



How-To Guide

# Integrate Google Workspace with Netsurion Open XDR

**Publication Date** December 07, 2023

© Copyright Netsurion. All Rights Reserved.



# 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	Ove	Overview						
2	Pre	Prerequisites						
3	Inte	egrating Google Workspace with Netsurion Open XDR	4					
	3.1	Creating Google Workspace Application for API Access						
	3.2	Integrating Google Workspace with Netsurion Open XDR	11					
4	Dat	a 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 <u>How-To-Upgrade-Google-Workspace-Integrator</u> 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 <a href="https://console.developers.google.com">https://console.developers.google.com</a>
- 2. Click the Select a Project drop-down.



≡	Google Cloud	95 🗸	Search (/) for resources, do	cs, products, and more		Q Search	毌	Þ Ó	?
API	APIs & Services	APIs & Services	+ ENABLE APIS AND SERVICES						
	Enabled APIs & services				1 hour 6 hours	12 hours 🗸	'1 day 2 days 4 da	ys 7 days	14 day
出	Library								
0+	Credentials	Traffic	≅ ~≾ <b>:</b>	Errors		Media	n latency	:	$\approx$
:9	OAuth consent screen								
Ξo	Page usage agreements	▲ No data is available fran	9 for the selected time 1e.	▲ No data is availab frai	•	No data is available fo frame.	r the selected	l time	
		UTC+5:30 6:00 PM No	v 7 6:00 AM	UTC+5:30 6:00 PM N	ov 7 6:00 AM	UTC+5:30	6:00 PM Nov 7	6:00 AM	1

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

	STARRED	ALL		
	Name		ID	
🗸 🏠 🐉		0	somashekar-1995	

- 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, proc			
New Project				
Project name * My Project 18517 Project ID; alpine-realm-386811. It cannot be changed later	e EDIT			
Organization *ce.com Select an organization to attach it to a project. This selection	n can't be changed later.			
Location *ce.com	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.

Search proj	iasta and foldera			
Q	ects and folders			
RECENT	STARRED	ALL		
	Name		ID	
✓☆	Netsurion 2		netsurion-384705	
₿		ce.com	821	

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



Ξ	Google APIs : Eventtrad	cker-Logger 🗸	
API	APIs & Services	APIS & Services + ENABLE APIS AND SERVICES	
	Dashboard		
	Deshooard	• You don't have any APIs available to use yet. To get started, click "Enable APIs and services" or go to the API library	
出	Library		
0*	Credentials		

9. In the Search bar, type Admin SDK.

	<b>\$•</b> Ne	etsurion 👻		Q	册
RPI API Library			Q, Admin SDK		
API Library > "Admin SDK"					
= Filter Type to filter		3 results			
Visibility	^	O	Admin SDK API Google Enterprise API 🔮		
Public	(3)		With the Admin SDK API, Google Workspace account administrators can view and manage resources like users and groups." reports to audit usage within your account.	You can also i	run
Category	^				
Developer tools	(1)		Audit API		
Google Enterprise APIs	(2)		Google This API has been replaced by the Admin SDK API.		
Security	(1)				
Coords Workspoor	(0)		Oloud Identity		

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

	d 🚺 🕈 Netsurion 👻	
← Product detail	s	
0	Admin SDK API Google Enterprise API Manage Google Workspace account resources and audit usag	e.
	ENABLE TRY THIS API 🕑 🔗 API Enabled	
OVERVIEW	DOCUMENTATION SUPPORT RELATED PRODUCTS	
Overview		
With the Admin S view and manag to audit usage w	SDK API, Google Workspace account administrators can e resources like users and groups. You can also run reports ithin your account.	Additional details Type: <u>SaaS &amp; APIs</u>
Learn more 🛛		Last updated: 2/6/23 Category: <u>Google Enterprise APIs, Google Workspace</u> Service name: admin.googleapis.com

**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.

≡	Google Cloud	Netsurion   Search (/) for resources, docs, products, and more
API	APIs & Services	Edit app registration
¢	Enabled APIs & services	1 OAuth consent screen — 2 Scopes — 3 Summary
出	Library	
07	Credentials	App information
ijŹ	OAuth consent screen	This shows in the consent screen, and helps end users know who you are and contact
Ξo	Page usage agreements	App name *

