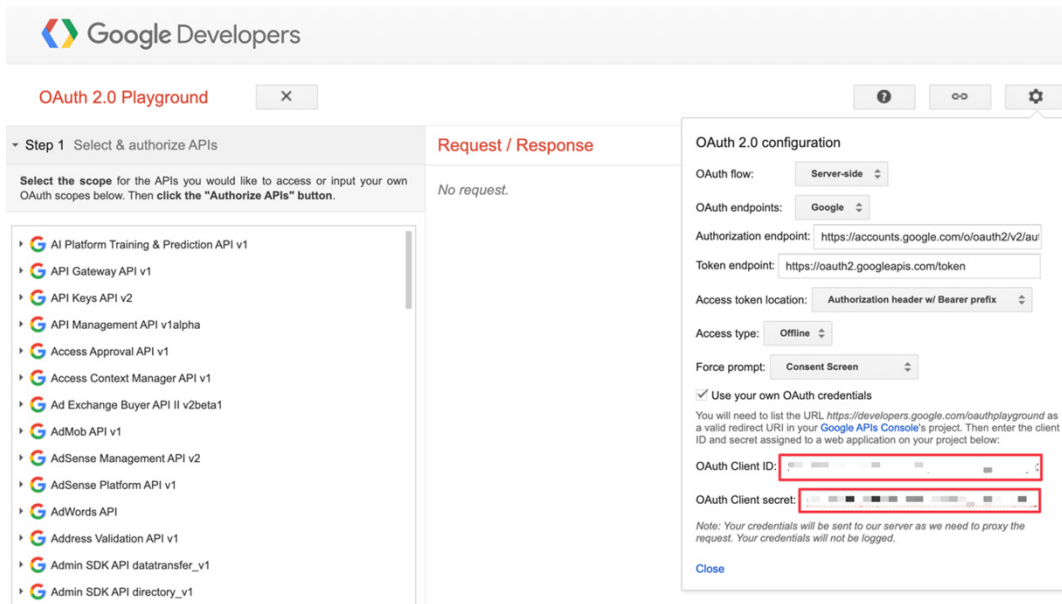


Figure 206. OAuth 2.0 Playground

3. Under **Select & authorize APIs**, search for Google Sheets API v4 and check the <https://www.googleapis.com/auth/spreadsheets.readonly> scope.
4. Click **Authorize APIs**.

