Permissions Overview

Last Modified on 10/09/2026 2:49 pm EDT

DevResults manages access using permissions groups. In plain English:

- Users are assigned to a single group.
- A group is defined with an access level for each part of the site.

This makes it easy to see a user's permission and to update permissions quickly for a type of user. As soon as you add or remove permissions from the group, permissions are updated for all users in the group.

This page includes information about:

- **Permissions groups**
- **Permissions categories**
- **Partner permissions**
- **Editing permissions**
- **Deleting users**
- **Special permissions for owners**
- **Permission overrides**

Note: Permissions for **internal** user groups (groups without the "partner" designation) apply to all projects, indicators, etc. It is not possible to grant access to some indicators and projects but not others.

In contrast, access for **partners** and **partner managers** is automatically limited to their projects, indicators, data, documents, etc. **Learn more** about how partners gain access to projects.

Permissions Groups

Every site comes pre-built with several permissions groups. You can edit the permissions for these groups or create additional groups:

- **Owners**: Can configure the system's global settings and lists. Can manage user accounts and logins, reset passwords, and assign permissions.
- **Managers**: Can mark checklist items as approved. Can sign off on results data submitted by partners.
- **Partner Managers**: Can manage users for their organization and also edit information for their organization's projects
- **Partner Contributors**: Users from other organizations with limited access to projects they implement.
- **Contributors**: Can log into the system to manage projects.
- **Viewers**: Can log into the system, browse projects, and view reports. Cannot change anything.
- **No Access**: Cannot log into the system. (Generally used when users have left your organization.)

back to top

Permissions Categories

For each group, permissions are defined for each part of DevResults:

Note: Bolded categories must be set to View or View & Edit for users to have access to results data.

- Project Discussions -- grants users access to discussion boards
- Project Forms -- grants users access to project and project reporting period forms
- **Project Overview** -- grants users access to project name, descriptive fields, status, mechanism, dates, sectors, tags, and assignments to reporting periods, indicators, organizations, users, and geographies.
- Mechanism Manager -- grants users access to the global mechanism list
- Sector Manager -- grants users access to the global sector list
- Calendar -- grants users access to calendars of events
- Checklists -- grants users access to checklists and milestones
- Custom Queries -- grants users view and download access to custom query results
- Data Table Contributor -- grants users access to data table data
- Data Table Manager -- grants users access to data table design
- Diagnostics -- grants users access to site diagnostics
- Documents -- grants users access to document libraries
- Embed Codes -- grants users access to dashboard tile embed code
- Financial -- grants users access to budgets, funding sources, expenses and disbursements
- **Geographic Information** -- grants users access to locations and administrative divisions
- Groups -- grants users access to user permission groups
- **Indicator Definitions** -- grants users access to indicator name, descriptive fields, definition fields, disaggregations, classifications, indicator forms, and assignments to projects
- **Indicator Results** -- grants users access to indicator data
- Indicator Targets -- grants users access to indicator targets
- Organizations -- grants users access to organizations and organization types
- People -- grants users access to individual user's name, email, organization details, and assignment to projects
- Photos -- grants users access to photo galleries
- Settings -- grants users access to system configuration, system announcements, custom fields, change history, checklist templates, form templates, logic checks, and API keys
- **Reporting Periods** -- grants users access to reporting cycles and reporting periods
- Status Option Manager -- grants users access to the global status option list

For each category, you can assign one of three levels of access:

- View & Edit
- View
- No Access

There are additional roles for each group with a yes/no checkbox:

