GAT LABS TRAINING RESOURCES

Email Auditing + Delegation

GAT labs

Training Resources

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:

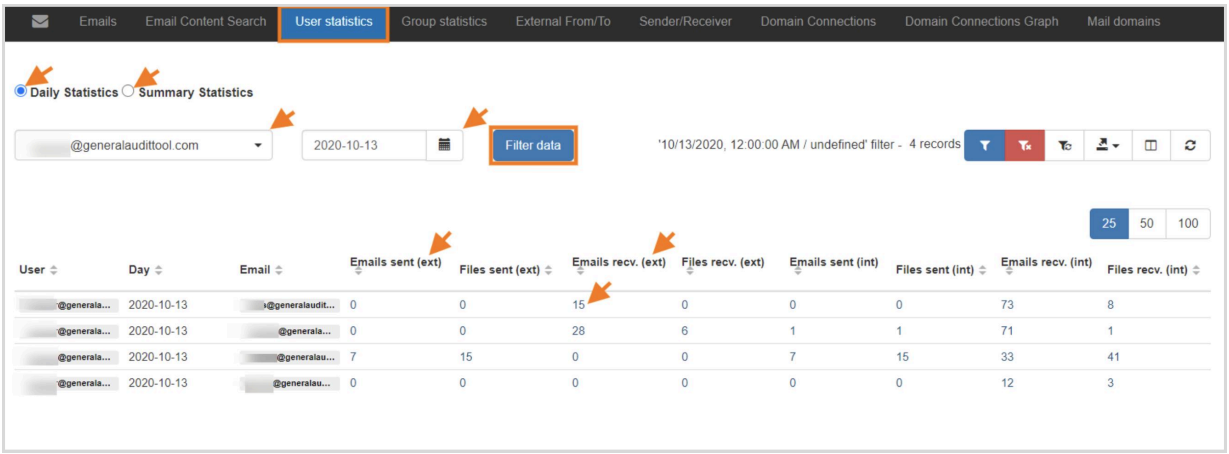
- Identify top senders/recipients
- Investigate suspicious email spikes
- Audit email flow for internal vs external traffic

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.



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

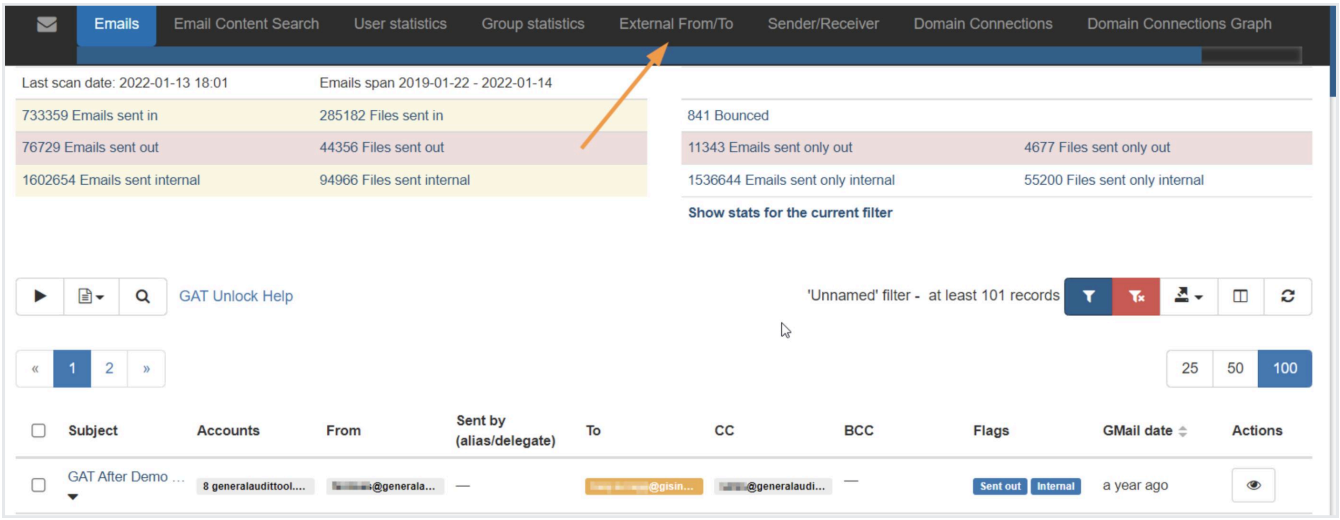
See which internal and external users communicate with the employee.