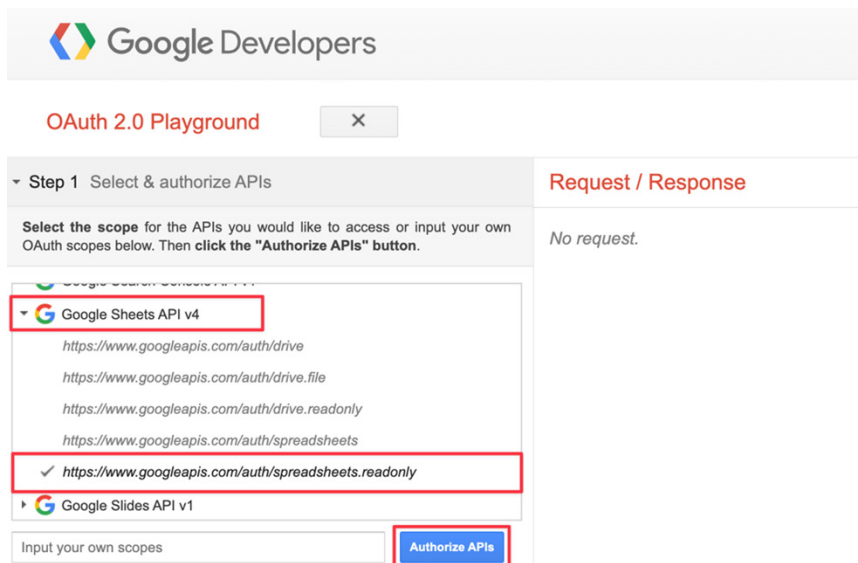


Figure 207. Authorize APIs

5. Authorize the API using your user account.

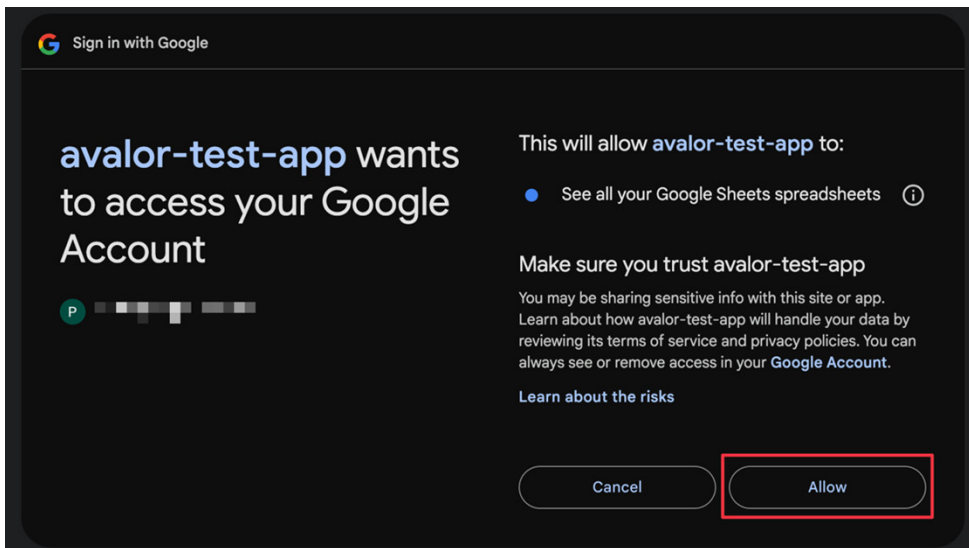


Figure 208. Allow avalor-test-app

6. Click **Exchange authorization code for tokens** to generate your refresh token. Take note of your refresh token.

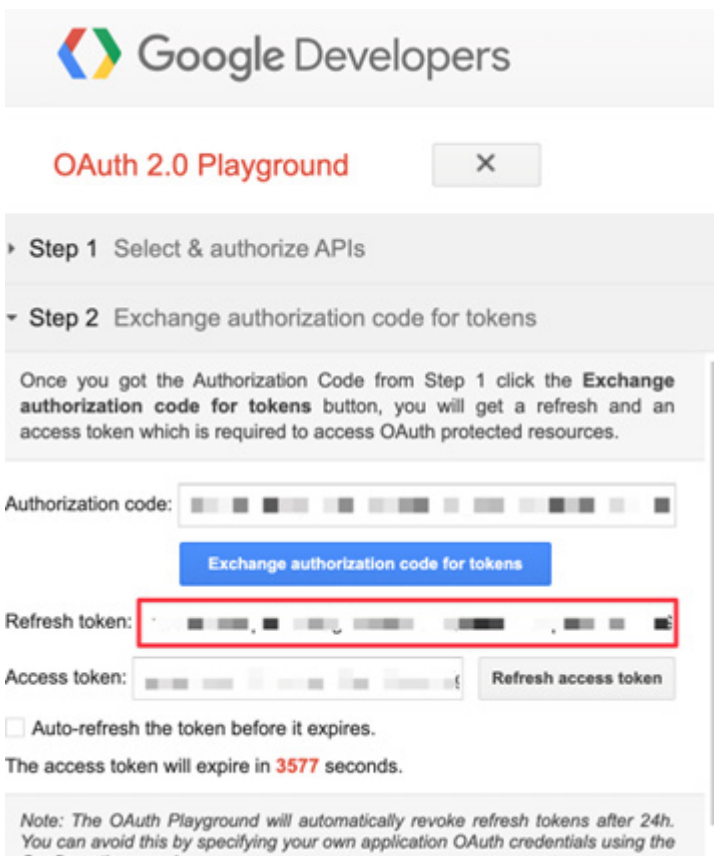


Figure 209. Exchange authorization code

Configure the Google Sheets Source

1. Log in to the Avalor UVM Platform.
2. Click **Configure**.

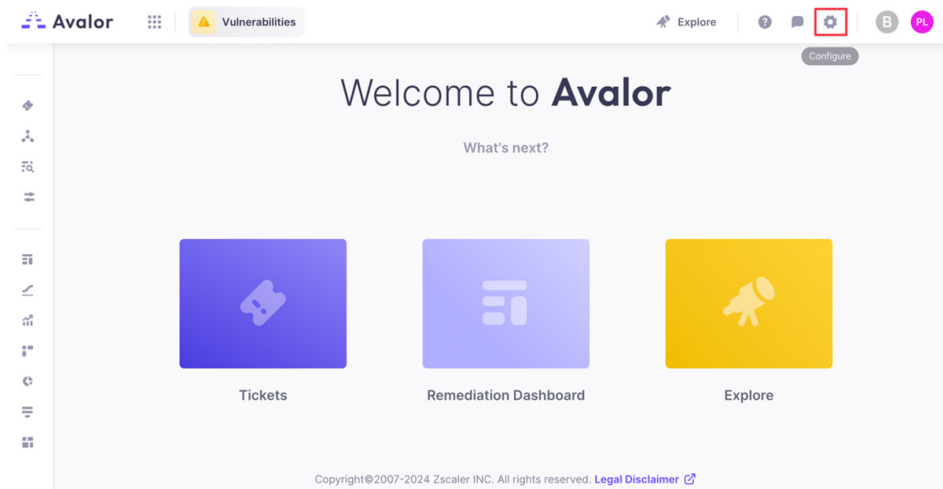


Figure 210. Configure

3. Click **Create**, then search for Google Sheets.

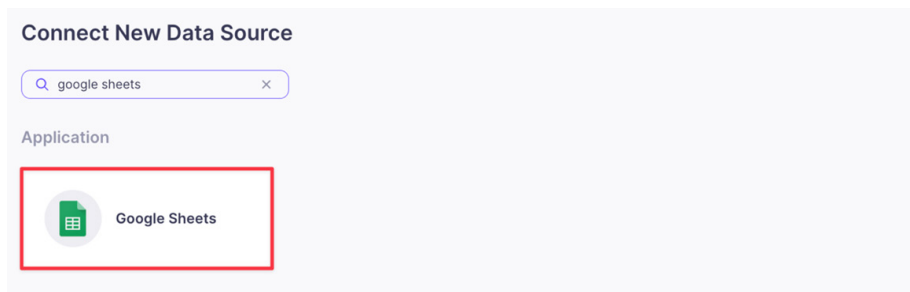


Figure 211. Google Sheets

4. Click the **Google Sheets** application.
5. On the **Sheets** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Spreadsheet Id:** The ID of the spreadsheet you want to access. You can find this value in the URL of the spreadsheet in between /d/ and /edit, as shown in the following figure:

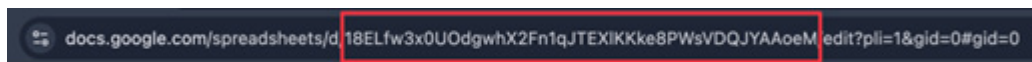


Figure 212. Spreadsheet Id

- d. **Sheets:** The name of the sheet.
- e. **Client Id:** The Client ID of the OAuth client you created earlier.
- f. **Client Secret:** The Client Secret of the OAuth client you created earlier.
- g. **Refresh Token:** The Refresh token created via the OAuth 2.0 Playground.
- h. **Scheduling:** Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.

- i. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - j. **Advanced Settings > Suppression Rules:** Define rules and conditions to remove specific data before it enters the Avalor system. To learn more, refer to the [Avalor documentation](#).
6. Click **Test**. If the credentials are entered correctly, the system responds with Test Passed.

