Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Google Workspace with EventTracker

EventTracker 9.2x and Above

Publication Date:

August 3, 2021

Abstract

This guide helps you in configuring **Google Workspace** with EventTracker to receive **Google Workspace** events. In this guide, you will find the detailed procedures required for monitoring **Google Workspace.**

Scope

The configuration details in this guide are consistent with EventTracker version v9.2x or above and **Google Workspace.**

Audience

Administrators, who are assigned the task to monitor and manage **Google Workspace** events using **EventTracker.**

Table of Contents

1. Overview

This guide helps you in configuring **Google Workspace (formerly known as Gsuite)** with EventTracker to receive **Google Workspace** events. In this guide, you will find the detailed procedures required for monitoring **Google Workspace.**

EventTracker helps to monitor events from **Google Workspace**. Its dashboard, alerts, and reports will help you to detect attacks and suspicious host and accounts.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

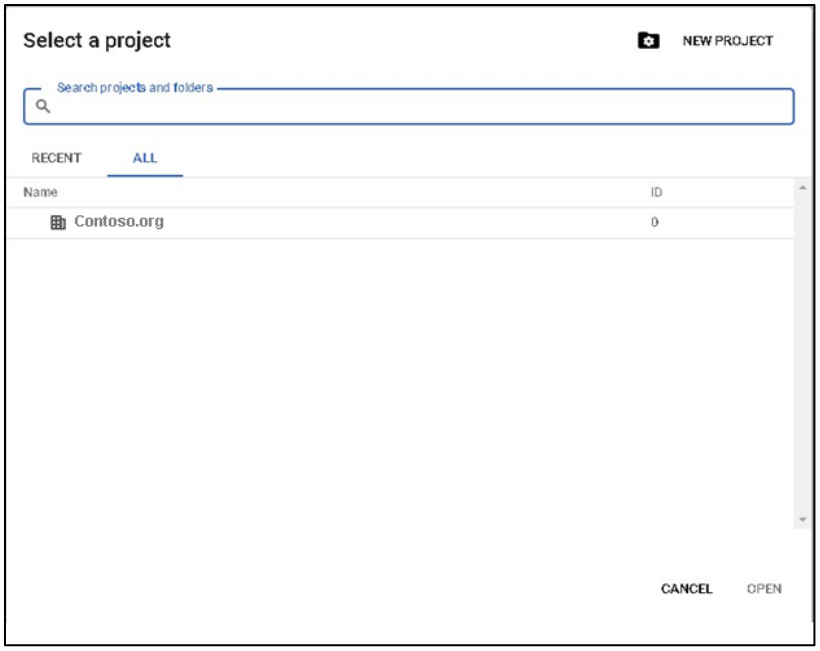
- **EventTracker v9.x** or **above** should be installed.
- **Google Workspace** should be configured.
- **Admin permission** should be there for configuring Google Workspace API.
- **Local admin permissions** for the workstation.
- **PowerShell 5.0** should be installed on the EventTracker Manager.

3. Integrating Google Workspace with EventTracker

3.1 Creating Google Workspace Application for API access

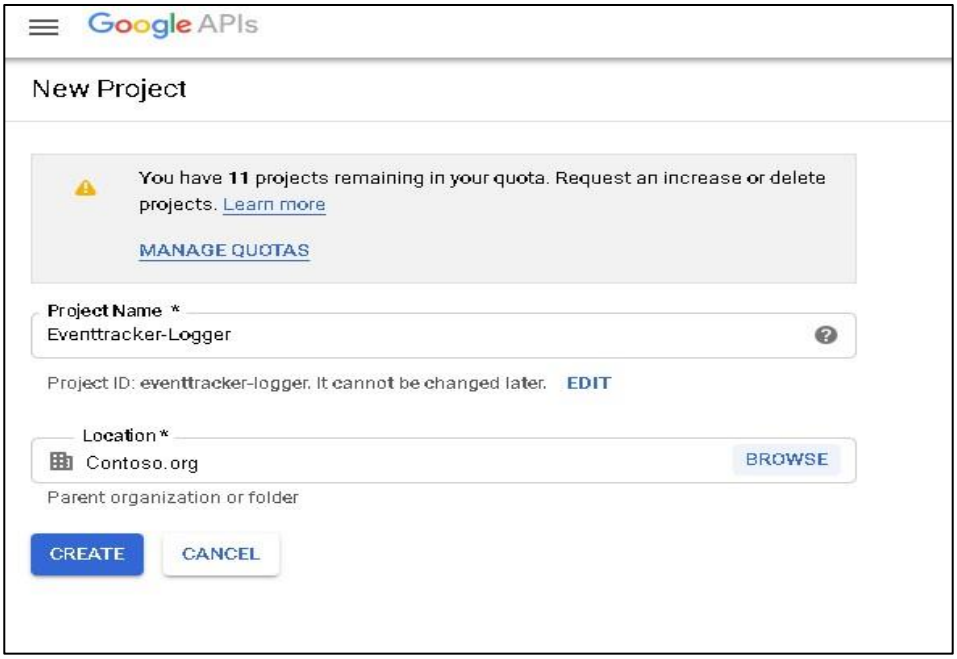
1. Login to https://console.developers.google.com
2. Click on **Select a Project** dropdown.

3. A pop-up window that appears, click on **NEW PROJECT.**

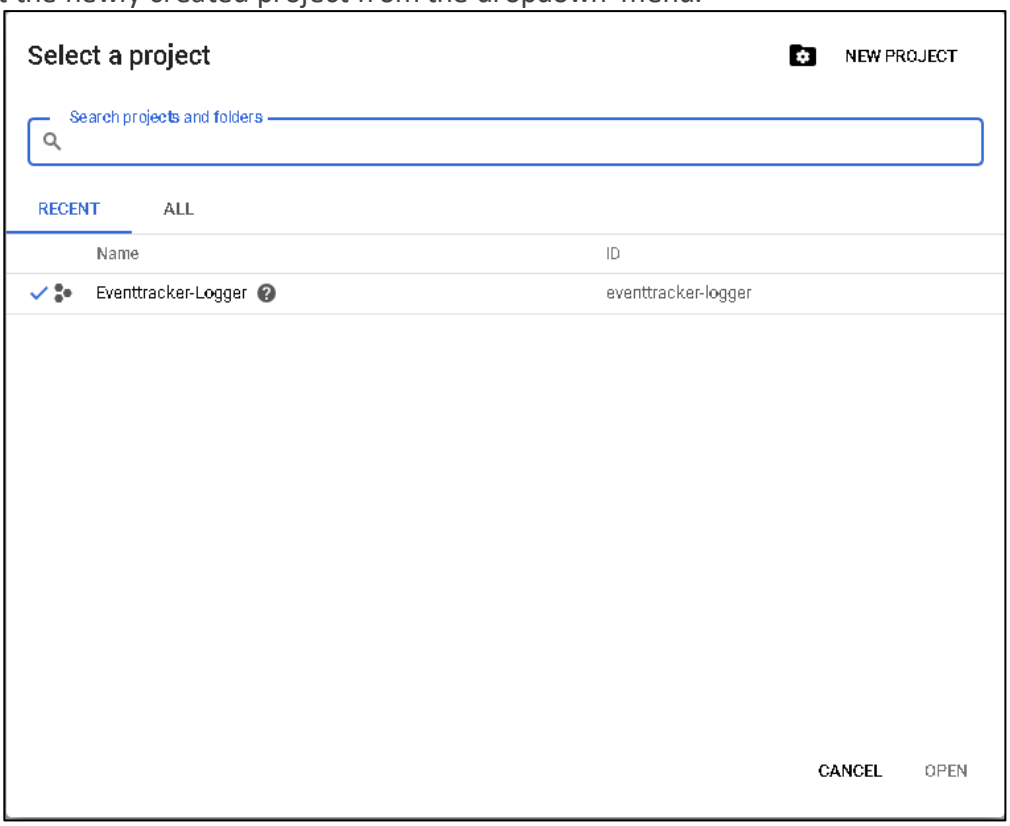


4. Enter the Project Name.
5. Under **Location,** click on **Browse** and select the parent organization from the popped-up window.

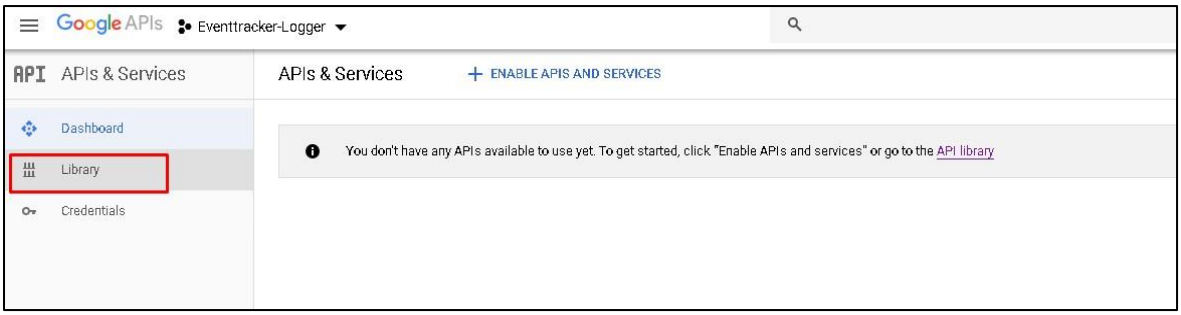
6. Click **Create**.



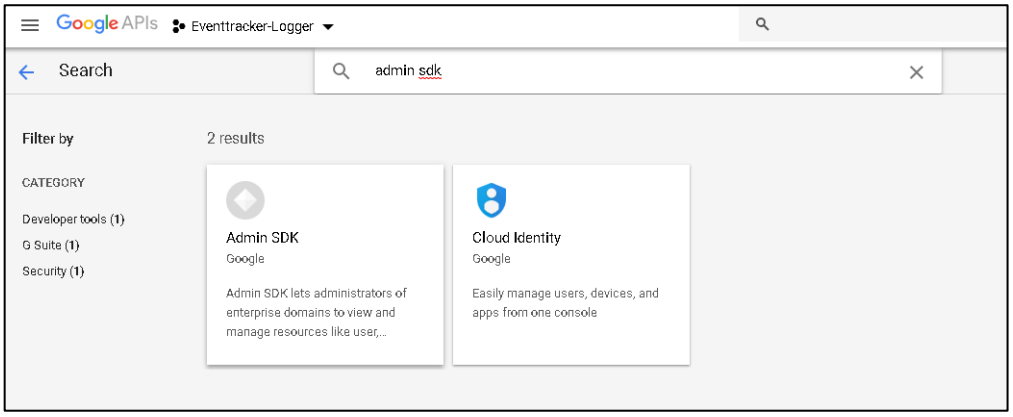
7. Select the newly created project from the dropdown menu.



