

Email Auditing + Delegation



Email Auditing + Delegation



Gain visibility into Gmail activity, manage access securely, and automate delegation at scale using GAT+ and GAT Flow.

1. Auditing Email Activity in GAT+

Gain visibility into email traffic patterns across your organization: who's emailing whom, how often, and where the data is going.

Use Cases:

- Identify top senders/recipients
- Investigate suspicious email spikes
- Audit email flow for internal vs external traffic

Navigate:

GAT+ > Email

What You'll See:

- Email and file activity broken down by user
- Sent and received counts for both external and internal traffic
- Precise time ranges and export options for reporting

Tip: Click the funnel icon to apply filters by email direction, dates, or keywords. You can export the data or schedule reports for ongoing audits.

User	Day	Email	Emails sent (ext)	Files sent (ext)	Emails recv. (ext)	Files recv. (ext)	Emails sent (int)	Files sent (int)	Emails recv. (int)	Files recv. (int)
@generalau...	2020-10-13	v@generalaudit...	0	0	15	0	0	0	73	8
@generalau...	2020-10-13	@generalau...	0	0	28	6	1	1	71	1
@generalau...	2020-10-13	@generalau...	7	15	0	0	7	15	33	41
@generalau...	2020-10-13	@generalau...	0	0	0	0	0	0	12	3

Training Resources: Email Auditing + Delegation



How Admins Use This:

- Spot users sending large volumes of emails externally
- Compare internal collaboration between teams or OUs
- Identify inactive accounts or high-risk external communication

Use this when investigating:

- Unusual spikes in outbound traffic
- Users who may be exfiltrating data
- Department-level communication patterns

Related Articles:

- [Find Emails Sent and Received by the User with GAT](#)
- [Schedule Users' Email Exchanges Report with GAT](#)
- [Group Email Statistics](#)

2. Analyzing Email Workload

There are many reasons to analyze an employee's email workload, whether you're monitoring performance, ensuring fair workload distribution, or investigating unusual activity.

GAT+ provides multiple ways to break down both external and internal Gmail activity by user.

Navigate:

GAT+ > Email

Apply a filter for the user (or group) and desired date range (e.g., last 12 months). Use "Any Email" as your search operand.

Once the filter is applied, GAT+ will begin gathering and indexing the metadata.



Key Analysis Tabs:

External From/To

See all interactions between your user and external domains.

Quickly identify:

- Which external domains contact them most
- If they're responding, or only receiving
- Volume of incoming vs outgoing emails

Sender/Receiver

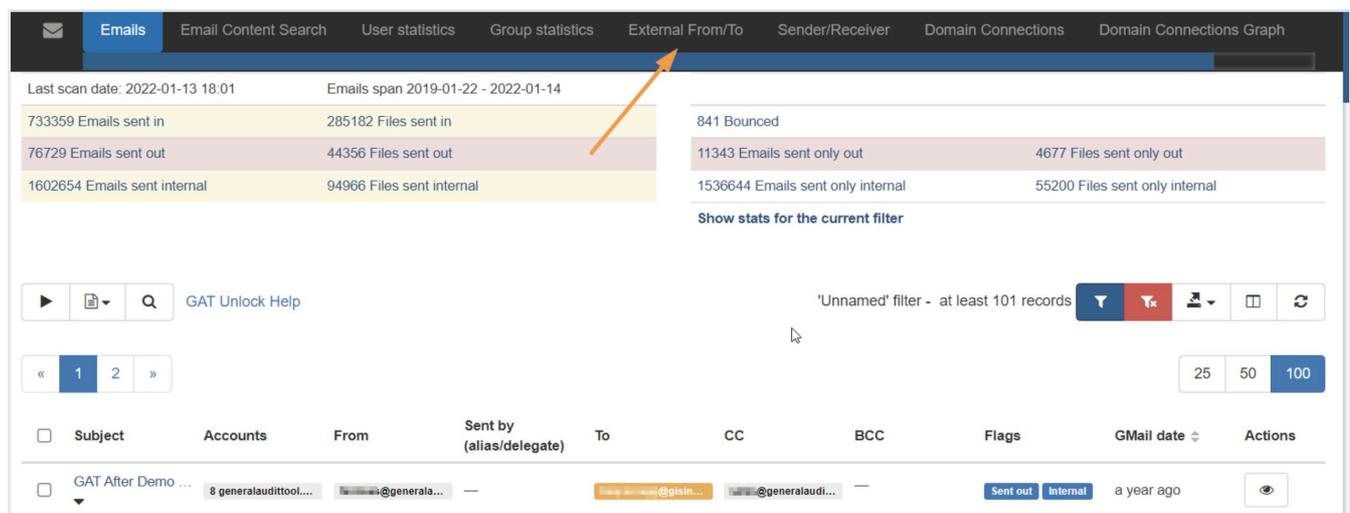
See which internal and external users communicate with the employee.

