Google Workspace Security Investigation tool

Retrieved on: 24-02-2022
Retrieved from: https://support.google.com/a/topic/7563358?hl=en&ref_topic=7492529
Compiled by: Abdul Shareef Pallivalappil, Assistant Professor Digital Forensics, JAIN (Deemed-to-be University), JC Road, Bangalore

As a super administrator, you can use the security investigation tool to identify, triage, and take action on security and privacy issues in your domain.

For example, you can use the investigation tool to:

- Access data about devices.
- Access device log data to get a clear view of the devices and applications being used to access your data.
- Access data about Gmail messages, including email content.
- Access Gmail log data to find and erase malicious emails, mark emails as spam or phishing, or send emails to users' inboxes.
- View search results that list suspended users.
- Access Drive log data to investigate file sharing in your organization, investigate the creation and deletion of documents, investigate who accessed documents, and more.

To run a search with the investigation tool:

- Sign in to your Google Admin console.

  Sign in using an *administrator account*.

1. On the Admin console home page, go to Security - Investigation tool.
2. Choose a data source for your search. For example, choose Device log events, Devices, Drive log events, or Gmail log events.
   Note: Available data sources will vary depending on your Google Workspace edition.
3. Click ADD CONDITION.
   You can include one or more conditions in your search. For details about conditions that are available for each data source, see the sections below. You also have the option to customize your search with *nested queries*—searches with 2 or 3 levels of conditions (for details, see the section below).
4. Click SEARCH.

Note: If you narrow the date range for your search, your results will appear in the investigation tool sooner. For example, if you narrow the search to events that happened in the last week, the query will return faster than if you search without restricting the query to a shorter period of time.

Investigate file sharing

(Supported editions for this feature: Enterprise; Education Standard and Plus.)

As an administrator, you might need to search for a sensitive document that's been shared externally, or shared too broadly.

Follow the instructions in this article to investigate a file that's been shared externally by a specific user in your organization.

Get started with your investigation

1. Sign in to use the investigation tool.
2. From the Data source menu, click Drive log events.
3. Click ADD CONDITION.
4. From the Condition menu, click Visibility change.
5. Make sure the condition is set to External.
6. Click ADD CONDITION.
7. From the Condition menu, click Actor.
8. In the User field, enter the username of the user who shared the file—for example, *user@example.com*.
9. Click ADD CONDITION.
10. From the Condition menu, click Date.
11. Change the condition to After.
12. In the Date field, enter the earliest date and time when the file may have been shared externally.
13. Click SEARCH.

After you finish the above steps, the search results are displayed in a table at the bottom of the page. The table displays the date and time the file was shared externally, the document ID, document type, visibility, the title, the event type (for example, *Change user access*), the actor's username, and the owner of the document.

Customize your search with nested queries

When customizing your search in the investigation tool, you can include one or more conditions in your search. If you're customizing a search that has at least 2 conditions, you also have the option to create *nested queries*—in other words, searches that include 2 or 3 levels of conditions.

Using nested queries enables you to narrow your search by specifying queries that are much more granular and that are targeted to specific types of events. Do this by clicking Add condition group while customizing your search.

For example, you might want to run a search about inbound emails in your organization to investigate users who are receiving attachments. Additionally, you might want to narrow your search by including only users who are opening those attachments *or* clicking links within the emails. When customizing your search, you would base the search on the *Gmail log events* data source, and you would set up the following conditions for your search:

- The email must have an attachment.
- AND the user must either open the attachment OR click a link in the email.

Note: Most data sources enable 3-level nested queries. The *Users* data source enables only 2-level nested queries, while the *Chrome browsers* data source doesn't enable nested queries.

Data sources & conditions in the investigation tool

Device log events

Supported editions: Enterprise, Education, Cloud Identity Premium

Condition		
Date	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Device ID	• Is • Is not	Type a value in the *Device ID* field.
Event	• Is • Is not	Choose from the following: • Account registration change • Device compliance status • Device OS update • Work profile support • Device settings change • Device compromise • Failed password attempts • Suspicious activity • Device application change • ADB events • Screen lock events • Device ownership change • Network event • Device action event
Device owner	• Is • Is not • Contains • Does not contain	Type a value in the Device owner field (valid email address).
Device type	• Is • Is not	Choose from the following: • Android • iOS • Mac • Windows • Chrome OS
Device model	• Is • Is not • Contains • Does not contain	Type a value in the *Device mode*l field.