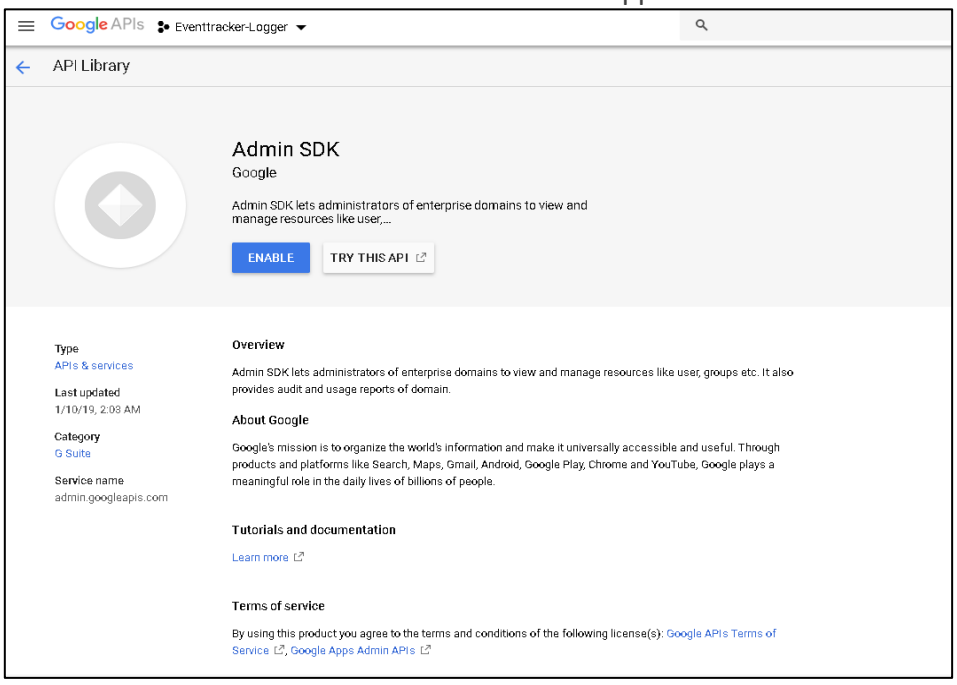
8. Click on **Library** or **Enable APIS and Services** to enable API.



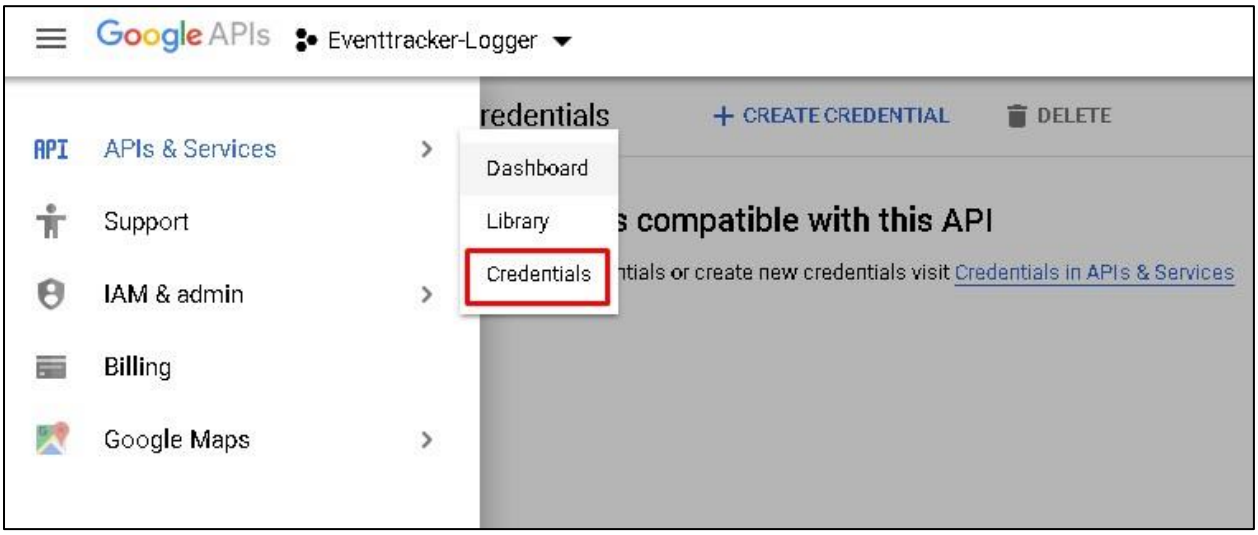
9. Search for **Admin SDK** in search tab.



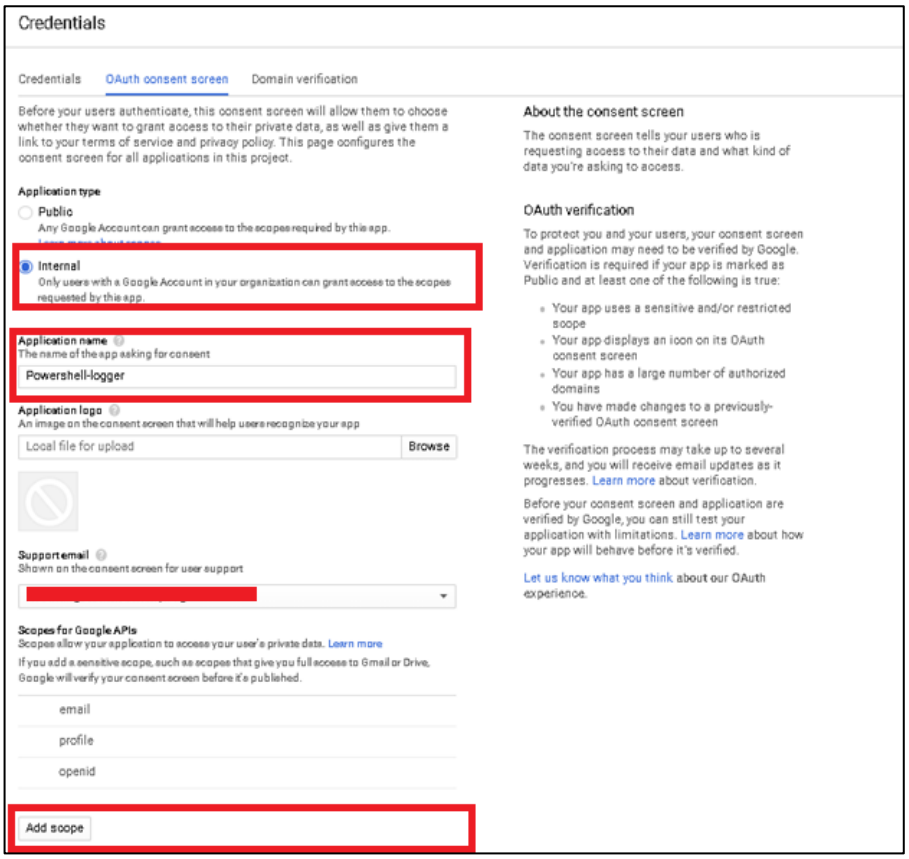
10. Click **Enable** to enable Admin SDK API service for the app we created.



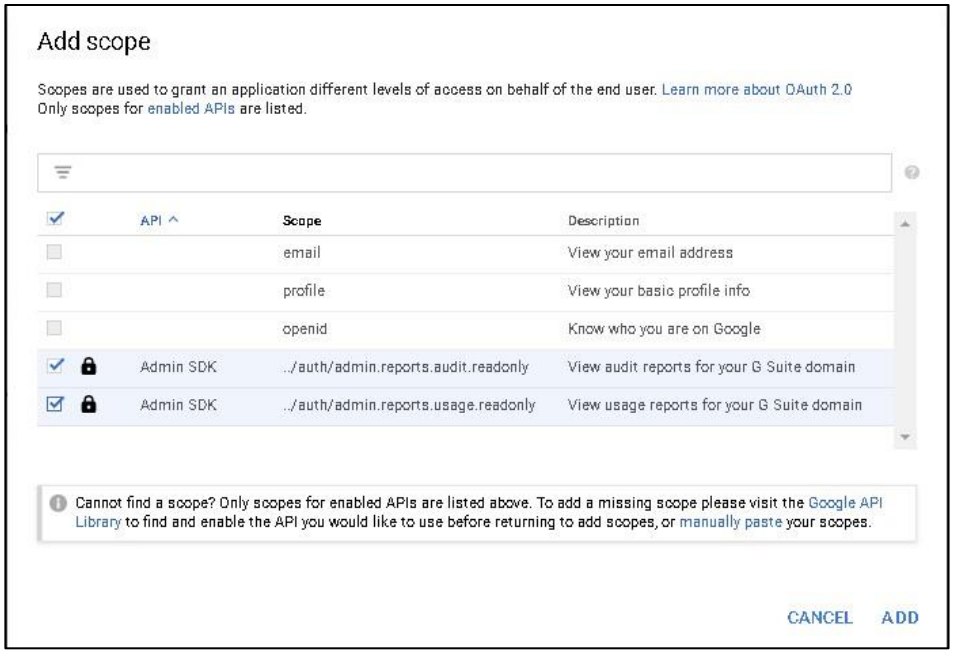
11. On the Menu in the right side, **select APIs & Services** and click on **credentials** to create credentials for the app.



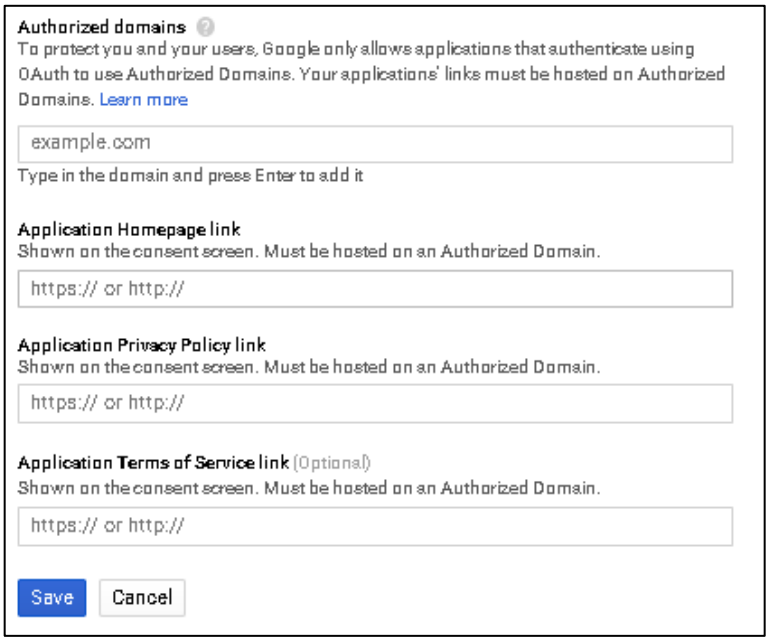
12. Select OAuth consent screen.



