Manage external sharing for your organization

Archived: 2026-04-06 00:47:41 UTC

This article is for administrators. To learn how to share or set permissions for your own files, go to Share files from Google Drive.

Supported for all Google Workspace, Cloud Identity, and G Suite editions

As an administrator, you can control if users can share files and folders from Google Docs, Sheets, Slides, Sites, My Maps, and shared drives with people outside of your organization. You can also turn on an indicator to show that a shared drive or Drive file is owned by or shared with someone outside of your organization.

Note: Gems are stored and shared in Google Drive, so the sharing settings for Drive also apply to Gems. Any Google files included in a Gem are shared with anyone who has access to the Gem. For details, see Turn Gem sharing on or off.

Note: The sharing settings for Drive also apply to sharing in Gemini Business. For details, see Control Gemini Business and Enterprise access to Workspace data.

On this page

Note: To control sharing with external non-Google users, turn visitor sharing on or off.

Example sharing setting scenarios

Set up custom sharing for a group or organizational unit

You might want to allow users only in certain groups or organizational units to share content externally, and block external sharing for everyone else. You can do this with Drive sharing settings or with trust rules.

With Drive sharing settings:

1. If you haven't already, put the users in organizational units or configuration groups.
2. Turn off external sharing for the top organizational unit, as described in the next section.
3. At the left, click the group or organizational unit you want to allow to share externally.

Important: Group settings override organizational unit settings. If a user belongs to multiple groups, the setting for the group with the highest priority is applied to the user.

4. Turn on external sharing.

With trust rules: Learn how in Create and manage trust rules for Drive sharing.

You can let users share files and folders with external users who don't have Google Accounts by turning on visitor sharing. You can choose to allow visitor sharing with anyone or only trusted domains. For instructions, see Allow sharing to non-Google users with visitor sharing.

Allow only content in specific folders to be shared externally

Supported editions for this feature: Business Starter, Business Standard, and Business Plus; Enterprise Standard and Enterprise Plus; Education Fundamentals, Education Standard, and Education Plus; Essentials, Enterprise Essentials, and Enterprise Essentials Plus; Nonprofits; G Suite Business. Compare your edition

The sharing settings available in your Admin console apply to users by organizational unit or groups. You don't have control over individual folders in users My Drives.

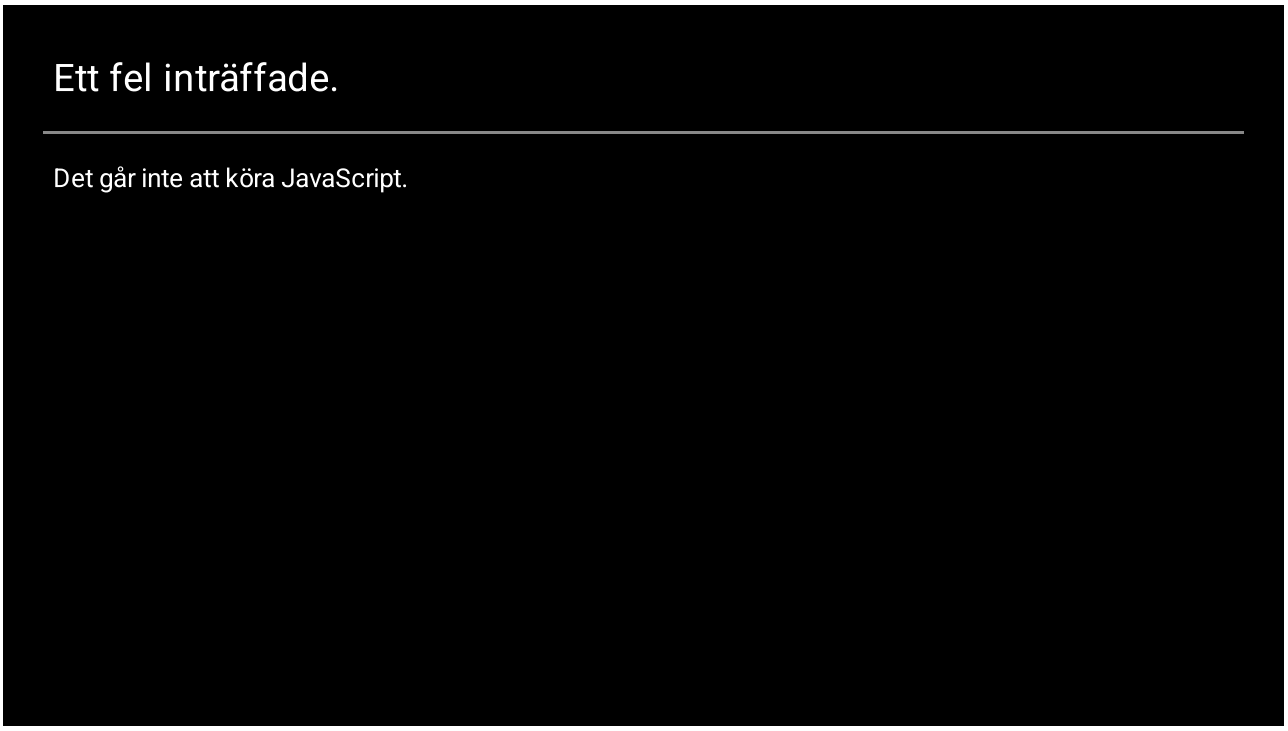
To allow only certain files to be shared externally, you can use shared drives instead. With this approach, the shared drive acts as the folder.

