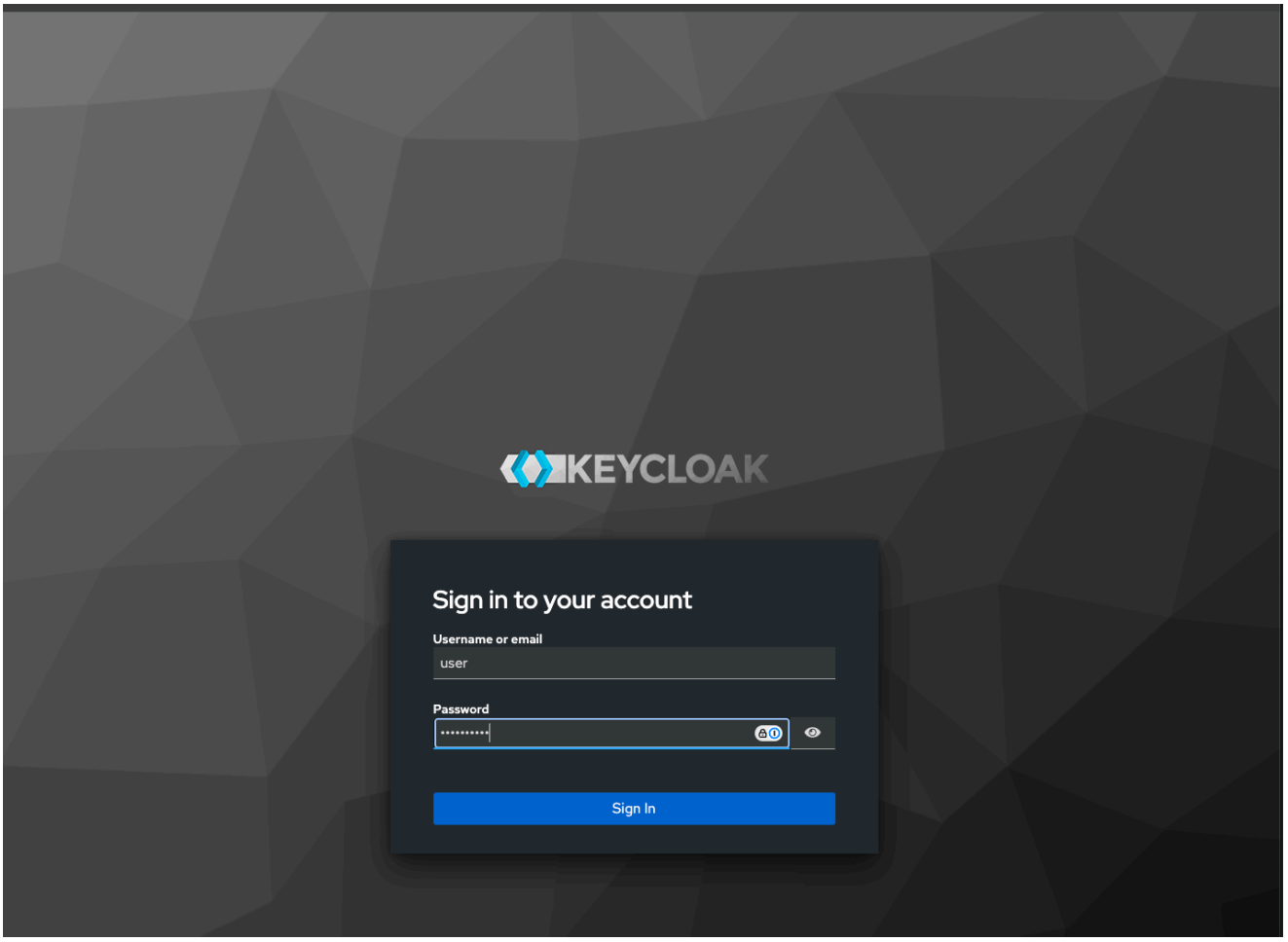
Keycloak Setup Instructions

Configuring Keycloak

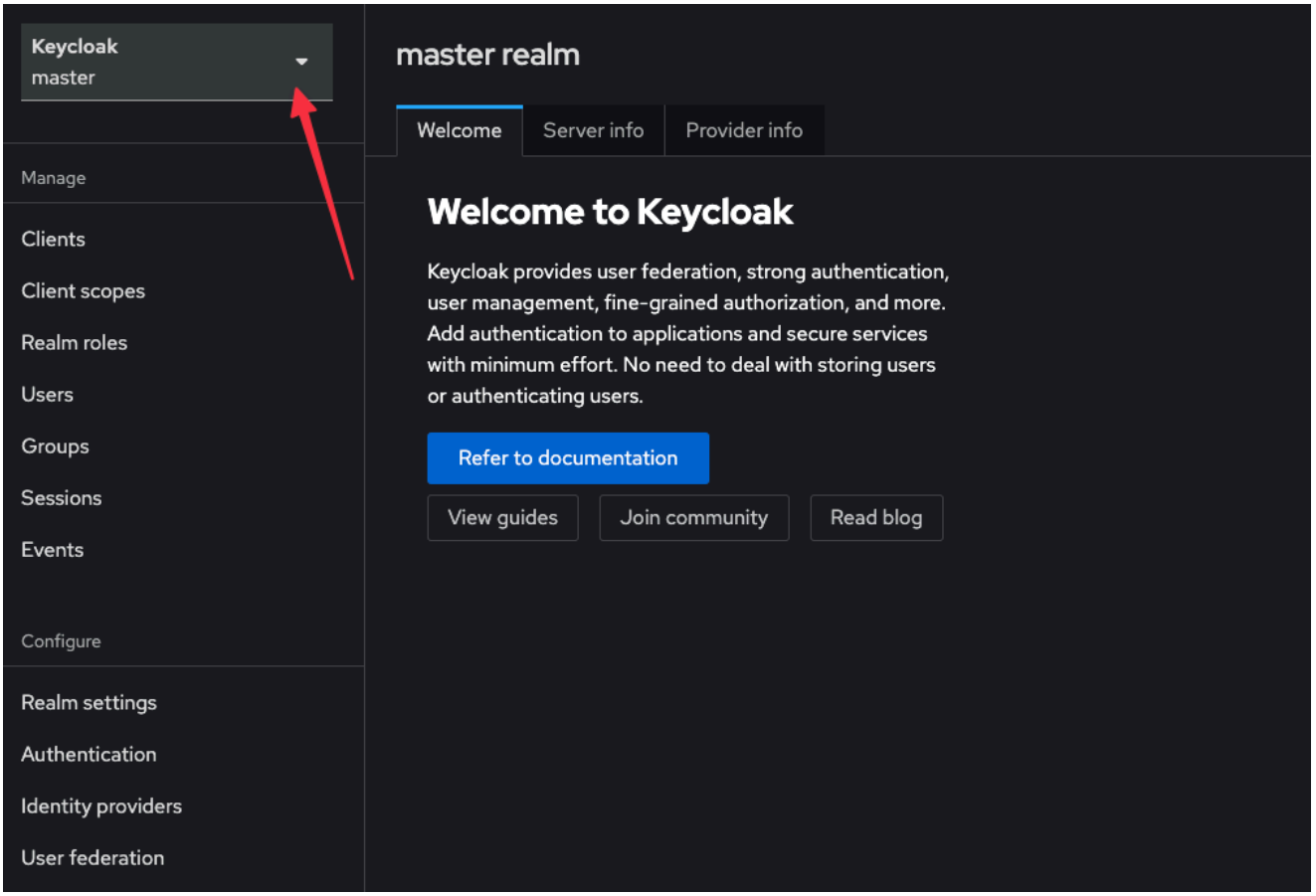
Once you have created a DNS entry, the next step will be to configure Keycloak as the OpenID Connect (OIDC) provider for the DPN software. Navigate to the admin console `keycloak-data-sharing.YOUR_DOMAIN/admin` or