Google Workspace Artifact Reference Guide

SANS DFIR

This reference guide provides a list of log events that are worth reviewing when investigating Google Workspace incidents. The availability of some events may be limited based on your subscription edition.

Admin Log Events

- Admin privileges grant
- 2-step verification
- User creation
- Data export initiated
- Change recovery email
- Enable non-admin user password recovery
- Add privilege
- Assign role
- Add application to allowlist
- All third-party API access unblocked
- Delegated admin privileges grant

Gmail Log Events

- Attachment download
- Attachment link click
- Link click
- Open
- Send
- Autoforward
- Late spam classification
- User spam classification

Drive Log Events

- Download
- Edit
- Delete
- Trash
- Script trigger created
- Owner changed
- Owner changed from parent folder
- Change document visibility
- Shared drive settings change
- User sharing permissions change
- Change access scope
- Change ACL editors
- Change document visibility
- Change shared drive membership
- Change user access from parent folder

OAuth Log Events

- API call
- Request
- Grant
- Revoke
- Deny

Chat Log Events

- Attachment downloaded
- Attachment uploaded
- Direct message started
- Invite accept
- Room member added

Takeout Log Events

- User completed a takeout
- User downloaded a takeout
- User initiated a takeout
- User scheduled takeout(s)

User Accounts Log Events

Sign-in Activity

- Failed login
- Leaked password
- Login challenge
- Login verification
- Logout
- Sensitive action allowed
- Successful login
- Suspicious login
- Suspicious login (less secure app)
- Suspicious programmatic login
- User signed out due to suspicious session cookie

Settings Changes

- Out of domain email forwarding enabled
- 2-step verification disable
- 2-step verification enroll
- Account password change
- Account recovery email change
- Account recovery phone change

User suspended

- User suspended (spam through relay)
- User suspended (spam)
- User suspended (suspicious activity)