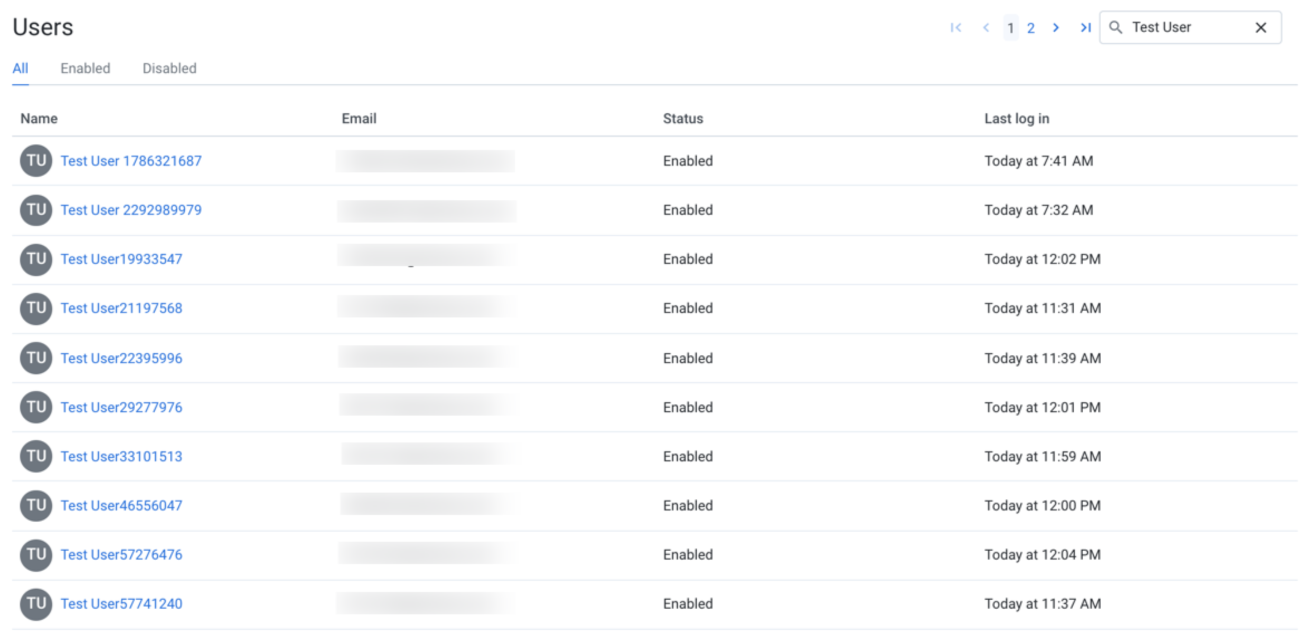
# Users Page

The Users page enables adding, disabling, or removing users from your project or workspace. You can also reset passwords and change roles.



| Name | Email | Status | Last log in |
|---|---|---|---|
| TU Test User 1786321687 | [redacted] | Enabled | Today at 7:41 AM |
| TU Test User 2292989979 | [redacted] | Enabled | Today at 7:32 AM |
| TU Test User19933547 | [redacted] | Enabled | Today at 12:02 PM |
| TU Test User21197568 | [redacted] | Enabled | Today at 11:31 AM |
| TU Test User22395996 | [redacted] | Enabled | Today at 11:39 AM |
| TU Test User29277976 | [redacted] | Enabled | Today at 12:01 PM |
| TU Test User33101513 | [redacted] | Enabled | Today at 11:59 AM |
| TU Test User46556047 | [redacted] | Enabled | Today at 12:00 PM |
| TU Test User57276476 | [redacted] | Enabled | Today at 12:04 PM |
| TU Test User57741240 | [redacted] | Enabled | Today at 11:37 AM |

***Figure: Users Page***

**Tabs:**

- Click one of the tabs to display all users or a filtered list based on user status.

