Audit and Policy for Google Workspace Apps

Users Audit & Management · https://gatlabs.com/knowledge/tech-tips/audit-and-policy-for-google-workspace-apps/

With the GAT+ you can audit and set policies for additional apps running in your G Suite (Google Apps) environment. These third-party G Suite apps are given permission to access user data via API access which users enable once installing those apps.

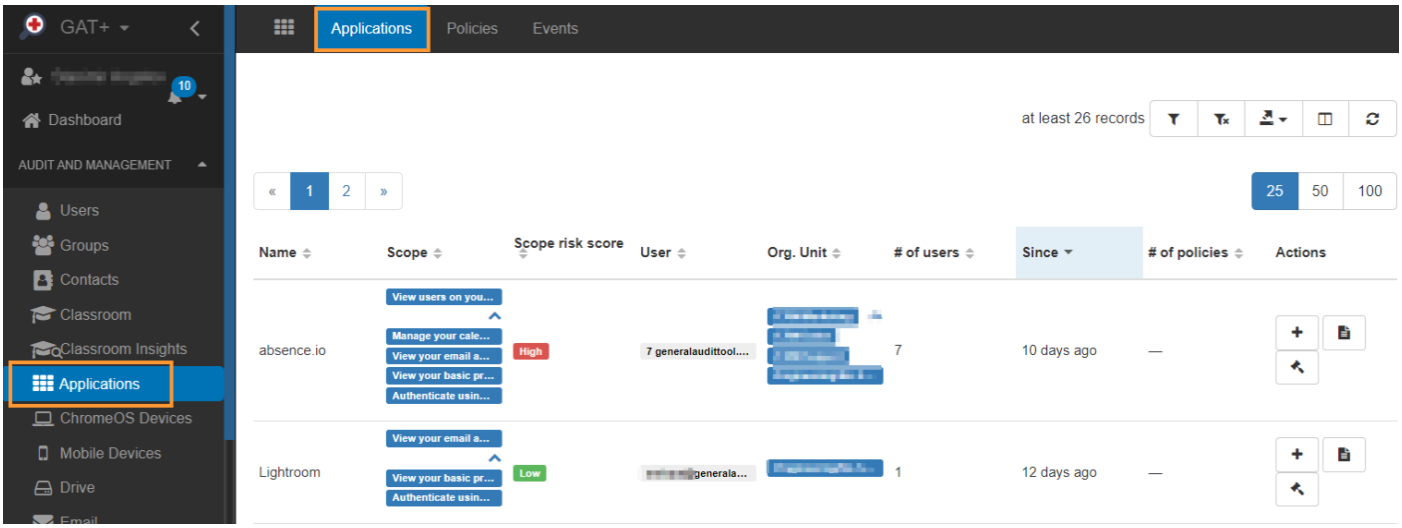
GAT+ provides two different audit areas to analyze this information.

In **GAT+ > User > Applications**

You can then search for any user, group, or OU to focus on a subset of users.

This will show all the **Users** - **Last apps used - Installed apps** (number)

For more of an in-depth look of 3rd party apps, navigate to the **Applications audit** section.



The Applications tab will display:

- **Name** - The name of the apps installed
- **Scope** - The scope of the application is required from your domain
- **Scope risk score** - where we give a score based on the permissions required from the domain (view file/user/email etc data)

    - **Low -** This is where the applications require just basic access.
    - **Moderate** - when the medium is where more access is required.
    - **High -** This is where full access is required like access to drive content, email content, and directory contacts.

- User - users who have the application installed
- Org. Unit - users are part of the visible org. units
- Number of users - who have this application
- Since - since when the application was installed
- Number of **policies** applied for them

Policies

From this page, you can search for apps under a wide range of criteria. For any given app you can set a number of policy conditions, these are for both enforcement and classification.

