Manage Users under SSO

Contents:

This section covers additional requirements for managing users in SSO environments.

Enable SSO

The Trifacta® platform requires additional configuration to integrate with your SSO provider. Available methods:

Method	Description
SAML IDP	Integrate the platform with enterprise SAML identity provider. See *Configure SSO for SAML*.
Native LDAP-AD	Using native functionality in the platform, it can integrate with enterprise LDAP/AD. For more information, see *Configure SSO for AD-LDAP*.
LDAP-AD via reverse proxy	A reverse proxy server outside of the platform can be set up for integration with enterprise LDAP/AD. **NOTE:** This method is likely to be deprecated in a future release. For more information, see *Configure SSO for AD-LDAP*.

Configure Auto-Registration

Tip: By default, user auto-registration is enabled. It is recommended.

How users are managed depends on whether auto-registration is enabled:

- If auto-registration is enabled, after users provide their credentials, the account is automatically created for them.
- If auto-registration is disabled, a Trifacta administrator must still provision a user account before it is available. See below.

User Management with Auto-Registration

After SSO with auto-registration has been enabled, you can still manage users through the Trifacta application, with the following provisions:

- The Trifacta platform does not recheck for attribute values on each login. If attribute values change with your identity provider, they must be updated in the configuration.
  - For more information, see *Configure SSO for AD-LDAP*
  - For more information, see *Configure SSO for SAML*.

- If the user has been removed from AD, the user cannot sign in to the platform.
- If you need to remove a user from the platform, you should just disable the user through the Trifacta application.
    - If the user is deleted, then if the user returns to the platform in the future, a new account is created for the user.

For more information, See *Workspace Users Page*.

Disable Auto-Registration

To disable auto-provisioning in the platform, please verify the following property:

1. You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`. For more information, see *Platform Configuration Methods*.
2. Set the following property:

```
"webapp.sso.enableAutoRegistration" : false,
```

3. Save your changes and restart the platform.
4. New users of the Trifacta platform must be provisioned by a Trifacta administrator. See below.

Provision new users under SSO without auto-registration

If SSO auto-registration is disabled, admin users can provision new users of the platform through the following URL:

```
https://<hostname>:<sso_port_number>/register
```

where:

- `<hostname>` is the host of the Trifacta platform
- `<sso_port_number>` is the port number.

The user's password is unnecessary in an SSO environment. You must provide the SSO principal value, which is typically the Active Directory login for the user.

- If you are connected to a Hadoop cluster, you must provision the Hadoop principal value.
- See *Create User Account*.

User access for reverse proxy method

Users access the application through the Trifacta node using the standard hostname and the port that you specified:

> **NOTE:** All users must be use this URL to access the Trifacta application. If they use the non-SSO URL, they may receive an `Unprovisioned User` error.

```
https://<hostname>:<sso_port_number>
```