

Integration Guide

Integrating Google Workspace with EventTracker

EventTracker 9.2x and Above

Publication Date:

August 3, 2021

© Copyright Netsurion. All Rights Reserved.

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

Τa	able of	Contents	3
1.	Ove	view	4
2.	Prer	equisites	4
3.	Inte	grating Google Workspace with EventTracker	4
	3.1	Creating Google Workspace Application for API access	4
	3.2	Integrating Google Workspace to EventTracker	11
4.	Evei	ntTracker Knowledge Pack	13
	4.1	Category	13
	4.2	Alert	14
	4.3	Report	14
	4.4	Dashboards	16
5.	Imp	orting Google Workspace knowledge pack into EventTracker	19
	5.1	Category	20
	5.2	Alert	21
	5.3	Knowledge Object	22
	5.4	Report	23
	5.5	Dashboards	24
6.	Veri	fying Google Workspace knowledge pack in EventTracker	26
	6.1	Category	26
	6.2	Alert	27
	6.3	Knowledge Object	28
	6.4	Report	28
	6.5	Dashboards	29
	About	Netsurion	30
	Conta	t Us	30

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.**



 Search projects and folders Q, 	
RECENT ALL	
lame	ID
Contoso.org	0

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

Search folders		
ne	ID	
Reputeen arg	0	
Hild Contoso.org	Ū	
	SELECT	CANCEL

6. Click **Create**.



	-	
4	You have 11 projects remaining in your quota. Request projects. <u>Learn more</u>	an increase or delete
	MANAGE QUOTAS	
Projecti	Name *	
Eventtra	acker-Logger	0
Project	ID: eventtracker-logger. It cannot be changed later. EDIT	
_ Loc	ation*	
💼 Co	ntoso.org	BROWSE
Parent	organization or folder	

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

Select a project	NEW PROJECT
Search projects and folders	
RECENT ALL	
Name	ID
✓ 🐤 Eventtracker-Logger 🔞	eventtracker-logger
	CANCEL OPEN

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

	Google APIs : Eventtra	cker-Logger 🔻	Q	
API	APIs & Services	APIs & Services + ENABLI	LE APIS AND SERVICES	
ب	Dashboard	• You don't have any APIs available	le to use yet. To get started, click "Enable APIs and services" or go to the <u>API libra</u>	ſΥ
0-	Credentials			

9. Search for Admin SDK in search tab.



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

=	Google APIs Seventte	racker-Logger 🔻	٩
<	API Library		
		Admin SDK Google Admin SDK lets administrators of enterprise domains to view and manage resources like user, ENABLE TRY THIS API	
	Type APIs & services Last updated 1/10/19, 2:03 AM Category G Suite Service name admin googleapis.com	Overview Admin SDK lets administrators of enterprise domains to view and manage resources like of provides audit and usage reports of domain. About Google Google's mission is to organize the world's information and make it universally accessible products and platforms like Search, Maps, Gmail, Android, Google Play, Chrome and You'n meaningful role in the daily lives of billions of people. Cutorials and documentation Learn more L ² Terms of service	user, groups etc. It also and useful. Through ube, Google plays a
		By using this product you agree to the terms and conditions of the following license(s): Go Service L^2 , Google Apps Admin APIs L^2	ogle APIs Terms of



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

	Google APIs : Eventtracke	er-Logger 🔻
API	APIs & Services >	redentials + CREATE CREDENTIAL Delete
Ť	Support	Library s compatible with this API
Θ	IAM & admin >	Credentials in APIs & Services
	Billing	
2	Google Maps >	

12. Select OAuth consent screen.

Before your users authenticate, this consent screen will allow	them to choose	About the consent screen
whether they want to grant access to their private data, as wel link to your terms of service and privacy policy. This page confi consent screen for all applications in this project.	l as give them a igures the	The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.
Application type		
Public Any Google Account can grant access to the scopes required by thi	ie app.	OAuth verification To protect you and your users, your consent screen
Internal		and application may need to be verified by Google. Verification is required if your app is marked as Public and at least one of the following is true:
only users with a badge Account in your organization can grant ac requested by this app.	cess to the scopes	 Your app uses a sensitive and/or restricted
Application name 💿 The name of the app asking for consent		 Your app displays an icon on its OAuth consent screen
Powershell-logger		 Your app has a large number of authorized domains
Application loga 🛞 An image on the consent acreen that will help users recognize your app		 You have made changes to a previously- verified OAuth consent screen
Local file for upload	Browse	The verification process may take up to several weeks, and you will receive email updates as it processes. Learn more about verification
Supportemail @		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.
Shawn an the cansent screen for user support	*	Let us know what you think about our OAuth experience.
Scopes for Google APIs		
f you add a sensitive scope, such as scopes that give you full access to Google will verify your consent screen before it's published.	Gmail ar Drive,	
email		
email profile		