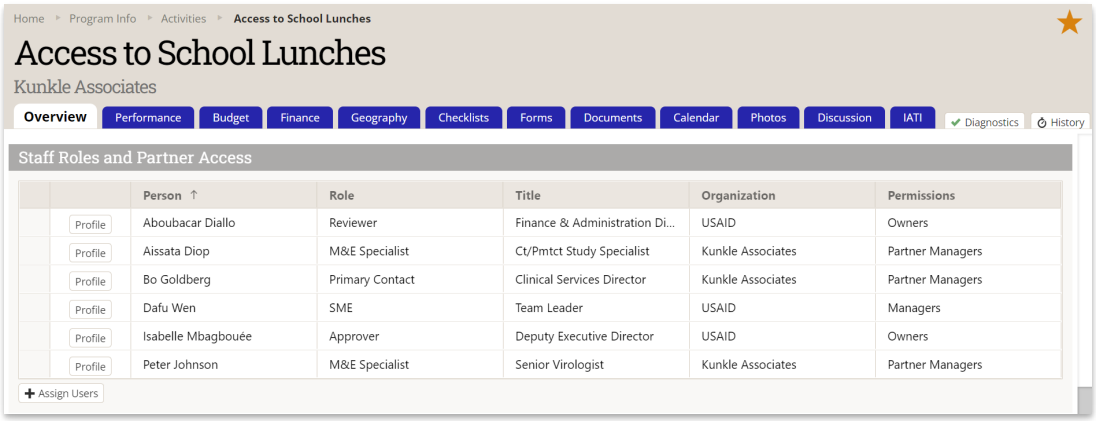
- Checklist Approver -- can mark tasks as approved in project checklists
- Dashboard Manager -- can push dashboards to other users and set default for new users
- Deliverable Approver -- can approve deliverables
- No Access -- cannot log into the system
- Owner -- can see/edit all objects, edit approved/locked data, impersonate users, manage integrations, and more; use only for site administrators
- Partner Manager -- can manage users for their organization and edit their organization's details
- Partner -- can only access information for projects they are assigned to
- Results Data Approver -- can approve indicator data submitted by partners
- Submit Indicator Results -- can submit indicator data for approval

back to top

Partner Permissions

Partners are users who belong to a permission group with either the "partner" or "partner manager" role checked. Partners are granted access to individual projects when they are assigned to a project. Partners can be assigned to projects:

- On the user's profile page (**Administration > Users > *select user***), or
- On each project's overview tab in the **Staff Roles and Partner Access** section.



back to top

Editing Permissions

For instructions on how to add a user to a group or change their group, see **Change a User's Permission Group**.

To edit permissions for a group, see **Change a Group's Permissions**.

back to top

Deleting Users

What happens when you delete a user?

- No indicator results, indicator result comments, narrative responses, discussion posts, photos, documents, or calendar events are affected.
- The user is unassigned from all projects and will no longer appear in the "Staff Roles and Partner Access" section on any project page.
- Discussion posts still show the name of the user who posted it, even if that user has been deleted.
- The user's dashboards are not deleted. The owner of the dashboard is shown as blank, and dashboard managers can give the dashboard a new owner if desired.
- The user's name is removed from checklist item assignments and the item can be re-assigned to another user.
- The user's name is removed from deliverable approvals and checklist completion approvals, but the date remains.
- The user's changes are included in the change history log, but the user is removed from the left-hand user filter.
- If the user is re-added to the site (using the same email address):
  - The user is **not** re-assigned to the projects they were previously assigned to.
  - The user's dashboards are re-enabled for them, if they haven't been transferred to another user.
  - The user's checklist items are re-assigned to them.
  - The user's name is again displayed for deliverable approvals and checklist completion approvals.
  - The user is re-added to the left-hand user filter in the change history log and all of their previous changes will

be filterable.

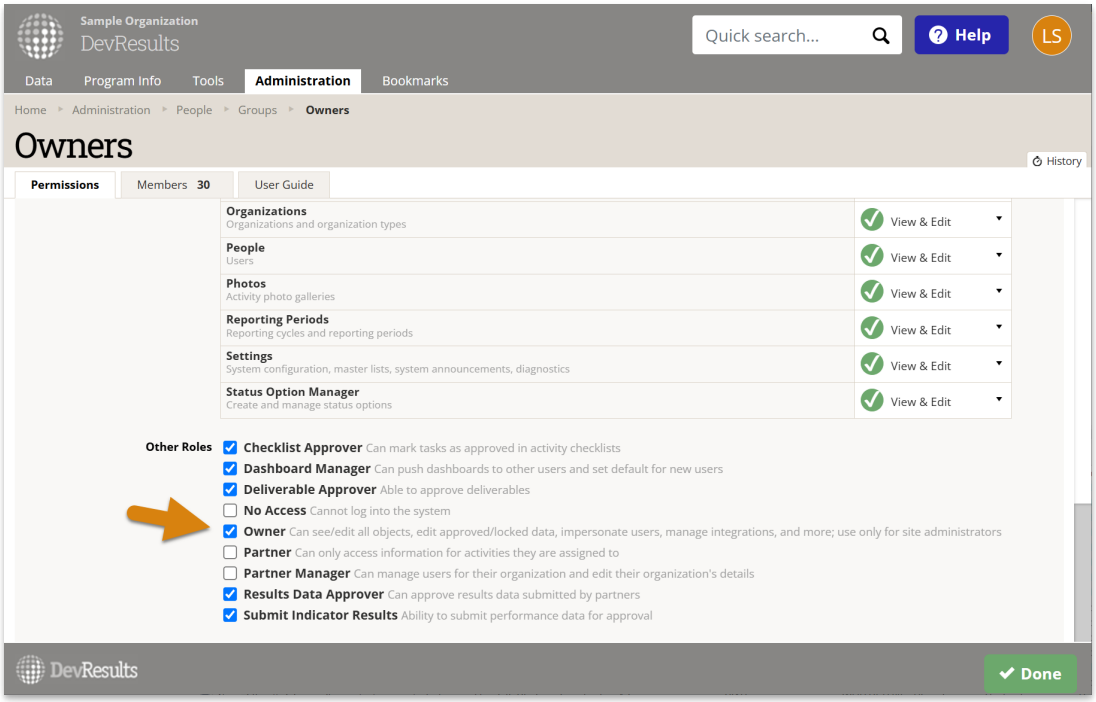
- Users are not erased from the DevResults database behind the scenes, because they might have access to a different DevResults site. If you need all personal information about a user wiped from the DevResults database and its backups, please see our **article about GDPR**.

