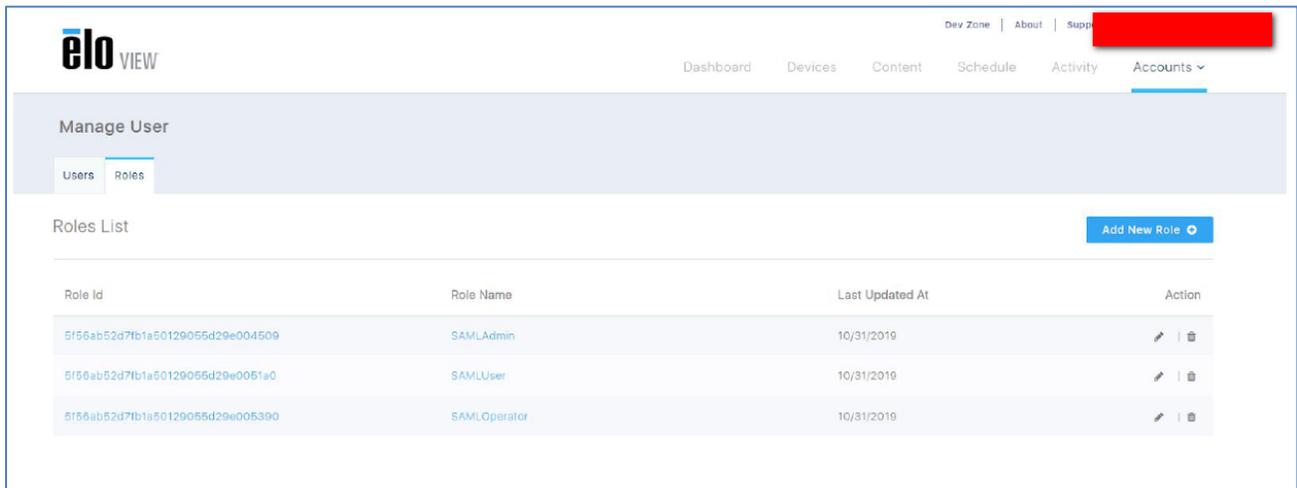


Executive Summary

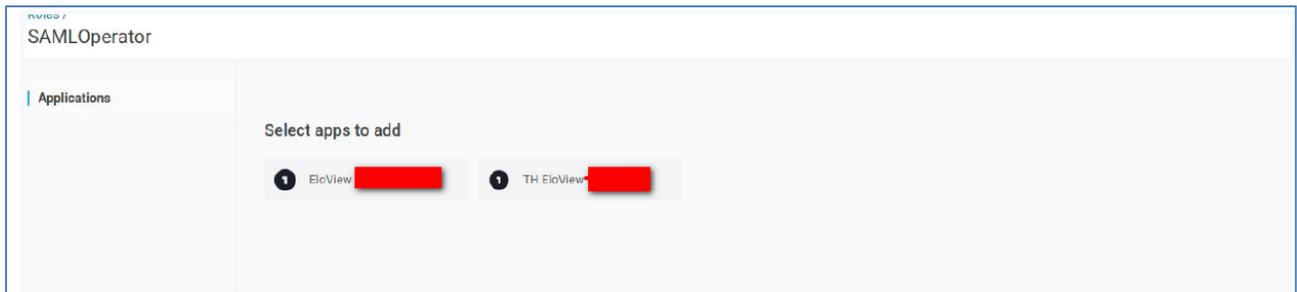
This Technical Bulletin describes how to add SAML Users with Specific Roles in Elo View

Steps

1. Add custom Roles into your Eloview Account
 - a. Navigate to Accounts -> Manage Users -> Roles Tab
 - b. Create as many roles as you need