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

Ξ				
7	API ^	Scope	Description	
		email	View your email address	
		profile	View your basic profile info	
		openid	Know who you are on Google	
🖌 🔒	Admin SDK	/auth/admin.reports.audit.readonly	View audit reports for your G Suite domain	
🗹 🔒	Admin SDK	/auth/admin.reports.usage.readonly	View usage reports for your G Suite domain	
O Canne	ot find a scope? Only	scopes for enabled APIs are listed above. To	add a missing scope please visit the Google AP	F

- 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.

OAuth to u	e Authorized Domains. Your applications' links must be hosted on Authorize
Domains. L	earn more
example	com
Type in the	domain and press Enter to add it
Application	I Homepage link
Shown on t	he consent screen. Must be hosted on an Authorized Domain.
ena nu an	
https://	er http://
https:// e	x http://
https:// (pr http://
https:// (pr http:// Privacy Policy link
https:// of Application	pr http:// Privacy Policy link he consent screen. Must be hosted on an Authorized Domain.
Application Shown on t	or http:// I Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. or http://
Application Shown on the https:// (pr http:// I Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. pr http://
Application Shown on t https:// (pr http:// Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. pr http://
https:// (Application Shown on t https:// (Application	or http:// Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. or http:// Terms of Service link (Optional)
Application Shown on the https:// (Application Shown on the shown on	or http:// Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. or http:// Terms of Service link (Optional) he consent screen. Must be hosted on an Authorized Domain.
https:// (Application Shown on t https:// (Application Shown on t https:// (or http:// Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. or http:// Terms of Service link (Optional) he consent screen. Must be hosted on an Authorized Domain. or http://
https:// (Application Shown on t https:// (Application Shown on t https:// (or http:// I Privacy Policy link he consent screen. Must be hosted on an Authorized Domain. or http:// I Terms of Service link (Optional) he consent screen. Must be hosted on an Authorized Domain. or http://

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.

API APIs & Services	Credentials	Crestentials								
Dashboard	Oredentials OAuth consent sorten Domain verification	Ziedemials OAurh consern soven Comain verification								
iiii Library	Crana crustemata 🔹 Debra									
o- Credentiala	Inter andretitalit to access your enabled APIs. For more information, set the submittation documentation.									
	OAuth 2.0 client IDs									
	Name	Creation date ~	Туре	Client ID						
	Eventracker-logger Peb 11, 2019 Web application apps googlessersonem com									

Client ID	for Web application	2 DOWNLOAD JSON	C RESET SECRET	TELETE					
Client ID	ZwerefihEadfdffdfiiek54	41er1sdf33412dfsq.apps.goog	leusercontent.com						
Client secret	Client secret adda da fa i a h dfu an flau u a a dfal								
Creation date	Creation date Feb 11, 2019, 1:10:31 PM								
Name @									
Eventtracker-logge	d								
Restrictions									
Enter JavaScript origin	s, redirect URIs, ar both Learn Mare								
Origins and redirect do	mains must be added to the list of Auth	orized Domains in the OAuth consent s	settings.						
Authorized JavaS For use with reque (https://*.example in the origin URI.	cript origins sts from a browser. This is the origin UR com) or a path (https://example.com/s	ti of the client application. It can't contain subdir). If you're using a nonatandard po	n a wildcard ort, you must include it						
https://www.ex	ample.com								
Type in the domain	n and press Enter to add it								
Authorized redire For use with reque suthenticated with Cannot contain UF	ct URIs ate from a web server. This is the path in Google. The path will be appended wit 1L fragments or relative pathe. Cannot b	n your application that users are redirects In the authorization code for access. Mu e a public IP address.	ed to after they have ust have a protocol.						
ht	tp://localhost:5432		ĩ						
https://www.ex	ample.com								
Type in the domain	n and press Enter to add it								
and the second se									

- 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.

Help				
(i About				
How-To Guide				
Organisation				
Client Id				
Client Secret				
	Get Author	ization Code		
	Finish	Cancel	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.

