

Google Workspace Integration - Elastic

Google Workspace Integration

The Google Workspace integration collects and parses data from the different [Google Workspace audit reports APIs](#)(external, opens in a new tab or window).

If you want to know more about how you can fully leverage the Google Workspace integration, there is a multipart blog from our Security Labs that will help you:

1. To understand what Google Workspace is in [Part One - Surveying the Land](#)(external, opens in a new tab or window)
2. To set it up, step by step, in [Part Two - Setup Threat Detection with Elastic](#)(external, opens in a new tab or window)
3. And to use the collected information to your advantage in [Part Three - Detecting Common Threats](#)(external, opens in a new tab or window)

Compatibility

It is compatible with a subset of applications under the [Google Reports API v1](#)(external, opens in a new tab or window). As of today it supports:

Google Workspace Service	Description
SAML (external, opens in a new tab or window) help (external, opens in a new tab or window)	View users' successful and failed sign-ins to SAML applications.
User Accounts (external, opens in a new tab or window) help (external, opens in a new tab or window)	Audit actions carried out by users on their own accounts including password changes, account recovery details and 2-Step Verification enrollment.
Login (external, opens in a new tab or window) help (external, opens in a new tab or window)	Track user sign-in activity to your domain.

Google Workspace Service	Description
Rules(external, opens in a new tab or window) help(external, opens in a new tab or window)	View a record of actions to review your user's attempts to share sensitive data.
Admin(external, opens in a new tab or window) help(external, opens in a new tab or window)	View administrator activity performed within the Google Admin console.
Drive(external, opens in a new tab or window) help(external, opens in a new tab or window)	Record user activity within Google Drive including content creation in such as Google Docs, as well as content created elsewhere that your users upload to Drive such as PDFs and Microsoft Word files.
Groups(external, opens in a new tab or window) help(external, opens in a new tab or window)	Track changes to groups, group memberships and group messages.
Group Enterprise(external, opens in a new tab or window) help(external, opens in a new tab or window)	The Group Enterprise activity report returns information about various types of Enterprise Groups Audit activity events.
Device(external, opens in a new tab or window) help(external, opens in a new tab or window)	The Mobile activity report returns information about various types of Device Audit activity events.
Token(external, opens in a new tab or window) help(external, opens in a new tab or window)	The Token activity report returns information about various types of OAuth Token Audit activity events.
Access Transparency(external, opens in a new tab or window) help(external, opens in a new tab or window)	The Access Transparency activity report returns information about various types of Access Transparency activity events.
Context Aware Access(external, opens in a new tab or window) help(external, opens in a new tab or window)	The Context Aware Access activity report returns information about various types of Context-Aware Access Audit activity events.
GCP(external, opens in a new tab or window)	The GCP activity report returns information about various types of Google Cloud Platform activity events.

Requirements

In order to ingest data from the Google Reports API you must:

- Have an *administrator account*.
- [Set up a ServiceAccount\(external, opens in a new tab or window\)](#) using the administrator account.
- [Set up access to the Admin SDK API\(external, opens in a new tab or window\)](#) for the ServiceAccount.
- [Enable Domain-Wide Delegation\(external, opens in a new tab or window\)](#) for your ServiceAccount.

This integration will make use of the following *oauth2 scope*:

- `https://www.googleapis.com/auth/admin.reports.audit.readonly`

Once you have downloaded your service account credentials as a JSON file, you are ready to set up your integration.

Click the Advanced option of Google Workspace Audit Reports. The default value of "API Host" is `https://www.googleapis.com`. The API Host will be used for collecting `access_transparency`, `admin`, `device`, `context_aware_access`, `drive`, `gcp`, `groups`, `group_enterprise`, `login`, `rules`, `saml`, `token` and `user accounts` logs.

“ NOTE: The `Delegated Account` value in the configuration, is expected to be the email of the administrator account, and not the email of the ServiceAccount.

Google Workspace Alert

The [Google Workspace\(external, opens in a new tab or window\)](#) Integration collects and parses data received from the Google Workspace Alert Center API using HTTP JSON Input.

Compatibility

- Alert Data Stream has been tested against `Google Workspace Alert Center API (v1)`.
- Following Alert types have been supported in the current integration version:
 1. Customer takeout initiated
 2. Malware reclassification
 3. Misconfigured whitelist
 4. Phishing reclassification
 5. Suspicious message reported
 6. User reported phishing
 7. User reported spam spike
 8. Leaked password
 9. Suspicious login
 10. Suspicious login (less secure app)
 11. Suspicious programmatic login
 12. User suspended
 13. User suspended (spam)
 14. User suspended (spam through relay)
 15. User suspended (suspicious activity)
 16. Google Operations
 17. Configuration problem
 18. Government attack warning
 19. Device compromised
 20. Suspicious activity

21. AppMaker Default Cloud SQL setup
22. Activity Rule
23. Data Loss Prevention
24. Apps outage
25. Primary admin changed
26. SSO profile added
27. SSO profile updated
28. SSO profile deleted
29. Super admin password reset
30. Account suspension warning
31. Calendar settings changed
32. Chrome devices auto-update expiration warning
33. Customer takeout initiated
34. Drive settings changed
35. Email settings changed
36. Gmail potential employee spoofing
37. Mobile settings changed
38. New user added
39. Reporting Rule
40. Suspended user made active
41. User deleted
42. User granted Admin privilege
43. User suspended (spam)
44. User's Admin privileges revoked
45. Users password changed
46. Google Voice configuration problem detected

Requirements

In order to ingest data from the Google Alert Center API, you must:

- Have an *administrator account*.
- [Set up a ServiceAccount\(external, opens in a new tab or window\)](#) using the Administrator Account.
- [Set up access to the Admin SDK API\(external, opens in a new tab or window\)](#) for the ServiceAccount.
- [Enable Domain-Wide Delegation\(external, opens in a new tab or window\)](#) for the ServiceAccount.

This integration will make use of the following *oauth2 scope*:

- `https://www.googleapis.com/auth/apps.alerts`

Once Service Account credentials are downloaded as a JSON file, then the integration can be setup to collect data.



NOTE: The `Delegated Account` value in the configuration, is expected to be the email of the administrator account, and not the email of the ServiceAccount.

NOTE: The default value of the "Page Size" is set to 1000. This option is available under 'Alert' Advance options. Set the parameter "Page Size" according to the requirement. For Alert Data Stream, The default value of "Alert Center API Host" is `https://alertcenter.googleapis.com`. The Alert Center API Host will be used for collecting alert logs only.

Logs

Google Workspace Reports ECS fields

This is a list of Google Workspace Reports fields that are mapped to ECS that are common to all data sets.

Google Workspace Reports	ECS Fields
<code>items[].id.time</code>	<code>@timestamp</code>
<code>items[].id.uniqueQualifier</code>	<code>event.id</code>
<code>items[].id.applicationName</code>	<code>event.provider</code>
<code>items[].events[].name</code>	<code>event.action</code>
<code>items[].customerId</code>	<code>organization.id</code>
<code>items[].ipAddress</code>	<code>source.ip</code> , <code>related.ip</code> , <code>source.as.*</code> , <code>source.geo.*</code>
<code>items[].actor.email</code>	<code>source.user.email</code> , <code>source.user.name</code> , <code>source.user.domain</code>
<code>items[].actor.profileId</code>	<code>source.user.id</code>