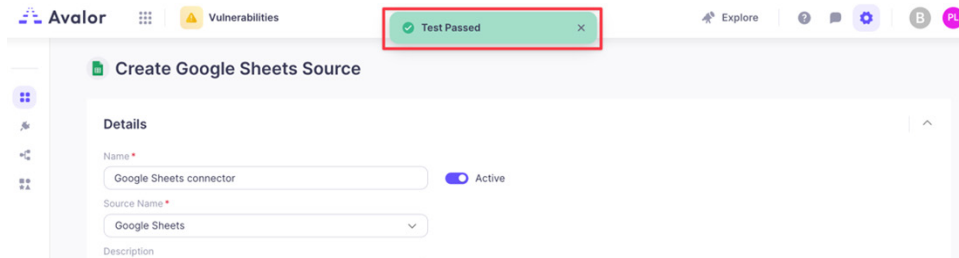


Figure 213. Test Passed

7. Click **Save**.

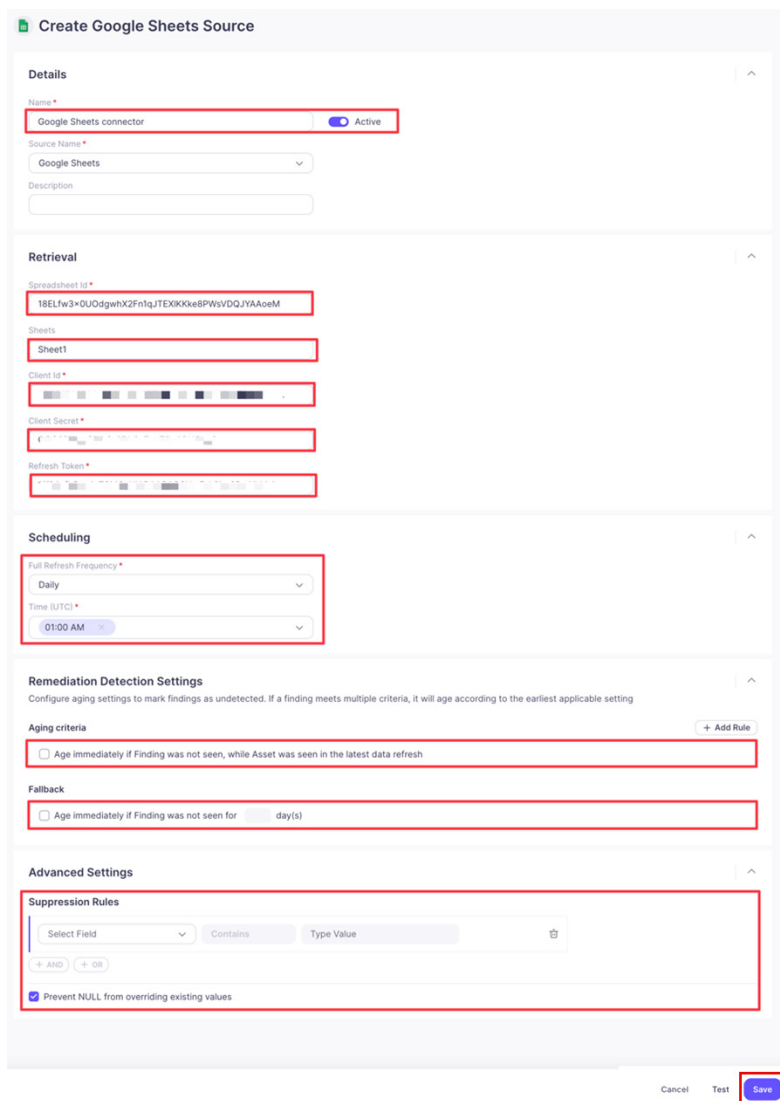


Figure 214. Create Google Sheets Source

Review and Adjust Data Model Mapping

(Optional) Avalor UVM automatically maps ingested data to the default Data Model, so analysis can begin immediately. However, many data sources also provide additional data points that might provide additional context to risk prioritization.

The following example shows how to leverage the Crown Jewel Data Model Entity based on a Google Compute Engine Virtual Machine label so that you can use the field as a Risk Factor when calculating risk for an Asset.

Create a Crown Jewel Label for a Google Cloud Compute Engine VM

The following steps describe how to create a crown jewel label for a Google Cloud compute engine VM.

