Manage Users

Contents:

Through the Admin Settings page, administrators can manage aspects of user accounts, as well as other aspects of the instance. See *Admin Settings Page*.

- To make changes to individual user accounts, click **Edit Users**.

  NOTE: You must be an administrator to access this feature.

Important Note on Permissions

Depending on your instance, access to stored assets can be governed by multiple sets of permissions. Access can be governed by:

- Trifacta® permissions
- Domain authentication (e.g. SSO) permissions
- Storage environment (e.g. Hadoop) permissions

When a Trifacta user shares a resource with another user, that second user may not have access to the underlying resource if one of the other permission sets does not provide it. In the Designer Cloud application , the issue may be surfaced as a generic read or access error, which may be difficult for end users to debug.

Tip: Where possible, you should use a single principal user for Trifacta users. If that is not possible, you should verify consistency in access permissions between Trifacta platform and the underlying storage environment.

User Account Fields

- **Name:** Display name for the user.
- **Email:** The value is the user ID. It must resolve to a valid, accessible email address. Some features of the platform fail to work correctly with invalid email addresses.
- **Trifacta Administrator:** Set this value to `true` to allow the user administrator privileges.

  NOTE: You should limit the number of administrator accounts, which have extensive privileges in the application.

- **Roles:** Trifacta platform roles assigned to the user. See *Platform Roles* below.
- **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:** 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.

- **Created:** Timestamp when the account was created.
- **Updated:** Timestamp when the account was last modified.
- **Disabled:** If `true`, the account is currently disabled. Else, the account is active. Edit the user to change access.
- **Last Login Time:** Timestamp for when the account was last used to access the application.
  - A value of `Never` indicates that the account has never been used.

Edit Users

Password Reset

> **NOTE: Wrangler Enterprise desktop application** users cannot complete this method for password reset. Users of this version must use the self-service method of password reset, which must be enabled in the Trifacta platform. For more information, see *Enable Self-Service Password Reset*.

To reset a user's account password, click **Reset Password**. Copy the URL and paste it into an email to send the user.

> **Tip:** If you are using Chrome for Windows, press `CTRL+C` in the popup to select the password reset URL.

Platform Roles

The following platform roles are supported in the Trifacta platform.

- **Trifacta Administrator:** Provides administrator roles, which include administering users, changing configuration, and deletion of objects created by other users.

  > **Avoid granting Trifacta Administrator role to many users.**

- **Data Admin:** Enables user to use file browsers to browse external file systems such as HDFS, S3, and WASB.

> **NOTE:** The Data Admin role is required to browse HDFS or other non-relational datastores. If an account lacks this role, dataset upload and download and access to JDBC data sources, including Hive, are still supported.

- **Deployment:** In a Development environment, this role can be added to a user's account to enable access to the Deployment Manager.
  - 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*.
- **wrangler:** Enables access to the Designer Cloud application . All users accounts must have this role.

> **NOTE:** All users accounts must have this role, which cannot be modified.

AWS Config

To review and modify the user's settings for AWS authentication, click **Configure**.

> **NOTE:** When you return from configuring your S3 access, your changes there have already been saved.

For more information, see *Configure Your Access to S3*.

Disable User

Non-admin users can be enabled or disabled as needed.

- To disable a user, click the checkbox in the Disabled column. Then, click **Submit**.

Manage Users from the Command Line

The Trifacta platform provides a command line interface that enables administrators to create, edit, and delete users. The CLI can also be used to generate password reset URLs.

For more information, see *CLI for User Admin*.