**Fields:**

- **Name:** Display name for the user. Click the name of the user to review details about the user account. See *User Details Page*.
- **Email:** Username (email address of users)
- **Status:** Current status of the user. See "Status" below.
- **Last login:** Timestamp for the last time that the user logged in to the  Designer Cloud application

**Actions:**

- **Search:** Enter text to begin searching for specific usernames or email addresses.

**Context menu actions:**

For each user, you can perform the following actions in the context menu:

- **Configure storage:** If per-user access is enabled, you can configure the access credentials for individual users, either using key-secret combinations or IAM roles. For more information, see *Configure Your Access to S3*.

- **Edit:** Modify user properties, including platform roles. See "Edit Users" below.

- **Reset password:** Self-service password reset is enabled by default. If enabled, click this option to send an email to the user to reset his or her password.

> **NOTE:** Only platform administrators can reset a user's password. Workspace admins cannot.

**Disable:** When a user is disabled, the user cannot access the Designer Cloud application .

- The disabled user still counts against the project or workspace limit.
- All of the user's flows and datasets are retained.

> **NOTE:** Schedules owned by a disabled user continue to execute. An admin can disable the schedule. See *Schedules Page*.

- Resources such as connections and flows that are owned by the user become inaccessible to other users that have access.
- To permit access again, select **Enable.**

## Status

Users can be set to one of the following statuses:

- **Enabled:** User can log in and use the Designer Cloud application normally.
- **Disabled:** User account has been disabled by an administrator. User cannot use the project or workspace.

> **NOTE:** A disabled user's flows and datasets are still stored within the Designer Cloud application . However, the user cannot access them. Ownership of these objects has not been transferred. An administrator has ownership privileges on the user's objects.

## Edit Users

To modify a user account, please complete the following steps.

> **NOTE:** For security reasons, an administrator is not permitted to edit some settings in the administrator's own account.

**Steps:**

1. Locate the user in the list of users.
2. In the context menu on the right side of the user's listing, select **Edit**.
3. In the Edit User dialog, modify the following properties as needed:

**Name:** The display name of the user.

**Email:** The email address is used as the login identifier. This value cannot be modified.

**Roles:** Select or remove the roles to assign to the user. For more information, see *Roles Page*.

**SSO Principal:** If SSO is enabled, set this value to be the SSO principal value associated with this user.

> **NOTE:** Required value for each user if SSO is enabled. See *Configure SSO for AD-LDAP*.

**Hadoop Principal:** If secure impersonation is enabled, set this value to be the Hadoop principal value associated with this user.

> **NOTE:** The user principal value should not include the realm.

> **NOTE:** Hadoop principal is a required value if secure impersonation is enabled. See *Configure for Secure Impersonation*.

> **NOTE:** If Kerberos is enabled, verify that all user principals that use the platform are also members of the group of the keytab user.

**Deployment management:** When selected, this user is assigned the deployment role in the platform. In a Development environment, this role can be added to a user's account to enable access to the Deployment Manager.

> **NOTE:** Deployment management user accounts are intended for managing production execution of flows. These users have a different and limited user interface in the Designer Cloud application . There should be a limited number of these accounts.

> **NOTE:** Only platform administrators can assign the Deployment management role. Workspace admins cannot.

> **Tip:** A deployment user should be assigned the flow author role. Lesser flow roles may prevent the deployment user from properly importing and managing flows. See *Roles Page*.

- In a Production environment where the Deployment Manager applies to the entire instance, this role does not apply.
- For more information, see *Configure Deployment Manager*.
- For more information on Deployment Manager, see *Overview of Deployment Manager*.

**Platform admin:** When selected, the user is granted admin privileges over the platform. These privileges include user administration, ability to modify platform settings, and permissions to use admin-only API endpoints.

> **NOTE:** Avoid providing the Platform admin permission to a large number of users.

To save your changes, click **Edit user**.