GAT+ Overview

Products Overview · https://gatlabs.com/knowledge/tech-tips/gat-overview/

GAT+ Overview video

Embedded media:

https://www.youtube.com/embed/gxnwBHPTqjU?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_lo

What is GAT+?

GAT+ is a third-party app developed for Google Workspace — It offers Super Admins powerful Google Workspace auditing and reporting for their domain.

GAT+ is an alternative to the '**Reports'** feature within the Admin console.

GAT+ is included in all our pricing plans, and it's the prerequisite tool for all other GAT products we offer.

When GAT+ is installed, it requires access to API permissions for each Google Workspace app *(Each Workspace app has its own set of API permissions.)*

GAT+ requires access to most of these permissions as it produces unique reports that are not found in the Admin console's Reports section.

****Prerequisite**: GAT+ needs to be installed from the Google Marketplace using a Google Super Admin account. Click here to learn more about the installation process.

****Availability:** We offer an automatic 15-day free trial for GAT+, for all domains.

If you've trailed GAT in the past and would like to run a fresh trial again, please enquire through this form.

Launching Apps

GAT Labs offers many products within different plans, you can access these products from the top right corner of **each** app.

That applies whether you're viewing the App Launcher from within GAT+, GAT Flow, or GAT Shield.

See Launching other Suite of Products from within GAT+ for more information.

Side Menu Layout

The GAT+ Side Menu hosts all of the sections within the GAT+ tool.

See User Profile Settings and Preferences for more information.

Audit and Management

The Audit and Management section is home to all of GAT+'s auditing areas:

Users

Users audit focuses on the following areas:

a. Basic tab – Overview of all users' key settings, like which OU they were in when they last signed in.

b. Drive tab, and Drive Productivity tab – Overview of all files users have access to, and how they're shared with different permissions.

The difference between the 'Drive tab' and 'Drive Productivity tab' is: The Drive tab covers all files a user owns or has access to. Whereas, The Drive Productivity tab only focuses on the files a user has created/uploaded directly onto their own "MyDrive".

c. File Types tab – Shows audited information on all the different file types, and who owns the most number of files for each file type.

d. Quota tab – How much Google Drive quota (file storage in megabytes) is being used by each user.

e. Security tab – Shows security risks and insights for each user, ex: if they have 2FA turned off and when they failed to log in.

f. Applications tab – Shows each 3rd Party App connected to a user's Google account — Apps can access different permissions from Google accounts.

g. Calendars tab – Shows each Calendar the user has access to, and the number of future events the user is participating in.

h. Devices tab – Summarises the number of smartphones or ChromeOS devices connected to the user's account.

i. Email Info tab – View Gmail settings in place for each user, see things like auto-forwarding policies, and if someone has given Gmail delegation access to other users.

j. Meet tab – Summary of Google Meet calls for each user.

k. Events tab – The events a user has taken in relation to security — These logs can show when a user changed their password or changed their 2FA enrolment.

Users Audit Use Case Examples

- How to Find the Space Used on Google Drive
- Google Drive Use Productivity Measured

Google Groups

a. Groups tab – In this tab, you'll see all Google Groups within your Workspace domain.

Each Group will be displayed in the result table. You can find any Google Group using many filtering parameters.

You can modify any Group's permissions or settings, see who is a member of that Group, or if a Group has members from outside your organization.

b. Group Members – In this tab, you'll be able to easily see which users are in certain Google Groups.

You can add or remove any user from an existing Group.

c. Events tab – Shows all actions taken on Group settings or membership. Examples of action history: "New user added", "User removed from Group", "New Group Created".

d. Last Used Address tab – GAT+ runs a metadata scan for each Google Group to audit the following:

- When an email was sent to the Group
- When a file was shared with the Group
- If Calendar events were sent to the Group
- When a user was last added to the Group

Based on that information you can easily decide if a Google Group is no longer needed.