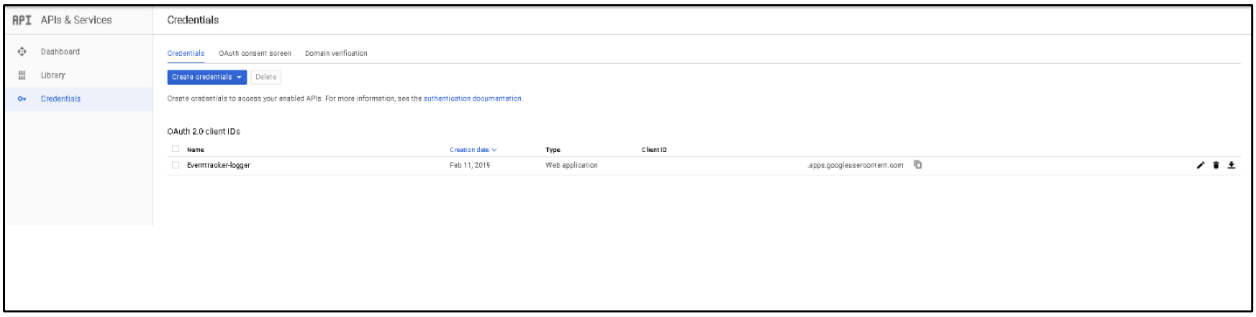
13. Select Application type to Internal.
14. Enter Application name.
15. Under Scopes for Google APIs, click Add scope.

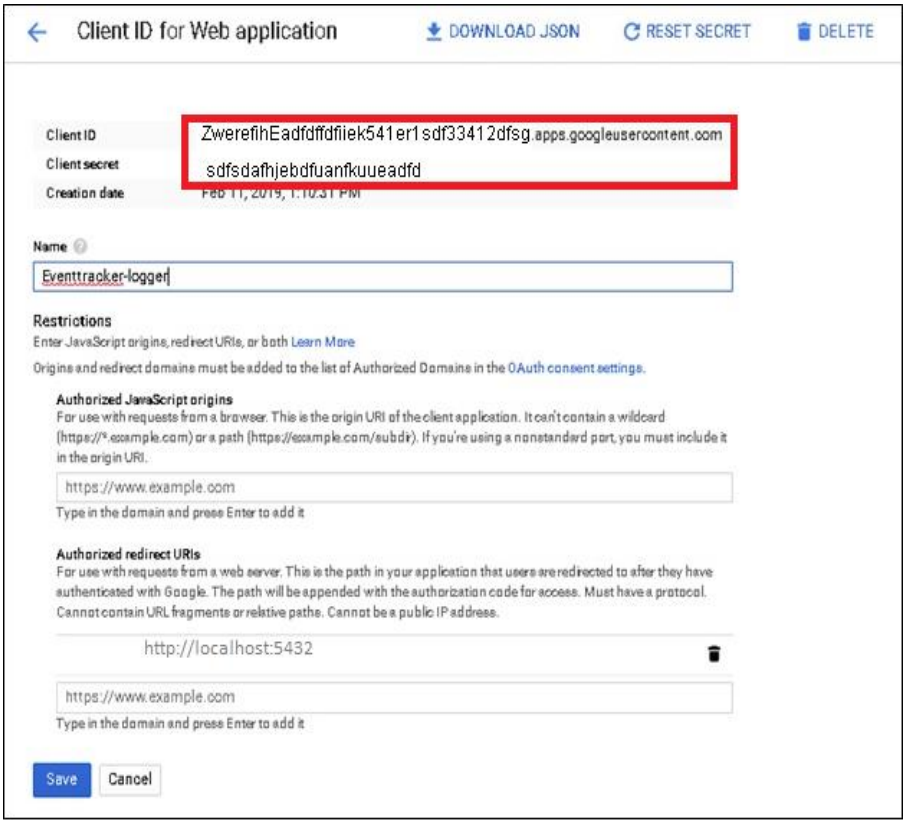


16. Select the Admin SDK.
    - **./auth/admin.reports.audit.readonly** and
    - **./auth/admin.reports.usage.readonly**
17. Click **ADD** to save.
18. Click **Save** from the oAuth consent page.



19. After App credentials are created, click on the project name to see the Client Id and Client secret as shown in the images below.





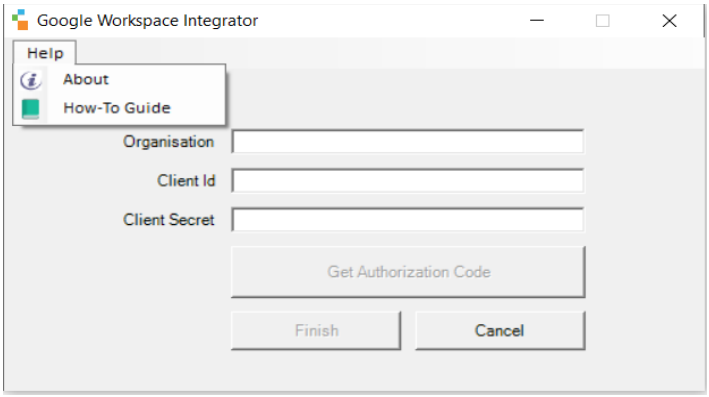
20. Enter Redirect URI as **http://localhost:5432.**
21. Copy the **Client ID, Client Secret,** and the **redirect URIs** which we will use in our EventTracker Google Workspace Integration.

3.2 Integrating Google Workspace to EventTracker

Note: Integrator version: 3.0.1

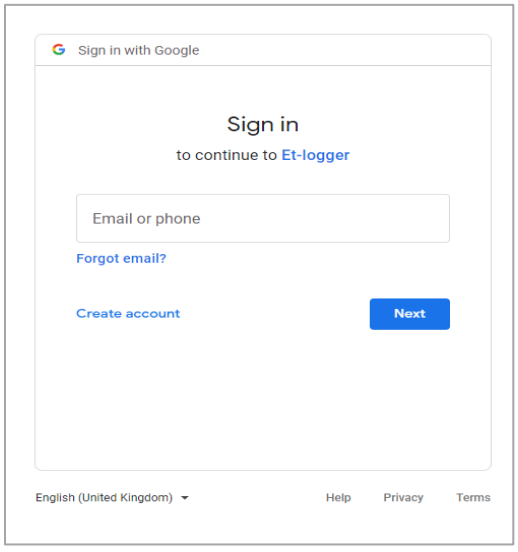
1. Download the Google Workspace Integrator on EventTracker manager/EventTracker agent machine from below link: https://downloads.eventtracker.com/kp-integrator/ETS_GoogleWorkspace_Integrator.exe
2. Run the downloaded **ETS_GoogleWorkspace_Integrator.exe**. Integration window will open.
3. Provide your Organisation name which will get displayed under the EventTracker manager.
4. To check the Integrator version, go to **Help** > **About.** Make sure you are using the latest version of integrator.
5. Provide the **Client Id**, **API Key (Client Secret)** which we got from Google app.

   Note: Latest integrator version is 3.0.1

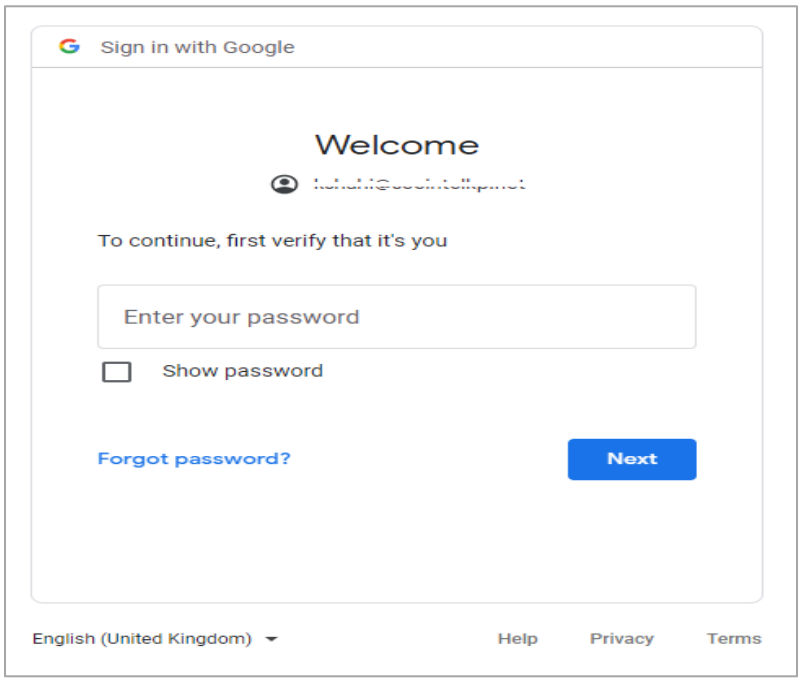


NOTE: Make sure ClientId and Client secret provided in the integrator is correct. If any of them are wrong, close the Integrator and run again.

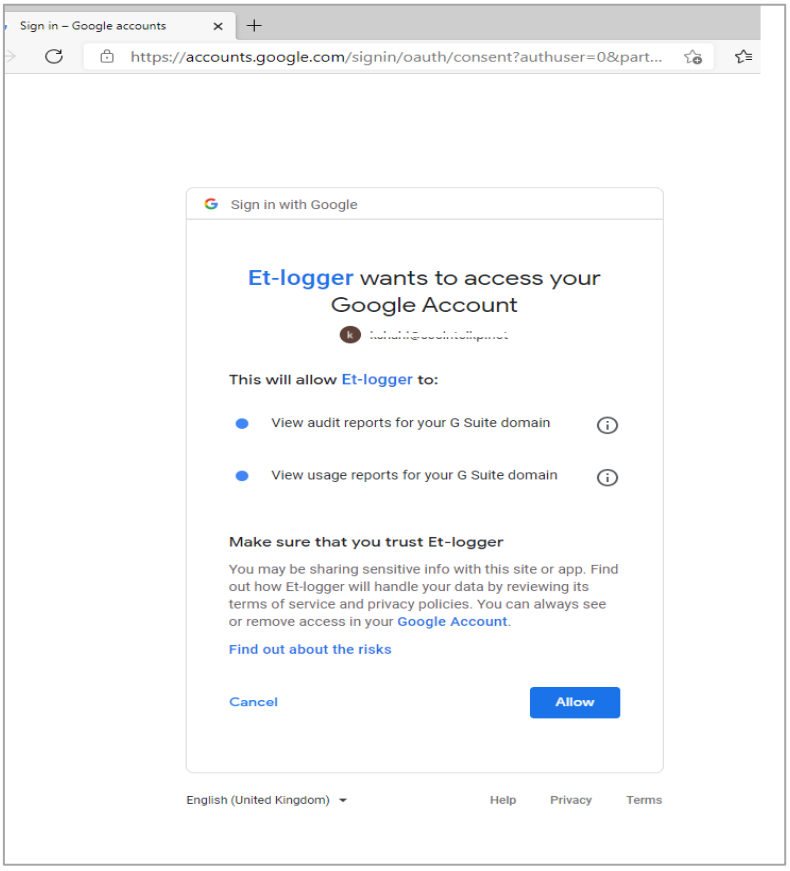
6. It will open a tab asking for credentials.