Note: Latest integrator version is 3.0.1

Sig	n in		
to continue	to Et-logger		
Email or phone			
Forgot email?			
Create account		Next	
English (United Kingdom) 👻	Help	Privacy	Term



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

G Sign in with Google			
	e 		
To continue, first verify that it's you			
Enter your password			
Show password			
Forgot password?		Next	
English (United Kingdom) 👻	Help	Privacy	Terms

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

Sign in - Google accounts Inttps://accounts.google.com/signin/oauth/consent?authuser=0∂ <a href="https://accounts.google.com/signin/oauth/consent?authuser=0&part</th> <th></th> <th></th>		
 https://accounts.google.com/signin/oauth/consent?authuser=0&part. fsign in with Google fL-logger wants to access your Coogle Account fsign in with Blow Et-logger to: fis will allow Et-logger to: fwe usage reports for your G Suite domain f View usage reports for your G Suite domain f fue usage reports for your G Suite domain f fue usage reports for your G Suite domain f fue usage reports for your G Suite domain f fue usage reports for your G Suite domain f fue usage reports for your G suite domain f fue usage reports for your G suite domain f fue usage reports for your G suite domain f fue usage reports for your G suite domain f fue usage reports for your G suite domain f fue usage reports for your G suite domain f f	ign in – Google accounts	× [+
<section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header>	C 🗅 https://a	accounts.google.com/signin/oauth/consent?authuser=0∂ ᡬ₀ ᡬ≡
 Is given in the Google Is given in the Google Accounts Is conclusted accounts 		
 g sign with Google G Sign with Google G Coogle Account Definition of the sign of the sign		
 g sign in with Google G Laboration Status for access syours access in your cost of a cost		
 G Sign in with Google Et-logger wants to access your Cocle Account Cocle Account Allow 		
<section-header><section-header> Etablic Coccession Support Immediate independent Immediate independent independent independent Immediate independent independent independent independent Immediate independent independent independent Immediate independent independent independent independent independent Immediate independent independent independent independent Immediate independent independent independent Immediate independent independent Immediate independent independent Immediate independent</section-header></section-header>		G Sign in with Google
Et-logger wants to access your Concelled Account Immediate accession Immediate accession <		
Google Account Intersection <!--</td--><td></td><td>Et-logger wants to access your</td>		Et-logger wants to access your
 intridecontinuity of the construction of the construction		Google Account
This will allow Et-logger to: View audit reports for your G Suite domain View usage reports for your G Suite domain View usage reports for your G Suite domain View usage reports for your G Suite domain View usage reports for your G Suite domain View usage reports for your G Suite domain Make sure that you trust Et-logger Make sure that you frust genstitive info with this site or app. Find out how Et-logger will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account. Find out about the risks Cancel Allow 		(hundrig out in the purch
 View audit reports for your G Suite domain View usage reports for your G Suite domain View usage reports for your G Suite domain Make sure that you trust Et-logger Mu may be sharing sensitive info with this site or app. Find out how Et-logger will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account. Find out about the risks Cancel Allow English (United Kingdom) • Heip Privacy Tems		This will allow Et-logger to:
 View usage reports for your G Suite domain Make sure that you trust Et-logger Make sure that you trust Et-logger Toy may be sharing sensitive info with this site or app. Find out how Et-logger will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account. Find out about the risks Cancel Allow 		• View audit reports for your G Suite domain
Make sure that you trust Et-logger You may be sharing sensitive info with this site or app. Find out how Et-logger will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account. Find out about the risks Cancel Allow English (United Kingdom) Help Privacy Terms		 View usage reports for your G Suite domain
You may be sharing sensitive info with this site or app. Find out how Et-logger will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account. Find out about the risks Cancel Allow English (United Kingdom) Help Privacy Terms		Make sure that you trust Et-logger
Find out about the risks Cancel Allow English (United Kingdom) - Help Privacy Terms		You may be sharing sensitive info with this site or app. Find out how Et-logger will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.
Cancel Allow English (United Kingdom) - Help Privacy Terms		Find out about the risks
English (United Kingdom) - Help Privacy Terms		Cancel Allow
	1	English (United Kingdom) - Help Privacy Terms



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

Google Workspace	integrator		×
Organisatio	njet	-	
Client	Information	X	
Client Secr			
	Credential validated successfully		
	ОК		

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

Google Workspace	Integrator		-		×			
Help								
Organisation	ET							
Client Id								
Client Secret								
	Get Authorization Code							
	Finish	Cancel						