1. Sign in to your Google Cloud Console.
2. Select **Compute Engine** > **VM instances**.

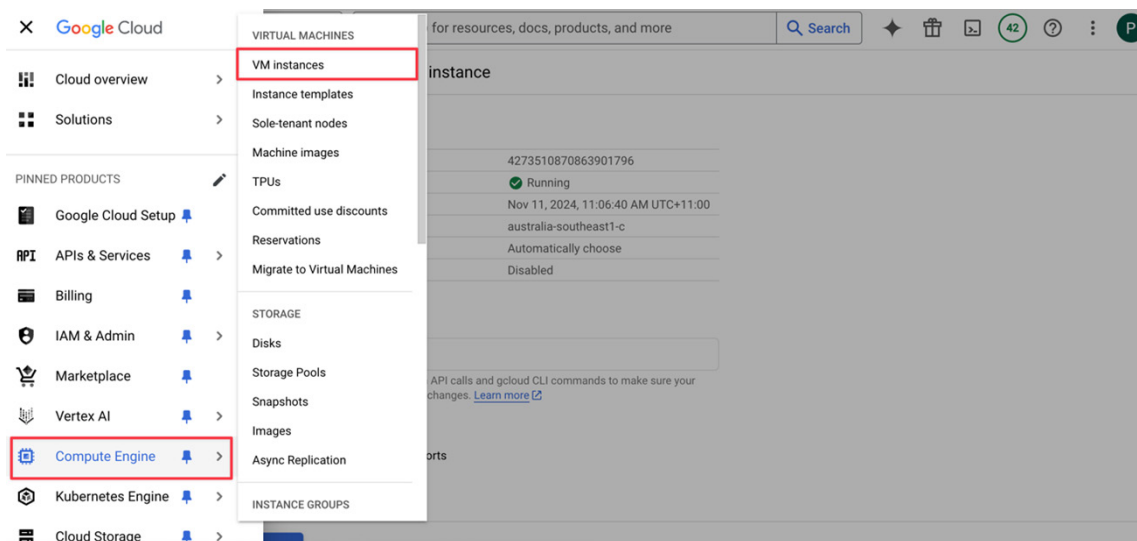


Figure 215. VM instances

3. Click the instance to which you want to add the label.

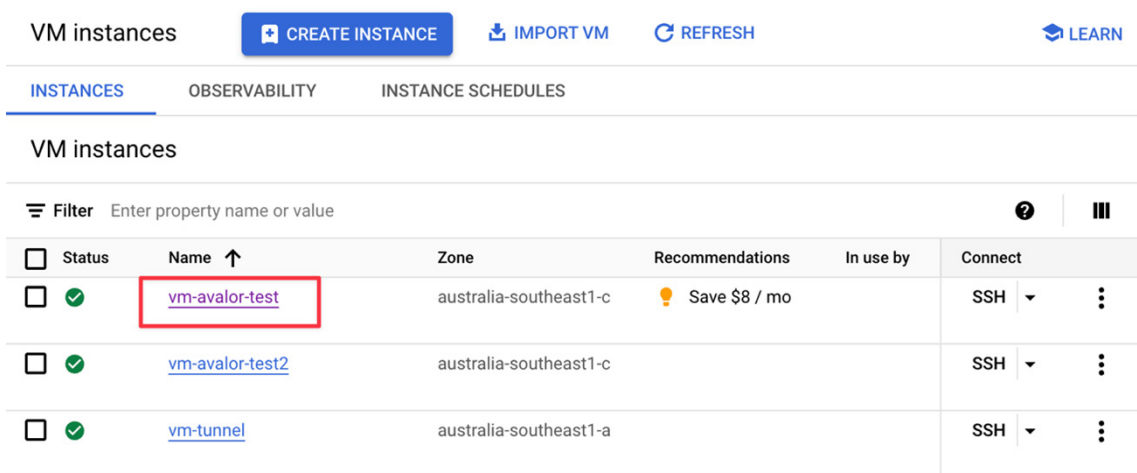


Figure 216. VM Instances

4. Click **Edit**.

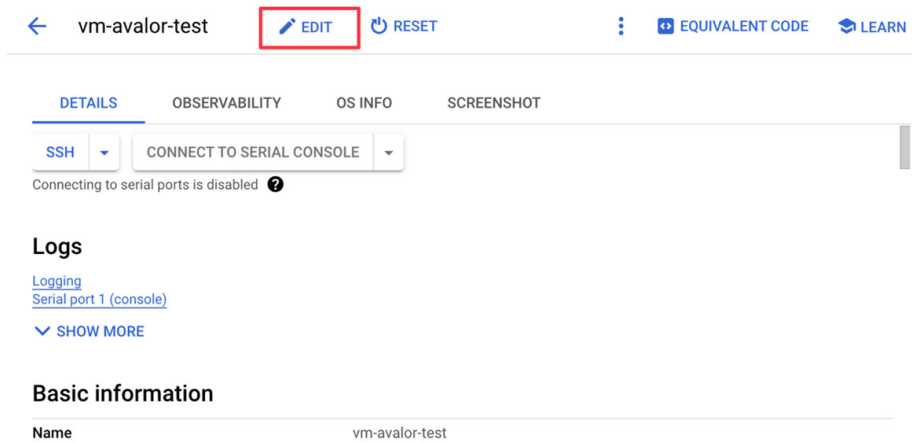


Figure 217. Edit

5. Click **Manage Labels**.

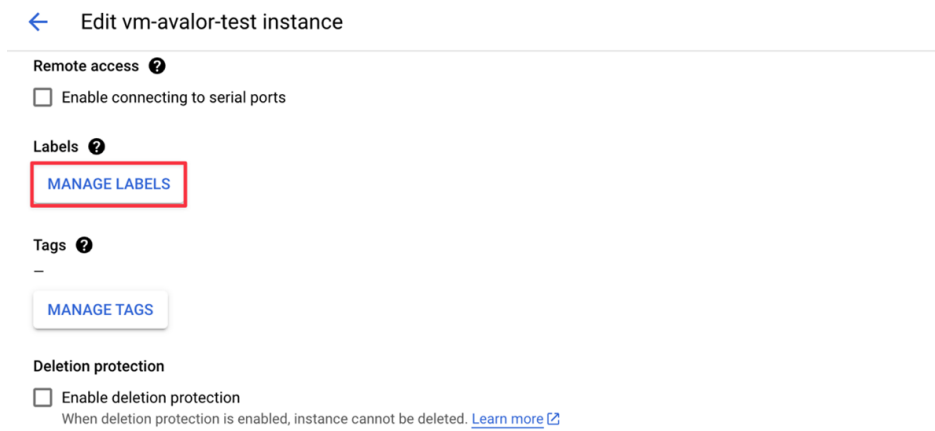


Figure 218. Manage labels

6. Click **Add label** and enter:
 - a. **Key 1:** classification
 - b. **Value 1:** crownjewel

7. Click **Save**.

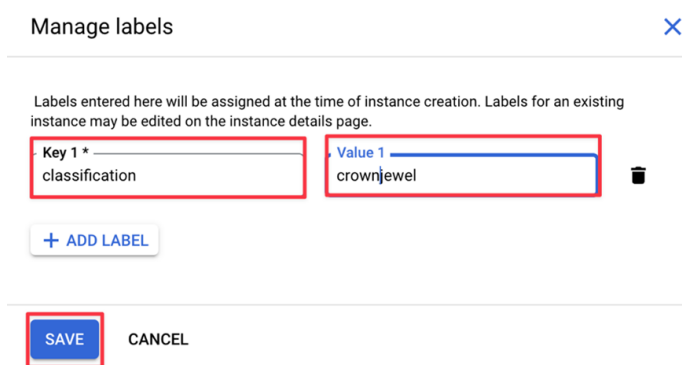


Figure 219. Manage labels

Map the Google Platforms Assets Data Source

1. Select **Configure** and the newly created **Google Cloud Platform Assets** connector.
2. Click **Map Data**.

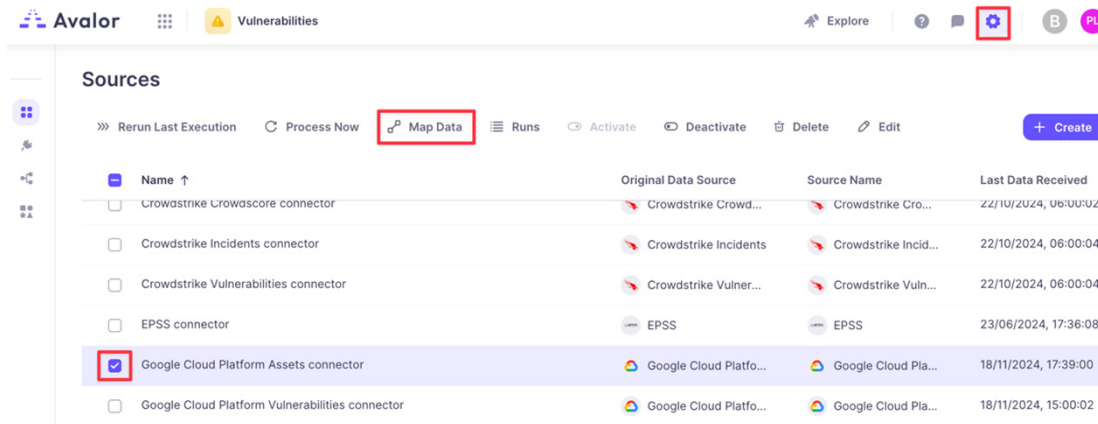


Figure 220. Configure Map Data

3. In the **Map connector** window:
 - a. Create a new **Asset Key** with the internal DNS hostname:
 - i. On the right side, under **Asset**, drag **Key** to the **Create New Connection** element.
 - ii. On the left side, click **Editor**.