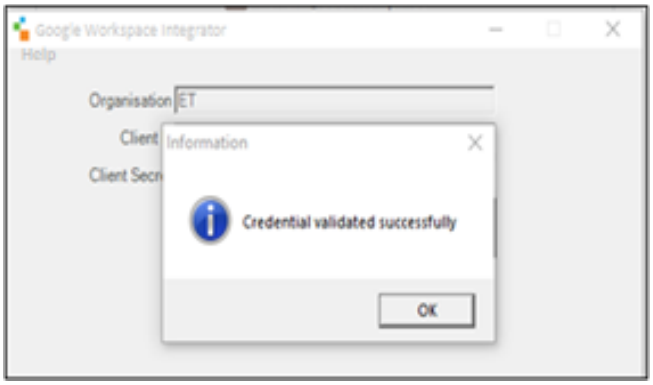
7. Sign-in with the user who has privilege to access the admin reports.
8. Enter your password.



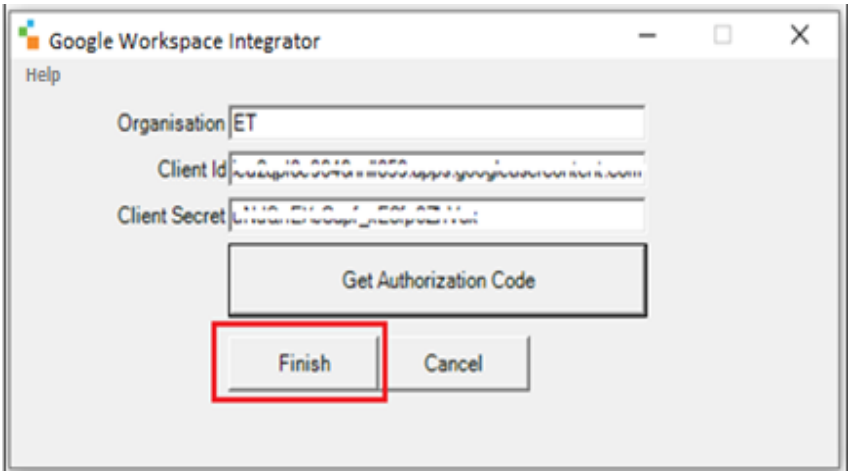
9. Click **Allow** to authorize the app which we created.



10. A message window will pop up stating **Credentials are validated successfully**. Click **OK.**



11. Click **Finish** on the Google Workspace Integrator to complete the integration.



4. EventTracker Knowledge Pack

After logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following knowledge packs are available in EventTracker to support Google Workspace.

4.1 Category

- **Google Workspace: Suspicious Login -** This category provides information related to any suspicious login detected in Google Workspace.
- **Google Workspace: Login Activity –** This category provides information related to all the login and logout activities performed by users in Google Workspace.
- **Google Workspace: Mobile Activity –** This category provides information related to mobile activities performed by users in Google Workspace.
- **Google Workspace: Token Activity –** This category provides information related to auth token logins detected in Google Workspace.

- **Google Workspace: Admin Activity –** This category provides information related to all the admin activities such as user creation, email search, alert views etc.
- **Google Workspace: Login Success –** This category provides information related to all the successful logins detected in Google Workspace.
- **Google Workspace: Login Failure –** This category provides information related to all the login failure detected in Google Workspace.

4.2 Alert

- **Google Workspace: Login Failure -** This alert is generated when any login failure is detected in Google Workspace.
- **Google Workspace: Suspicious Login –** This alert is generated when any suspicious login is detected in Google Workspace.

4.3 Report

- **Google Workspace: Admin Activities-** This report gives the information about the admin activities performed such as user creation, email log search, google chrome, hangout activities, etc. Reports contains IP address, username, customer ID, log type and other fields which will be helpful for further investigation.

LogTime	EventId	Computer	EventSource	EventDescription	Application Name	User Type	Customer ID	src user name	Log type	Source IP Address
04/08/2020 02:36:36 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	admin	USER	C02ab3xxh	gurmukh@secintelkp.com	EMAIL_SETTINGS	182.74.xxx.xxx
04/08/2020 02:36:36 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	admin	USER	C02ab3xxh	gurmukh@secintelkp.com	EMAIL_SETTINGS	182.74.xxx.xxx
04/08/2020 02:36:36 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	admin	USER	C02ab3xxh	gurmukh@secintelkp.com	ALERT_CENTER	103.5.xxx.xx

- **Google Workspace: Mobile Activities -** This report gives the information about all the mobile activities such as device application change, OS update, device compliance status, device action, device ownership, device settings change etc. Reports contains user email, device ID, device type, device events, etc. which can be used for further investigation.

LogTime	EventId	Computer	EventSource	EventDescription	Application Name	User Type	Customer ID	Device ID	Device Type	src user name
04/08/2020 02:36:28 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	mobile	USER	C02ab3xxh	312d6363cec56f5e	ANDROID	kritika@secintelkp.com
04/08/2020 02:36:28 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	mobile	USER	C02ab3xxh	312d6363cec56f5e	ANDROID	kritika@secintelkp.com
04/08/2020 02:36:28 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	mobile	USER	C02ab3xxh	312d6363cec56f5e	ANDROID	kritika@secintelkp.com

- **Google Workspace: Token Activities –** This report gives information about all the OAuth token audit activity events like authorize and revoke. Reports contains IP address, application name which used the token, action as authorize or revoke and other useful details for further investigation.

LogTime	EventId	Computer	EventSource	EventDescription	App Name	Application Name	Client Type	Customer ID	src user name	Log type
04/08/2020 02:36:28 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	Powershell-logger	token	WEB	C02ab3xxh	gurmukh@secintelkp.com	authorize
04/08/2020 02:36:28 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	Powershell-logger	token	WEB	C02ab3xxh	gurmukh@secintelkp.com	authorize
04/08/2020 02:36:28 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	Cloudready Free	token	NATIVE_APPLICATION	C02ab3xxh	kritika@secintelkp.com	authorize

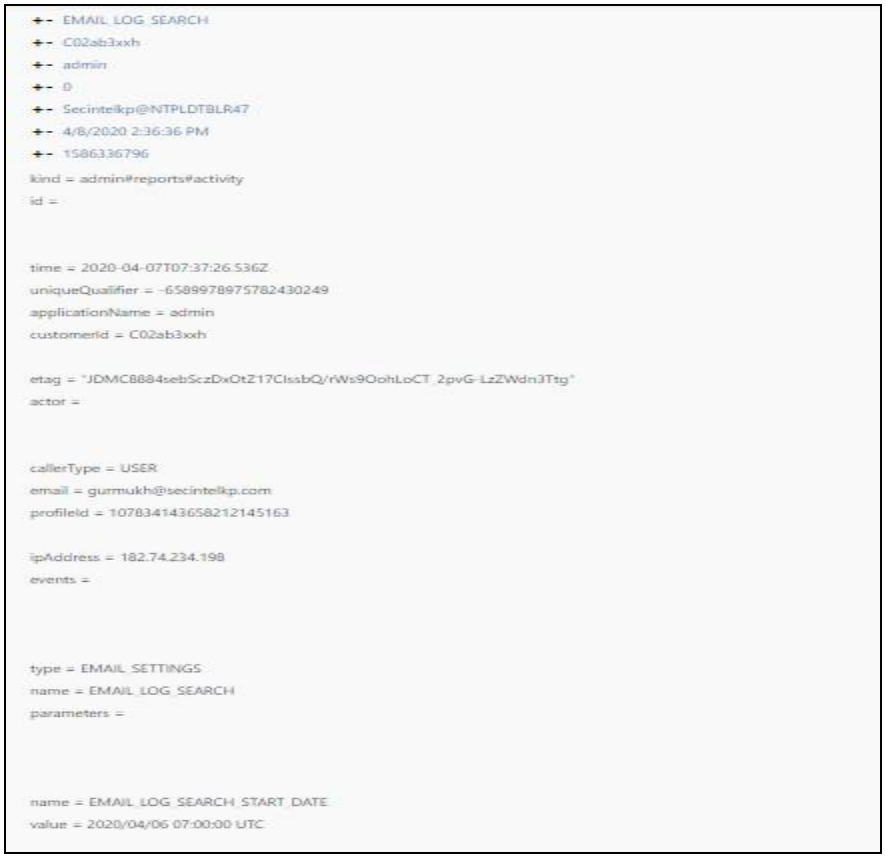
- **Google Workspace: Login and Logout Activities –** This report gives information about all the login and logout activities detected in Google Workspace. Report contains IP address, username, action as logout, successful login or login failure, logon type and if the login is suspicious, and other useful information.

LogTime	EventId	Computer	EventSource	EventDescription	Application Name	Customer ID	src user name	Source IP Address	Suspicious login
04/08/2020 02:36:26 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	gurmukh@secintelkp.com	182.74.xxx.xxx	False
04/08/2020 02:36:27 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	gurmukh@secintelkp.com	182.74.xxx.xxx	False
04/08/2020 02:36:27 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	kritika@secintelkp.com	182.74.xxx.xxx	False

- **Google Workspace: Login Failure -** This report gives information regarding all the login failures detected in Google Workspace. Reports contains IP address, logon type, username, and other useful information for further analysis.

