



How-To Guide

Integrate Google Workspace with Netsurion Open XDR

Publication Date

December 07, 2023

Abstract

This guide provides instructions to configure and integrate Google Workspace with Netsurion Open XDR to retrieve its event logs via API integration and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purposes and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Google Workspace and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Google Workspace in Netsurion Open XDR.

Table of Contents

1	Overview	4
2	Prerequisites	4
3	Integrating Google Workspace with Netsurion Open XDR.....	4
3.1	Creating Google Workspace Application for API Access	4
3.2	Integrating Google Workspace with Netsurion Open XDR.....	11
4	Data Source Integration (DSI) in Netsurion Open XDR	18
4.1	Alerts.....	18
4.2	Reports.....	18
4.3	Dashboards	19
4.4	Saved Searches	19

1 Overview

Google Workspace (formerly G Suite) is a package of cloud computing, productivity, and collaboration tools, software, and products developed by Google. Google Workspace comprises Gmail, Hangouts, Calendar, Docs, Sheets, Slides, Keep, Forms, Currents, Drive and Sites. Also, it consists of an admin panel and vault for managing users and services.

Netsurion Open XDR manages the logs retrieved from Google Workspace. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Google Workspace.

2 Prerequisites

- Netsurion Open XDR 9.3 or later.
- Must have Admin permission for configuring Google Workspace API.
- PowerShell version 5.0 and above must be installed.
- Upgradation of the existing version v3.1.0 of Google Workspace Integrator (if configured).

Note

Refer to [How-To-Upgrade-Google-Workspace-Integrator](#) guide to upgrade the Google Workspace Integrator from v3.1.0 to 4.0.0. There is no need to follow further instructions in this document when the integrator is being upgraded.

- The Data Source Integrator package

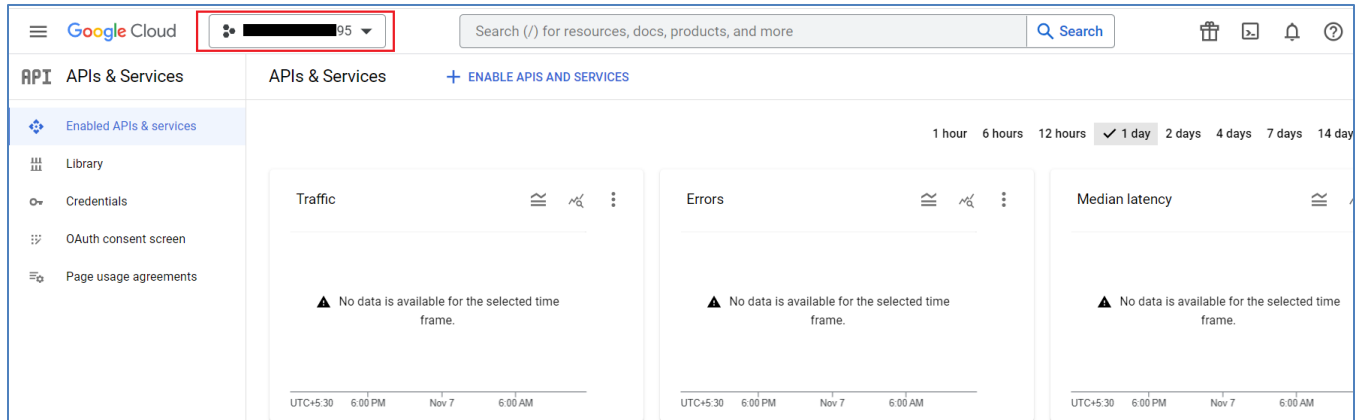
Note

To get the Data Source Integrator package, contact your Netsurion Account Manager.

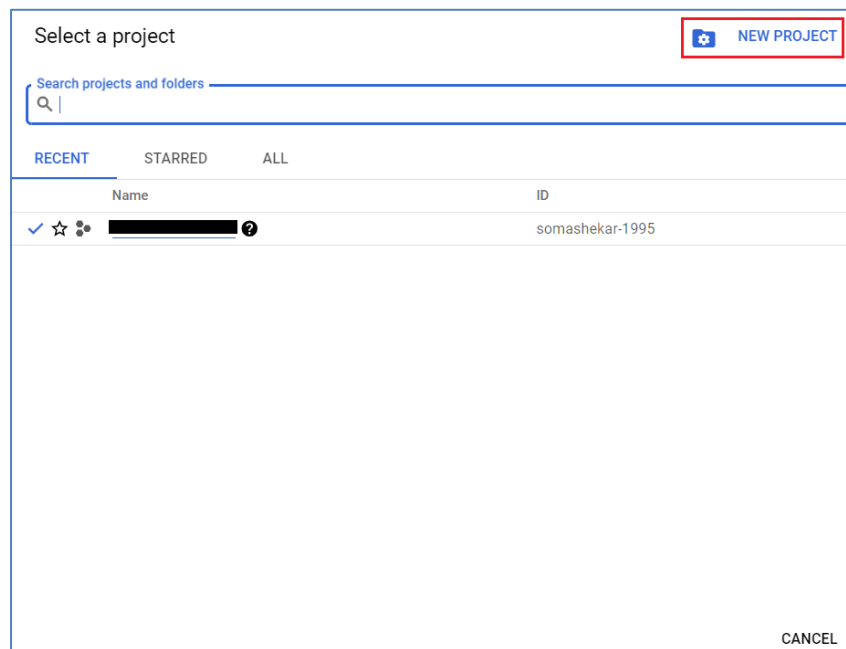
3 Integrating Google Workspace with Netsurion Open XDR

3.1 Creating Google Workspace Application for API Access

1. Login to <https://console.developers.google.com>
2. Click the **Select a Project** drop-down.

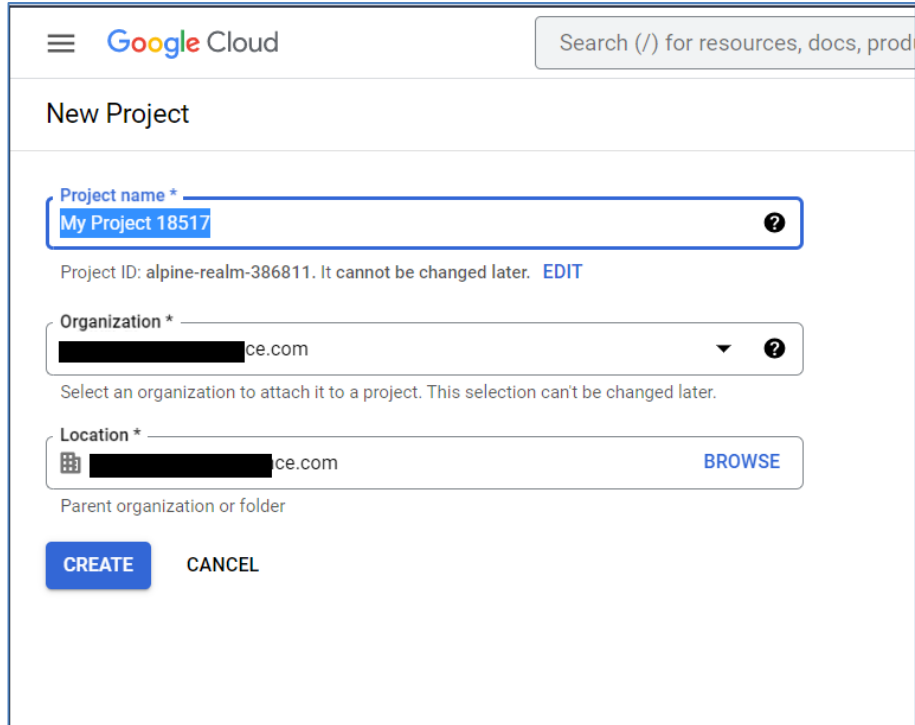


3. On the pop-up screen, click **New Project**.



4. On the **New Project** window, enter the **Project Name** and **Organization Name**.

5. In the **Location** field, click **Browse** and select the parent organization from the appearing window.



Google Cloud

Search (/) for resources, docs, prod

New Project

Project name *

Project ID: alpine-realm-386811. It cannot be changed later. [EDIT](#)