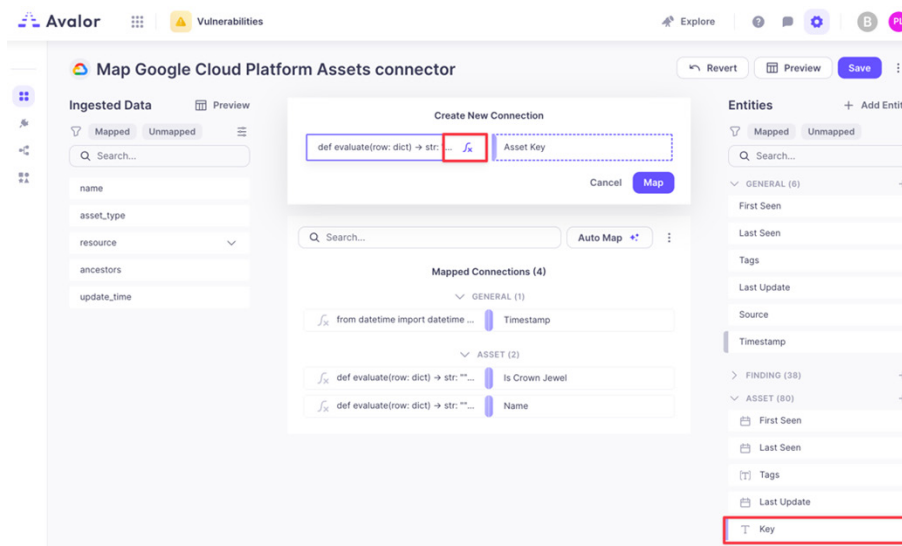


Figure 221. Create Asset Key

iii. Replace the text in the script field with the following:

```
def evaluate(row: dict) -> str:

    asset_type = row.get("asset_type")

    if asset_type == "compute.googleapis.com/Instance":

        data_section = row.get("resource", {}).get("data", {})

        network_interfaces = data_section.get("networkInterfaces", [])

        if isinstance(network_interfaces, list) and network_interfaces:

            first_interface = network_interfaces[0]

            network_ip = first_interface.get("networkIP")

            return network_ip or ""

        else:

            return ""

    else:

        return ""
```

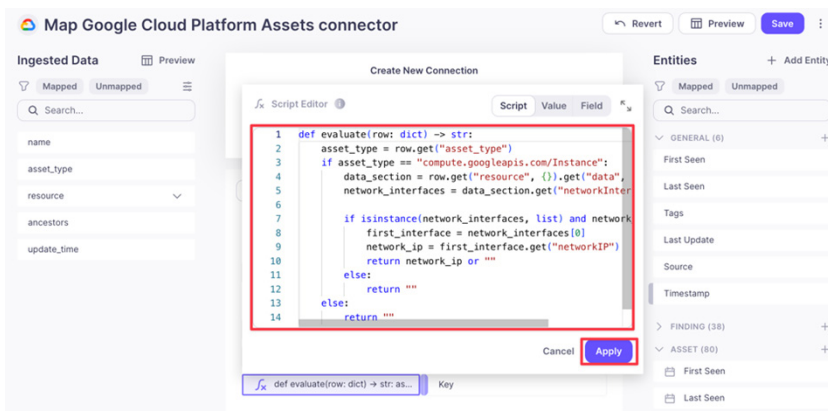


Figure 222. Script field

iv. Click **Apply**.

v. Click **Map**, then the **Key** icon next to the **Asset Key** to set as a key.

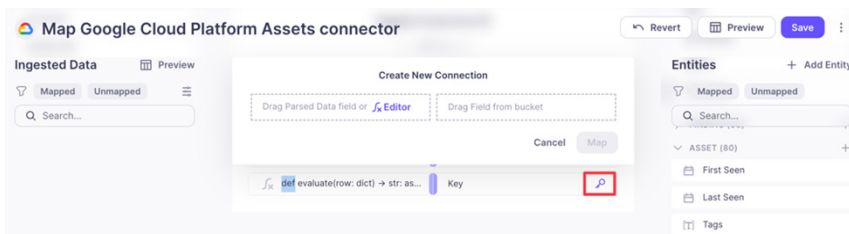


Figure 223. Map Google Cloud Platform Assets connector

- b. Map the **Is Crown Jewel Asset** entity to the **Crown Jewel** label by:
 - i. Under **Asset**, drag **Is Crown Jewel** to the **Create New Connection** element.
 - ii. On the left side, click the **Editor** element.

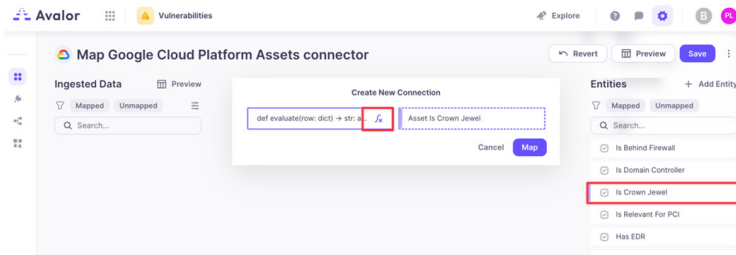


Figure 224. Create New Connection element

- iii. Replace the text in the script field with the following:

```
def evaluate(row: dict) -> str:

    asset_type = row.get("asset_type")

    if asset_type == "compute.googleapis.com/Instance":

        data_section = row.get("resource", {}).get("data", {})

        labels = data_section.get("labels")

        if labels is None:

            return False

        elif labels.get("classification") == "crownjewel":

            return True

        else:

            return False

    else:

        return False
```

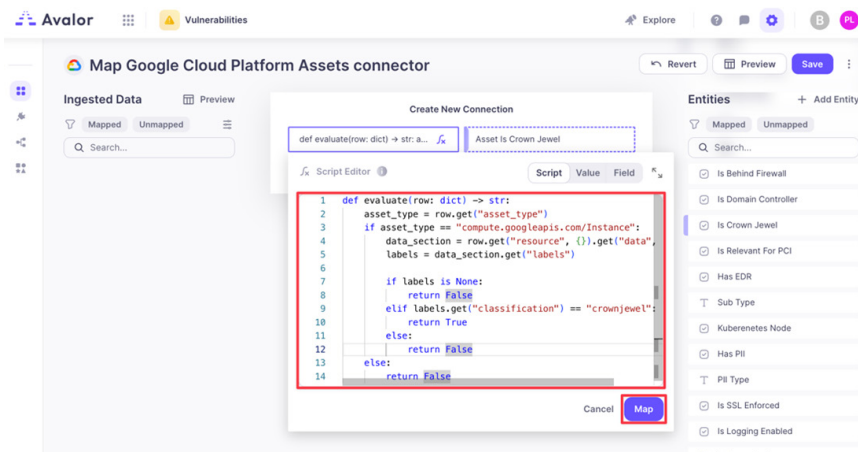


Figure 225. Script field

- iv. Click **Map**.