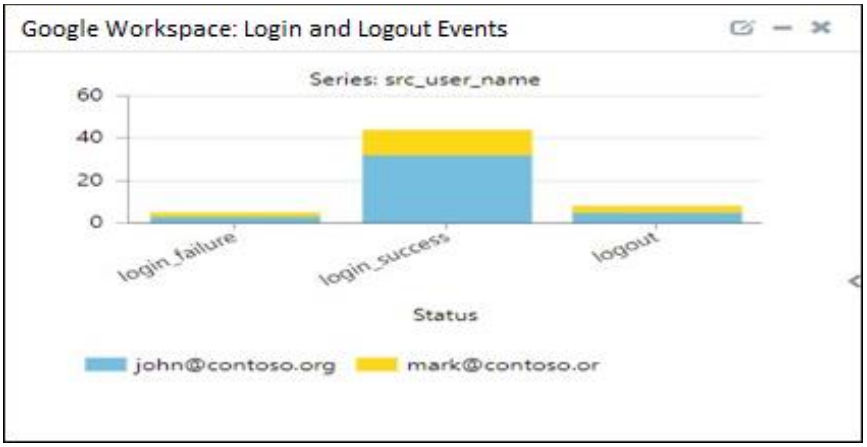
LogTime	EventId	Computer	EventSource	EventDescription	Application Name	Customer ID	src user name	Source IP Address	Logon type	Login action
04/08/2020 02:36:27 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	gurmukh@secintelkp.com	182.74.xx.xx	google_password	login_failure
04/08/2020 02:36:27 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	kritika@secintelkp.com	182.74.xx.xx	google_password	login_failure
04/08/2020 02:36:27 PM	3230	SECINTELKP@NTPLxxxxxxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	kritika@secintelkp.com	182.74.xx.xx	google_password	login_failure

Logs Considered

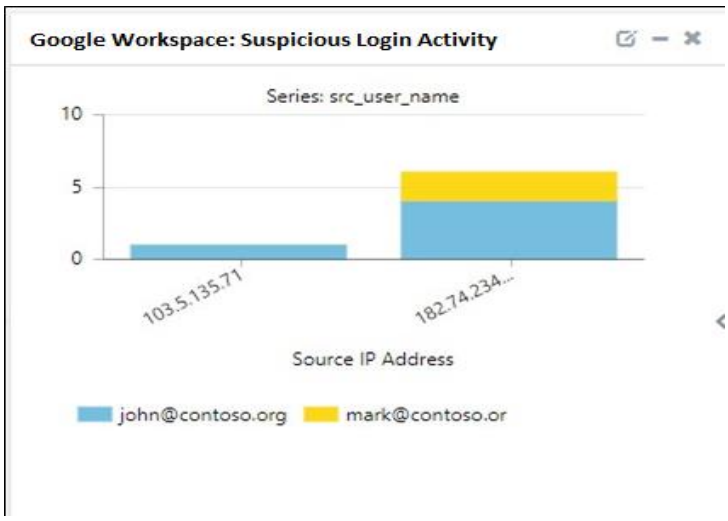


4.4 Dashboards

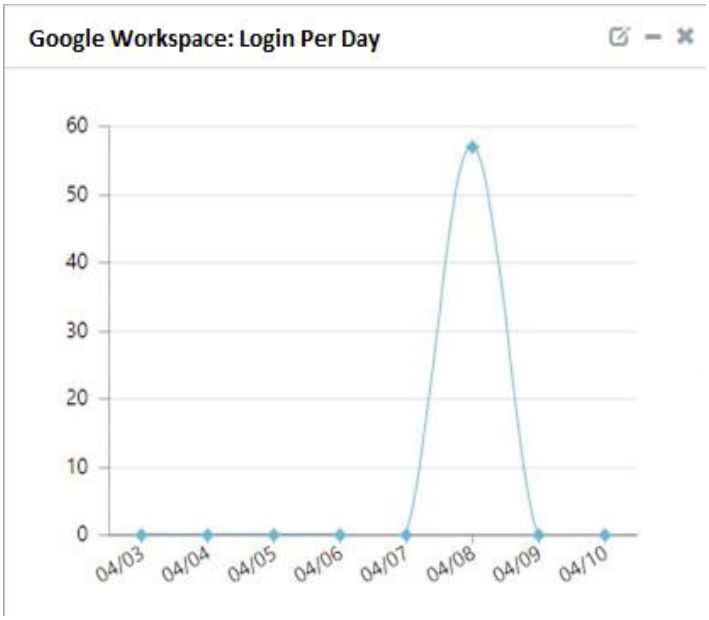
- **Google Workspace: Login and Logout Events**



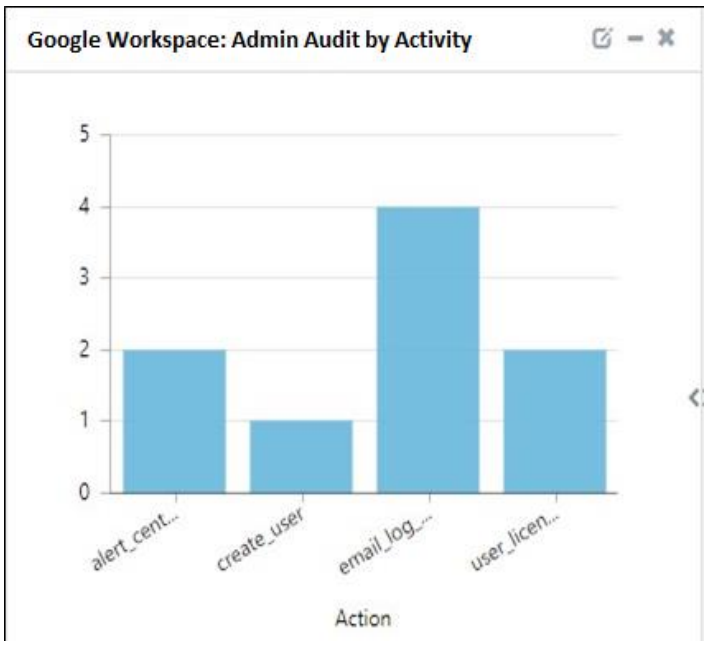
- **Google Workspace: Suspicious Login Activity**



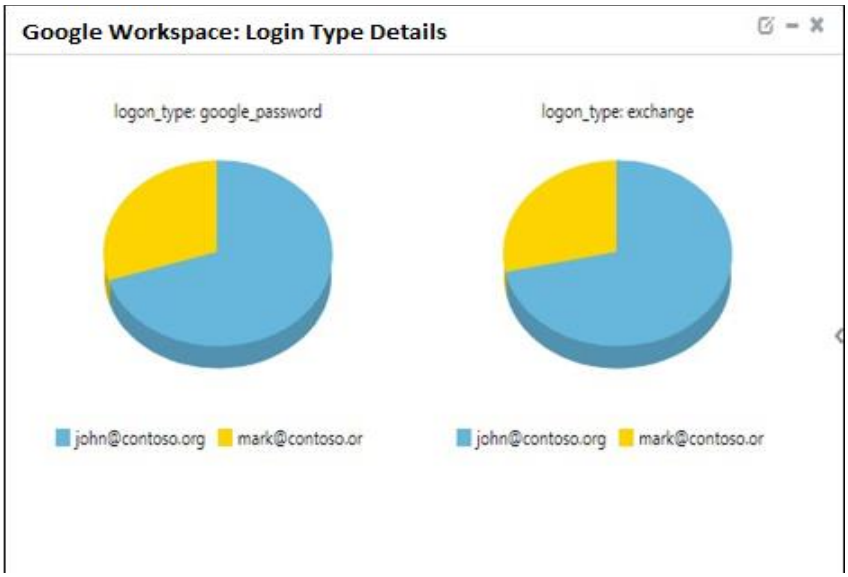
- **Google Workspace: Login Per Day**



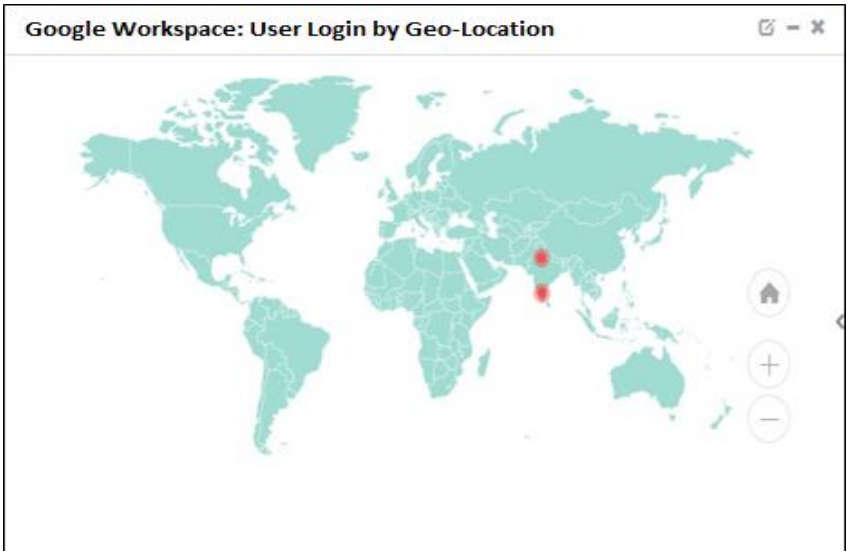
- **Google Workspace: Admin Audit by Activity**



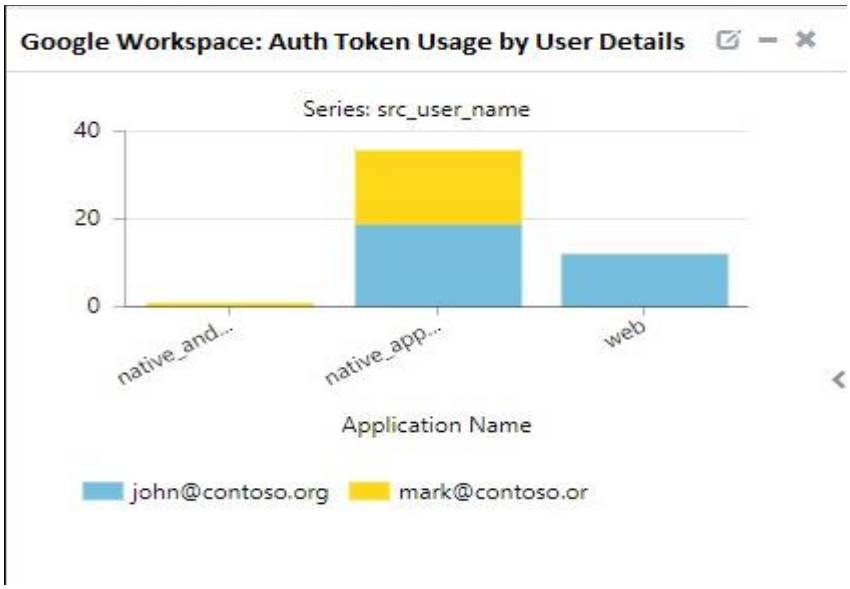
- **Google Workspace: Login Type Details**