1. Create an organizational unit with no members.
2. Turn off external sharing for the top organizational unit, as described in the next section.
3. Turn on external sharing for the new organizational unit, overriding the setting for the top organizational unit.
4. (Optional) To allow sharing with people outside your organization without Google Accounts, turn on visitor sharing for the new organizational unit.
5. Create a shared drive to contain files and folders for external sharing.
6. Identify the people allowed to share the files externally and add those people as members of the shared drive with the **Contributor**, **Content manager**, or **Manager** access level. If you have many users, add them as a group.

   Note:

   - You can add people outside of your organization as members of a shared drive if they have Google Accounts. If they don't have Google Accounts, you can turn on visitor sharing so your users can share content with them.
   - Review and understand the permissions granted by each access level. Determine the right access level for the shared drive members based on your organization's specific needs.
7. Assign the shared drive to the new organizational unit.
8. Move content into the shared drive.
9. (Optional) If you want to be notified when content is added to the shared drive and shared externally, you can set up a reporting rule based on Drive log events.

Turn on or off external sharing of files and folders in Drive



Sharing content in Drive with people outside your organization can be an important collaboration process, but it also carries risk of data leaks. If you turn on external sharing, you have options to limit sharing, such as warning users before they share or blocking link sharing.

If you turn off external sharing, users can't share the following items with external users:

- Invitations to items created in Docs, Sheets, and Slides
- Links to files stored in Drive
- Items attached to emails, either uploaded directly from devices or stored in Drive

External users also lose access to any items previously shared with them.

You can also block these same items coming from external users to users in your organization. These restrictions apply to external group members. When files are shared with a group that has external users, those external users can't access the file.

Note: Restrictions apply at the user level, not at the group level. So while files can be shared with an external group, external users in that group who are blocked by your sharing settings can't access the files.

To turn external sharing on or off:

1. In the Google Admin console, go to Menu and then **Apps** and then **Google Workspace** and then **Drive and Docs**.

   Requires having the Service Settings administrator privilege.

2. Click **Sharing settings** and then **Sharing options**.

3. (Optional) To apply the setting only to some users, at the side, select an **organizational unit** (often used for departments) or configuration **group** (advanced).