Organization *

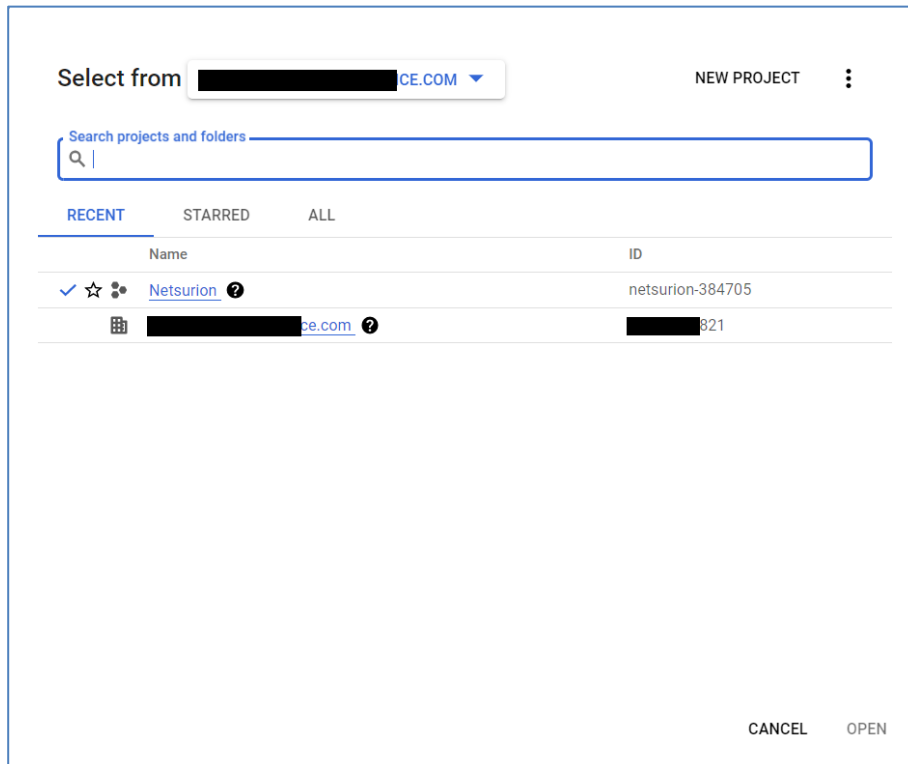
Select an organization to attach it to a project. This selection can't be changed later.

Location * [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)

6. Click **Create** to complete the project creation.
7. Select the newly created project from the drop-down menu.



Select from

NEW PROJECT

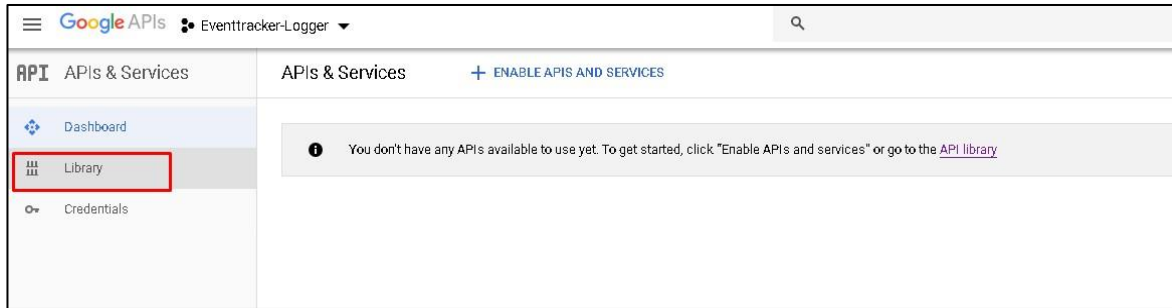
Search projects and folders

RECENT STARRED ALL

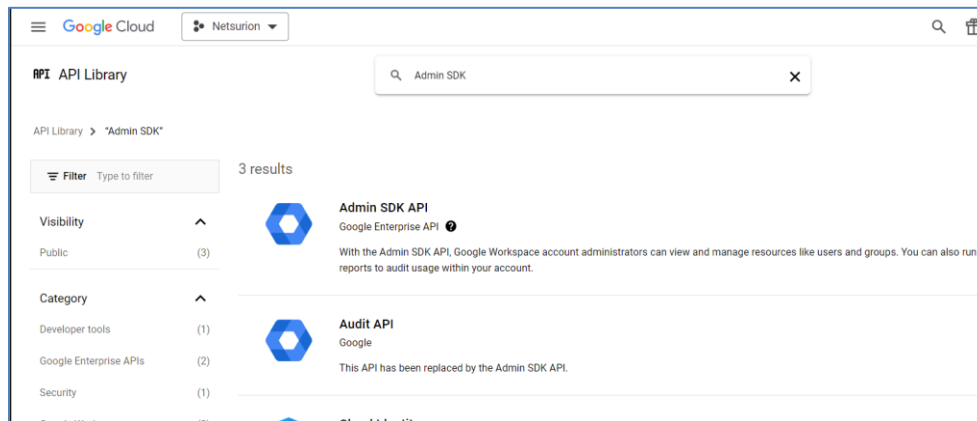
Name	ID
✓ ☆ Netsurion	netsurion-384705
<input type="checkbox"/> ce.com	ce.com 321

[CANCEL](#) [OPEN](#)

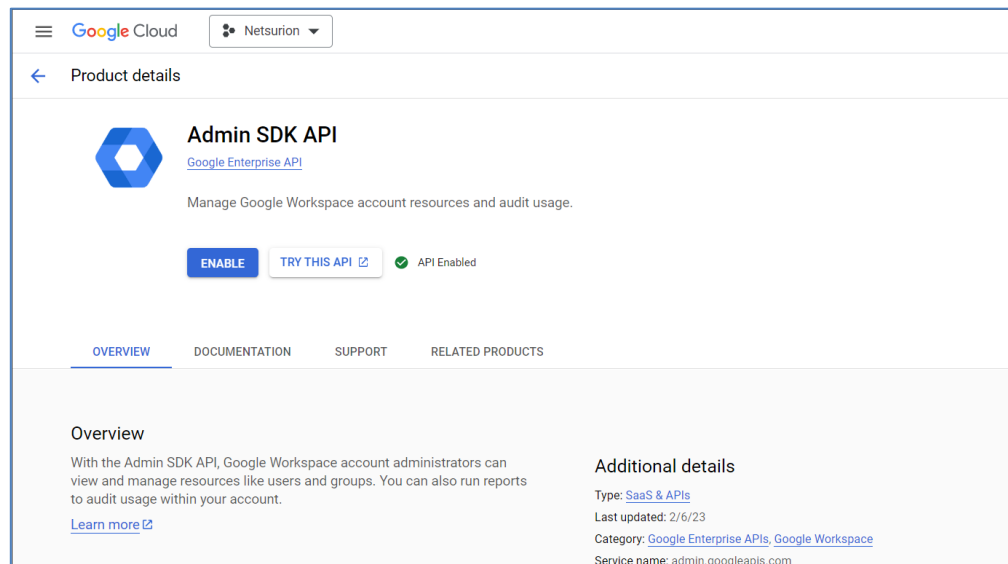
8. Click **Library or Enable APIs and Services** to enable the API.