- c. Map the Name Asset entity to the virtual machine's IP address:
 - i. Under **Asset**, drag **Name** to the **Create New Connection** element.
 - ii. On the left side, click the **Editor** element.

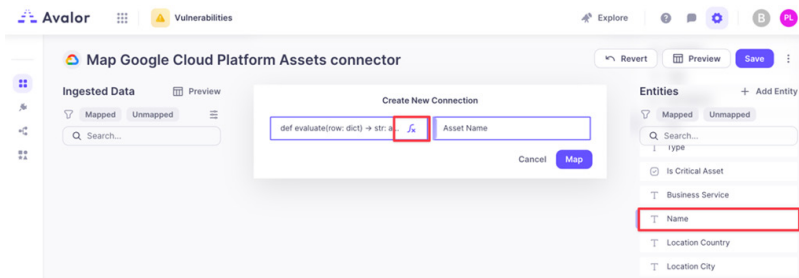


Figure 226. Editor element

- iii. Replace the text in the script field with the following:

```
def evaluate(row: dict) -> str:
    asset_type = row.get("asset_type")
    if asset_type == "compute.googleapis.com/Instance":
        data_section = row.get("resource", {}).get("data", {})
        network_interfaces = data_section.get("networkInterfaces", [])
        if isinstance(network_interfaces, list) and network_interfaces:
            first_interface = network_interfaces[0]
            network_ip = first_interface.get("networkIP")
            return network_ip or ""
        else:
            return ""
    else:
        return ""
```

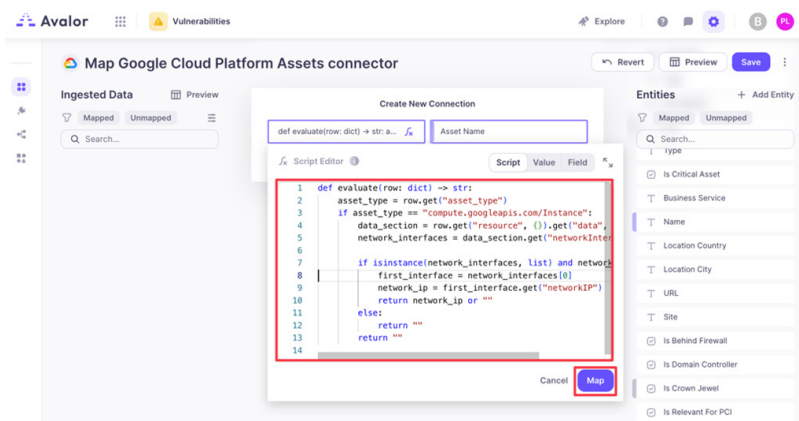


Figure 227. Script field

- iv. Click **Map**.

- d. Click **Preview**, and see if an Asset has been marked as a Crown Jewel based on its label and the assets name based on its IP address.

< Back to Mapping

Preview Google Cloud Platform Assets connector

asset.@type	Asset Is Crown Jewel	asset.first_seen	asset.last_seen	Asset Name
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	10.152.0.6
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	10.152.0.5
type.googleapis.com/io.avalor.prot...	true	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	10.152.0.2
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	
type.googleapis.com/io.avalor.prot...	false	2024-11-18T00:00:00Z	2024-11-18T00:00:00Z	

Figure 228. Asset list

- e. Click **Back to Mapping**, then **Save**.
- f. To apply the mappings to the ingested data, select the **Google Cloud Platform Assets** connector, and click **Process Now**.

Avalor | Vulnerabilities | Explore | ? | ⚙️ | B | PL

Sources

>> Rerun Last Execution | **Process Now** | Map Data | Runs | Activate | Deactivate | Delete | Edit | + Create

Name ↑	Original Data Source	Source Name	Last Data Received
<input type="checkbox"/> Crowdstrike Crowdscore connector	Crowdstrike Crowd...	Crowdstrike Cro...	22/10/2024, 06:00:04
<input type="checkbox"/> Crowdstrike Incidents connector	Crowdstrike Incidents	Crowdstrike Incid...	22/10/2024, 06:00:04
<input type="checkbox"/> Crowdstrike Vulnerabilities connector	Crowdstrike Vulner...	Crowdstrike Vuln...	22/10/2024, 06:00:04
<input type="checkbox"/> EPSS connector	EPSS	EPSS	23/06/2024, 17:36:08
<input checked="" type="checkbox"/> Google Cloud Platform Assets connector	Google Cloud Platfo...	Google Cloud Pla...	18/11/2024, 17:39:00
<input type="checkbox"/> Google Cloud Platform Vulnerabilities connector	Google Cloud Platfo...	Google Cloud Pla...	18/11/2024, 15:00:02

Figure 229. Process Now

Review and Adjust Risk Scoring

When ingested, data has been normalized and mapped to the Data Model and Avalor UVM can evaluate risk.

The following example shows how the Is Crown Jewel field is added as a Risk Factor for risk scoring. A value of True increases the risk calculation (since the asset is a Crown Jewel application).

1. From the **Vulnerabilities** tab in the Avalor dashboard (Remediation Hub):
 - a. Select **Settings > Score** in the left-side navigation.

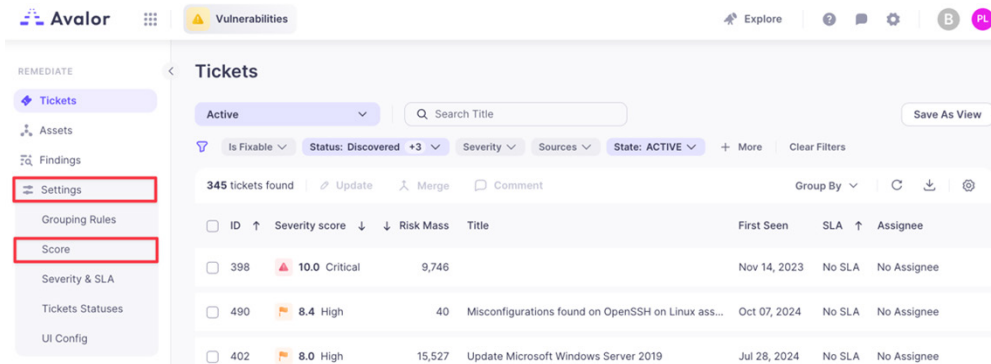


Figure 230. Score

2. Click **Add Factor** in the **Risk & Mitigating Factors** section.



Figure 231. Add Factor

3. If **Crown Jewel** is not already a **Risk Factor**, in the **Add new factor** modal:
 - a. Choose **Risk Factors** for **Factor Type** (Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
 - b. Enter a **Name**.
 - c. Choose **Crown Jewel** for **Field**.
 - d. In the **Boolean** login section, under **True** enter a percentage by which the risk is increased.