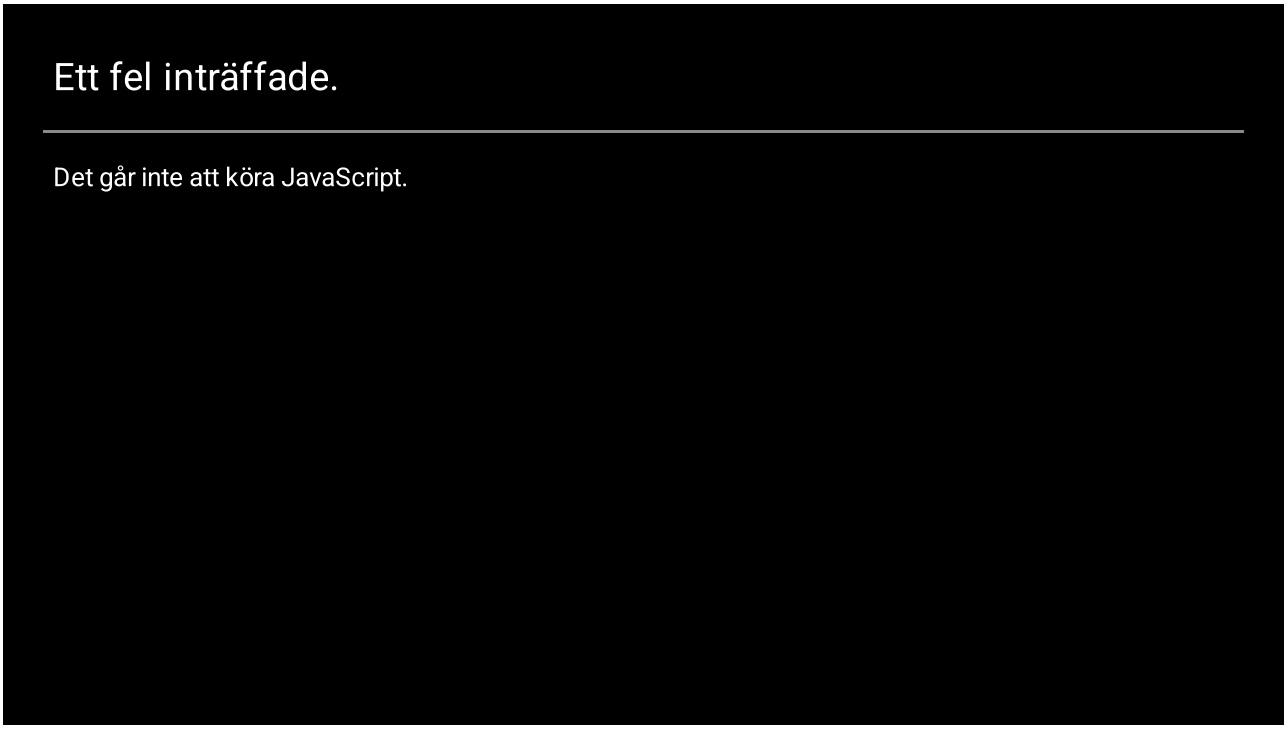
   Group settings override organizational units. Learn more

4. To turn on external sharing, click **On** and choose sharing options.
5. To turn off external sharing, click **Off**. You can also block external content from being shared with your users, including content in third-party storage systems.
6. Click **Save.** Or, you might click **Override** for an organizational unit.

   To later restore the inherited value, click **Inherit** (or **Unset** for a group).

It can take up to 24 hours to see changes. During this time, old and new settings might be intermittently enforced.

Allow external sharing with only certain domains



You can allow file sharing with only trusted (allowed) domains. When you use an allowlist to restrict sharing:

- The domain must be a Google Workspace domain unless you're using visitor sharing.
- You can't select only certain domains in the allowlist for file sharing. All trusted domains are included.
- Users can't share files with personal accounts.
- If your organization has a mix of Cloud Identity and Google Workspace licenses, the allowlist applies to Cloud Identity users, too.

Before you begin: If needed, learn how to apply the setting to a department or group.