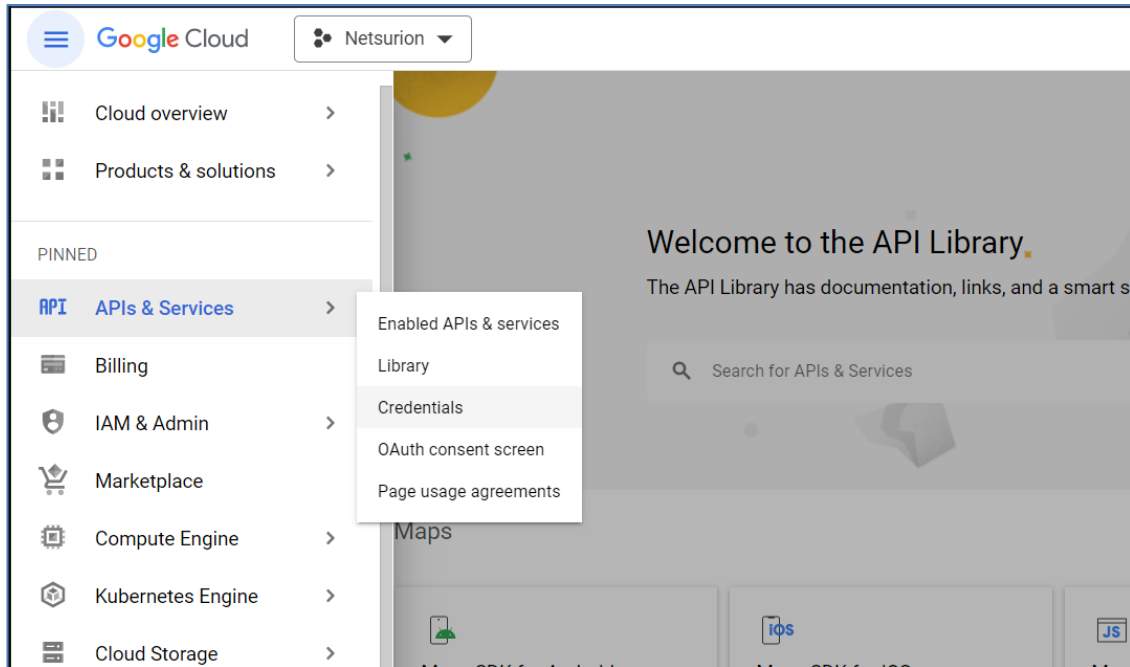
9. In the Search bar, type **Admin SDK**.



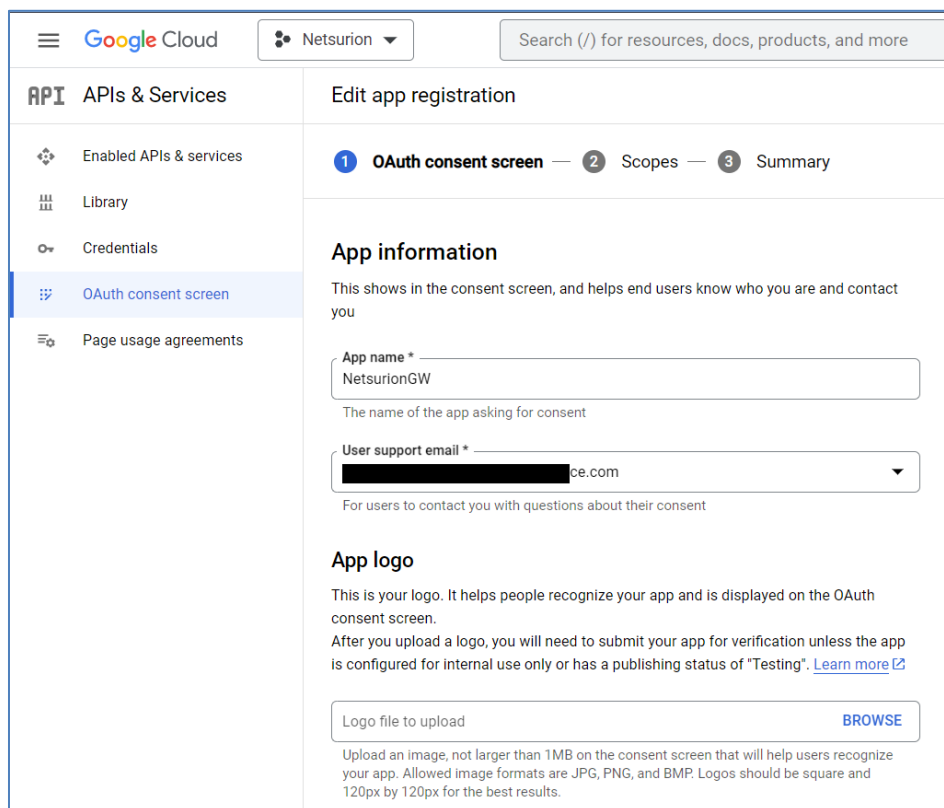
10. Click **Enable** to enable the Admin SDK API service for the application that has been created.



11. On the left panel, select **APIs & Services** and click **Credentials** to create the credentials for the application.



12. In the next step, select the **OAuth consent screen**.



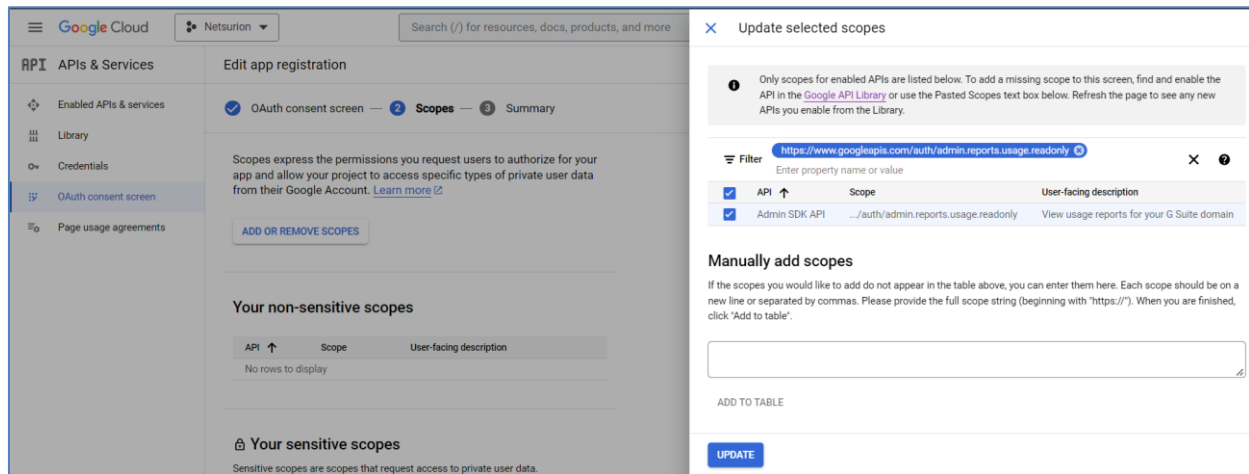
13. Select the Application type as **Internal**.