4. Click **Apply**, then **Save & Run**.

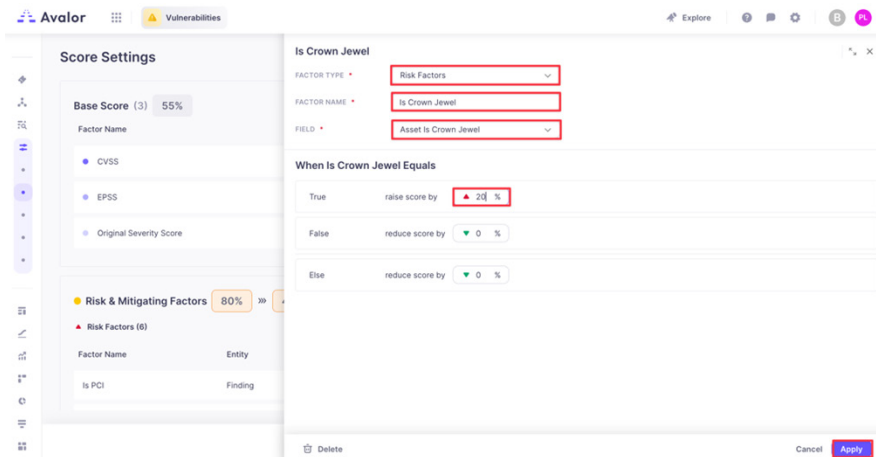


Figure 232. Add new factor

5. In the left-side navigation, select the **Assets** dashboard. From the **Assets** dashboard:

- Set a filter by clicking **More** and adding the **Is Crown Jewel = True** entity.

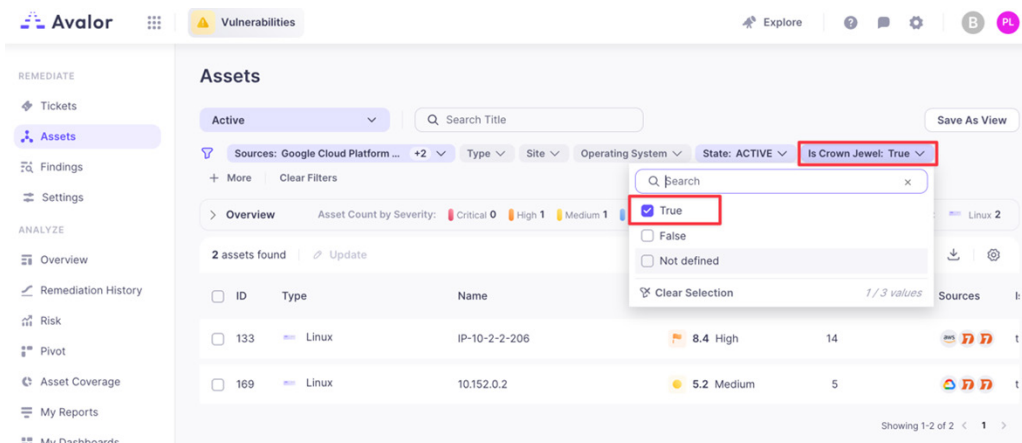


Figure 233. Assets dashboard

- Click one of your **Assets** in the filtered list.
- In the **Asset** modal that appears, click **Findings**.

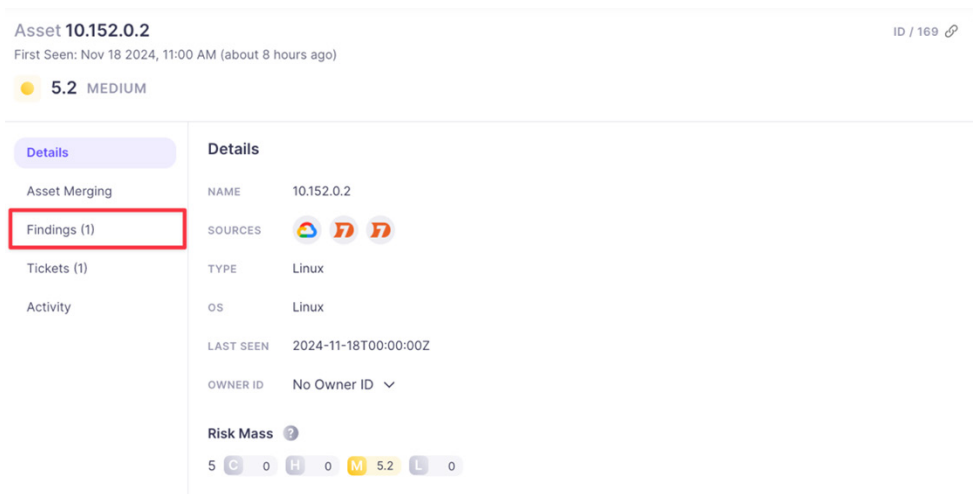


Figure 234. Findings

- d. Click one of the **Findings**.
- e. Review the output (notice the **Score Adjustment** section and whether **Is Crown Jewel** has modified the risk scoring).

Asset **10.152.0.2** ID / 189

First Seen: Nov 18 2024, 11:00 AM (about 8 hours ago)

5.2 MEDIUM

Details

Asset Merging

Findings (1)

Tickets (1)