Failed password attempts	• Equals • Less than or equal to • Greater than or equal to	Type a number in the *Numeric value* field.
Device compromised state	• Is • Is not	Choose from the following: • Compromised • Not compromised
Device property	• Is • Is not	Choose from the following: • Device Model • Serial Number • IMEI Number • MEID Number • WiFi MAC Address • Device Policy App Privilege • Manufacturer • Device Brand • Device Hardware • Bootloader Version
Device setting	• Is • Is not	Choose from the following: • Developer Options • Unknown Sources • USB Debugging • Verify Apps
Application SHA-256 hash	• Is • Is not	Type a value in the *SHA-256 hash* field.
Application ID	• Is • Is not	Type a value in the *Application ID* field.
Application state	• Is • Is not	Choose from the following: • Installed • Uninstalled • Updated
Account state	• Is • Is not	Choose from the following: • Registered • Unregistered
Register privilege	• Is	Choose from the following:

	• Is not	• Device Administrator • Device Owner • Profile Owner
Device ownership	• Is • Is not	Choose from the following: • Company Owned • User Owned
New device ID	• Is • Is not	Type a value in the *Device ID* field.
Resource ID	• Is • Is not	Type a value in the *Resource ID* field.
Serial number	• Is • Is not	Type a value in the *Serial number* field.
iOS vendor ID	• Is • Is not	Type a value in the *iOS vendor ID* field.
Domain	• Is • Is not • Contains • Does not contain	Type a value in the *Domain* field.
Device compliance state	• Is • Is not	Choose from the following: • Compliant • Non-compliant
OS property	• Is • Is not	Choose from the following: • OS version • Build number • Kernel version • Baseband version • Security patch • Device bootloader
Actor organizational unit	• Is	Choose an organizational unit from the list.

Devices

Supported editions: Enterprise, Education, Cloud Identity Premium

Condition		
Device ID	• Is • Is not	Type a value in the *Device ID* field.
Device owner	• Is • Is not	Type a value in the *Device owner* field (valid email address).
Device type	• Is • Is not	Choose from the following: • Android • iOS • Mac • Windows • Chrome OS
Device model	• Is • Is not	Type a value in the *Device model* field.
Status	• Is • Is not	Choose from the following: • Pending • Running • Blocked • Wiping • Wiped • Unprovisioned • Account Wiping • Account Wiped • Registered • Unregistered • Deactivated • Approved
Last sync date	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Device compromised state	• Is • Is not	Choose from the following: • Compromised • Not compromised
Password status	• Is • Is not	Choose from the following: • On

		• Off
Management type	• Is • Is not	Choose from the following: • None • Basic • Advanced
Security patch update	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Registered date	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Carrier	• Is • Is not	Type a value in the *Carrier* field.

Drive log events

Supported editions: Enterprise Plus, Education

Condition		
Date	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Document ID	• Is • Is not	Type a value in the *Document ID* field.
Title	• Is • Is not • Contains • Does not contain	Type a value in the *Title* field.
Document type	• Is • Is not	Choose from the following: • Google Document • Google Spreadsheet • Google Presentation • Folder • Google Form • Google Drawing • Shared drive • Text file • JPEG • PDF • PNG • MP4 • Microsoft Word

		• Microsoft Excel • HTML • MPEG • Quicktime • Microsoft Powerpoint • Google Sites
Prior visibility	• Is • Is not	Choose from the following: • Private • Shared internally • People within domain with link • Public in the domain • Shared externally • People with link • Public on the web
Visibility	• Is • Is not	Choose from the following: • Private • Shared internally • People within domain with link • Public in the domain • Shared externally • People with link • Public on the web
Event	• Is • Is not	Choose from the following: • Create • Upload • Edit • View • Rename • Move • Add to folder • Remove from folder • Trash • Delete • Remove from trash • Download • Preview • Print • Change owner • Change ACL editors • Change access scope • Change document visibility • Change user access • Change shared drive membership

Actor	• Is • Is not • Contains • Does not contain	Enter a value for *Actor* field (user email address). Note: The actor is the user that triggered an event by modifying a file.
Owner	• Is • Is not • Contains • Does not contain	Type a username in the *Owner* field.
Target	• Is • Is not • Contains • Does not contain	Type a value in the *Target* field. Note: The target is the user or group that was added or removed from a file.
Visibility change	• Is • Is not	Choose from the following: • Internal • External • None
IP address	• Is • Is not • Contains • Does not contain	Type a value in the *IP address* field.
Domain	• Is • Is not • Contains • Does not contain	Type a value in the *Domain* field.
Actor organizational unit	• Is	Choose an organizational unit from the list.

About the visibility of files in a shared drive

In your My Drive folder, a file that's only visible to the owner has a visibility of *Private*. However, In a shared drive, even if a file is not explicitly shared with other users, it has a visibility of *Shared internally* (shared drive files cannot have a visibility of *Private*).