Useful for:

- Spotting internal collaboration bottlenecks
- Detecting unusual spikes or isolation

Use Cases:

- Use this view to measure collaboration balance between departments.
- Spot risky behavior (e.g. only sending to external recipients, no replies).
- Compare external engagement across job functions like Sales vs Finance.



Related Articles: [Analyze Employee Email Workload](#)

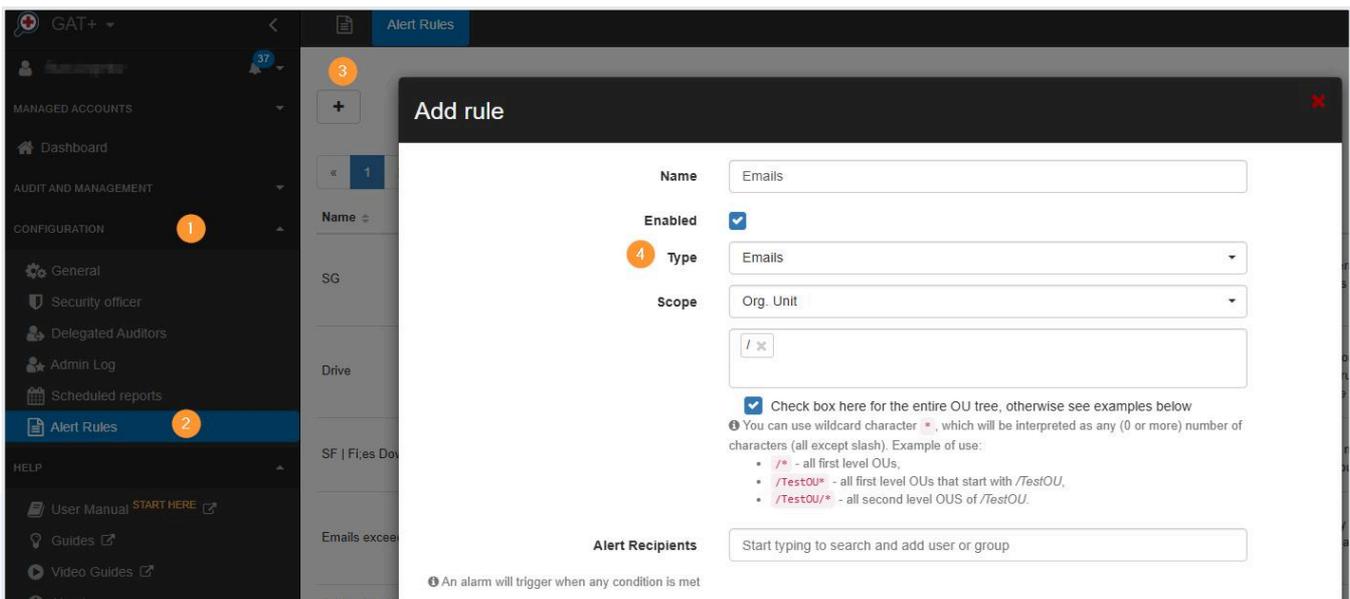
3. Gmail Alert Rules in GAT+

Use alert rules to detect risky Gmail behaviors, such as unauthorized forwarding or mass emailing.

Navigate: *GAT+ > Configuration > Alert Rules*

How to do it:

- Click "+"
- For the Type Select Emails
- Choose scope: User, Group, or OU
- Select recipient(s) for alert
- Enable the alert



Email Alert Types:

- External email forwarding enabled
- Email delegation set
- New Gmail filters added
- New "Send as" configured
- High volume of emails (sent/received)
- Internal email activity

Training Resources: Email Auditing + Delegation

Why it matters:

These signals can indicate shadow inboxes, data leaks, or unauthorized configurations.

