Setting up Data Sharing Rules

The Data Sharing Rules, allow you to define access rights for users to the various modules in your help desk. This capability offers several significant benefits for your organization:

1. **Enhanced security:** Data Sharing Rules help restrict access to sensitive information, ensuring that only authorized personnel can view or modify certain data in a module.

2. **Privacy compliance:** They enable organizations to comply with privacy regulations (e.g., GDPR, HIPAA) by controlling access to personal or confidential data.

3. **Customization:** Organizations can tailor access rules to match their unique workflows and security requirements, ensuring a precise fit for their needs.

4. **Improved collaboration:** Data Sharing Rules strike a balance between security and collaboration, allowing team members to access and work on shared data while maintaining controlled access.

Availability

ⓘ **Permission Required**
Administrators have the default access to edit and manage data sharing rules permissions. **Agents** with the "Manage Permissions" privilege within the Administrative Permissions can edit and manage data sharing rules permissions.

Check Feature Availability and Limits

You can provide the following types of access levels in Zoho Desk modules:

- **Private**: Only the record owner and their superior can view the record. For example, with Private access to Tickets module, only the person who created a ticket and their manager can see and work on it.

- **Public Read-only**: Users can view others' records but cannot modify and delete the records. For example, with Public Read-only access to Tickets module, all support team members can see the tickets, but they can't change or delete them.

- **Public Read/Write/Delete**: Other users can view, modify and delete the records. For example, with Public Read/Write/Delete access to Tickets module, any team member can view, update, or close a ticket as needed.

Imagine a customer support team using Zoho Desk's Tickets module has configured Public Read/Write/Delete access to foster collaborative ticket resolution. With this access level, any team member can view, update, or close support tickets, enabling efficient collaboration. Support agents can efficiently exchange information, assign tickets, and make necessary updates without access restrictions, resulting in faster issue resolution and improved customer service. This flexibility allows the organization to adapt to various support scenarios seamlessly, ultimately enhancing the overall customer support experience.

Key Features

- By default, all the modules have a **Private** option.
- If the Organization-wide permission is set as **Public Read/Write/Delete**, everyone can access and update all the users' data. Role Hierarchy will not be applied in this case.
- If the Organization-wide permission is set as **Read Onl**y, everyone can only view the other users' records. In this case, other users cannot modify the owner's records.
- If the Organizational permission is set as **Private**, Role Hierarchy can be applied.
- In the Import History, records that belong to you and your subordinates (if any) will always be shown.
- All Attachments, Comments, and Time Entries belonging to a record are accessible if you can view that record.

To manage default permissions

1. Go to **Setup** (⚙) > **User Management > Data Sharing**.
2. In the *Data Sharing Settings* page, click **Edit Data Sharing**.
3. In the *Edit Default Organization Permissions* page, update the following **Access Privilege** for modules:
    - Private
    - Public Read Only
    - Public Read/Write/Delete
4. Click **Save**.

Note: The *organization-level data sharing* permission is not supported for the following modules - Chat, Social, Community, Reports, and Dashboards.