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@NTPLxxxxx	Gsuite	kind = admin#reports#activity	admin	USER	C02ab3xxh	gurmukh@secintelkp.	EMAIL_SETTING	182.74.xxx.xxx
		хх		id =				com	S	
04/08/2020 02:36:36 PM	3230	SECINTELKP@NTPLxxxxx	Gsuite	kind = admin#reports#activity	admin	USER	C02ab3xxh	gurmukh@secintelkp.	EMAIL_SETTING	182.74.xxx.xxx
		хх		id =				com	S	
04/08/2020 02:36:36 PM	3230	SECINTELKP@NTPLxxxxx	Gsuite	kind = admin#reports#activity	admin	USER	C02ab3xxh	gurmukh@secintelkp.	ALERT_CENTER	103.5.xxx.xx
		хх		id =				com	1.35	

• **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@NTPLxxxxxxxx	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@NTPLxxx xxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	gurmukh@secintelkp.co m	182.74.xx.xx	google_password	login_failure
04/08/2020 02:36:27 PM	3230	SECINTELKP@NTPLxxx xxx	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@NTPLxxx xxx	Gsuite	kind = admin#reports#activity id =	login	C02ab3xxh	kritika@secintelkp.com	182.74.xx.xx	google_password	login_failure

Logs Considered



+- EMAIL LOG SEARCH	
+- C02ab3xxh	
+- admin	
+- 0	
+- Secintelkp@NTPLDT8LR47	
+- 4/8/2020 2:36:36 PM	
+ - 1586336796	
kind = admin#reports#activity	
id =	
time = 2020-04-07107:37:26.536Z	
uniqueQualifier = -6589978975782430249	
applicationName = admin	
customerid = C02ab3xxh	
etag = "JDMC8884sebSczDxOtZ17ClssbQ/rWs9OohLoCT_2pvG-LzZWdn3Ttg	t)
actor =	
callerType = USER	
email = gurmukh@secintelkp.com	
profileld = 107834143658212145163	
ipAddress = 182.74.234.198	
events =	
type = EMAIL_SETTINGS	
name = EMAIL LOG SEARCH	
parameters =	
name = EMAIL LOG SEARCH START DATE	
value = 2020/04/06 07:00:00 UTC	

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.

4	Export Import Utility	 2	x
Export Import	Export Import Utility e of the Categories file. Use the '' button to browse and locate the import file. Location Source :		x
Behavior Correlation	Import	Close	

- 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.

Export Import Utility						
xport Import						
1. Provide the path and file n 2. Click the Import button.	ame of the Alerts file. Use the '' butto	n to browse and locate the import file.				
Options	Location					
Category	Import E-mail settings					
	Set Active					
O Filters	 Only if notifications set 	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on				
 Alerts 	○ By default	"Active" key available in the configuration section.				
O Systems and Groups	Watchlist Configuration					
O Talvas Valua	 Import Watchlist configuration 	n				
	This setting is applicable only for	alerts which have Advanced watchlist configured.				
O Reports	on the console where the alerts	are imported.				
O Bahaurian Completion						
	Source :					
	*.isalt					
		Import Close				

- 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.

≡	EventTracker					🐥 🛛 Admin-	Tools 🕶
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	1 Diagnostics	💮 Knowledge Objects		
~			🗞 Behavior Correlation Settings	🔁 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	🧭 Parsing Rules		
				FAQ Configuration	Report Settings		
	Attacker			– News			

2. Click on Import \mathbb{T} button as highlighted in the below image:

	Knowledge Obj	ects		🕈 / Admin / Knowledge Objects
Q R	Search objects	Q	Q Activate Now	Objects 🕀 📳 🏦 🌣
	Groups	+		L
	E Cylance			
	• EventTracker			

3. Click on Browse.



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



Import)
Select file			🚍 Browse_ Upload	
8	Object name	Applies to	Group name	
	Google Workspace	Google Workspace	Google Workspace	
			Import	lose

6. Knowledge objects are now imported successfully.



5.4 Report

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

Note : If report(s) contains terr	plate, first import template and proceed with exportimport utility.
Options	Location
 Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation 	C Legacy (*issch) New (*.etcrx) Source : *issch

2. Locate the file named Reports_Google Workspace.etcrx and select the check box.

	reports					
e	This		Frequency Show all	• • • •	Contamp.	5
	I Tie	min Activities	B1S5J/M20	Groups	Systems	Undefined
EDI	DIT Google Workspace- Lo	nin and Longet	B1S5-VM30			Undefined
	DIT Google Workspace-Lo	gin Failure	R1S5-VM30			Undefined
ED	DIT Google Workspace- Mo	bile Activities	R1S5-VM30			Undefined
EDI	DIT Google Workspace- To	ken logs	R1S5-VM30			Undefined