- **Google Workspace: User Login by Geo-Location**



- **Google Workspace: Auth Token Usage by User Details**



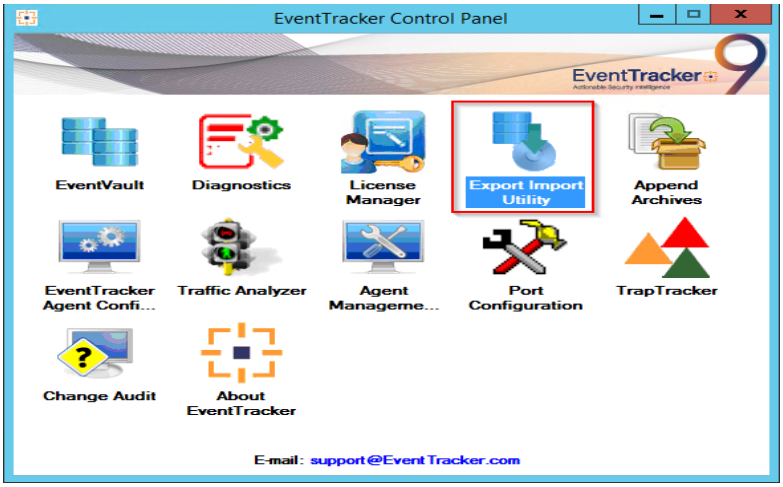
5. Importing Google Workspace knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object

- Report
- Dashboard

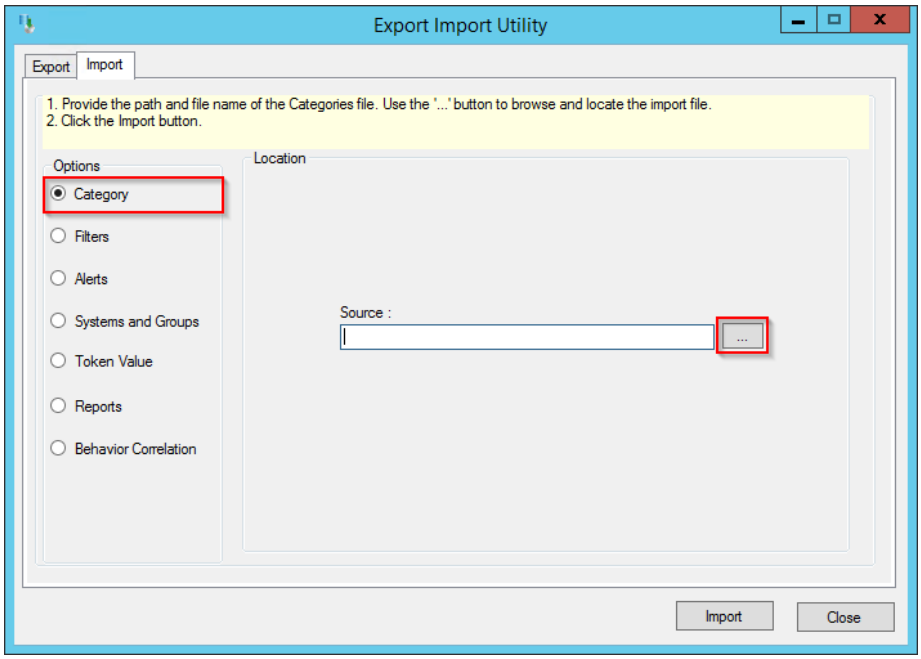
1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

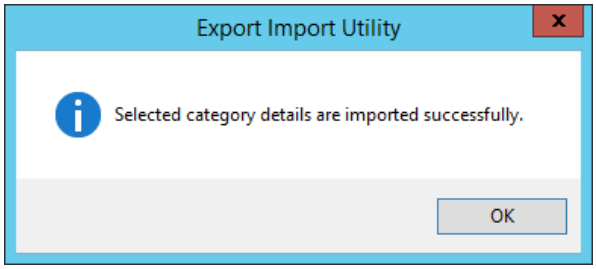
5.1 Category

1. Click **Category** option, and then click the Browse ... button.



2. Locate **Category_Google Workspace.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

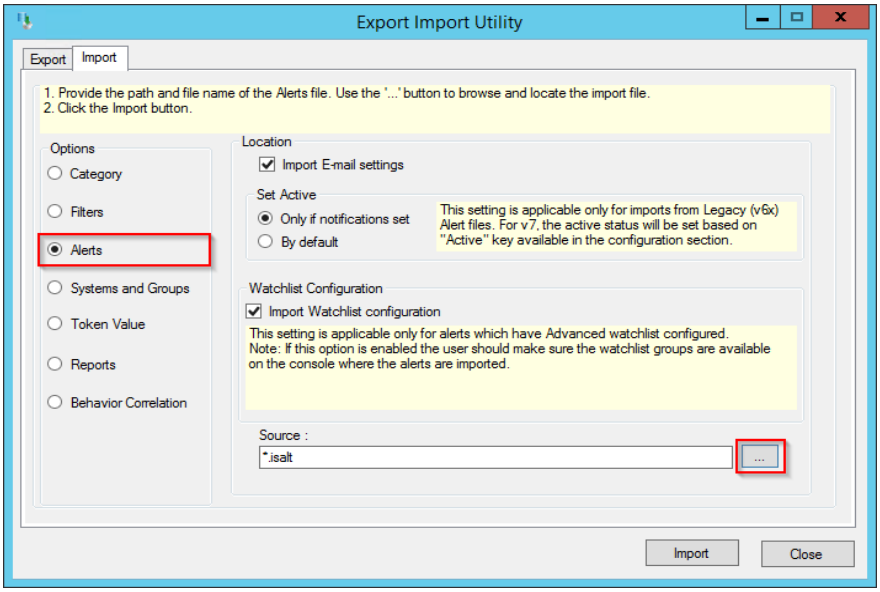
EventTracker displays success message.



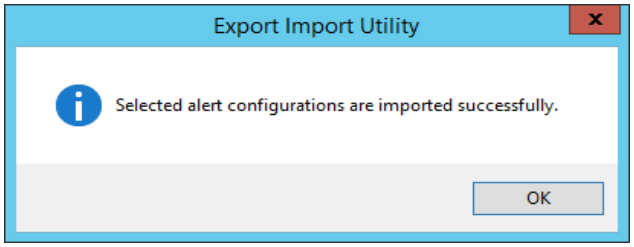
4. Click **OK,** and then click the **Close** button.

5.2 Alert

1. Click **Alert** option, and then click the **Browse** ... button.



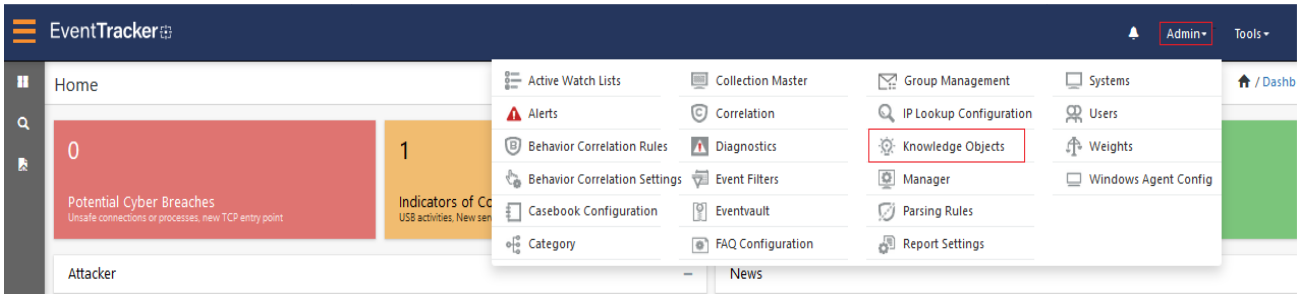
2. Locate **Alert_Google Workspace.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.



4. Click **OK**, and then click **Close**.

5.3 Knowledge Object

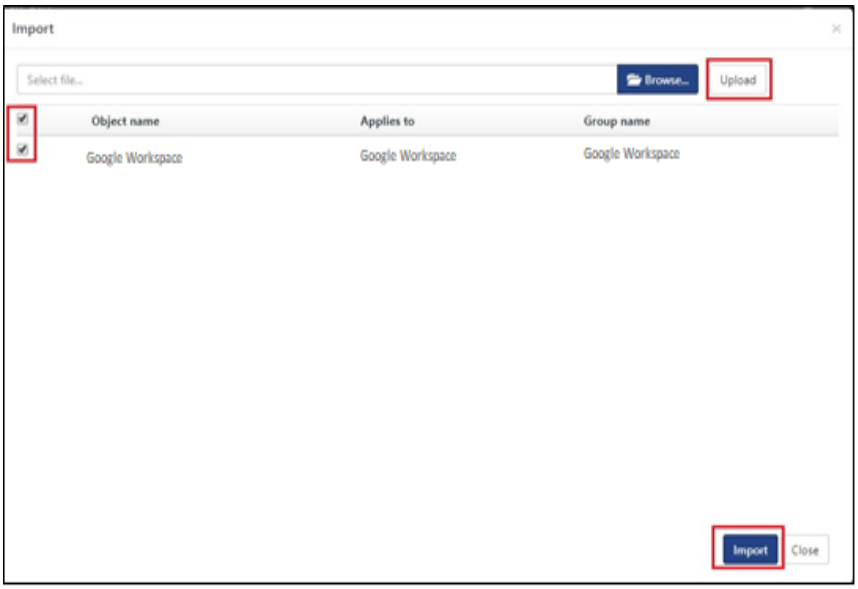
1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.