14. Enter the Application name.

15. In the **Scopes** section, click **Add Scope**.

16. Select the Admin SDK and search for the below keywords to add the scopes of Admin SDK.

- `./auth/admin.reports.audit.readonly` and
- `./auth/admin.reports.usage.readonly`



Update selected scopes

Only scopes for enabled APIs are listed below. To add a missing scope to this screen, find and enable the API in the [Google API Library](#) or use the Pasted Scopes text box below. Refresh the page to see any new APIs you enable from the Library.

Filter:

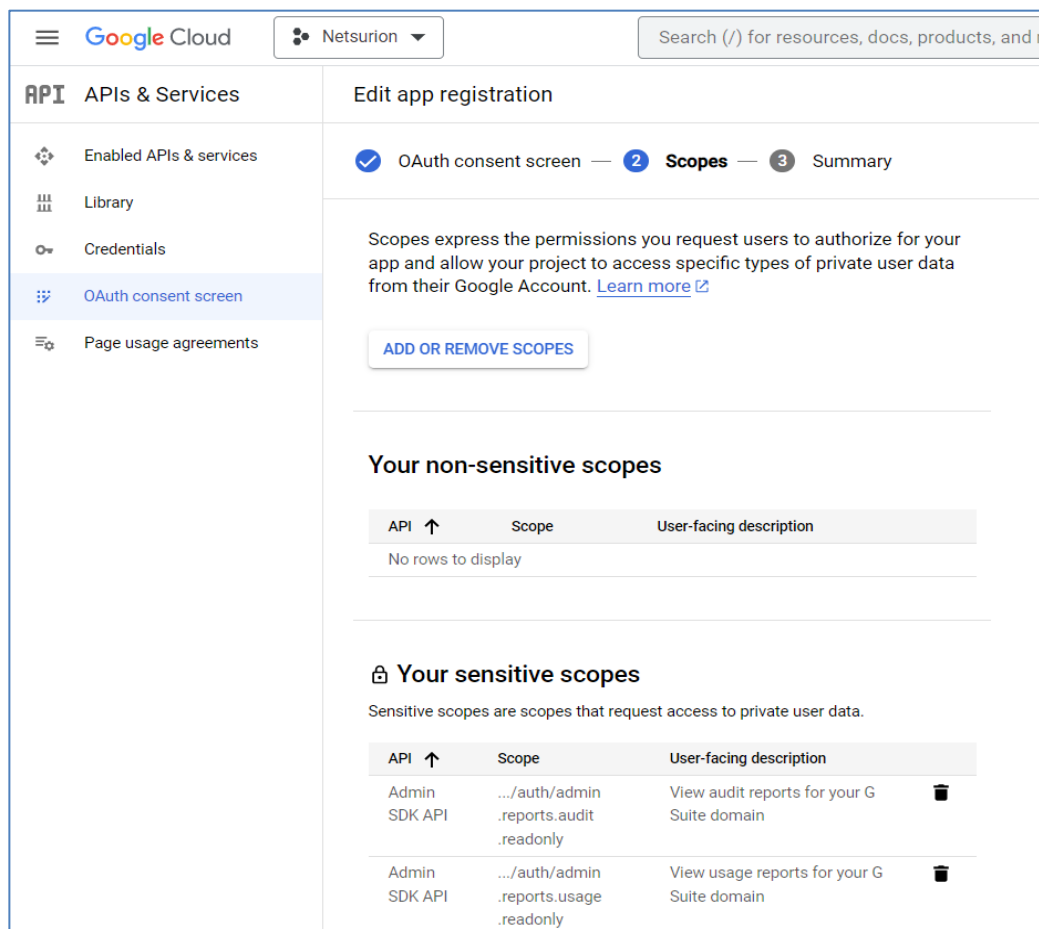
API	Scope	User-facing description	
<input checked="" type="checkbox"/>	Admin SDK API	.../auth/admin.reports.usage.readonly	View usage reports for your G Suite domain

Manually add scopes

If the scopes you would like to add do not appear in the table above, you can enter them here. Each scope should be on a new line or separated by commas. Please provide the full scope string (beginning with "https://"). When you are finished, click "Add to table".

ADD TO TABLE

UPDATE



Edit app registration

☒ OAuth consent screen — **2 Scopes** — ☒ Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

[ADD OR REMOVE SCOPES](#)

Your non-sensitive scopes

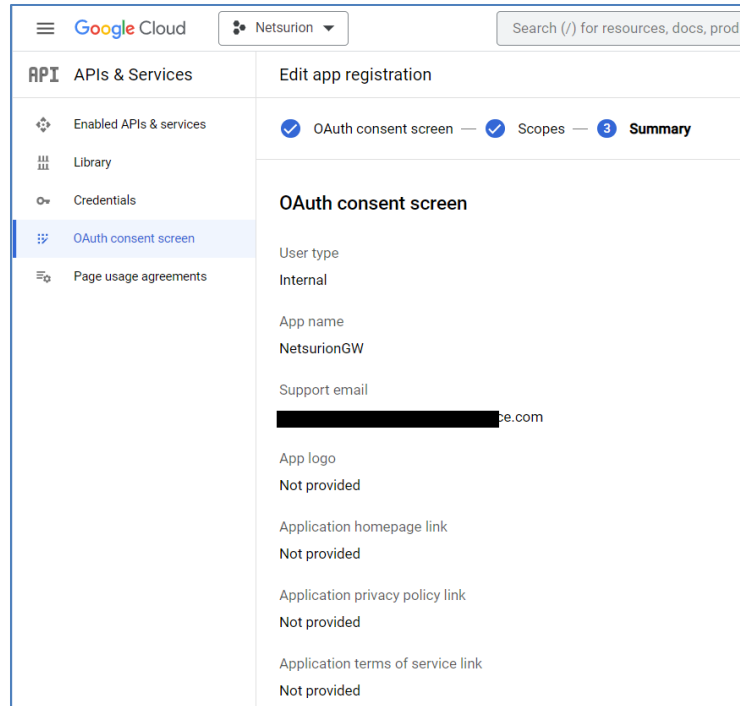
API	Scope	User-facing description
No rows to display		

