Setting up view rights

Use this article to learn how to set up your organization’s view rights within the app. If you do not know what the different view rights are, start with learning about the types of view rights to gain a better understanding of the different options available.

In this article

Where can I set view rights?

How are the view rights structured?

Contributor vs Viewer

Viewing across multiple teams

A word of caution

Who can use this?

<table>
<thead>
<tr>
<th>Core</th>
<th>Plus</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Where can I set view rights?

Within the app you can set view rights at the following levels:

1. Organization defaults
2. Role (Advanced setup recommended with SAML connection only)
3. User
4. Team

back to top

How are the view rights structured?

As with many permission structures, view rights use a waterfall system that inherits from the permission settings above it. You can override these settings at each level for full control.

1. Default view rights set by organization
   To set your organization's default view rights, you need the Manage organization permission.

   Under the Settings menu click Role management, then Set default view rights. From here, you can set the view rights that every member of your organization will be granted—unless you explicitly set a new
view right value for a user’s role, user or team.

Default view rights for org
View rights can be modified at multiple levels, with each level inheriting the view rights from the level before it. Any level can be set more restrictive than what it inherited.

Organization view rights
These set the default view rights of your organization. You can control the visibility at a team level and individual level, or using roles. A user without explicitly set values will inherit these values.

Roles: advanced view rights

Tip: If you are configuring view rights manually without SAML, assign view rights by users and teams only.

Clicking on **Enable advanced view rights** on the organization view rights page unlocks the role level view rights. Only turn this on if you are using Flow with a SAML integration.

You can assign different templates of view rights and report access within the tab. This allows you to quickly assign a preset group of view rights to users with that role.

3. **Users**

To override the specific view rights of an individual user, locate and click on the individual from the **Users** page.

On the **User detail** page, locate the **View rights** tab to adjust settings.
4. **Teams**

There are two final customizations you can make at the team level view right. Make these customizations from the **team details** page.

- Adjust whether members of a team see individual contributors' metrics.
- Make team members a **Contributor** or **Viewer**.

---

**Contributor vs Viewer**

By default, anyone you add to a team will be a **Contributor**. This means their data is included in Flow reports and metrics.

If you want to grant someone visibility to a team's data, but do not want their data included when viewing team-level reports or metrics, change their membership to **Viewer**. This is especially useful for team members who may not contribute code frequently, but do so rarely.

---

**Note**: If you view data for multiple teams in a Flow report, if a user is listed as a **Contributor** on any of those teams, their data is included in the reports, even if they are a **Viewer** on one or more of the teams. If you view data for a system team, like **Users on teams**, data for all users that meet the criteria is included, regardless of if they're **Viewers** or not for any teams they're members of.
Viewing across multiple teams

Anyone with permissions to view multiple teams will inherit the rules their organization, role or user provides them with. If you want to change their level of visibility for a specific team that they are part of, you can set this at the team level.

For example: If management agrees that they want to see their fellow manager's team-level statistics, but don't want to see the individual contributors' metrics, grant managers the ability to see either All Teams or Their Own Teams, but not the ability to see individual contributors' metrics. Then, for teams they are directly responsible for, increase their permissions so that they can see individual contributors' metrics.

A word of caution

If you decide to manually change permissions other than the organization defaults, proceed with caution. Combining overrides in roles, user, and team view rights is complex and difficult to track manually. It is highly recommended you connect via SSO/SAML.

In addition, consider creating a test user first and experiment with the view rights so you understand the permissions changes you are making.

If you need help, please email Pluralsight Support (opens email form) for 24/7 assistance.