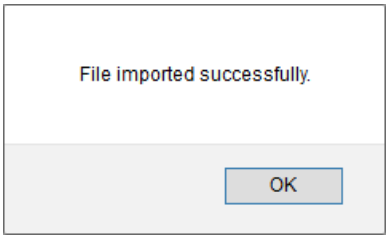
2. Click on **Import** button as highlighted in the below image:

3. Click on **Browse**.

4. Locate the file named **KO_Google Workspace.etko**.
5. Select the check box and then click on **Import** option.

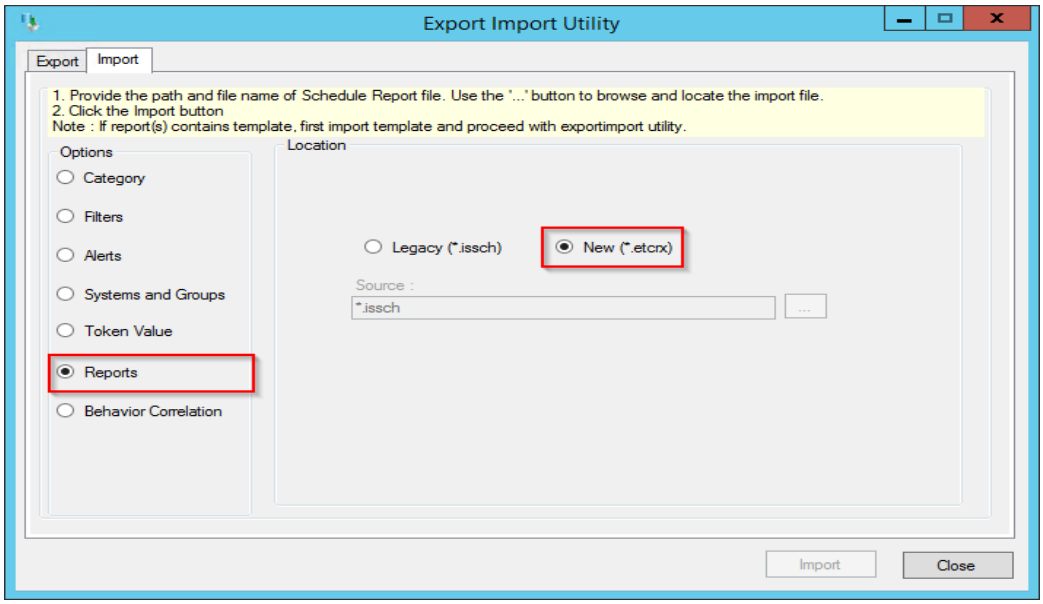


6. Knowledge objects are now imported successfully.

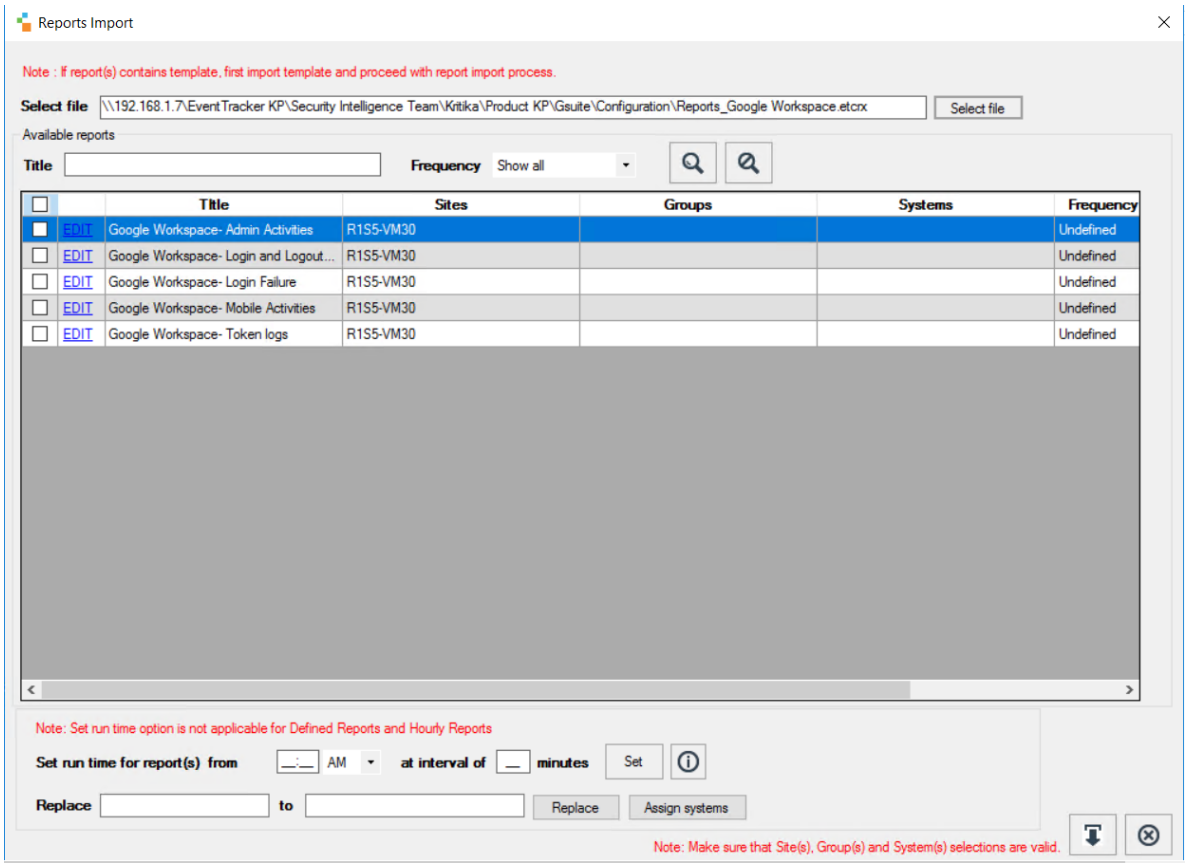


5.4 Report

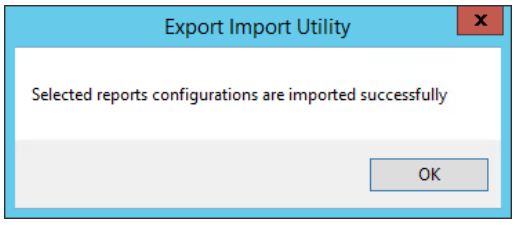
1. Click **Reports** option and select **New (*.etcrx)** option.



2. Locate the file named **Reports_ Google Workspace.etcrx** and select the check box.



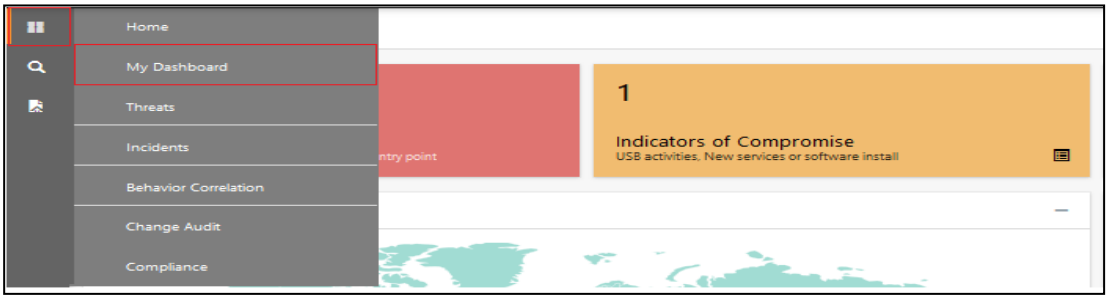
3. Click the **Import** button to import the report. EventTracker displays success message.



5.5 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

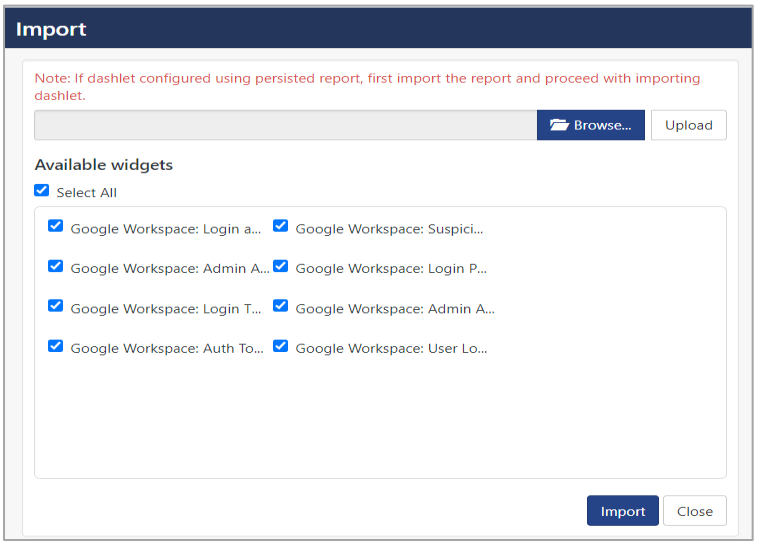
1. Open **EventTracker** in browser and logon.



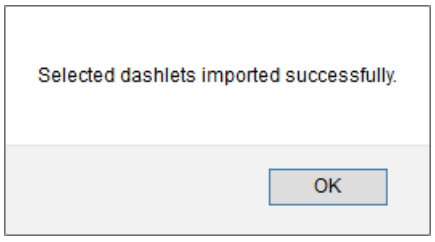
2. Navigate to **My Dashboard** option as shown above.

3. Click on the **Import** button as show below:

4. Import dashboard file **Dashboard_Google Workspace.etwd** and select **Select All** checkbox.
5. Click on **Import** as shown below:

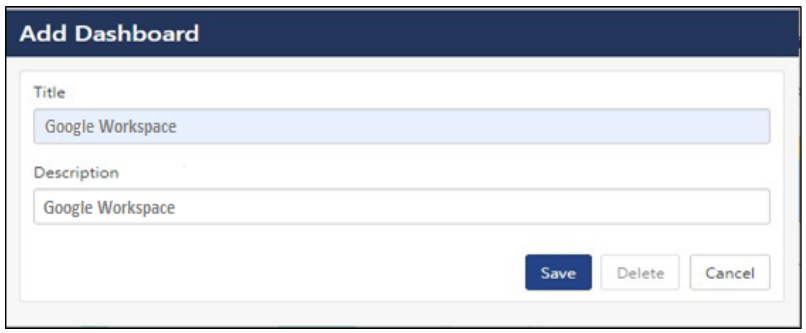


6. Import is now completed successfully.



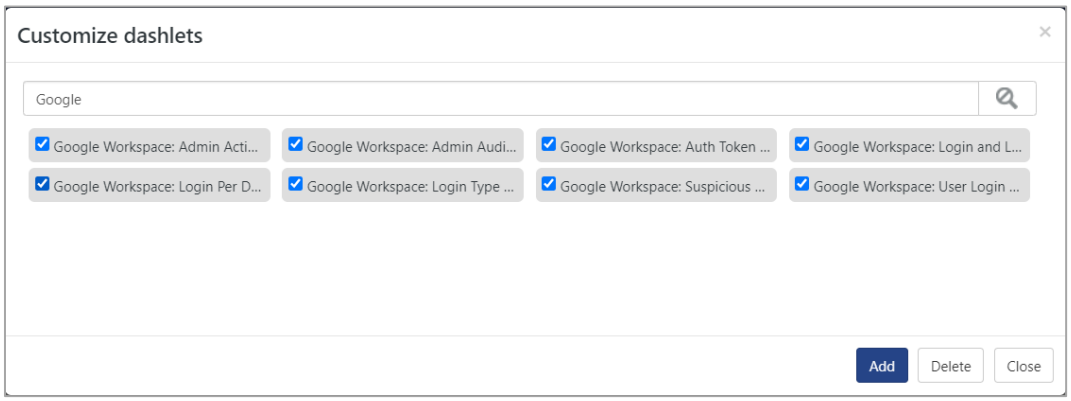
7. In **My Dashboard** page select ⊕ to add dashboard.