Groups Audit Use Case Examples

- Manage Workspace Google Group Members
- Find Empty Google Groups and their Aliases – Last Used Address

Organization Units

a. Org. Units tab - This tab will show all the Org. Units of the domain. It lists the number of users in the Org unit and sub Org units.

Google Contacts

a. Contacts tab – This tab shows you all contacts across your entire organization — If they've been entered in contacts.google.com they'll appear in the Contacts audit.

You can apply search parameters to find any contact. You can take action on these contacts, whether it's to copy or delete them. You can also create contacts in users' accounts.

b. Domain Shared Contacts - This tab allows you to view, add or delete all Domain Shared Contacts

Contacts Audit Use Case Examples

- Google Contacts Management
- Create and Manage domain-shared contacts

Classroom

a. Classroom tab – You can view ALL Google Classrooms from this tab, i.e. Every single Classroom created by your Workspace domain users.

From here you can edit, delete or create any Google Classroom. You can also apply search parameters to find the Classroom you're looking for.

Below are Some actions that are usually taken in this tab:

- Adding or removing Co-teachers to a Classroom
- Adding or removing students from a Classroom
- Creating new Classrooms
- Editing details of existing Classrooms

b. Classwork tab – The Classwork tab lists every assignment and question created by teachers within Google Classrooms. From this tab, you can generate a report about all the work teachers have created for students.

c. Classwork Submissions tab – This tab shows all of the responses submitted by students to assigned assignments.

This tab covers all of the answers given by students. You can identify which students have not submitted any work for a particular assignment.

d. Teachers tab – Shows all Classrooms where a teacher is a participant. Whether that Classroom is Archived or Active. You can also see the number of assignments created by the teacher in the last 30 days.

e. Students tab – This tab lists every single student from all of the Google Classrooms. It will also show the guardian's information. Each student will be listed with the number of Active and Archived Classrooms they're a participant.

Classroom Audit Use Case Examples

- How to find Google Classroom groups
- Students who have Not Submitted Work for Assignments (Google Classroom)

Classroom Insights

f. Classes tab – This tab lists every single Google Classroom in a visual way. Showing details like the Number of teachers and students, and the number of classwork that has been published by teachers.

g. Class Info tab – Clicking on a classroom in the Classes tab will redirect you to the Class Info tab.

There you'll find much more details on the Classroom, and if the GAT Shield extension has been deployed to students, you'll be able to generate browsing stats.

h. Students Submission Summary tab – This tab summarizes student performance and provides an overall grade for the total number of submitted assignments for a particular Classroom.

You can use this tab to view student performance across all their Google Classrooms.

Classroom Insight Audit Use Case Examples

- Google Classroom Insights
- Classroom Insights | Google Classroom Student Submission Summary

Applications

a. Applications tab – This tab lists all 3rd Party Apps which have been authorized to access different privileges from a user's Google account.

It shows you what permissions 3rd Party Apps have access to and rates the risk of those privileges. You'll also see how many users have authorized that app.

If you don't approve of an App you can set up a policy to ban it from extracting data from its privileges.

b. Policies tab – In this tab, you'll see all Trusted or Banned App policies. These policies can cover all or some users, depending on their scope.

c. Events tab – Each time a privilege is invoked by a 3rd Party App a record of the event is stored.

Application Audit Use Case Examples

- How to set up alerts for newly installed applications in Google Workspace
- Ban Chrome Third-party apps in real-time

ChromeOS Devices

ChromeOS devices tab – In this tab, you'll see all enrolled Chromebooks within your domain. You'll also see all their details. You can edit these details and take action on them.

A key feature in this tab is the ability to export the results to make changes within the Google Spreadsheet, then import the changes to make them final.

ChromeOS devises Audit Use Case Examples

- Device Audits
- Export your Entire Chromebook Asset Collection Directly to Asset Tiger

Mobile Devices

a. Mobile Devices tab – Leveraging Google Workspace Mobile Device Management features, the Mobile Device tab shows you all connected mobile devices, Android or iOS.