Navigate: **GAT+ > Dashboard > Alerts**

The screenshot displays the GAT+ Alerts dashboard. On the left is a navigation sidebar with categories like 'MANAGED ACCOUNTS' and 'AUDIT AND MANAGEMENT'. The main area shows an 'Alerts feed' table with columns for Rule Name, Rule Type, User, Summary, and Created. Below the table are six summary cards for different alert categories over the last 7 days.

Rule Name	Rule Type	User	Summary	Created
SG	EMAIL	...	received external emails violations: 1	22 minutes ago
SG	EMAIL	...	received external emails violations: 1	2 hours ago
SG	EMAIL	...	received external emails violations: 1	3 hours ago
Storage exceeded 350 MB	USER	...	storage alert - value 350.77 MB (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	...	storage alert - value 350.63 MB (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	...	storage alert - value 546.49 MB (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	...	storage alert - value 370.70 MB (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	...	storage alert - value 350.82 MB (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	...	storage alert - value 361.27 MB (threshold : 350 MB)	8 hours ago

Alerts in last 7 days	Email alerts in last 7 days	Application alerts in last 7 days	Drive alerts in last 7 days	Youtube alerts in last 7 days	Mobile device alerts in last 7 days
126	11	0	23	0	0

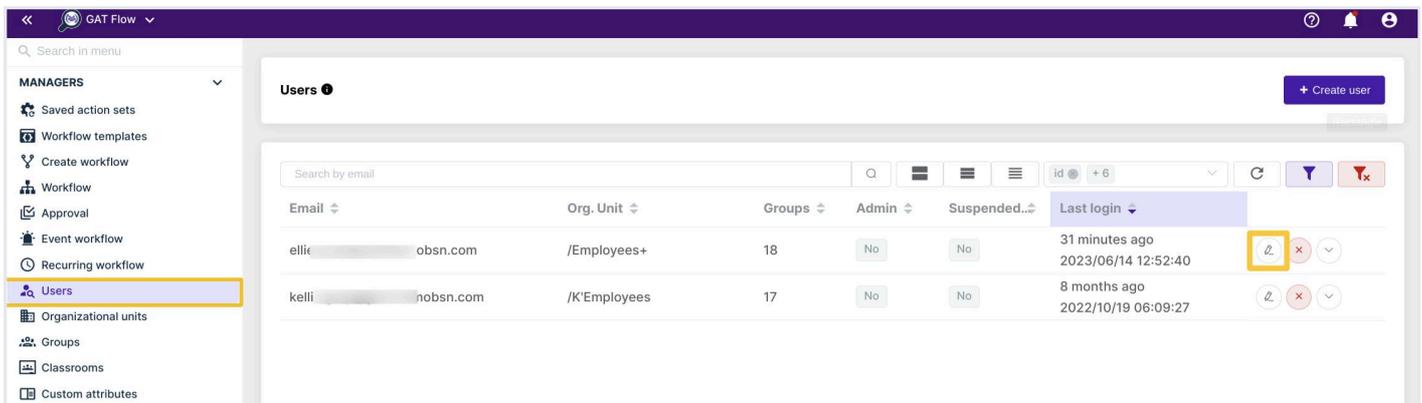
Related Articles: [Set Up Gmail Alerts for Google Workspace Users](#)

4. Manage Auto-Forwarding with GAT Flow

Control Gmail forwarding across your domain without relying on user action, reducing the risk of data leaks.

Navigate: [GAT Flow > Users](#)

Click the 'pencil icon' to display all details about the user.



Available Actions:

- Set up forwarding without end-user confirmation
- Select destination mailbox
- Choose disposition (Keep, Read, Delete, Archive)
- Add a forwarding address to bypass Gmail token confirmation

Note: Forwarding to external addresses may be restricted by domain settings. Internal forwarding works instantly.