Your sensitive scopes

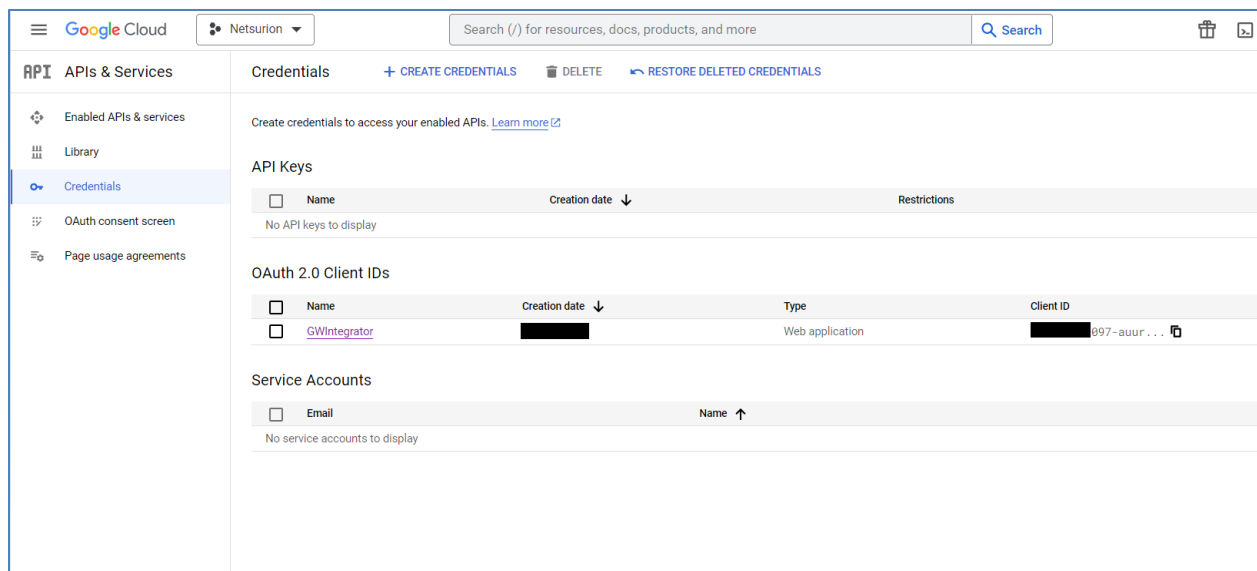
Sensitive scopes are scopes that request access to private user data.

API	Scope	User-facing description	
Admin SDK API	.../auth/admin.reports.audit.readonly	View audit reports for your G Suite domain	
Admin SDK API	.../auth/admin.reports.usage.readonly	View usage reports for your G Suite domain	

17. On the Summary page, validate the provided details and click **Save**.

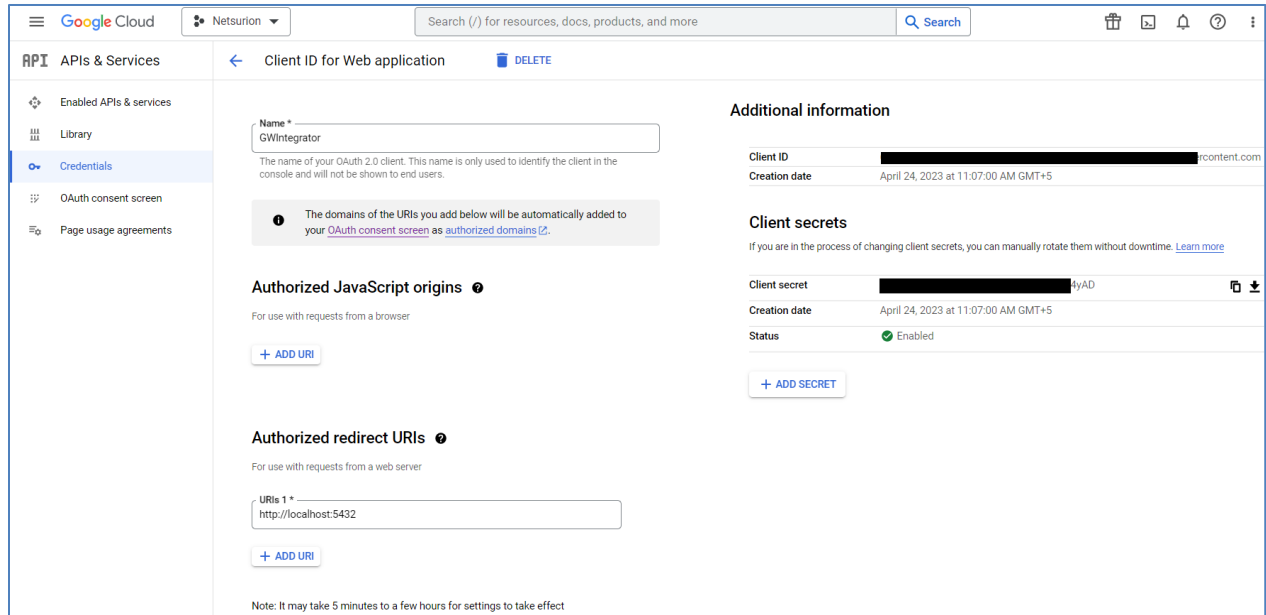


18. Once the **OAuth consent screen** details are saved, navigate to the **Credentials** menu to view the created API details.



Name	Creation date	Type	Client ID
GWIntegrator	[redacted]	Web application	[redacted]997-aaur...

19. After the application credentials are created, click the project name to view the **Client ID** and **Client Secret** as shown below.



The screenshot shows the Google Cloud console interface for configuring a 'Client ID for Web application'. The left sidebar shows the 'APIs & Services' menu with 'Credentials' selected. The main content area is titled 'Client ID for Web application' and includes a 'DELETE' button. The configuration fields are as follows:

- Name:** GWIntegrator
- Additional information:**
 - Client ID:** [Redacted]
 - Creation date:** April 24, 2023 at 11:07:00 AM GMT+5
- Client secrets:**
 - Client secret:** [Redacted]
 - Creation date:** April 24, 2023 at 11:07:00 AM GMT+5
 - Status:** Enabled
- 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 + [http://localhost:5432]
 - + ADD URI

A note at the bottom states: 'Note: It may take 5 minutes to a few hours for settings to take effect.'

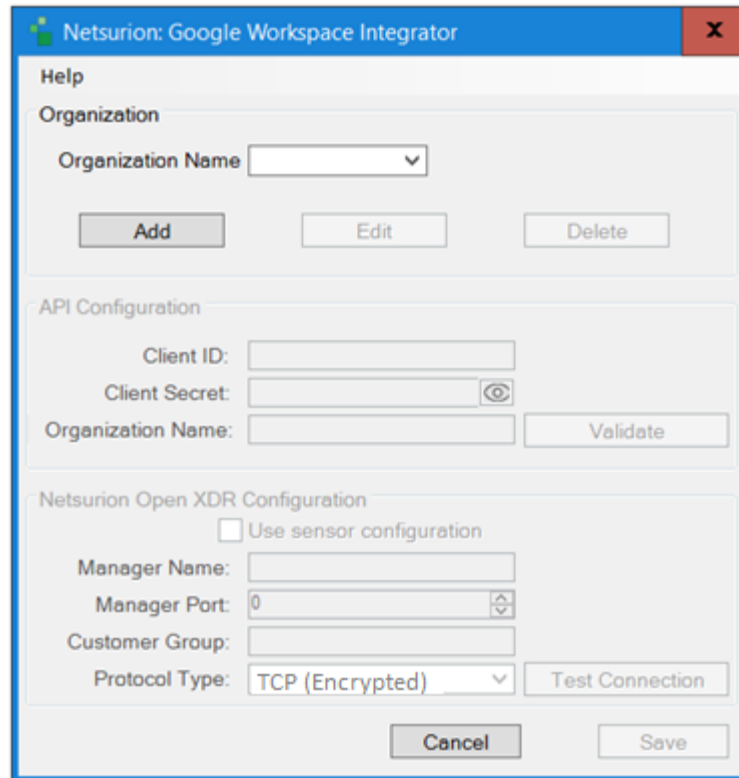
20. Enter the redirect URI as **http://localhost:5432**.
21. Copy the **Client ID**, **Client Secret**, and the **redirect URIs** that will be used in Google Workspace Integration.