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

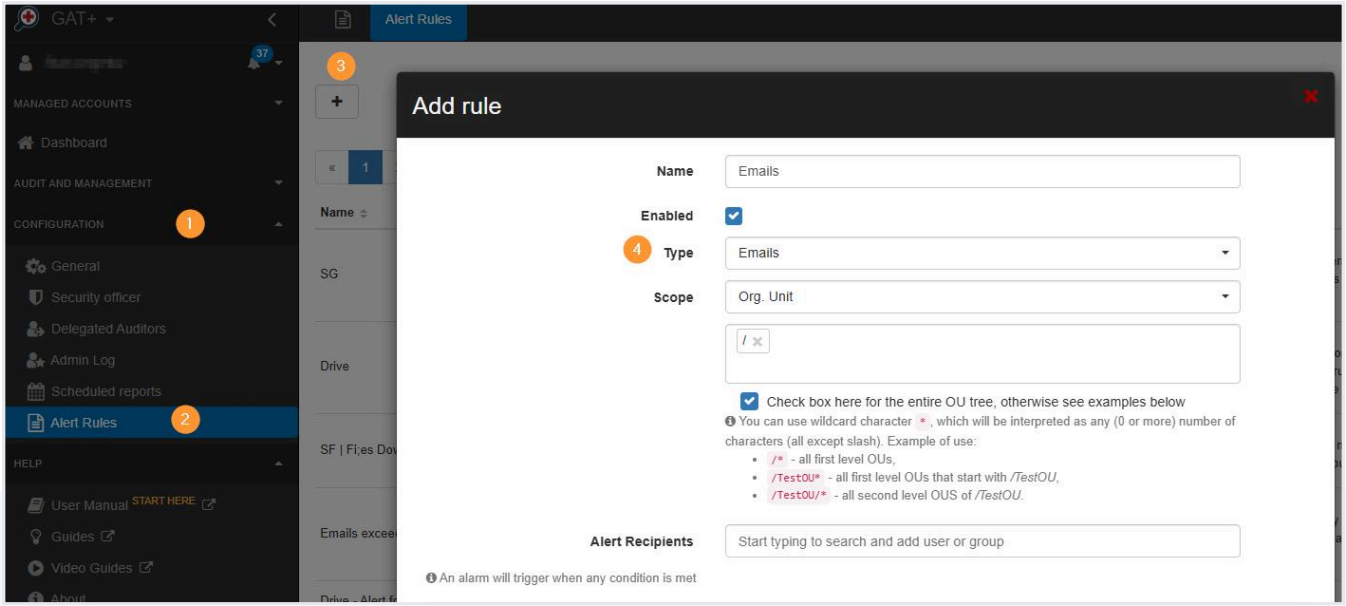
3. Gmail Alert Rules in GAT+

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:

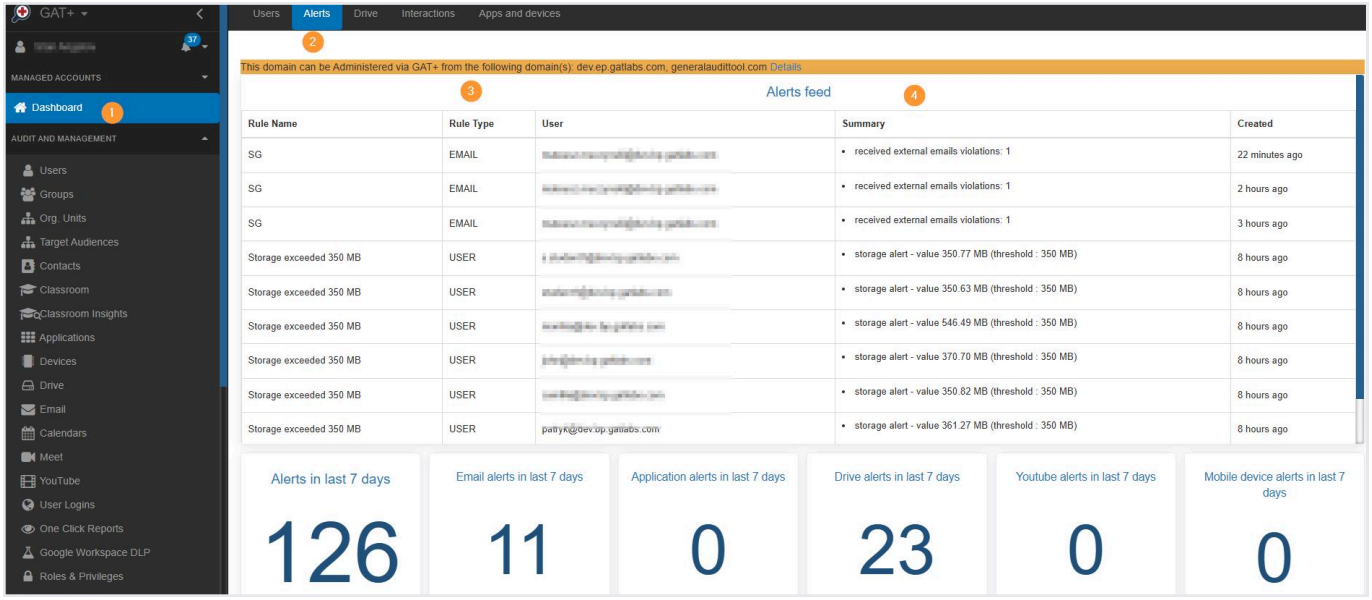
- External email forwarding enabled
- Email delegation set
- New Gmail filters added
- New "Send as" configured
- High volume of emails (sent/received)
- Internal email activity

Training Resources: Email Auditing + Delegation

Why it matters:

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

Navigate: *GAT+ > Dashboard > Alerts*



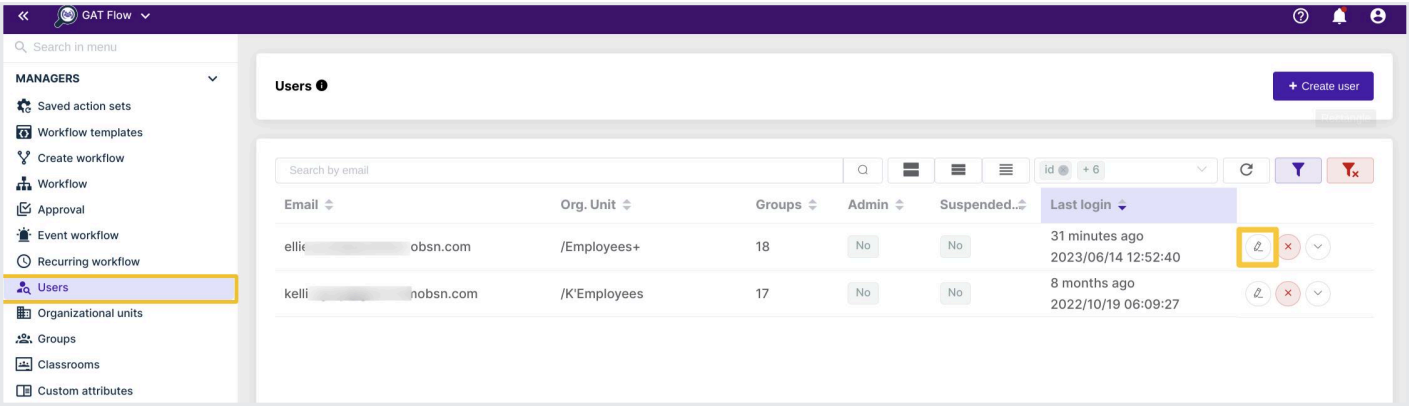
Related Articles: Set Up Gmail Alerts for Google Workspace Users

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:

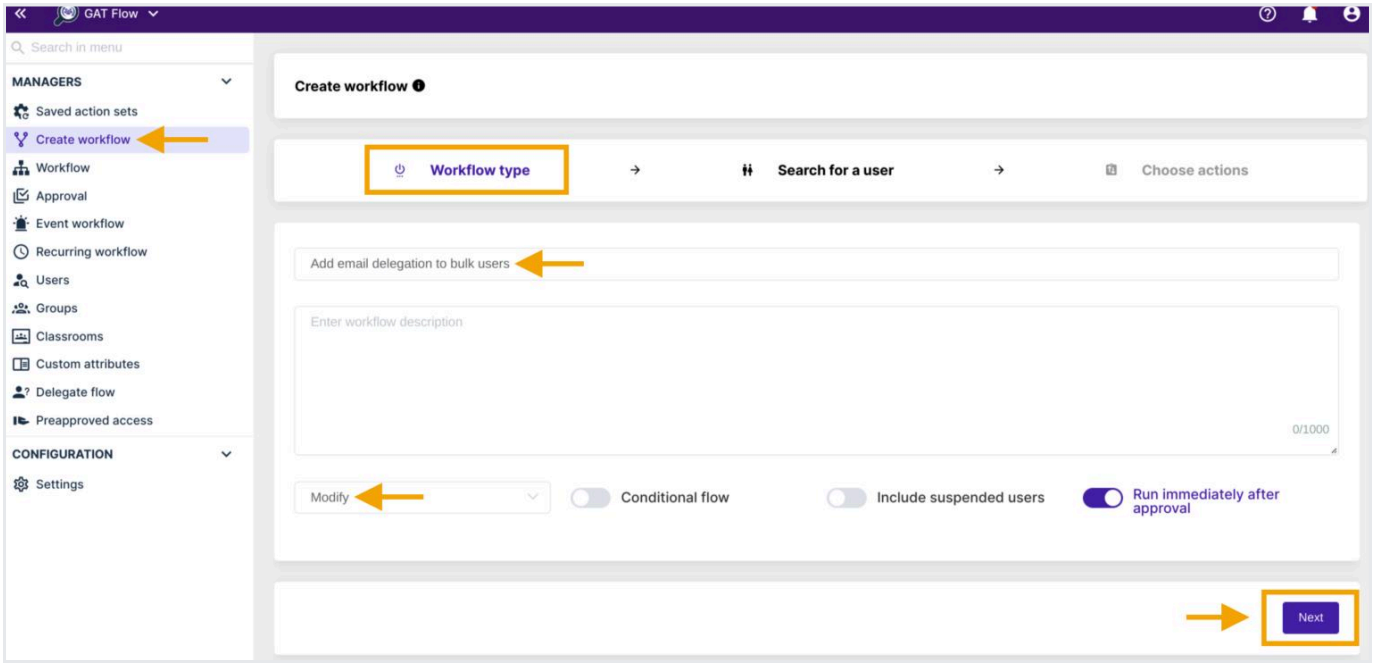
- Forward HR inboxes during leave
- Auto-forward alerts to security team
- Set supervision for new joiners or interns