- **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

≡ G <mark>o</mark> ogle	e Cloud	• Netsurion 👻	Search (/) for resources	, docs, products, and more	× Update selected scopes				
PI APIS & S	Services	Edit app registratio	on Icreen — 😢 Scopes — 🕄 Sumr	Only scopes for enabled APIs are listed below. To add a missing sco API in the <u>Google API Library</u> or use the Pasted Scopes text box beli APIs you enable from the Library.					
Library Credential OAuth con To Page usag	ls nsent screen ge agreements	Scopes express the app and allow your from their Google A ADD OR REMOVE SC	permissions you request users to authororgiect to access specific types of priva cocount. <u>Learn more</u> 2 OPES	prize for your te user data	■ Filter               Mittps://www.googleupia.com/wuith/admin.reports.usage.readonly          ■ Enter property name or value         ■ All ↑       Scope         ■ All ↑       Scope         ■ Admin SDK API       _/auth/admin.reports.usage.readonly         View usage reports for your G Suit         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 show you would like to add a not appear in the table above, you can enter them here. Each scope show you can enter them heree. Each scope show you can enter them heree enter them heree ent				
		Your non-sens	tive scopes		cick Add to table".				
		No rows to display	pe User-tacing description						
					ADD TO TABLE				
		Your sensitive scopes are so	ve scopes		UPDATE				
		construction of the second sec							
-		o <mark>gle</mark> Cloud	🗣 Netsurion 👻		Search (/) for resources, docs, products, and r				
A	PI API	s & Services	Edit app reg	istration					
	🔅 Enabl	ed APIs & services		onsent screen —	Scopes — 3 Summary				
-		v							
		entials	Scopes expr	Scopes express the permissions you request users to authorize for your					
			app and allo from their G	app and allow your project to access specific types of private user data from their Google Account. Learn more 🖄					
	:v OAuti	r consent screen							
	= <sub>\$</sub> Page	usage agreements	ADD OR REI						
			Your non	-sensitive scop	es				
			API 🛧	Scope	User-facing description				
			No rows to	display					
			Sensitive score	ensitive scopes	suest 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**.



≡	Google Cloud	*	Netsurion 👻
API	APIs & Services		Edit app registration
٢	Enabled APIs & services		✓ OAuth consent screen — ✓ Scopes — ③ Summary
Ш	Library		
0.	Credentials		OAuth consent screen
12	OAuth consent screen		Liser type
Ξo	Page usage agreements		Internal
			App name NetsurionGW Support email pe.com App logo Not provided Application homepage link Not provided Application privacy policy link Not provided Application terms of service link Not provided

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

≡	Google Cloud	Petsurion ▼		Search (/) for resources, docs, proc	ducts, and more	(	Q Search	毌	>
API	APIs & Services	Credential	IS + CREATE C	REDENTIALS 🝵 DELETE 🖛 RES	STORE DELETED CREDENTIALS				
¢	Enabled APIs & services	Create creden	Create credentials to access your enabled APIs. Learn more 🖄						
쁐	Library	API Keys							
o <del>.</del>	Credentials	□ Na	ime	Creation date		Restrictions			
:17	OAuth consent screen	No API key	rs to display						
≡¢	Page usage agreements	OAuth 2.0	Client IDs						
		Na Na	ime	Creation date 🔸	Туре		Client ID		
		GV GV	VIntegrator		Web application		097-auur	Ō	
		Service Ac	ccounts						
		Em Em	nail		Name 🛧				
		No service	accounts to display						

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



≡	Google Cloud	<b>\$•</b> N	Vetsurion	·	Search (/) f	for resources, de	locs, products,	and more		C	२ Search	]	毌	>-	Ļ	?	:
API	APIs & Services		← c	lient ID for Web applic	ation	DELETE											
٢	Enabled APIs & services								Additional inform	nation							
Ш	Library		GW	ne * (Integrator													
0+	Credentials		The	name of your OAuth 2.0 client. T sole and will not be shown to en	"his name is only u d users.	used to identify the o	client in the		Client ID Creation date	April 24	4, 2023 at 11:	:07:00 AM GMT+5				rcontent	t.com
32	OAuth consent screen																
Ξo	Page usage agreements			I he domains of the URI your OAuth consent scr	een as authorize	will be automatica	ally added to		Client secrets								
									If you are in the process	of changing cl	lient secrets, y	you can manually rotate	them withou	t downtir	ne. <u>Lear</u>	n more	
			Aut	horized JavaScript	origins 🛛				Client secret				4yAD			ſ	ð±
			For u	se with requests from a browser					Creation date	April 24	4, 2023 at 11	:07:00 AM GMT+5					
						Status	🕑 Ena	abled									
			+	ADD URI													
									+ ADD SECRET								
			Aut	horized redirect UR	s 0												
			For u	se with requests from a web serv	rer												
			URI	s 1 *													
			+	ADD URI													
			Note	: It may take 5 minutes to a fev	v hours for settir	ngs 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.