3.2 Integrating Google Workspace with Netsurion Open XDR

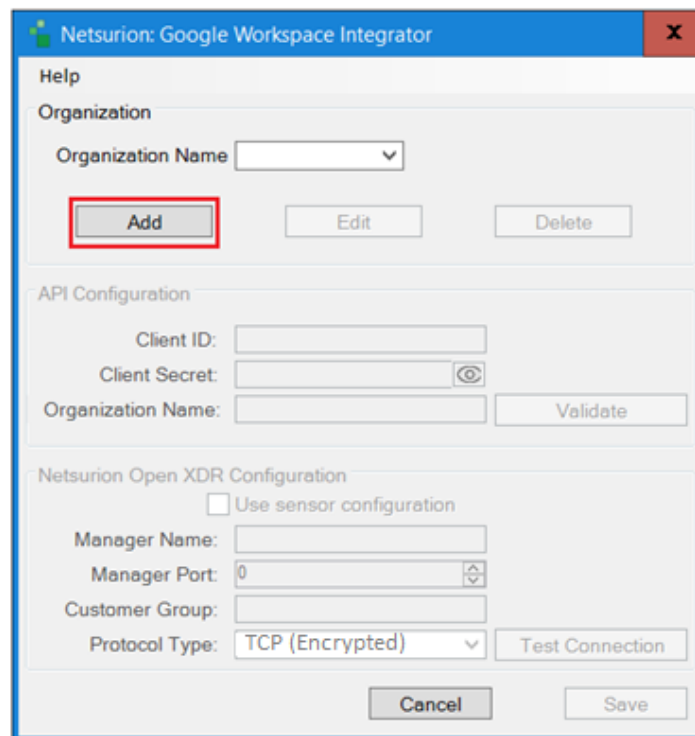
1. Once the API is configured, the following window will open once the user runs **Google_Workspace_Integrator.exe**.

Note

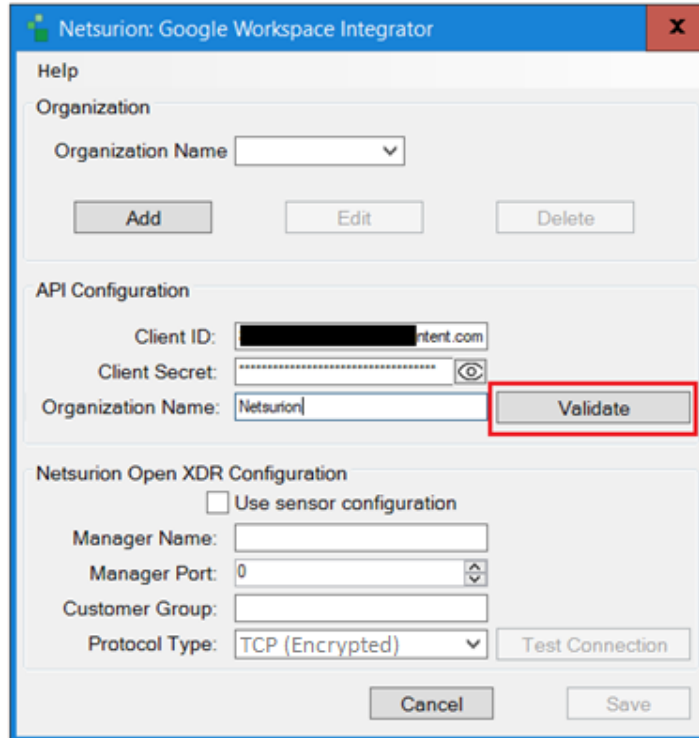
1. By default, the configuration of organizations has been limited to **five** in the Google Workspace integrator. The **Add** button will be disabled once the limit has been attained. The limit can be increased or decreased by changing the digit value in the **Limit.xml** file present in the **Config** folder.
2. The user should log in to the Google Workspace account to validate the API credentials and provide access to the requested permissions.



2. Click **Add** to add a new organization, and the current integrator supports adding multiple organizations.



3. Enter the **Client ID**, **Client Secret**, and **Organization Name**. Click **Validate** to validate the credentials.

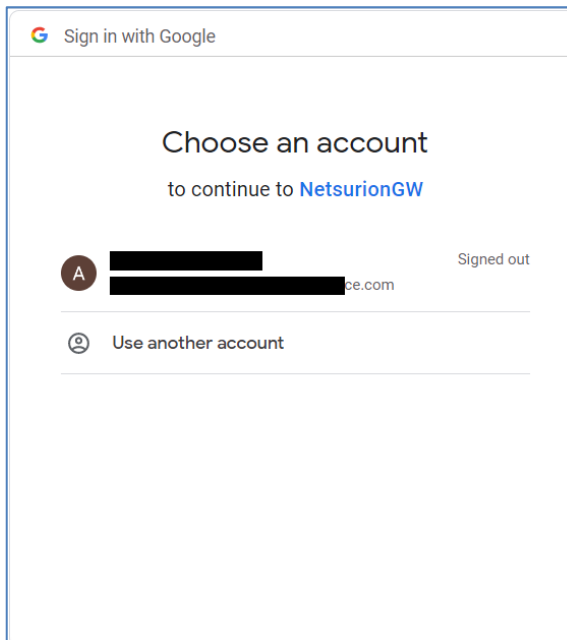


The dialog box is titled "Netsurion: Google Workspace Integrator". It contains the following sections:

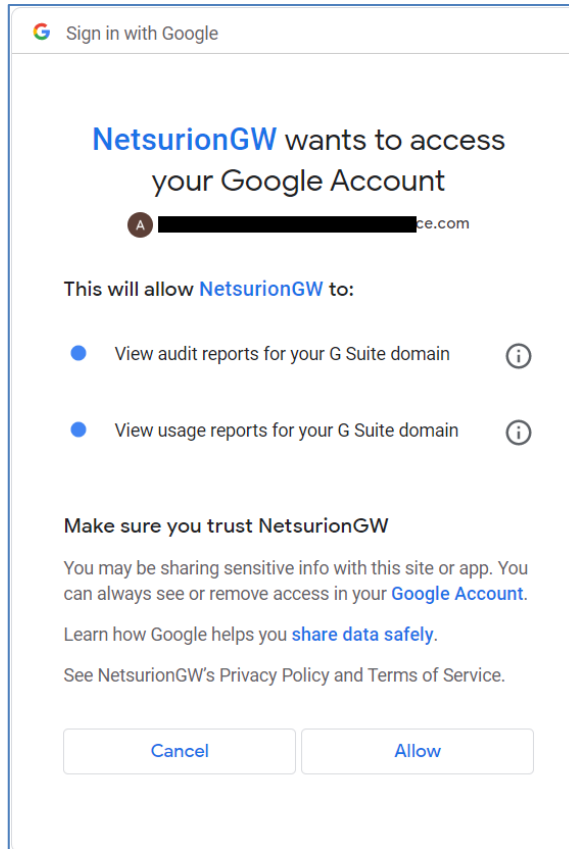
- Help**: A link to help documentation.
- Organization**: A dropdown menu for "Organization Name" with "Add", "Edit", and "Delete" buttons below it.
- API Configuration**: Fields for "Client ID" (containing a redacted value and ".intent.com"), "Client Secret" (with a toggle icon), and "Organization Name" (containing "Netsurion"). A "Validate" button is highlighted with a red rectangle.
- Netsurion Open XDR Configuration**: A checkbox for "Use sensor configuration" (unchecked), and fields for "Manager Name", "Manager Port" (set to 0), "Customer Group", and "Protocol Type" (set to "TCP (Encrypted)"). A "Test Connection" button is next to the protocol type.

At the bottom are "Cancel" and "Save" buttons.