Alternatively, you have the option of **changing a user's permission group** to **No Access** instead of removing them from the site if you'd like to have a record of previous users. A user with no access cannot log in, but no other changes are made in DevResults.

back to top

Special permissions for owners

The **Owner** role for a group grants special permissions that (unless otherwise noted) are unrelated from any other permission that you can define for a group.



These permissions consist of the ability to:

- Visit the Merge Duplicate Locations page
- Visit the Bulk Imports page
- Visit the Notifications page
- Visit the IATI page
- View the User Guide
- Add users to owner groups
- Remove users from owner groups
- Manage permissions of owner groups
- Add the owner role to a non-owner group
- View/run all custom queries assigned to the instance
- Change what other groups can run individual custom queries
- Delete other users' saved reports
- Change the owner of a saved report
- Manage authentication providers

- Import data into locked project-reporting periods
- Edit data in locked project-reporting periods
- View the projects that a user can access
- Export project-reporting period discussion board comments (via the manifest)
- Delete data table data by import
- Delete data tables with locked rows
- Modify/delete data in locked rows
- Bulk delete data from data tables
- Impersonate other (non admin) users
- Set the default dashboard for users (users with **edit** on **Program Settings** can also do this)
- Push dashboards to users (dashboard managers can also do this)
- Delete logic checks
- Enable google drive document integration (must also be a beta tester)
- Enterprise permissions (for DevResults sites that publish to other DevResults sites):
  - Change the status of any non-certified project-reporting period
  - Edit group membership across the enterprise

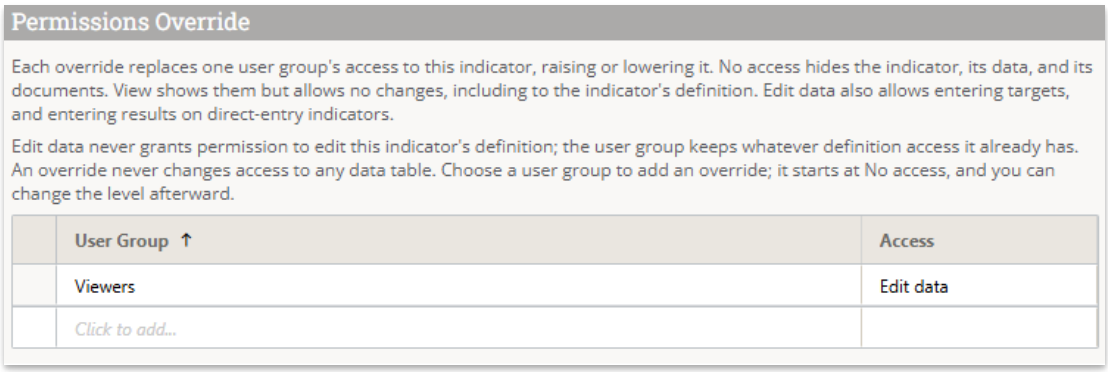
back to top

Permission overrides

DevResults now allows you to grant or deny access to view or edit targets and results for individual indicators, view or edit data within individual data tables, or view data within a custom query. To use this feature, reach out to **help@devresults.com** to enable the permissions override feature.

Once the feature has been enabled on your site, navigate to the definition page for the indicator, data table, or custom query whose permission you want to adjust.

In the permissions override section, select the group you want to give or restrict permissions to. Then select between 'No access', 'View', and 'Edit data.'



NOTE: Overrides cannot raise a group's permission level beyond wat that group already has access to, except for custom queries which can grant access even if the group permissions block it.

> Didn't answer your question? Please email us at **help@devresults.com**.

Related Articles