Netsurion: Google Workspace Integrator
Help
Organization
Organization Name
Add Edit Delete
API Configuration
Client ID:
Client Secret:
Organization Name: Validate
Netsurion Open XDR Configuration
Manager Name:
Manager Port: 0
Customer Group:
Protocol Type: TCP (Encrypted)
Cancel Save

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

🖕 Netsurion: Google	Workspace Integrator	x
Help		
Organization		
Organization Name	~	
Add	Edit Delete	
API Configuration		
Client ID:		
Client Secret:	0	
Organization Name:	Validate	
Netsurion Open XDR	Configuration Use sensor configuration	
Manager Name:		
Manager Port:	0	
Customer Group:		
Protocol Type:	TCP (Encrypted) V Test Connec	tion
	Cancel	/e

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



🖕 Netsurion: Google	Workspace Integrator	×
Help		
Organization		
Organization Name	×	
Add	Edit	Delete
API Configuration		
Client ID:	ntent.com	
Client Secret:	·····	
Organization Name:	Netsurion	Validate
Organization Name: Netsurion Open XDR	Netsurion Configuration	Validate
Organization Name: Netsurion Open XDR	Netsurion Configuration Use sensor configuration	Validate
Organization Name: Netsurion Open XDR Manager Name:	Netsurion Configuration Use sensor configuration	Validate
Organization Name: Netsurion Open XDR Manager Name: Manager Port:	Netsurion Configuration Use sensor configuration 0	Validate
Organization Name: Netsurion Open XDR Manager Name: Manager Port: Customer Group:	Netsurion	Validate
Organization Name: Netsurion Open XDR Manager Name: Manager Port: Customer Group: Protocol Type:	Netsurion	Validate Test Connection

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





Sign in with Google					
NetsurionGW wants to access your Google Account					
This will allow Netsurion	GW to:				
• View audit reports for y	our G Suite domain	i			
• View usage reports for	your G Suite domain	i			
Make sure you trust Nets	urionGW				
You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.					
Learn how Google helps you share data safely.					
See NetsurionGW's Privacy Po	licy and Terms of Servic	e.			
Cancel	Allow				

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:

- Netsurion: Google Workspace Integrator (Not Responding)					
Help					
Organization					
Organization Name	Y				
Add	Edit Delete				
API Configuration					
Client ID:					
Client Secret:	·····				
Organization Name:	Validate				
Netsurion Open XDR Config	uration				
Г	Use sensor configuration				
Manager Name:					
Manager Port:	- -				
Customer Group:					
Protocol Type:	TCP (Encrypted) Test Connection				
	Cancel Save				

- 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		x
Help			
Organization			
Organization Name	~		
Add	Edit	Delete	
API Configuration			
Client ID:	ontent.com		
Client Secret:			
Organization Name:	Netsurion	Validate	
Netsurion Open XDR	Configuration Use sensor configuration		
Manager Name:	urion.com		
Manager Port:	14505		
Customer Group:	Test		
Protocol Type:	TCP (Encrypted) 🗸	Test Connecti	on
	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:	ntent.com				
Client Secret:					
Organization Name:	Netsurion	Validate			
Netsurion Open XDR Configuration					
Manager Nieman	Use sensor configuration				
Manager Name:					
Customer Group:	V.				
Protocol Type:	TCP (Encrypted)	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.



Information				
1	Integrator is connected with Netsurion Open XDR manager successfully.			
	ОК			

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

📲 Netsurion: Google	Workspace Integrator		x	
Help				
Organization				
Organization Name	×			
Add	Edit	Delete		
API Configuration				
Client ID:	ntent.com			
Client Secret:				
Organization Name:	Netsurion	Validate		
Netsurion Open XDR Configuration				
Manager Name:	Use sensor configuration		-	
Manager Port:				
Customer Group:				
Protocol Type:	TCP (Encrypted)	Test Connecti	on	
	Cancel	Save	è	

**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 <u>DSI Configuration</u> 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 geo- location.
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<sup>®</sup> 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 <u>www.netsurion.com</u>.

## **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