From this tab, you can view all device's specs and details. You can also take actions on a device, like for example wiping an account of the device.

b. Apps tab – When Advanced Mobile Management is enabled in the Google Workspace Admin console and users are forced to install the Google Device Policy app you can report on all installed Apps on their mobile device.

This tab will then show you all installed Apps on each user's device, and what privileges that app requires.

Mobile Devices Audit Use Case Examples

- Manage Your Organization’s Mobile Devices
- How to Set Alert Rules for Not Synchronised and Idle Mobile Devices
- Mobile Devices – Apps

Drive

a. Files tab – Allows Super Admins or delegated auditors to apply custom search filters to find any file or folder within myDrives or Shared Drives for any Google account.

In this area, you’ll also find all actions you can take on these files.

b. File Content Search tab – This section leverages Google’s content search API. You can enter any string/character query, this search is then passed to Google to be performed.

It does not rely on the GAT+ metadata scan mechanism. Once Google completes the search the answer is given back in real-time. From this section, you can also take any actions on the files returned by the search.

c. Files Deleted tab – This shows you all permanently deleted files. It is a log of deleted files, where you can view the metadata for them, they cannot be restored from here. You can export the results of any filter you apply.

d. Shared Drive tab – In this tab, you’ll find all root folder structures for a Shared Drive.

You can also manage the membership and settings of any Shared Drive and enter inside any Shared Drive if you wish to.

e. Events tab – This tab shows all event actions taken on files and folders. Each file or folder has an event record log.

In this tab, you can search for a user and all actions they’ve taken on a file or folder.

f. Folders Tree tab – This tab shows in a visual way all folder structures. You can clearly see subfolder levels within a root folder.

g. External Domains tab – This tab gives insights into which domains files are being shared with.

It also shows you the number of files shared out with external domains.

h. Domain Connection Graph tab – This tab is very similar to the External Domains tab, but it presents the information in a simple visual view.

You can also apply filters to see which domains have access to files on your domain.

i. External Users tab – This tab lists all external users who have access to files on your domain. It also shows you what these users can view and edit.

Drive Audit Use Case Examples

- Google Drive File Access Control – Enforce 'Restricted' to files and folders
- Identify Shared-in Google Drive Files from External users
- Send users a report of Google Drive Files they have exposed
- Add, remove, and replace Google Shared Drive permissions
- Google Shared Drives Management

j. **File management log** - This tab shows all the actions and logs that are taken via File Management.

k. File copy requests - This tab shows all the Copy files requests and their details.

Email

a. Emails tab – This tab allows Google Super Admins or Delegated auditors to apply any search filter to find any email within their domain.

The search can cover every Google account within the domain. As long as the email is not permanently deleted it will appear in the metadata scan.

From this tab, you can also take action on the emails leveraging the GAT Unlock functionality.

b. Email Content Search tab – Within this tab, you can apply any string or character-based search. Your search parameters are passed to Google's email content search API and results are returned in real-time.

This tab does not leverage GAT+ metadata scans. Within this tab, you can also take any actions on the emails returned.

c. User Statistics tab – This tab gives insights into each user's email activity. It shows every Google account and the number of emails they send and receive from their own email address, or

if they used a Google Group email to send that email.

You can also quickly see in this tab which user is sending or receiving the most amount of emails and the person who is receiving the least amount of emails.

d. Groups Statistics tab – This tab shows Google Groups stats about emails sent and received by Google Groups. For each day you'll see how many emails were sent or received, and how many emails included attachments.

e. External From/To tab – This tab shows every external email address that's been receiving or sending emails to/from users on your domain.

f. Sender/Receiver tab – When you apply a filter within the Emails tab, click on the 'Sender/Receiver tab' to get a breakdown of all of the 'External Senders/Receivers' and see a breakdown of all 'Internal Senders/Receivers' too.

This tab is super useful when you navigate from the Emails tab directly to the 'Sender/Receiver tab'.

g. Domain Connections tab – This tab shows a list of domains that are sending emails to your domain.

It shows you the date of their first email interaction with your domain, as well as their most recent interaction with your domain.

h. Domain Connections Graph tab – This tab is very similar to the 'Domain Connections tab' but presents the information in a simple visual view.

