Audit and manage third-party Applications in Google workspace

Users Audit & Management · https://gatlabs.com/knowledge/tech-tips/audit-and-manage-third-party-applications-in-google-workspace/

The Applications section in GAT+ presents all the third-party applications the users have or had installed using their Google Workspace accounts.

Those are all 3rd party applications that have been authorized to access different permissions from their Google account. This will allow an Admin to view All applications a user has installed using their Google Workspace account and what permissions the applications require from the end-users accounts.

GAT+ will show all the applications and present all the permissions that are required from the Application itself to your Google Workspace data.

The permissions that the Applications require from your Google Workspace APIs are graded under "Scope risk score".

GAT+ will automatically rank these applications and show a "Scope risk score." This is based on the permissions third-party applications require from your Google Workspace API.

Super Admin can examine if those applications are malicious or not and apply a policy on them.

Manage Applications

Ban Third-party apps in real-time

For 3rd party Applications, we have introduced **real-time** policies that can be applied. An Admin can choose to **ban** or allow an Application to the end-user account.

How the GAT+ Ban Applications work

GAT+ can **block an app from accessing your domain's data** by revoking its permissions. This doesn't completely remove the app from a user's account, but it makes it unusable.

- When a user tries to use the app, they'll see a screen asking them to **re-grant permissions**.
- If the user agrees and grants access, GAT+ is **notified automatically**.
- GAT+ then **proactively and immediately revokes those permissions again**, preventing the app from functioning.

This means that while the app stays on the user's account, GAT+ creates a cycle where it **repeatedly blocks the app's access** every time a user tries to use it. This ensures the app cannot access any sensitive data on your domain, effectively banning it without having to completely delete it from the user's account.

How to create real-time banning of third-party apps

Find the Applications

Navigate to **GAT+ → Applications → Apply custom filter → Search for the Applications**

[GAT+ | Ban Chrome Third-party apps in real-time 1]

Set up policy

When the result is found, click on the **+ sign** button on the right side under **Actions**

A pop-up window will be displayed, fill in the policy

- Add application policy for “name of the application"
- Policy name – Enter the policy name
- Policy type – Trust or **Ban**
- Select users whom the Ban will occur.
  - User
  - Group
  - Org. Unit
- Click on the “**Add**” button
- Click on the “**Save**” button to enable the policy

[GAT+ | Ban Chrome Third-party apps in real-time 2]

> **Note:** GAT+ will check and if “Trust” policy applied it will take precedence over the **Ban polciy**

> *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.

Existing policies

From the top many select “Policies” to view all applied policies currently for the Applications of your domain.

Under the **Actions**, you can choose to Edit the ban (pen icon) or you can delete (bin icon) the ban policy.

[GAT+ | Ban Chrome Third-party apps in real-time 3]

Events

The '**Events**' tab allows admins to check the events from the perspective of the Applications. Admin can check and search by User and view the data, and what application had access granted to API, and access was authorized or revoked.

Result

As a result of the setup Ban policies, the **3rd party Applications will be Banned** from being used by the selected users.

GAT+ will remove the “scope” access from the Application to your Domain. However, as this is **not a permanent ban or removal of the applications**, the end-user can still “grant” or install the application again.

GAT+ will then "**see**" and **ban** the application again. It will be **proactive action based on the end-user behavior.**

This happens in **real-time** when a user tries to install the banned application, they will be **rejected** as soon as Google notifies GAT+ that a new App is being installed or access is being granted.

> **Note:** In some cases, the user can log in, because the revoke action **comes after the fact**, **b ut** the app can **not use** any **API** after. It will depends on the App behavior.

Video: How to ban third-party apps in Google Workspace

Embedded media:

https://www.youtube.com/embed/hH7Fc0KpVQI?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_lo