Apps can be:

- **Banned -** You can Ban an application for individual users by entering their email addresses or you can use Google Groups or Organisation Units to cover multiple users at once. A Ban policy will prevent in real-time the cloud-based application from gaining access to the API permission it once had. GAT+ will block the access of the Third-party app to your APIs.
- **Trusted -** GAT+ checks the Ban and if there are Trust apps then they will be used to remove users from the Ban. For example: If you ban an app for /Sales team, but trust the app for just one user who is part of the /Sales team, the ban rule will skip this account.

Proactive action

Important: Users **can manually enable these permissions again once the app is launched**. GAT+ will detect this in **real-time** and once and disable those permissions once more.

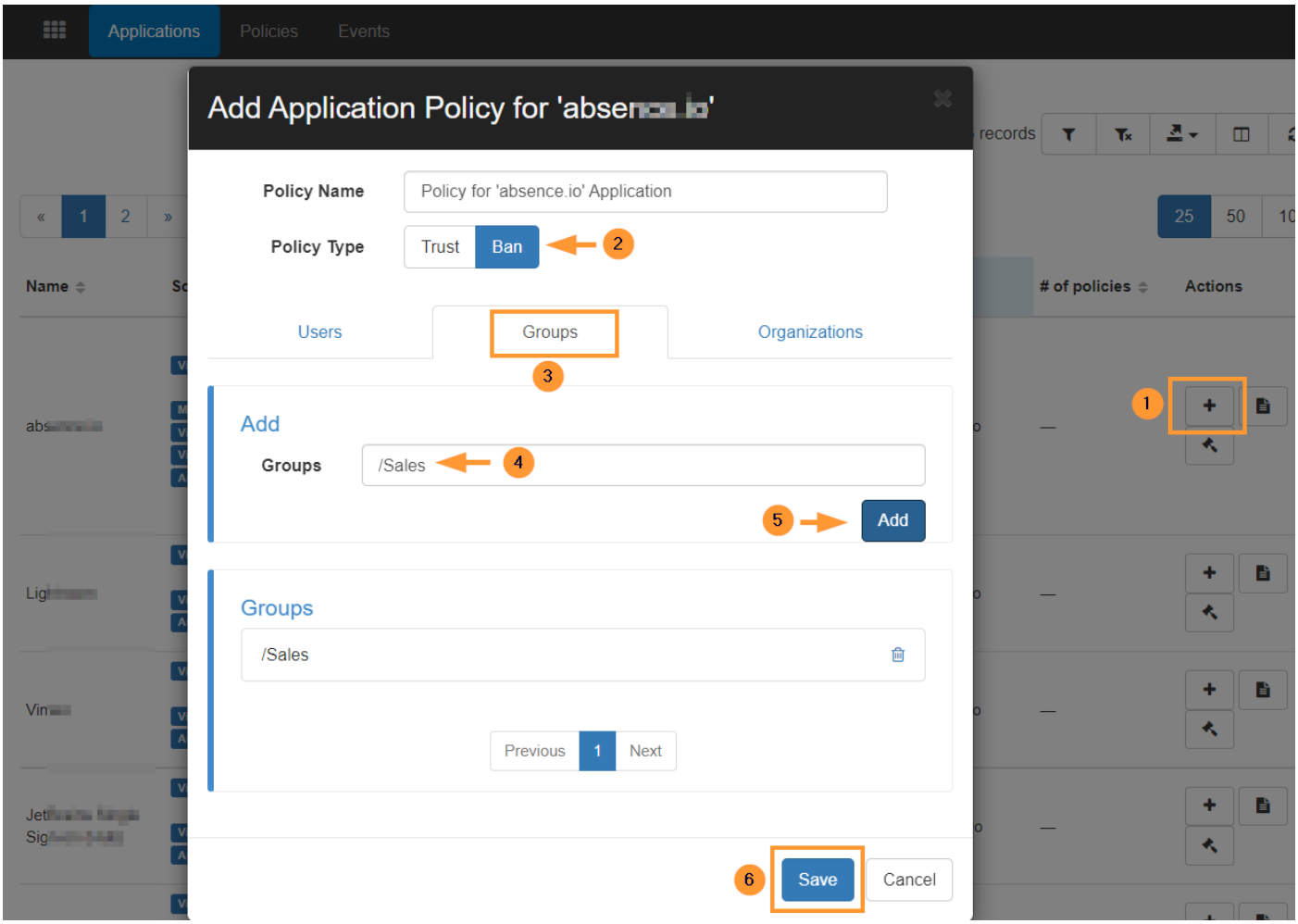
The Ban policy will not remove the application, it will revoke the permissions the Application requires from the domain.