Use Cases:

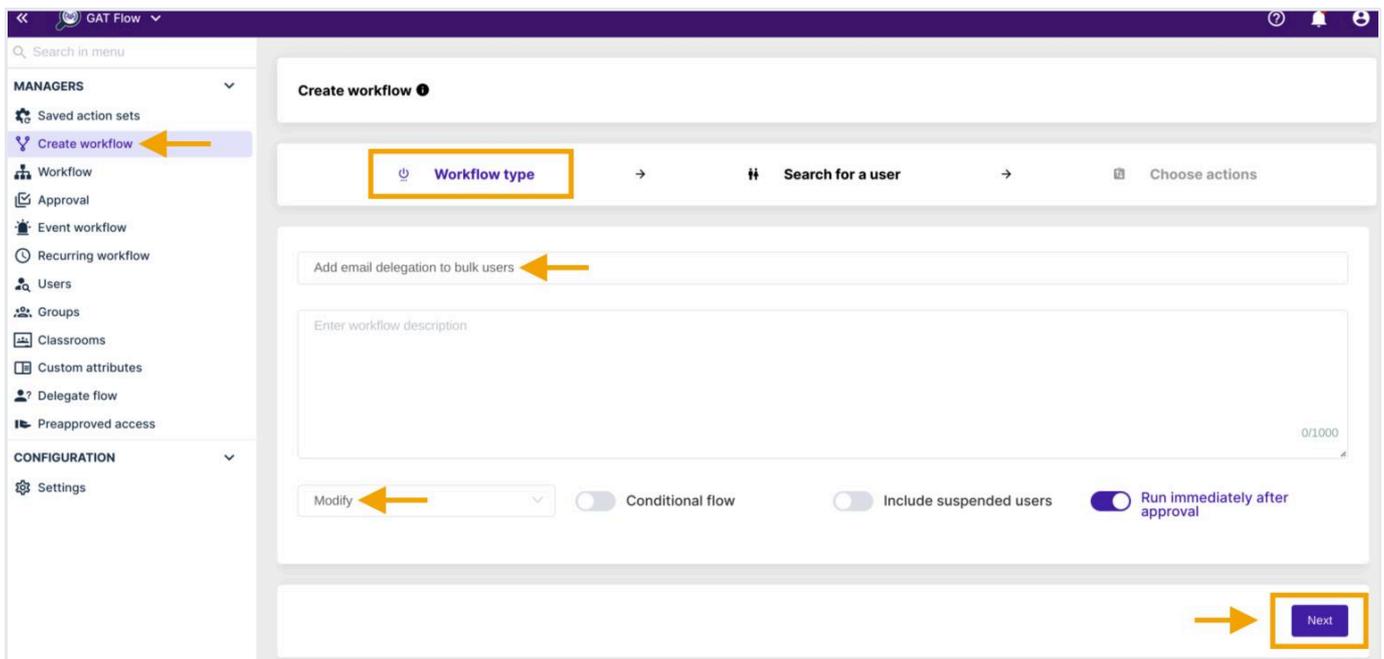
- Forward HR inboxes during leave
- Auto-forward alerts to security team
- Set supervision for new joiners or interns

Related Articles: [Manage Email Forwarding Options in GAT Flow](#)