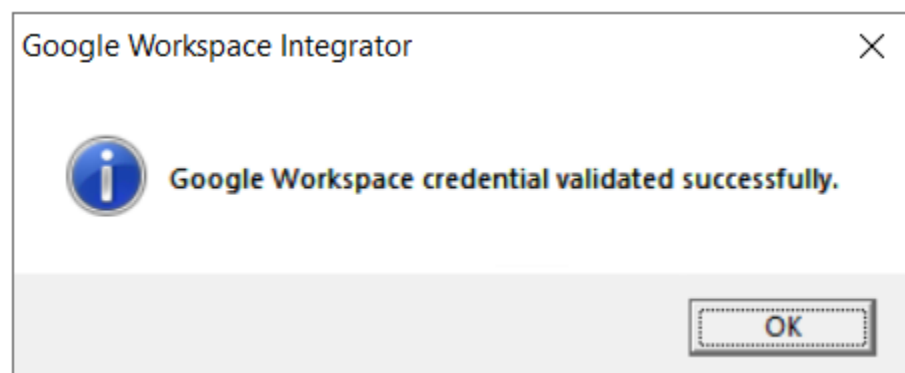
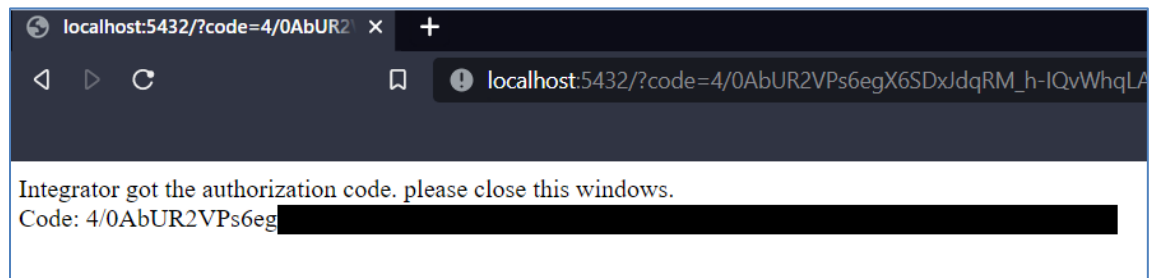
- After validating, the user has to log in to the Google Workspace account to provide access as shown below:



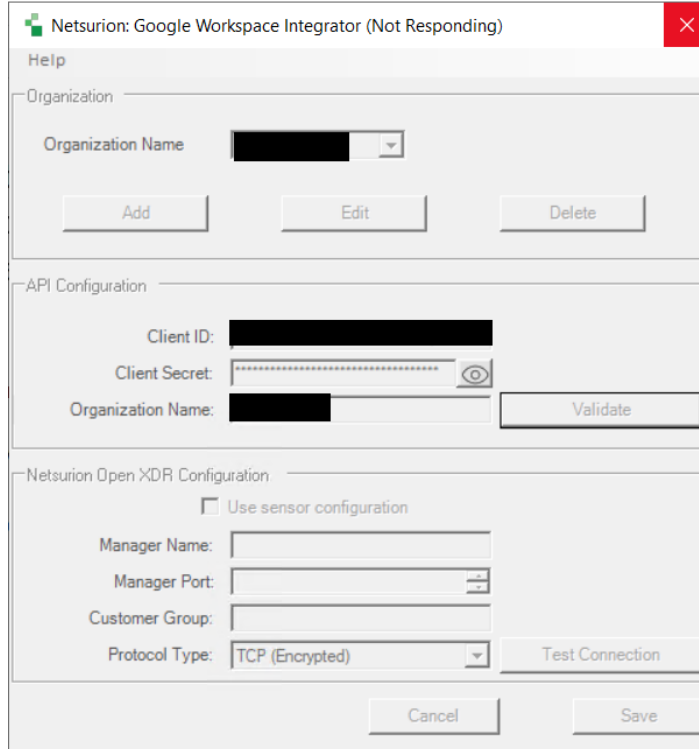
The screen shows the "Sign in with Google" interface. It prompts the user to "Choose an account to continue to NetsurionGW". A list of accounts is shown, with the first account (redacted name and email) marked as "Signed out". Below the list is a link to "Use another account".



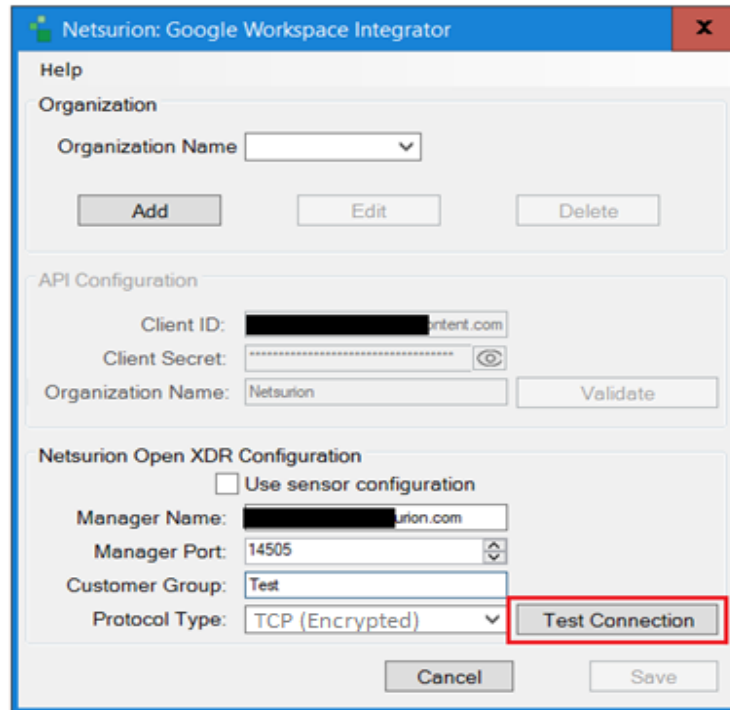
5. If the configuration is validated successfully, a success message 'Google Workspace Credential validated successfully' will be displayed on the screen.



6. If the credentials are not validated successfully, the Google Workspace integrator window will not respond as shown below:



7. Now, the user needs to run **Google_Workspace_Integrator.exe** again to complete the process.
8. Open the **Netsurion Google Workspace Integrator**. Under the **Netsurion Open XDR Configuration** section, either provide the Manager details to send the logs to a particular Netsurion Open XDR or use the sensor configuration.
 - Specify the **Manager Name**, **Manager Port**, **Customer Group**, and **Protocol Type** fields, and then click **Test Connection** to validate the information.