3. Click the Import I 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.

11				
٩	My Dashboard			
R			1	
	Incidents	ntry point	Indicators of Compromise US8 activities, New services or software install	
	Behavior Correlation			_
	Change Audit			_
	Compliance		The second second	

2. Navigate to My Dashboard option as shown above.



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



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

				Browse	Unload
vailable widgets					
Google Workspace: Lo	gin a 🗹 (Google Workspac	e: Suspici		
Google Workspace: Ac	dmin A 🗹 🤇	Google Workspac	e: Login P		
Google Workspace: Lo	gin T 🗹 (Google Workspac	e: Admin A		
Google Workspace: Au	uth To 🗹 🤇	Google Workspac	e: User Lo		
☑ Google Workspace: Au	uth To 🗹 (Google Workspac	te: User Lo		

6. Import is now completed successfully.

Selected dashlets impo	orted successfully.
	ОК

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



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

Title	
Google Workspace	
Description	
Google Workspace	

9. In **My Dashboard** page select ^(a) to add dashlets.

	👚 / Dashboard / My Dashboar
d Microsoft	⊕ ⊘ © ‡ ∓ ⊚
	d Micr Microsoft

10. Select imported dashlets and click Add.

ustomize dashlets			
Google			Q
Google Workspace: Admin Acti	Google Workspace: Admin Audi	Google Workspace: Auth Token	Google Workspace: Login and L
Google Workspace: Login Per D	Google Workspace: Login Type	Google Workspace: Suspicious	Google Workspace: User Login
			Add Delete Cl

6. Verifying Google Workspace knowledge pack in EventTracker

6.1 Category

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

≡	Event Tracker ⊕					🔶 Admin-	Tools -
-	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashi
0			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects		
~			🗞 Behavior Correlation Settings	🔛 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
		-	eteropy Category	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Category		
Category Tree	Search	
	e Workspace pogle Workspace- Admin activity pogle Workspace- Login activity pogle Workspace- Login Failure pogle Workspace- Login Success pogle Workspace- Mobile Activity pogle Workspace- Token activity pogle Workspace-Suspicious login	

6.2 Alert

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

	Event Tracker ⊕						🔎 🛛 Admin 🗸	Tools -
	Home		Active Watch Lists		Collection Master	Group Management	Systems	🕈 / Dashi
٩		_	Alerts		Correlation	🔍 IP Lookup Configuration	🕰 Users	
	0	2	Behavior Correlation	on Rules	Diagnostics	· Knowledge Objects	T Weights	
			🇞 Behavior Correlatio	on Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configu	iration	Eventvault	🧭 Parsing Rules		
			₀-[° Category		FAQ Configuration	Report Settings		
	Attacker				- News			

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

Alert Name A	Threat	Active	Email	Forward as SNMP
🗌 ନ୍ଦୁର୍ଣ୍ଣ Google Workspace- Login failure	•			
Google Workspace Google Workspace- Login failure	•			

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

EventTracker displays message box.

Successfully saved configu	ration. dditional dialogs
	ОК

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.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	C Correlation	🔍 IP Lookup Configuration	였 Users	
	0	1	Behavior Correlation Rules	Diagnostics	·@- Knowledge Objects		
.			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	Parsing Rules		
		_	o-[o Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

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

Knowledge Objects		
Search objects	Activate Now	
Groups 🕀 🧭 📋 🛛 Ot	oject name Google Worksp	ace
F5 Big IP DNS	plies to Google Workspace	
Forcepoint DLP	les	
	Title	Event sour
Google Workspace	Google Workspace	Google Wo
	Message Signature: (?	's)kind\s+\=\s+admin#reports#activity.*
Heroku	Message Exception:	
Imperva WAF	Expressions	
Infoblox DDI	Expression type	Expression 1
	Regular Expression	(? <key>\w+)\s+\=(?<value>.*?)(?:</value></key>
JumpCloud	Regular Expression	(?s)(?:type events)\s+\=\s+\w+.*?n
Juniper NetScreen Firewall	Regular Expression	(?s)name\s+\=\s+(? <key>\w+).*?(</key>

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**.

≡	Event Tracker ⊕			
	Home			
Q 	 Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer			
	Апаскег			-

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



Repo	rts configu	ration: Google Workspace
+	Ē 2,	
		Title
	1	Google Workspace- Login Failure
	£3	Google Workspace- Login and Logout Activities
	£3	Google Workspace- Token logs
		Google Workspace- Mobile Activities
	£\$3	Google Workspace- Admin Activities

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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

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