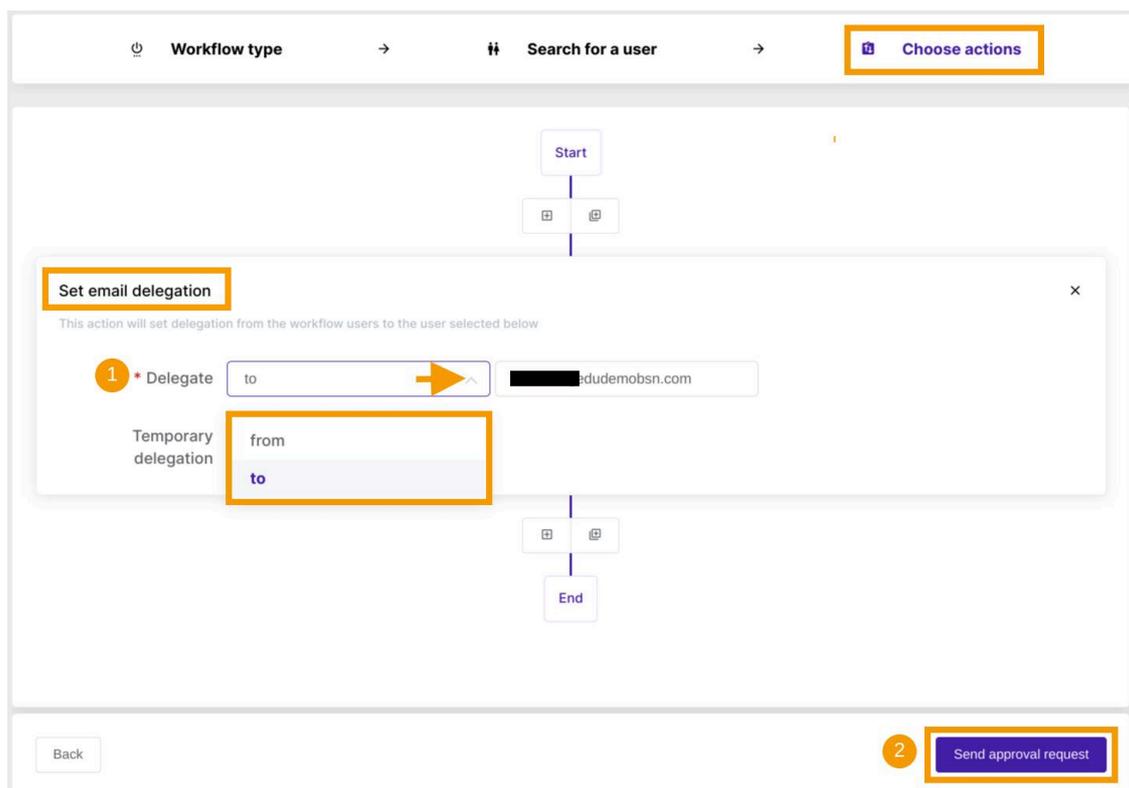
5. Delegation Management in GAT Flow

Delegate inbox access at scale for users and groups.

Navigate: **GAT Flow > Create Workflow > Select a Workflow Type**



Follow the steps, adding user and choosing an action (Set Email Delegation)



Available Features:

- Add/remove email delegates for users
- Assign delegation to entire Google Groups
- Bulk copy or move delegates between users
- Include delegation as part of onboarding/offboarding workflows

Related Articles:

- [Bulk Email Delegation](#)
- [Move or Copy Email Delegations](#)
- [Add Delegation to Group Members](#)
- [Delegation to Google Groups](#)
- [Set Email Delegation and Auto-Forward to Manager](#)

6. Deleting Risky Emails

Remove malicious or sensitive emails directly from inboxes to prevent breaches and enforce compliance.

Navigate: **GAT+ > Email**

The screenshot displays the GAT+ interface. On the left is a navigation sidebar with 'Email' selected. The main window shows an email inbox with a modal dialog titled 'Email messages filters'. The dialog has tabs for 'Current', 'Recent', and 'Saved'. The 'Name' field is 'Unnamed'. The 'Definition' section is set to 'AND' and contains one rule: 'Subject contains sensitive data'. Below the rule, there is a 'Scheduled' checkbox and metadata: 'Created 2 hours ago by monika@gedudemobsn.com' and 'Modified 2 hours ago by monika@gedudemobsn.com'. At the bottom of the dialog are buttons for 'Import', 'Export', '+ New', 'Apply' (highlighted with a yellow box and a '4' in a circle), 'Apply & Save', and 'Cancel'. A '3' in a circle highlights the rule definition area. In the background, the email inbox shows a '2' in a circle highlighting the 'Apply' button in the actions column.

Training Resources: Email Auditing + Delegation



Steps:

- Search by keyword, sender, subject, date, or recipient
- Filter results and select emails
- Choose “Remove” to delete from inboxes (Super Admin permissions required)

Use Cases:

- Clean up phishing attempts
- Remove confidential emails sent by mistake
- Enforce compliance after HR/legal request

Tip:

Deletion is a powerful action. Always review content with a delegated auditor or Security Officer using GAT Unlock before removing emails.

Related Articles: [Delete Domain Users' Emails That Pose Security Risks](#)

Best Practices for Email Auditing & Delegation

- 1.** Review email delegation regularly to remove unused or outdated access
- 2.** Set alerts for risky forwarding/filter behavior
- 3.** Automate recurring workflows (e.g., audits, onboarding) via GAT Flow
- 4.** Always export and save audit logs before making changes
- 5.** Use GAT Flow roles and approvals to delegate safely without full admin rights

Want To Learn More?

[VISIT OUR WEBSITE](#)

[VISIT OUR RESOURCES PAGE](#)

[TRAINING SESSIONS CALENDAR](#)