If you haven't already, add trusted domains to your allowlist.

1. In the Google Admin console, go to Menu  and then  **Apps** and then **Google Workspace** and then **Drive and Docs**.

   Requires having the Service Settings administrator privilege.

2. Click **Sharing settings** and then **Sharing options**.
3. (Optional) To apply the setting only to some users, at the side, select an **organizational unit** (often used for departments) or configuration **group** (advanced).

   Group settings override organizational units. Learn more

4. Click **Allowlisted Domains** and choose sharing options.
5. Click **Save.** Or, you might click **Override** for an organizational unit.

   To later restore the inherited value, click **Inherit** (or **Unset** for a group).

6. (Forms only) Under **Sharing settings**, click **Form responses**. Choose whether users in your domain can respond to forms that are created externally or share forms externally for responses.

   Note: If you turn these options off, Google Drive sharing settings are applied to form responders.

7. Click **Save.** Or, you might click **Override** for an organizational unit.

   To later restore the inherited value, click **Inherit** (or **Unset** for a group).

It can take up to 24 hours to see changes. During this time, old and new settings might be intermittently enforced.

Turn the indicator on or off for externally shared files

By default, when a shared drive or Drive file is owned by or shared with someone outside of your organization, an **External** warning indicator is shown. However, you can turn the setting on or off for some or all of your users. If you turn the setting off, you can still review the files that are externally shared in the Drive log events.

To turn the indicator on or off:

Before you begin: If needed, learn how to apply the setting to a department or group.

1. In the Google Admin console, go to Menu  and then  **Apps** and then **Google Workspace** and then **Drive and Docs**.

   Requires having the Service Settings administrator privilege.

2. Click **Sharing settings** and then **Sharing options**.
3. (Optional) To apply the setting only to some users, at the side, select an **organizational unit** (often used for departments) or configuration **group** (advanced).

   Group settings override organizational units. Learn more

4. Click **Highlight external files**  and then check or uncheck the **Highlight external files** box to turn on or off the indicator.
5. Click **Save.** Or, you might click **Override** for an organizational unit.

   To later restore the inherited value, click **Inherit** (or **Unset** for a group).

It can take up to 24 hours to see changes. During this time, old and new settings might be intermittently enforced.

Understand indicator display behavior

When the warning indicator is turned on, it's shown for Drive files that are owned by or shared with someone outside of your organization, with the following exceptions:

- The indicator isn't shown if a group in Google Groups owned by your organization can access the file, even if the group includes members outside of your organization.
- The indicator is always shown if any service accounts can access the file, regardless of whether the service account is owned by someone inside or outside of your organization.
- The indicator is always shown if any automatically generated Google Classroom groups can access the file.

Control who can move content to a shared drive owned by another organization

You can allow or block moving content from shared drives that involve an external source or target. For example:

- You can block moving content from a shared drive in your organization to an external shared drive or external user's My Drive.
- You can block moving content from a user's My Drive in your organization to an external shared drive.

For details, go to Restrict who can move content to external shared drives.

Try managing Drive sharing with trust rules

Supported editions for this feature: Frontline Plus; Enterprise Standard and Enterprise Plus; Education Standard and Education Plus; Enterprise Essentials Plus. Compare your edition

Instead of using Drive settings for sharing outside your organization, you can use trust rules to manage sharing both outside and inside your organization. Trust rules give you more control over who your users can share with. For details, see Create and manage trust rules for Drive sharing.

What about user accounts that no longer have Drive?

If a user in your organization no longer has the Drive and Docs service for their account—for example, the Google Workspace license was removed from their account—files they own can be shared *only within your organization*, even if the sharing settings applied to their files allow external sharing.

To remove the external-sharing restriction from the user's files, you can add an Archived User (AU) license to their account. For details, go to Add Archived User licenses.

- Set general access sharing options for your organization
- Restrict the access users can give to files
- Stop, limit, or change sharing