8. Choose appropriate name for **Title** and **Description**. Click **Save**.



9. In **My Dashboard** page select to add dashlets.

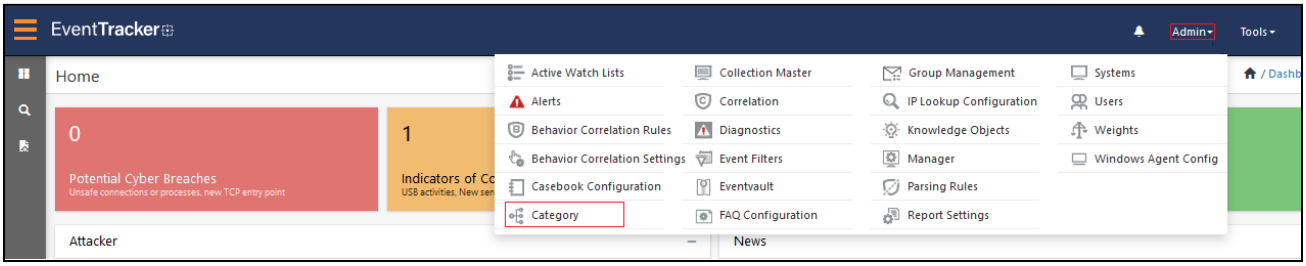
10. Select imported dashlets and click **Add**.



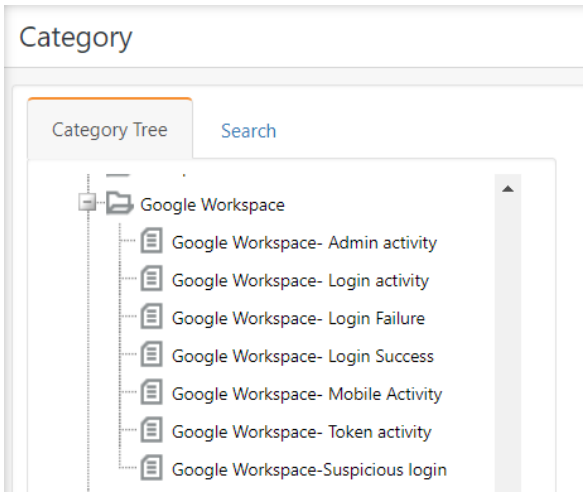
6. Verifying Google Workspace knowledge pack in EventTracker

6.1 Category

1. Logon to **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.

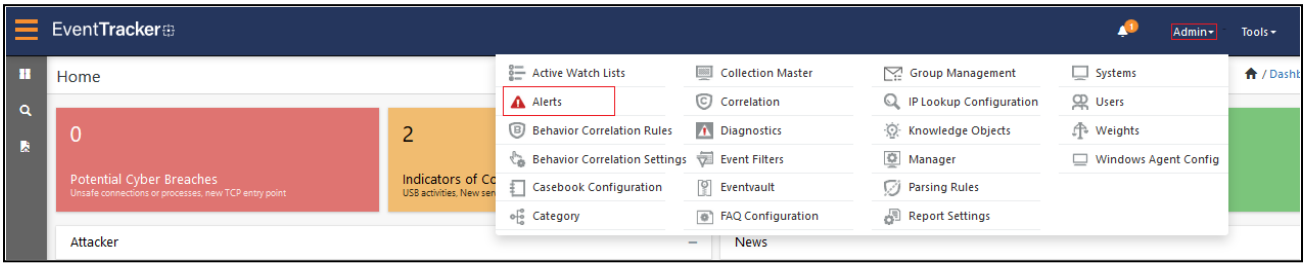


3. In **Category Tree** to view imported category, scroll down and expand **Google Workspace** group folder to view the imported category.

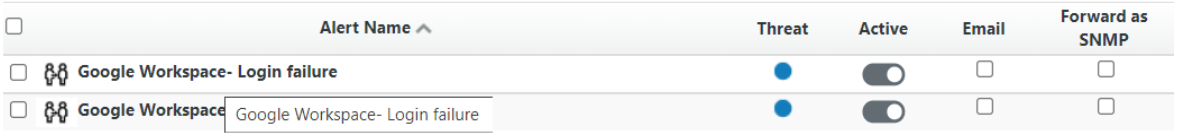


6.2 Alert

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

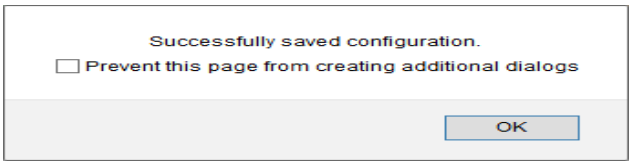


3. In the **Search** box, type **Google Workspace**, and then click the **Go** button.
   Alert Management page will display the imported alert.



4. To activate the imported alert, toggle the **Active** switch.

   EventTracker displays message box.

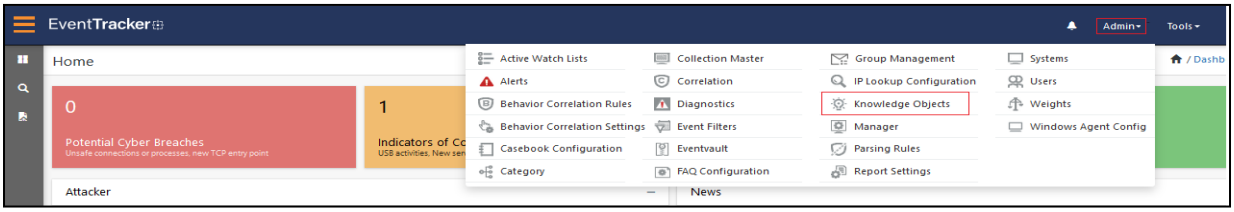


5. Click **OK**, and then click the **Activate Now** button.

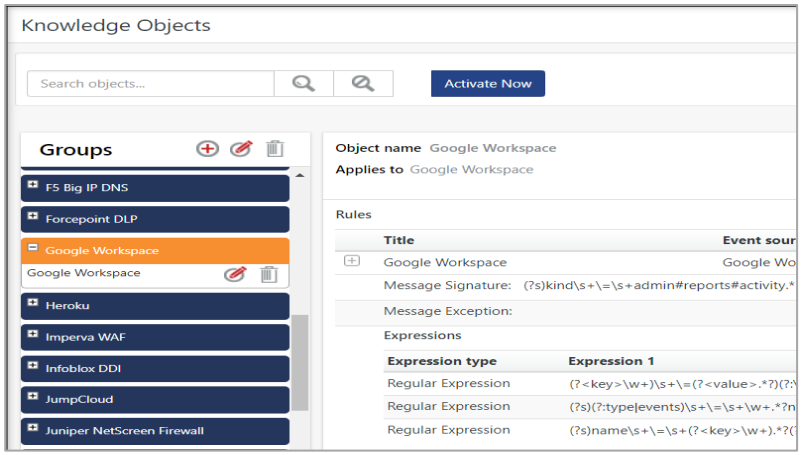
NOTE: Please specify appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects.**



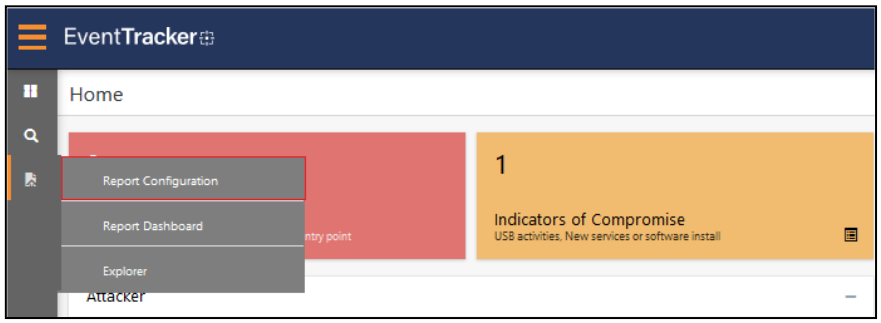
2. In the Knowledge Object tree, expand **Google Workspace** group folder to view the imported knowledge object.



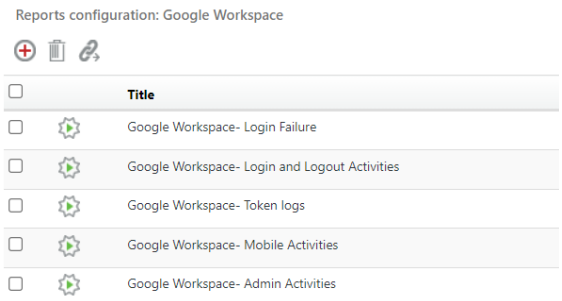
3. Click **Activate Now** to apply imported knowledge objects.

6.4 Report

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

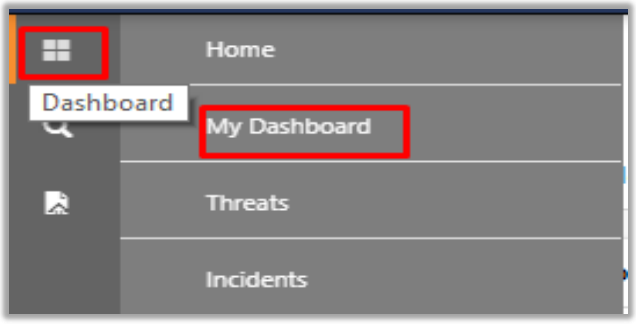


2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Google Workspace** group folder to view the imported reports.

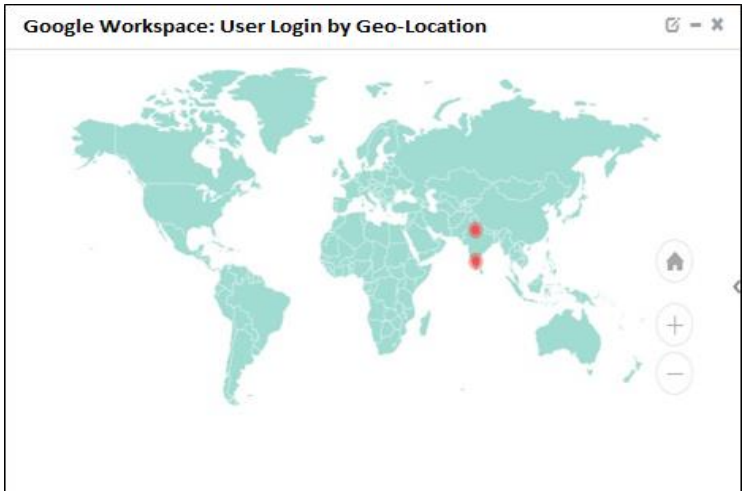


6.5 Dashboards

1. In the EventTracker web interface, Click on Home Button and select **My Dashboard**.



2. In the **Google Workspace** dashboard you will see the following screen.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

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

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support