Monitor & restrict data access

Archived: 2026-04-06 01:28:42 UTC

- This guide explains how Google Workspace administrators can monitor and manage the data access users grant to Apps Script through OAuth scopes.
- You can monitor specific OAuth grant events using the Investigation tool in the Google Admin console.
- Access granted to scopes can be revoked, but users can re-grant access afterward.
- Administrators can create alerts to be notified when users grant access to specific OAuth scopes.
- High-risk OAuth scopes for certain services like Gmail and Google Drive can be restricted to prevent unauthorized app access.

You need an Enterprise, Education Standard, or Education Plus Google Workspace account to monitor and restrict the data access that users grant to Apps Script.

Google Workspace users grant access to levels of data, known as scopes, when they run scripts or use apps like add-ons or web apps. This page describes how to monitor or revoke the scopes that users grant access to within their Google Workspace account.

Monitor OAuth grant events by scope

To view events where users grant access to a specific scope or scopes, follow these steps:

1. In the Google Admin console, go to Menu > **Security** > **Security center** > **Investigation tool**.

   Go to Investigation tool

2. Click **Data Source** and select **OAuth log events**.
3. Click **Add condition** > **Attribute** and select **Event**.
4. Click **Event** and select **Grant**.
5. Click **Add condition** > **Attribute** and select **Scope**.
6. For **Scope**, enter the scope you want to monitor. For a list of scopes, refer to OAuth 2.0 Scopes for Google APIs.
7. Click **Search**. A list of grant events displays for the scopes you specified.

Revoke OAuth grants

Important: After you revoke access to a scope, users can re-grant access. Set up alerts for scopes that you don't want users to grant access to so that you can revoke access as needed. Refer to Create an alert for OAuth grants.

To revoke access to a scope, follow the steps for Monitor OAuth grant events by scope, then select the events you want to revoke and click **Revoke access tokens for users**.

Create an alert for OAuth grants

To receive an alert when someone grants access to a specific scope, follow the steps for Monitor OAuth grant events by scope, then follow these steps:

1. At the top of the search, click **Create activity rule**.
2. For **Rule name**, enter a name for the alert.
3. Click **Next: View Conditions**. The conditions automatically populate from the search parameters. Edit them if needed, then click **Next: Add Actions**.
4. In **Threshold 1**, select a time frame and threshold for the rule and check the **Send to alert center** box.
5. Click **Add email recipients** and enter the email addresses that should receive alerts. Click **Done**.
6. Click **Next: Review**.
7. Review the details and click **Create Rule**.

For more information, refer to Create and manage activity rules.

Restrict access to high-risk OAuth scopes

You can restrict access to most Google Workspace services. For Gmail and Google Drive, restrict access to high-risk OAuth scopes while allowing users to give access to OAuth scopes that are not classified as high-risk. If an app requests access to a restricted high-risk OAuth scope, and you have not specifically trusted the app, users cannot authorize it.

To restrict access to high-risk OAuth scopes, refer to Restrict or unrestrict Google services.

Source: https://developers.google.com/apps-script/guides/admin/monitor-restrict-oauth-scopes