Related Articles: Manage Email Forwarding Options in GAT Flow

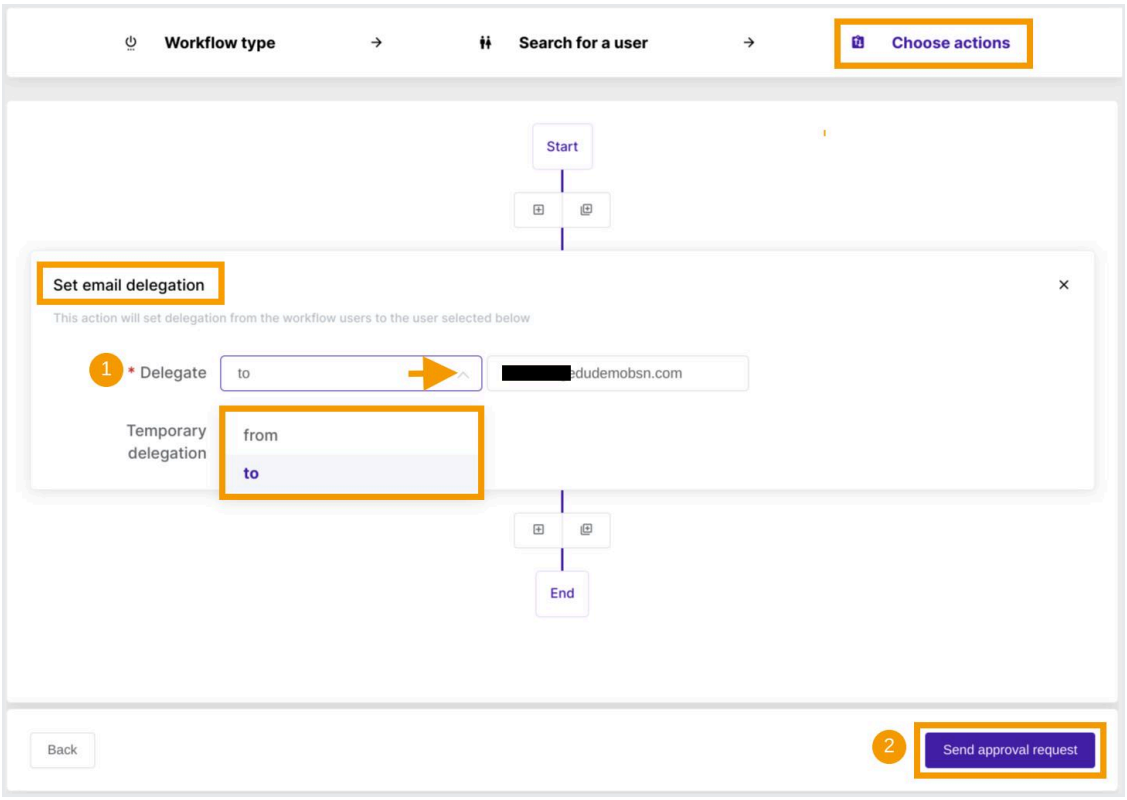
5. Delegation Management in GAT Flow

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

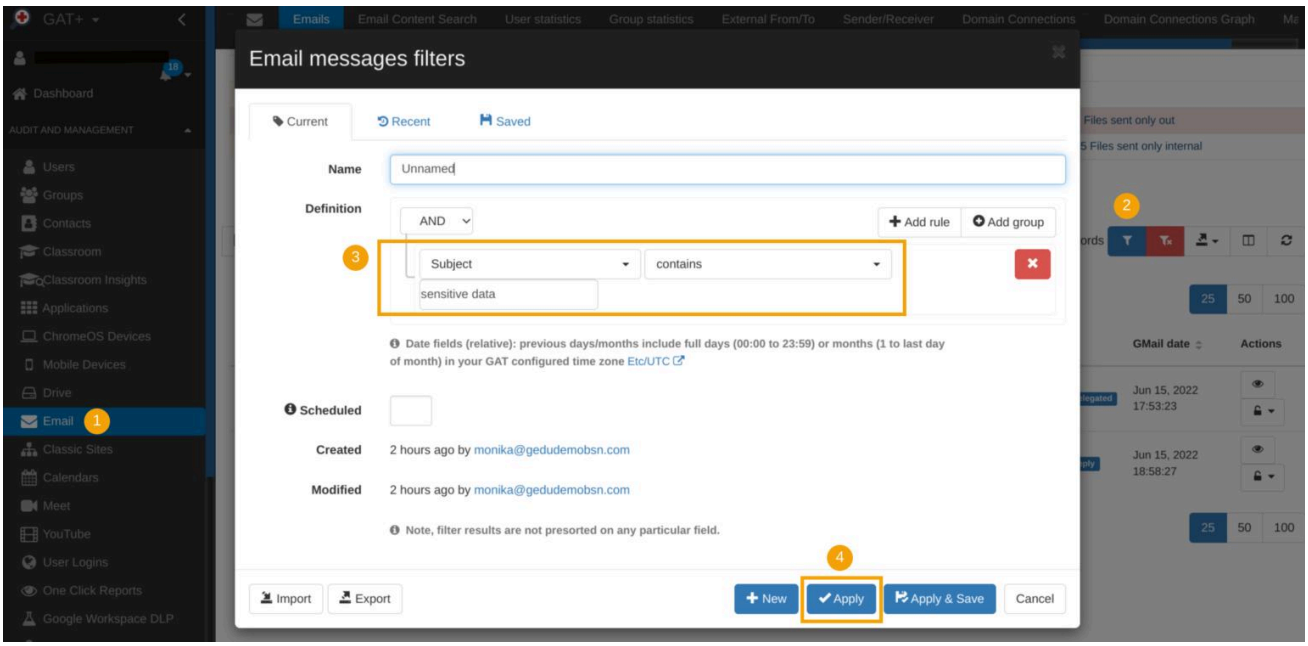
Related Articles:

- 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*



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

GAT labs