You can apply filters to see which external domains send or receive the most amount of emails from your domain.

i. Mail domains tab – This tab shows a list of all domains your domain connects with, and whether these domains are Google Workspace domains or Office365 domains.

If they're not Workspace or Office365 they're categorized as "Other", these could be self-hosted mail domains.

You'll also be able to see when these domains first connected with your domain.

Email Audit Use Case Examples

- How to Schedule Reports for Top Email Senders and Receivers
- How To Audit Email in Google Workspace
- View Email Threads from Any User in Google Workspace
- How to Find All Emails for a Gmail User
- Analyze the Gmail Workload of any Employee

Calendars

a. Calendars tab – In this tab, you'll see every user's Primary and Secondary Calendar details.

From there you can modify and edit any user's access to a Google Calendar. You can change ownership, add new users, or remove users from Calendar permission.

The key feature here is that you can search using the filter query menu to find all Calendars a user has access to.

b. Calendar Events tab – In this tab, you can find all Past or Future Calendar events. If you need to make changes to an upcoming future event you can do so from this tab too.

c. Calendar Resources tab – If you have defined Google Calendar Resources within your Workspace Admin console then you can search for these resources and find all associated Calendar events (past or future) in this tab.

Calendar Audit Use Case Examples

- Change the Organizer of a Google Calendar Event
- Remove Calendar Resources from an Event
- Google Calendar Audit: Add additional Owners to Any Existing Calendar
- Delegate Google Calendar Access to Another User

Meet

a. Activity tab – This tab shows weekly and monthly Google Meet activities.

You can see Google Meet call entries and details for each user. You'll be able to determine if any user had a Google Meet call, and how long it lasted.

b. Timeline tab – This tab is a visual representation of the ‘Activity tab’. You’ll see visual entries on a timeline for each hour of the day. If a user has a call at a particular hour, you’ll see a colorful dot appearing on the timeline.

c. Activity Graph tab – For each Meet conference call you’ll have a Conference ID. You can use this Conference ID to find the call and see a visual representation of all its participants, and how long they stayed within the conferencing room.

d. Map tab – Users who report back their IP address to Google while they have a Google Meet call will appear on the Map and their location can be identified.

e. Meetings without organizers tab – This tab will show Google Meet Calls where the Organizer is not present or has left a user's continued to stay within the room.

f. Meet cost tab – If you define the average hourly work rate for users within the GAT+ Configuration area then the Meet cost tab will show you a chart of the potential cost of a Google Meet call.

This is based on the concept that ”time is money”. So within a certain time range, you’ll see all of the potential spendings for Google Meets.

g. Summary 30 days tab – This tab shows you many Google Meet activity charts in a visual way. It will also show you the total number of calls occurring each day, and the average time spent on each.

Meet Audit Use Case Examples

- Google Meet with No Organizers Present
- Google Meet Users Activity Report
- Google Meet activity stats
- Google Meet Analytics and Auditing
- Track Google Meet Costs Per Hour

YouTube

a. Channels tab – All users will be presented with the total number of YouTube videos they published, and how many of those videos are set to be viewed by people from outside of the company.

Clicking on any values within the table will redirect you to the ‘Videos tab’ so you can take action.

b. Videos tab – In this tab, you’ll see more details on the YouTube video. From here you can also change the video’s visibility to Private or Unlisted if the video was set to Public.

Youtube Audit Use Case Examples

- What Are My Users/Students Publishing on YouTube?

User Logins

a. Events tab – This tab shows see all events related to Logins. You can identify who failed to enter their password correctly or who failed to pass the Login Challenge prompted to them.

If they were successful in Logging in the event will state ‘OK’, if they failed the event will state ‘Login Failure’. If Google has access to their IP, then a beacon will appear on the map.

b. Login IP tab – This tab focuses on the reported IP addresses and the Events reported from them. If IP is available a beacon will be placed on the map.