Gmail log events

Supported editions: Enterprise Plus, Education

Condition		
Date	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Message ID	• Is • Is not	Type a value in the *Message ID* field.
Subject	• Is • Is not • Contains • Does not contain	Type a value in the *Subject* field.
Event	• Is • Is not	Choose from the following: • Admin quarantine • Attachment download • Attachment link click • Attachment save to Drive • Autoforwarded • Drive item save to Drive • Late spam classification • Link click • Mark unread • Move out of trash • Move to inbox • Move to trash • Open • Receive • Release from quarantine • Reply • Send • User spam classification
From (Header address)	• Is • Is not • Contains • Does not contain	Type an address in the *From (Header address)* field.
From (Envelope)	• Is • Is not • Contains • Does not contain	Type an address in the *From (Envelope)* field.
To (Envelope)	• Is • Is not • Contains	Type an address in the *To (Envelope)* field.

	• Does not contain	
Owner	• Is • Is not • Contains • Does not contain	Type a username in the *Owner* field.
Domain	• Is • Is not • Contains • Does not contain	Type a name in the *Domain* field.
Has attachment	• Is • Is not	Choose from the following: • True • False
Attachment hash	• Is • Is not	Type a value in the *SHA-256 hash* field.
Attachment name	• Is • Is not • Contains • Does not contain	Type a name in the *Attachment name* field.
Attachment malware family	• Is • Is not	Choose from the following: • Known malicious program • Virus/worm • Content may be harmful • Potentially unwanted • Other
IP Address	• Is • Is not • Contains • Does not contain	Type a value in the *IP address* field.
From (Header name)	• Is • Is not • Contains • Does not contain	Type a name in the *From (Header name)* field.
Sender domain	• Is • Is not • Contains • Does not contain	Type a name in the *Sender domain* field.
Link domain	• Is • Is not	Type a name in the *Link domain* field.

	• Contains • Does not contain	
Attachment extension	• Is • Is not • Contains • Does not contain	Type an extension in the *Attachment extension* field.
SPF domain	• Is • Is not • Contains • Does not contain	Type a name in the *SPF domain* field.
DKIM domain	• Is • Is not • Contains • Does not contain	Type a name in the *DKIM domain* field.
Traffic source	• Is • Is not	Choose from the following: • External • Internal
Spam classification	• Is • Is not	Choose from the following: • Clean (not classified as spam, phishing, suspicious, or malware) • Spam • Phishing • Suspicious • Malware
Spam classification reason	• Is • Is not	Choose from the following: • Custom Rule • Default • Past User Action • Suspicious Content • Suspicious Link • Suspicious Attachment • Type • DMARC • Domain in Public RBLs • RFC Violation • GMAIL Policy Violation • Machine Learning Verdict • Sender Reputation • Blatant Spam • GMAIL Safety Setting
Geo location	• Is	Type a value in the *Geo location* field.

	• Is not • Contains • Does not contain	
OAuth project ID	• Equals • Less than or equal to • Greater than or equal to	Type a value for the *Oauth project ID*.
Target link URL	• Is • Is not • Contains • Does not contain	Type a value for the *Target link URL*.
Target attachment hash	• Is • Is not	Type a value for the *Target attachment hash*.
Target attachment name	• Is • Is not	Type a value for the *Target attachment name*.
Target attachment malware family	• Is • Is not	Choose from the following: • Content may be harmful • Known malicious program • Other • Potentially unwanted • Virus/worm
Target drive ID	• Is • Is not • Contains • Does not contain	Type a value for the *Target drive ID*.

Gmail messages

Supported editions: Enterprise Plus, Education

Condition		
Subject	• Is • Is not	Type a subject in the *Subject* field.
Message ID	• Is • Is not	Type a value in the *Message ID* field.
Date	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Sender	• Is	Type a sender in the *Sender* field.

	• Is not	
Recipient	• Is • Is not	Type a recipient in the *Recipient* field.
Label	• Is • Is not	Choose from the following: • Inbox • Trash • Spam • Unread • Starred • Phishing • Admin quarantine
Attachment name	• Is • Is not	Type an attachment name in the *Attachment name* field.
Has attachment	• Is • Is not	Choose from the following: • True • False
Cc	• Is • Is not	Type a valid email address in the *Cc* field.
Bcc	• Is • Is not	Type a valid email address in the *Bcc* field.
All content	• Contains word • Does not contain word	Type a value in the *All content* field.
Message size	• Greater than or equal to • Less than or equal to	Type a value in the *Message size* field.
	•	

Rule log events

Supported editions: Enterprise, Education, Cloud Identity Premium

Condition	**Operator**	
Actor	• Is • Is not • Contains	Enter a value for *Actor* (user email address).