Netsurion: Google Workspace Integrator

Help

Organization

Organization Name

Add Edit Delete

API Configuration

Client ID:

Client Secret:

Organization Name: Validate

Netsurion Open XDR Configuration

☐ Use sensor configuration

Manager Name:

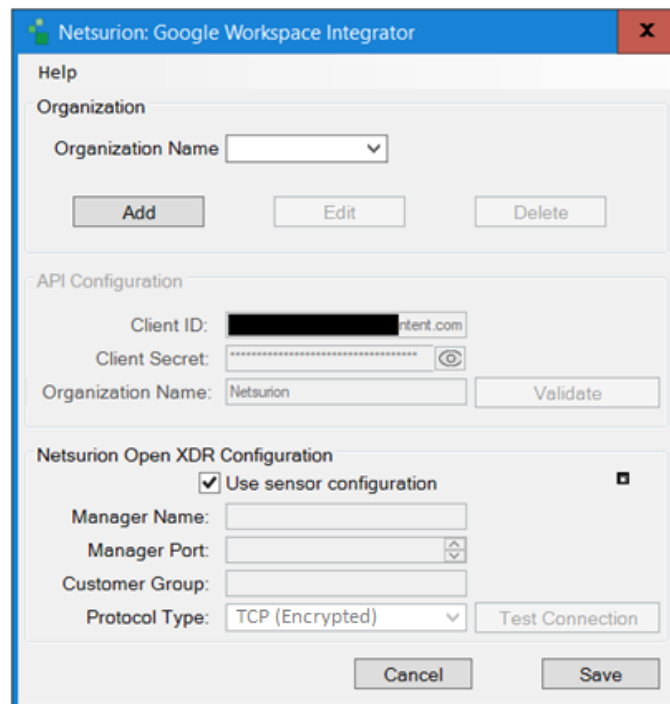
Manager Port:

Customer Group:

Protocol Type: Test Connection

Cancel Save

9. If the user wants to send logs to **Netsurion Open XDR sensor**, then select the **Use sensor configuration** checkbox.



Netsurion: Google Workspace Integrator

Help

Organization

Organization Name

Add Edit Delete

API Configuration

Client ID:

Client Secret:

Organization Name: Validate

Netsurion Open XDR Configuration

☒ Use sensor configuration

Manager Name:

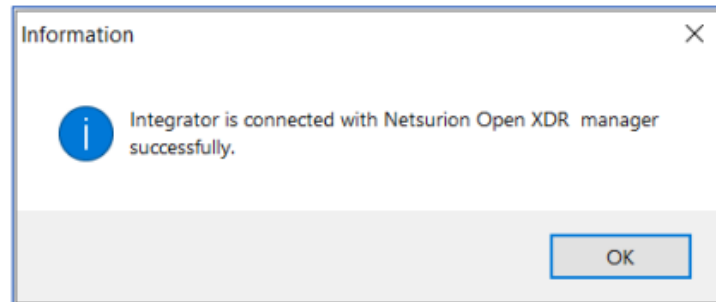
Manager Port:

Customer Group:

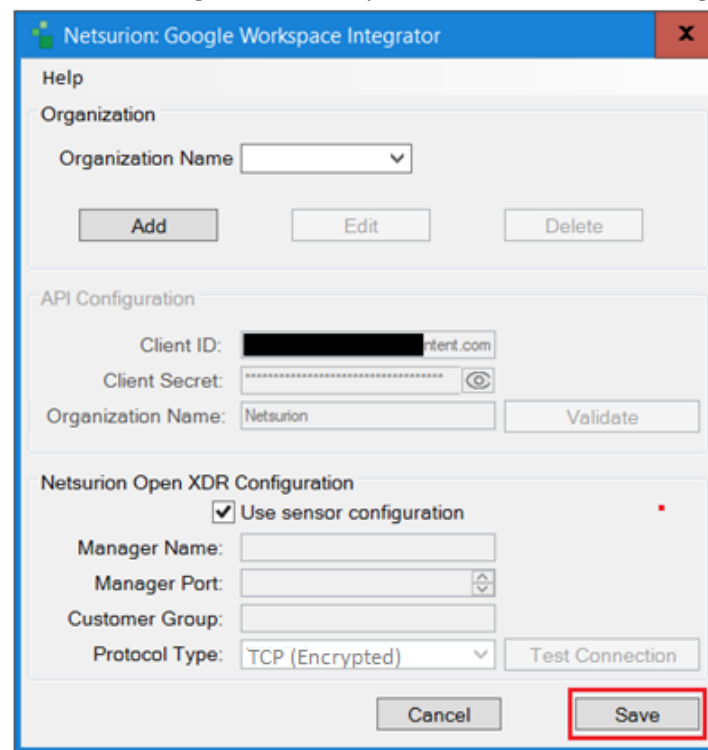
Protocol Type: Test Connection

Cancel Save

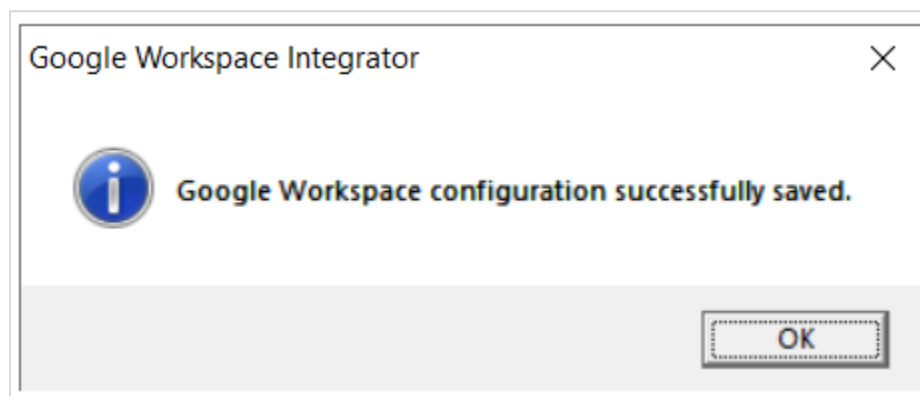
10. If the connection is validated successfully, a success message '**Integrator is connected with Netsurion Open XDR manager successfully**' will be displayed on the screen.



11. After validating the API and Manager successfully, click **Save** to save the Google Workspace configuration.



12. Upon successful completion, a success message appears as shown below:



4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integration package contains the following DSI assets for **Google Workspace**.

- Categories_Google Workspace.iscat
- Alerts_Google Workspace.isalt
- Reports_Google Workspace.etcrx
- KO_Google Workspace.etko
- Dashboards_Google Workspace.etwd

Note

Refer to the [DSI Configuration](#) guide for the procedures to configure the above DSI assets in Netsurion Open XDR.

The following are the key assets available in this Data Source Integration.

4.1 Alerts

Name	Description
Google Workspace: Suspicious login	Generated when a suspicious login activity has been detected in the Google Workspace account.
Google Workspace: Login failure	Generated when a login failure activity has been detected in the Google Workspace account.

4.2 Reports

Name	Description
Google Workspace - Login activities	Provides details of all login events that have happened in the Google Workspace account.
Google Workspace - Token logs	Provides details of token activities like token generation for a user, validation, etc. in the Google Workspace account.
Google Workspace - Mobile activities	Provides details of all the events that have occurred over mobile in the Google Workspace account.
Google Workspace - Admin activities	Provides details of all the admin events that have occurred in the Google Workspace account.

4.3 Dashboards

Name	Description
Google Workspace - Suspicious login by geolocation	Displays data of all the suspicious logins by the user's geolocation.
Google Workspace - Auth token usage by username	Displays multiple types of auth token methods used by username.
Google Workspace - Login activities	Displays data about login activities of all the users in the Google Workspace account.
Google Workspace - Admin activities by username	Displays data of all the admin activities of users in the Google Workspace account.

4.4 Saved Searches

Name	Description
Google Workspace - Admin activities	Provides details of all admin events that have occurred in the Google Workspace account.
Google Workspace - Login activities	Provides details of all login events that have happened in the Google Workspace account.
Google Workspace - Mobile activities	Provides details of all the events that have occurred over mobile in the Google Workspace account.
Google Workspace - Token logs	Provides details of token activities like token generation for a user, validation, etc. in the Google Workspace account.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the [form](#) to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

<https://www.netsurion.com/support>