Users Login Audit Use Case Examples

- Monitoring Google Cloud Login Behaviour
- Detailed Login Auditing (Location, Time, Attempts) [Visual Walkthrough]

One-Click Reports

a. Reports tab – This tab lists a few "useful" report types available in GAT+.

By clicking on a link you’ll be redirected and a search filter will be applied in that audit section.

This allows you to quickly schedule that filter search if you choose to.

One-Click Reports Use Case Examples

- One-Click Reports

Google Workspace DLP

This is an audit of the **Google DLP alerts that are already set up and exist in your Google Admin console.**

a. DLP Dashboard tab – This tab shows you charts and graphs of the Google DLP rules which were triggered. The **DLP rules must be defined within your Admin console.**

b. Drive Events tab – In this tab, you'll be able to view all triggered DLP events and view if a file had PII (Personal Identifiable Information) within it.

c. Drive Rules tab – This tab will list all the DLP rules that you created within your Admin console.

Google Workspace DLP Use Case Examples

- Better reporting for Google Workspace DLP

d. DLP Drive Events (BETA) - This tab will show you the new Google DLP alerts that are set up.

NOTE: Data will be shown only if you already have DLP alerts set up on Google's end.

Roles & Privileges

a. Roles tab – This tab lists all custom roles and standard roles within your Admin console.

Here you can quickly identify which users have which roles. The Google Workspace Super Admin role is the most important and most powerful role of course.

b. Privileges tab – In this tab, you'll see all privileges available and which roles use these privileges.

Roles & Privileges Use Case Examples

- User Roles and Privileges within Google Workspace Admin Console
- Workspace 'Role' Reporting in the Users Audit

Data studio

Data Studio (Looker studio) - This tab will show all the Data studio (Looker studio) files users of your domain have. You can take many actions on them such as Adding or Removing users

privileges to the files

a. Assets - This tab will show you all the Data Studio files that exist on your domain.

b. Events - This tab will show you the Events that happened on the Data Studio files

Devices

Devices audit - This tab will show you all the devices that are used to log in to your domain. It will show all types of devices users use to log in to your domain and additional metadata for it.

Devices use case example

- Audit all the devices used in your domain

Alerts

a. Alerts tab – Within the Configuration area of GAT+ you can develop **near-real-time** alerts called Alert Rules.

If these alerts are triggered you'll see the event details within this tab. You can then quickly identify which user triggered or violated the Alert Rule you have in place.

Alerts Use Case Examples

- View List of Google Drive File Downloads and Drive sharing from Alert Violation

---

Configuration

General

1. **Domain Info tab** – This tab shows you Google license information and active user count, GAT+ license type, and the list of the nominated Security Officer(s).
   You'll also find a field to enter your primary contact details so the GAT support team can reach out to you if needed.
2. **Settings tab** – This tab provides you with options to create custom tags that can later be assigned to Gmail email or Drive metadata.
   If you have other secondary domains you can declare them as "company-owned domains" so they don't appear as external within the auditing reports.

3. **Date and Time tab** – In this tab, you'll be able to configure the global settings for all users' dates and times.
4. **Scan Options tab** – You can hide and not report metadata from certain auditing areas.
5. **Reports tab** – The weekly activity report which is automatically generated by GAT+ can be disabled from this tab.
6. **Tasks tab** – This tab will show all of the recurring scheduled metadata scans. It will show their status and health. You can manually force a metadata scan to be scheduled to run quicker than normal. A normal metadata scan should run every 10 hours.
7. **Average Cost Per Hour tab** – You can declare the average hourly work rate for any employee. This will be used within the Meet auditing area.

Security Officer

The security officer area will only appear to users who have been nominated as Security Officer(s).