	• Does not contain	
Data source	• Is • Is not	Choose from the following: • Device • Drive • Gmail • User
Date	• Before • After	Type a date in the Date field. Use the following format: YYYY-MM-DDThh:mm:ss
Detector ID	• Is • Is not • Contains • Does not contain	Type a domain name in the *Detector ID* field.
Detector name	• Is • Is not • Contains • Does not contain	Type a domain name in the *Detector name* field.
Event	• Is • Is not	Choose from the following: • Action complete • Rule trigger
Recipient	• Is • Is not • Contains • Does not contain	Type a domain name in the *Recipient* field.
Resource ID	• Is • Is not	Enter a value in the *Resource ID* field.
Resource owner	• Is • Is not • Contains • Does not contain	Enter a value in the *Resource owner* field.
Resource title	• Is • Is not • Contains	Enter a value in the *Resource title* field.

	• Does not contain	
Resource type	• Is • Is not	Choose from the following: • Device • Document • Email • User
Rule ID	• Is • Is not	Enter a value in the *Rule ID* field.
Rule name	• Is • Is not • Contains • Does not contain	Enter a value in the *Rule name* field.
Rule type	• Is • Is not	Choose from the following: • Activity Rule • DLP
Scan type	• Is • Is not	Choose from the following: • Drive continuous scan • Drive single resource scan
Severity	• Is • Is not	Choose from the following: • High • Low • Medium
Suppressed action	• Is • Is not	Choose from the following: • Alert • Device account wipe • Device approve • Device block • Device cancel account wipe • Device cancel wipe • Device wipe • Drive block external sharing • Drive delete permission • Drive disable download, print, and copy for commenters and viewers • Drive insert permission • Drive update permission

		• Drive warn on external sharing • Gmail change envelope recipient • Gmail mark as phishing • Gmail mark as spam • Gmail modify headers • Gmail modify route • Gmail modify subject • Gmail quarantine • Gmail reject • Gmail restore • Gmail send to inbox • Gmail soft delete • User delete • User reset password • User restore • User suspend
Trigger	• Is • Is not • Contains • Does not contain	Enter a value in the *Trigger* field.
Triggered action	• Is • Is not	Choose from the following: • Alert • Device account wipe • Device approve • Device block • Device cancel account wipe • Device cancel wipe • Device wipe • Drive block external sharing • Drive delete permission • Drive disable download, print, and copy for commenters and viewers • Drive insert permission • Drive update permission • Drive warn on external sharing • Gmail change envelope recipient • Gmail mark as phishing • Gmail mark as spam • Gmail modify headers • Gmail modify route • Gmail modify subject • Gmail quarantine • Gmail reject • Gmail restore • Gmail send to inbox • Gmail soft delete • User delete

		• User reset password • User restore • User suspend
Triggering client IP	• Is • Is not • Contains • Does not contain	Enter a value in the *Triggering client IP* field.
Triggering user email	• Is • Is not • Contains • Does not contain	Enter a value in the *Triggering user email* field.
Actor organizational unit	• Is	Choose an organizational unit from the list.

User log events

Supported editions: Enterprise, Education, Cloud Identity Premium

Condition		
Affected user	• Is • Is not • Contains • Does not contain	Type a user in the *Affected user* field. Note: • Only include the *Affected user* filter in your search for system actions taken on a user account. • Include the *User* filter in your search to set the filter to the user account that you're investigating.
Challenge types	• Is • Is not	Choose from the following: • Backup code (user is asked to enter a backup verification code) • Google authenticator (user asked to enter OTP from authenticator app) • Google Prompt • IDV any phone (user is asked for a phone number and then enters a code sent to that phone) • IDV pre-registered phone • Internal two factor • Knowledge employee ID (user proves knowledge of employee ID) • Knowledge pre-registered email (uiser proves knowledge of pre-registered email) • Knowledge pre-registered phone (user proves knowledge of pre-registered phone)

		• Login location (user signs in from their usual login location) • None • Offline OTP (user enters OTP code they receive from settings on their Android phone) • Other • Security key (user passes the security key cryptographic challenge)
Date	• Before • After	Type a date in the Date field. Use the following format: YYYY-MM-DDThh:mm:ss
Domain	• Is • Is not • Contains • Does not contain	Type a domain name in the *Domain* field.
Event	• Is • Is not	Choose from the following: • Failed login • Leaked password • Login challenge • Login verification • Logout • Successful login • Suspicious login • Suspicious login (less secure app) • Suspicious programmatic login • User suspended • User suspended (spam through relay) • User suspended (spam) • User suspended (suspicious activity)
IP address	• Is • Is not • Contains • Does not contain	Type an IP address in the *IP address* field.
Is second factor	• Is • Is not	Choose from the following: • True • False
Is suspicious	• Is • Is not	Choose from the following: • True • False

