Configuring Looker To Impersonate Users

Follow these steps if you have a shared dashboard and wish to to send the end-user's identity to AtScale for use in run-time cube security decisions.

Before You Begin

Make sure you have created a connection in Looker. For details, see Creating Looker Connection.

Procedure

1. In Looker, locate the connection to the AtScale instance, and edit it by configuring the following settings:

   - **Username**: Enter an AtScale user name that has the permissions required to impersonate other users (see step 2 below for details).
   - **Password**: Password for the AtScale account.
   - **Additional Params**: `;hive.server2.proxy.user={{ _user_attributes['ldap_user_id'] }}`

2. In AtScale, go to the **Security/Setup** menu and set **PROXY USER ATTRIBUTE** to the attribute that contains the same value used by Looker.

   Usually this is sAMAccountName or userPrincipalName.

3. In the **Admin** section in Looker, go to the **LDAP** page in the **Authentication** section, and set **Login Attrs** to the same value as in step 2 above.
4. In AtScale, go to the **Security/Role Assignment** menu, and ensure that the Looker user account is assigned to a role that grants the following permissions:

   - Impersonate Users
   - Login
   - Query
   - Read Projects

5. Ensure that the Looker service account user has Runtime access to the desired cubes.

   Note that you must republish a project for security changes to take effect.

6. Ensure that the Looker report users have Runtime access to the desired cubes.

   Again, you must republish a project for security changes to take effect.

For more information about configuring Looker to authenticate users via LDAP, see LDAP authentication.