1. **Dashboard tab** – This tab explains all the tabs available within the Security Officer area.
2. **Access Log tab** – This tab shows if a Workspace Super Admin or a delegated auditor accessed file content or email content. It also shows if file-sharing permissions were changed or emails were deleted.
3. **Access Permissions tab** – In this tab, you'll see any requests coming from Workspace Super Admins or delegated auditors to view file or email content or to delete emails. Security Officers will have to decide what requests are approved or denied.
4. **File Management tab** – Any requests to make changes to file-sharing permissions will be displayed in this tab. Security Officers will have to decide what requests are approved or denied.
5. **Email delegation tab** – Email delegation requests will be displayed in this tab.
6. **Email Forwarding tab** – Email forwarding change requests will be displayed in this tab.
7. **Copy Management tab** – Requests to make duplicate copies of files will be displayed in this tab.

Delegated Auditors

By default, Google Workspace Super Admins are the only users able to access the GAT+ tool. If you wish to delegate GAT+ access to others then they'll need to be declared as a Delegated

Auditor(s).

Auditors tab – In this tab, you can declare new Delegated Auditor roles and view existing roles.

Delegated Auditors Use Case Examples

- Create Delegated Auditors

Admin Log

Admin Log tab – All actions taken within the GAT+ tool appear as a log within the 'Admin log'. This log is immutable and can not be deleted.

Scheduled reports

Schedule tab – This shows all scheduled reports that have been created. From here you can remove them, or assign an action to the scheduled reports.

Scheduled Reports Use Case Examples

- Create a scheduled report in the Drive audit

Alert Rules

Alert Rules tab – In this tab, you can create Alert Rules. Alert Rules policies that are near-real time.

They can trigger from 30 minutes to 2 hours after an incident occurs.

You can set up Alert Rules to trigger based on user activity, Drive sharing or Gmail settings changed.

Alert Rule Use Case Examples

- How to Set Alert Rules for Not Synchronised and Idle Mobile Devices
- Google Drive files that Contain Email Addresses
- Alert when 2FA is disabled for any user in your Google Workspace Domain
- Alert Logins from Users outside your City or Country

- Alert on Google Drive Shares to Specific Email Addresses
- How to Set Up Google Drive DLP Alerts for Shared Out Files

Help

User Manual

When you click on this option you'll be redirected to the gatlabs.com website where we discuss GAT+ features and functionalities.

Guides

When you click on this option you'll be redirected to the gatlabs.com website where you can select whether to see documentation, videos, or a contact form.

Video Guides

Video Guides will redirect you to youtube.com

Embedded media:

https://www.youtube.com/embed/gxnwBHPTqjU?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_lo

About

Will display a dialogue box that explains the version of GAT+.

GAT+ Key Features Explained

Apply filters within auditing areas

When you enter any auditing area in GAT+ you'll see the following icons:

[GAT+ Overview 1]

The funnel icon – allows you to apply a filter search on the metadata. The metadata is usually unorganized and random unless you apply a filter to change that.

The funnel icon with the x symbol – allows you to clear the search and start a new filter search.

The ability to apply a filter is a key feature of the GAT+ tool. You can query any part of the metadata and look for unique parameters within the metadata.

Exporting the metadata to CSV or Google Spreadsheet

Once you've filtered and found the metadata you're searching for it's always a good idea to export the information to a Google Spreadsheet or CSV for record-keeping purposes.

[GAT+ Overview 2]

Column Visibility

In all auditing areas, there are going to be hidden columns from the metadata tables. If you wish to see more columns you need to define this. Some columns are hidden because there's little space on the screen.

FAQs

How often are API permissions evoked by GAT+?

GAT+ uses API permissions to extract metadata which is later indexed and worked on to produce powerful reports for the Super Admins within the GAT+ console.

GAT+ evokes a fresh metadata scan at least once per day from the Google Workspace APIs.

How is metadata secured?

GAT+ encrypts the metadata at rest with AES-256 algorithm encryption. Metadata is stored on GCP (Google Cloud Platform).

Who has access to GAT+?

The app appears on all user's accounts because the super admin installs it Domain-wide. This is necessary to gather auditing reports for each user within the organization.

The only users who have access to the GAT+ interface **are Workspace Super Admin** privileged users.

Super Admins can give non-Super admin access to the tool by creating Delegated Auditor roles, these are roles that have fewer privileges.