Activity

Findings

Severity score Original Severity Score State + More Clear Filters

1 found

<input type="checkbox"/>	SEVERITY	ORIGINAL SEVERITY SCORE	STATUS	SOURCE	FIRST SEEN	LAST SEEN																								
<p>FIX</p> <p>Disable any MD5 or 96-bit HMAC algorithms within the SSH configuration</p> <p>AVALOR SCORE WAS DEFINED CONSIDERING:</p> <table><thead><tr><th>Base Score</th><th>Value</th><th>Score Share %</th><th>Score Change</th></tr></thead><tbody><tr><td>Original Severity Score</td><td>4.0</td><td>+80%</td><td>+3.2</td></tr><tr><td>CVSS, EPSS</td><td></td><td>0%</td><td>0</td></tr></tbody></table> <table><thead><tr><th>Score Adjustments</th><th>Value</th><th>Score Share %</th><th>Score Change</th></tr></thead><tbody><tr><td>Crown Jewel</td><td>True</td><td>+20%</td><td>+2.0</td></tr><tr><td>Is PCI, Known Exploited, Public...</td><td></td><td>0%</td><td>0</td></tr></tbody></table> <p>Final Score 5.2 Medium</p>							Base Score	Value	Score Share %	Score Change	Original Severity Score	4.0	+80%	+3.2	CVSS, EPSS		0%	0	Score Adjustments	Value	Score Share %	Score Change	Crown Jewel	True	+20%	+2.0	Is PCI, Known Exploited, Public...		0%	0
Base Score	Value	Score Share %	Score Change																											
Original Severity Score	4.0	+80%	+3.2																											
CVSS, EPSS		0%	0																											
Score Adjustments	Value	Score Share %	Score Change																											
Crown Jewel	True	+20%	+2.0																											
Is PCI, Known Exploited, Public...		0%	0																											

Showing 1-1 of 1 < 1 >

Figure 235. Score Adjustment

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration > Settings > Company Profile**.

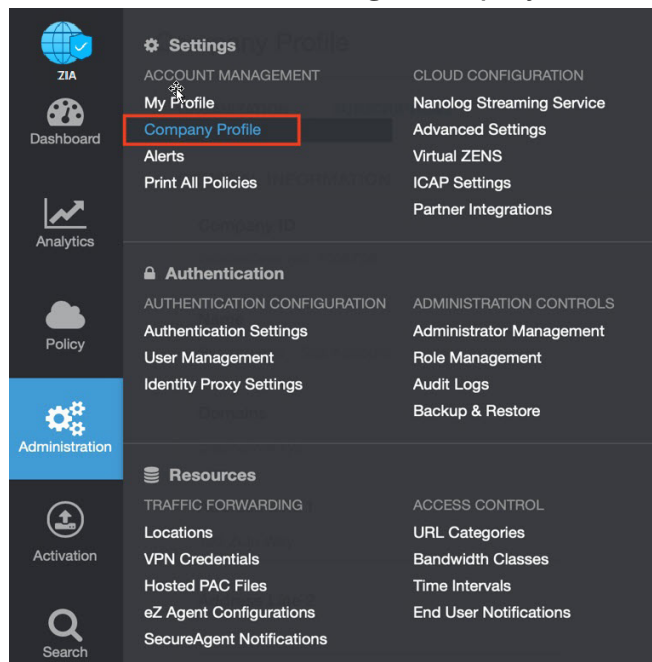


Figure 236. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

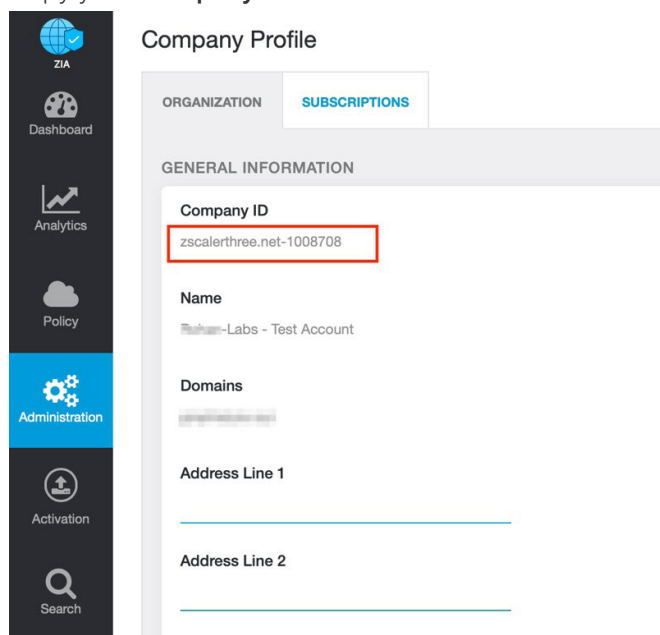


Figure 237. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

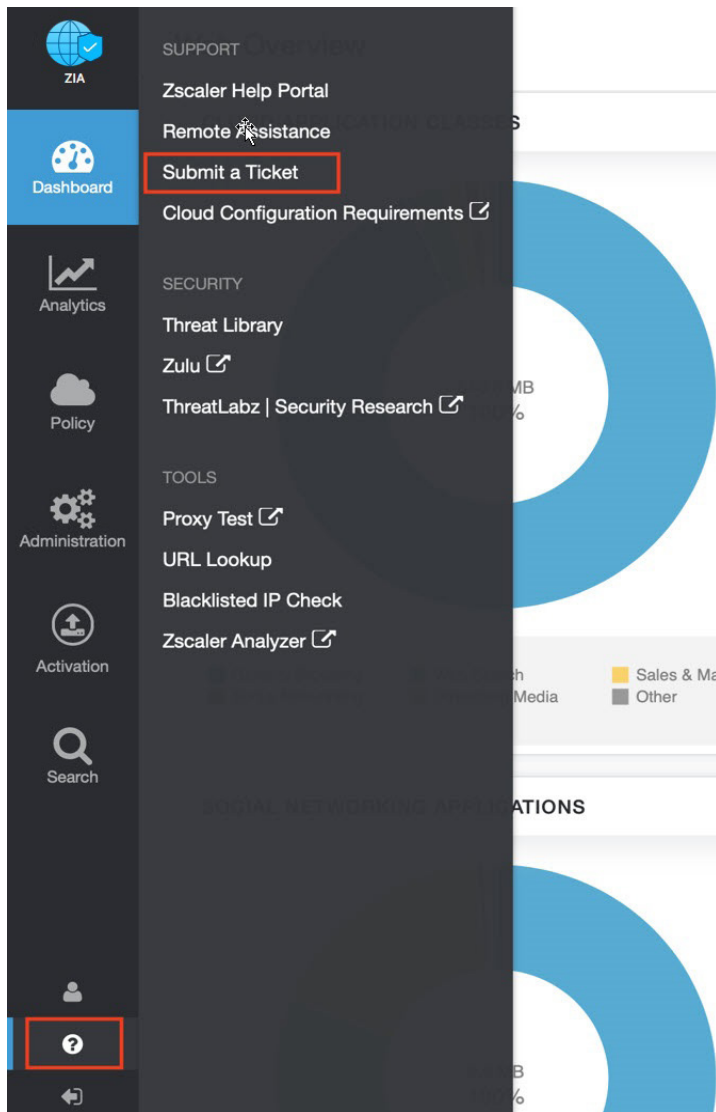


Figure 238. Submit a ticket