Login time	• Before • After	Choose from the following: • Before • After
Login type	• Is • Is not	Choose from the following: • Exchange • Google password • Re-auth • SAML • Unknown
User	• Is • Is not • Contains • Does not contain	Type a value in the *User* field. Note: • Include the *User* filter in your search to set the filter to the user account that you're investigating. • Only include the *Affected user* filter in your search for system actions taken on a user account.
Actor organizational unit	• Is	Choose an organizational unit from the list.

Users

Supported editions: Enterprise, Education, Cloud Identity Premium

Condition		
Email	• Is • Is not	Type a valid email address in the *Email* field. Note: This address can match the primary email address or other email addresses of a user.
First name	• Is • Is not	Type a value in the *First name* field.
Last name	• Is • Is not	Type a value in the *Last name* field.
Last login	• Before • After	Type a date in the *Date* field. Use the following format: *YYYY-MM-DDThh:mm:ss*
Super administrator	• Is • Is not	Choose from the following: • True • False
Delegated administrator	• Is	Choose from the following:

	• Is not	• True • False
Enrolled in 2SV	• Is • Is not	Choose from the following: • True • False
2SV enforced for org	• Is • Is not	Choose from the following: • True • False
Suspended ID	• Is • Is not	Choose from the following: • True • False
Change password at login	• Is • Is not	Choose from the following: • True • False
Mailbox setup	• Is • Is not	Choose from the following: • True • False
Actor organizational unit	• Is	Choose an organizational unit from the list.

Meet log events

Supported editions: Enterprise Plus, Education

Condition		
Action description	• Is • Is not • Contains • Does not contain	Enter a description for the action.
Action reason	• Is • Is not	This search criteria includes the possible reasons for a user submitting an abuse report in Meet. Choose from the following: • Child endangerment • Fraud, phishing, and other deceptive practices • Harassment and hateful content

		• Malware (distributed via link in the chat window in Meet) • Other abuse type selected by the reporter • Spam or unwanted content • Unwanted sexual content • Violence and gore
Actor	• Is • Is not	Enter a value for *Actor*.
Actor name	• Is • Is not • Contains • Does not contain	Enter a value for *Actor name*.
Actor type	• Is • Is not	Choose from the following: • Email address • Meet hardware device ID • Phone number
Calendar event ID	• Is • Is not • Contain • Does not contain	Enter a value for *Calendar event ID*.
Call rating	• Equals • Less than or equal to • Greater than or equal to	Enter a value for *Call rating*.
City	• Is • Is not • Contains • Does not contain	Enter a value for *City*.
Client type	• Is • Is not	Choose from the following: • Android • Chromebase • Chromebox • Endpoint joining over the 3rd party system • iOS • Jamboard • Other device type • PSTN dial-in • PSTN dial-out

		• Web browser
Conference ID	• Is • Is not • Contains • Does not contain	Enter a value for *Conference ID*.
Country	• Is • Is not • Contains • Does not contain	Enter a value for *Country* (a 2-character ISO code).
Date	• Before • After	Enter a value for the date.
Duration	• Equals • Less than or equal to • Greater than or equal to	Enter a value for *Duration.*
Endpoint ID	• Is • Is not • Contains • Does not contain	Enter a value for *Endpoint ID.*
Event	• Is • Is not	Choose from the following: • Abuse report submitted • Endpoint left • Livestream watched
IP address	• Is • Is not • Contains • Does not contain	Enter a value for *IP address.*
Livestream view page ID	• Is • Is not • Contains • Does not contain	Enter a value for *Livestream view page ID*.
Meeting ID	• Is • Is not • Contains	Enter a value for *Meeting ID.*

	• Does not contain	
Actor organizational unit	• Is	Select an organizational unit from the list.
Organizer email	• Is • Is not • Contains • Does not contain	Enter a value for *Organizer email.*
Participant outside organization	• Is • Is not	Choose from the following: • True • False
Product type	• Is • Is not	Choose from the following: • Classic Hangouts • Hangouts Meet • Other
Target	• Is • Is not • Contains • Does not contain	Enter the target email for the action.
Target display names	• Is • Is not • Contains • Does not contain	Enter the target display names for the action.
Target phone number	• Is • Is not • Contains • Does not contain	Enter the target phone number for the action.