A single app can be both partially banned and partially trusted. All other apps remain unclassified.

Add policy

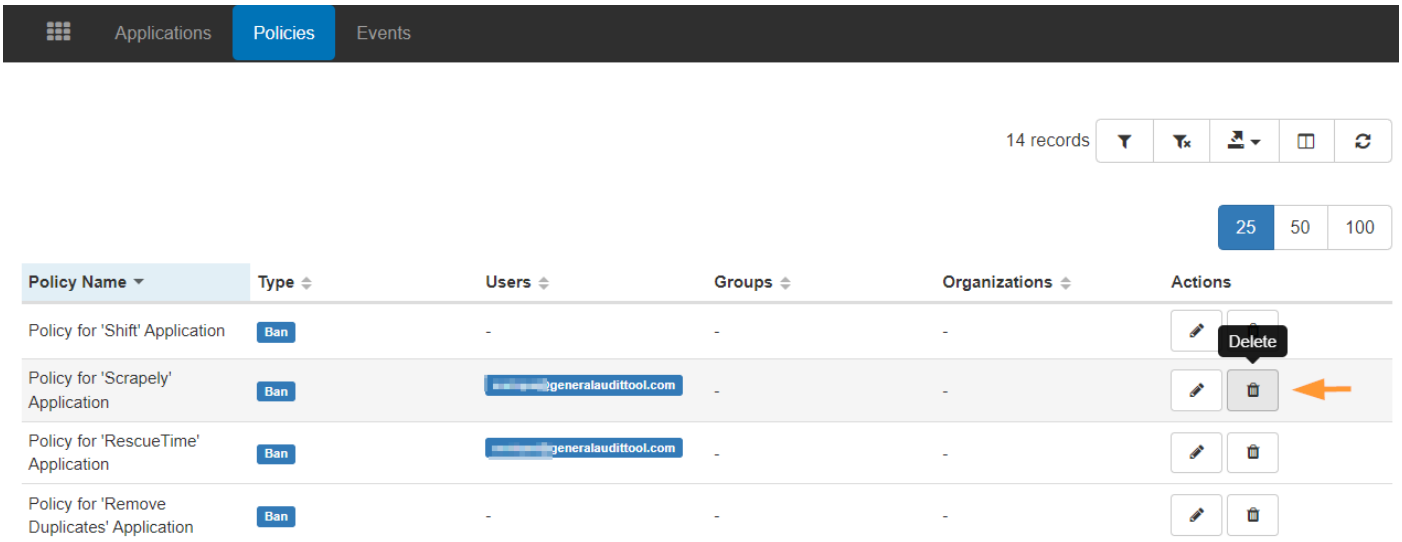
To create a policy for an application, click on the '**+**' button on the chosen application.

- Users - select what users to be banned for the applications
  - Add user - user for whom the **app will be banned for**
  - Add group - members of a group the **app will be banned for**
  - Organizations - members of an org. unit the **app will be banned for**



Remove policy

To Remove policy, click the 'bin' at the end of each individually named policy to remove that policy.



No data for users

In some cases the Users/Groups/ Organizations fields **are empty**.

In GAT+ we show a historical level of applications used by users and the permissions required.

If for example the user removed the application or the scope was removed by Ban policy.

If the application has no access to the domain, the Users field will be empty, but it might still be shown in the Applications tab, as historical data that the app was used in the domain.

In the end, it means **no user is using the application at the time of the GAT+ metadata scan.**