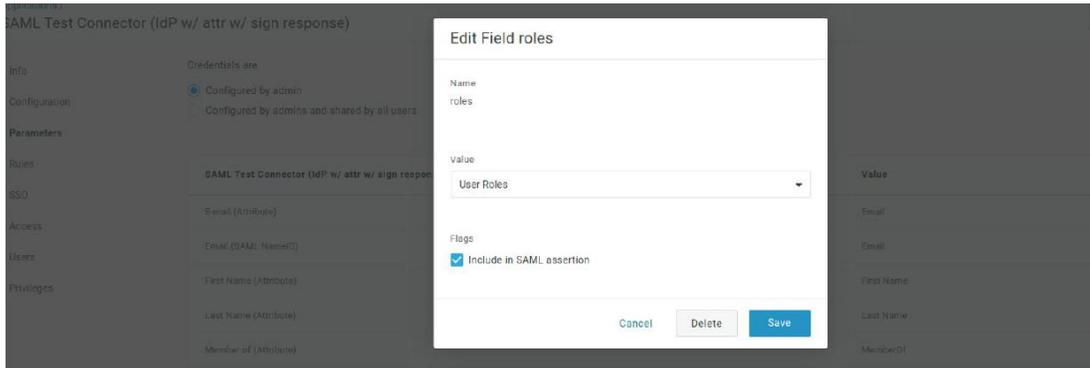


2. Add the Custom Roles to your IDP (onelogin is taken as an example)
 - a. Navigate to the Admin Role Creation Page
 - b. Create a Role Exactly with the same name as given in EloView Portal

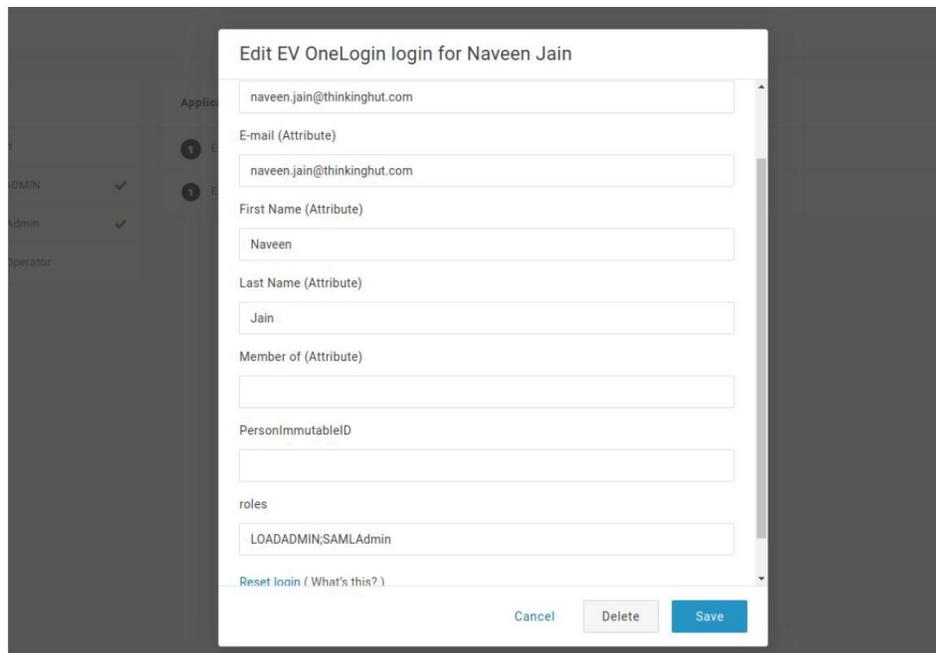


- c. Assign EloView App to be associated with the newly created Role
 - d. Assign the Eloview Users to that role

3. Modify your application config to add roles as additional attribute to be sent
 - a. Navigate to the EloView App Config in IDP -> Parameters
 - b. Add a new Attribute with name “roles” (all small letters) and map it to the “User Roles”



- c. Check the “Include in SAML assertion” else it will not be sent to the EloView Application
 - d. Save the configuration
4. Add EloView App to the User
 - a. Navigate to the User Configuration in the IDP.
 - b. Add the Elo View Application to the User
 - c. Check the parameters to be sent to the Application to ensure that includes the user’s Roles





- d. A User can have multiple roles for the same application. SAML Assertion will include all of them and separated by a “;”
- e. The SAML Assertion can also send roles which are not defined by the EloView Account. They will be ignored by EloView.
- f. If none of the roles assigned to the user have any permissions, by default the user will get the default “Viewer” capabilities.

Note: If the customer wants to use only the default System Roles, he can add the following role names to the IDP “Admin”, “Registered User”, “Viewer” and map them to the respective users.