Control access to apps based on user & device context

Assign Context-Aware access levels to apps

‹ Next: Assign access levels to private web apps ›

After you create access levels, you’re ready to assign them to apps. You can control access by user identity, device security status, IP address, and geographical location. You can also control access for apps attempting to access Google Workspace data through Application Programming Interfaces (APIs).

When you assign access levels...

- Selecting an access level sets it to **Monitor** mode by default. This ensures you won’t inadvertently block users when you turn on an access level.
- Users are granted access to the app when they meet the conditions specified in one of the access levels you select (it’s a logical OR of the access levels in the list). If you want users to meet the conditions in more than one access level (a logical AND of access levels), create an access level that contains multiple access levels. If you want to assign more than 10 access levels for an app, you can use nested access levels to do so.
- For mobile apps, if you use integrated Gmail, you can grant or deny access to Gmail, Google Chat, and Google Meet all at once. If Google Chat and Google Meet are implemented as separate apps (not as part of integrated Gmail), you need to grant or deny access to those apps separately.

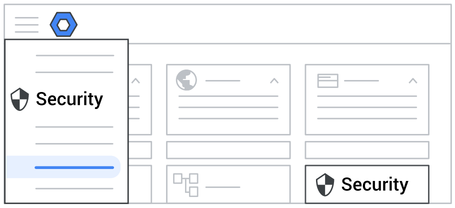
Assign Context-Aware access levels to an app

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

1. Sign in to your Google Admin console.

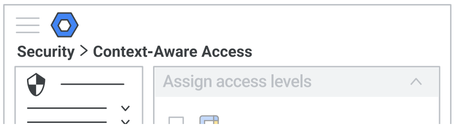
   Sign in using your *administrator account* (does *not* end in @gmail.com).

2. In the Admin console, go to Menu ≡ > **Security** > **Access and data control** > **Context-Aware Access**.

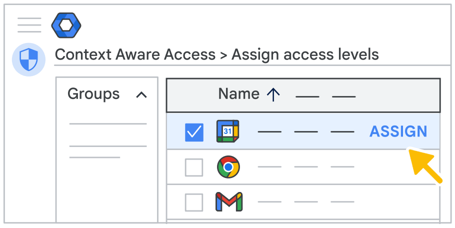


3. Click **Assign access levels**. You see a list of apps.
4. (Optional) To apply the setting only to some users, at the side, select an **organizational unit** (often used for departments) or configuration **group** (advanced). Show me how

   Group settings override organizational units. Learn more



5. Hover over an app and click **Assign**.
   To assign the same access levels to multiple apps at once, check the boxes next to the apps and, at the top, click **Assign**.



6. On the left, click one or more access levels (up to 10) to select them. Selected access levels are displayed to the right and are set to **Monitor** mode by default.
   - To test how selecting the access level will affect users without actually blocking access, leave the setting in **Monitor** mode.
   - If you've tested an access level setting and are ready to start applying it, change the setting to **Active**.
7. Click **Continue**.
8. (Recommended) Check the **Block users from accessing Google desktop and mobile apps if access levels aren't met** box to apply the access levels to users of native desktop, Android, and iOS apps and web apps. See App behavior based on access level settings, below.
9. (Optional) Check the **Block other apps from accessing the selected apps via APIs, if access levels aren't met** box to block apps from attempting to access Google Workspace data through exposed public APIs.
10. (Optional) To exempt trusted apps from being blocked through exposed APIs:
    Available for configuration by organizational unit, not configuration group, even though you can select a group in the Admin console. For details, see Use cases: Exempt trusted third-party apps from being blocked .
    a. Check the **Exempt allowlisted apps so that they can always access APIs for specific Google services, regardless of access levels** box.
    b. If you don't see a list of apps or the app you want to exempt, click **Go to app access control** and complete the steps to trust the app.
       - Any third-party apps you mark **Trusted** on the App Access Control page are listed in the table of allowlisted apps. Some might already be preselected if you marked them trusted and exempt from API enforcement.
       - You can't exempt Google apps (such as Drive, Calendar, or Apps Script) from API blocking. These apps appear grayed out in the list.

    c. If needed, select the apps you want exempted from API enforcement and click **Continue**.
11. Click **Continue**.
12. Review the selected scope, and the selected apps and selected access levels, and the access level mode (monitor or active).
13. Click **Assign**.

You're returned to the apps list page. The Access levels column shows the number of access levels applied to each app in both monitor mode and active mode.

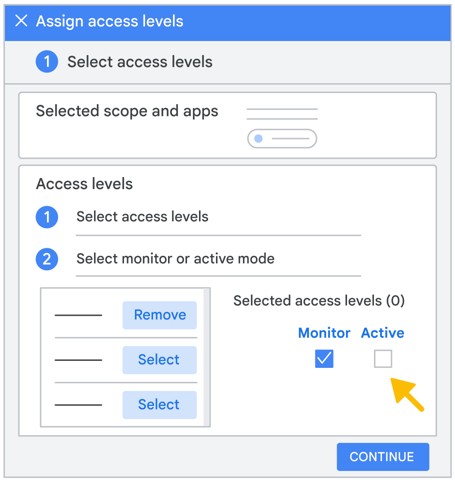
App behavior based on access level settings

1. Hover over the app and click **Assign**.

   Selected access levels are shown at right.

2. Do any of the following:
   - Click **Remove** at left to unassign an access level.
   - At right, change an assigned access level from **Monitor** to **Active** status, or vice versa.
   - To assign additional access levels, locate the desired level at left and click **Select**.

3. Click **Continue** to configure or change policy settings (see steps 8-13 in Assign access levels to an app, above).

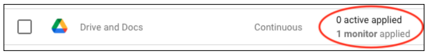


View logged events for an access level

Use the View report option to track whether your assigned access levels are functioning correctly to control user access to apps. Access levels set to either monitor or active mode generate events that are logged in the Context-Aware Access log.

1. Click **Assign access levels**.
2. Select the OU or group you want to review results for.

   In the app list, the **Access levels** column shows how many active and monitor access levels are applied to each app:

3. Hover over an app and click **View report** at right.

4. In the sidebar at right, click the **Link to Security Investigation Tool** to automatically run a search for Contex Aware access log events for the selected application.

The search results include the following information:

- **Access denied (Monitor mode)** events show users who would have been blocked if this access level were enforced.
- The **Actor** column shows the blocked user.
- Access levels applied, satisfied (access conditions met), and unsatisfied (access conditions not met)

For more information see Context-Aware Access log events .

Give feedback about this article

Was this helpful? Yes No

Need more help?

Try these next steps:

Post to the help community
Get answers from community members

Contact us
Tell us more and we'll help you get there

Sign in

- About Context-Aware Access
- Protect your business with Context-Aware Access
- Deploy Context-Aware Access
- Apply recommended access levels
- Create Context-Aware access levels
- **Assign Context-Aware access levels to apps**
- Assign access levels to private web apps
- Delete access levels (which are a shared resource)
- Use case: IP address enforcement
- Use case: Device policy enforcement
- Use case: Managed Chrome browser enforcement
- Use case: Require enterprise certificates
- Use cases: Exempt trusted third-party apps from being blocked
- Allow users to unblock apps with remediation messages in Context Aware Access
- Use Context-Aware Access with configuration groups
- Context-Aware Access examples for Basic mode
- Context-Aware Access examples for Advanced mode
- Assign Context-Aware access levels to the Admin console
- Context-Aware Access FAQ
- Context-Aware Access log events

Language
English