other DNS name forward slash to admin. The default username is `user` the password can be retrieved from the kubernetes secret. You can run the below command to retrieve the password.

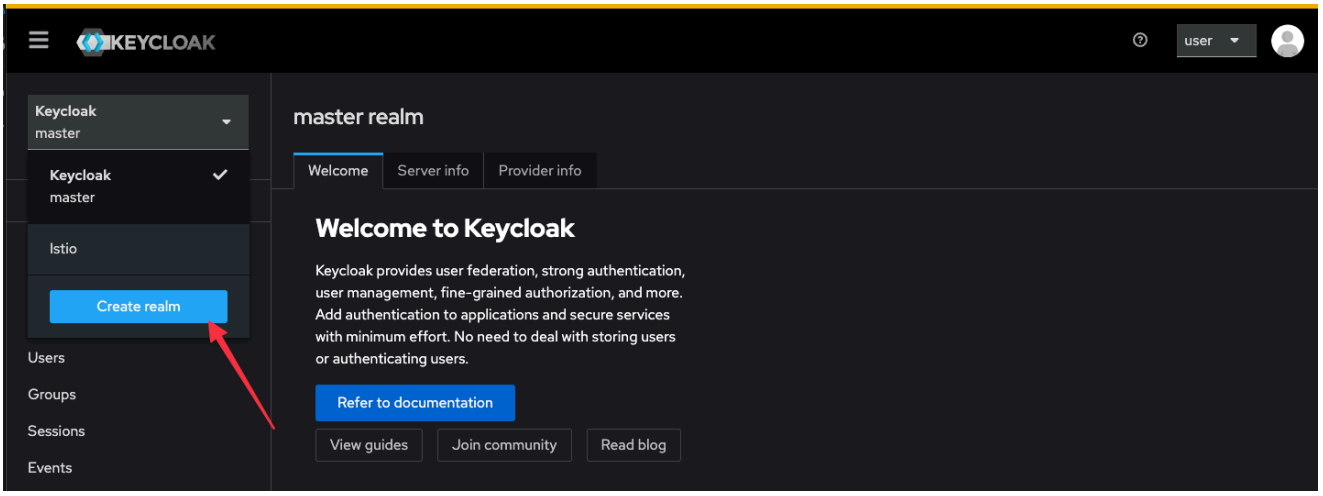
```
kubectl get secret -n keycloak keycloak -o jsonpath="{.data.admin-password}" | base64 --decode
```



Step 1

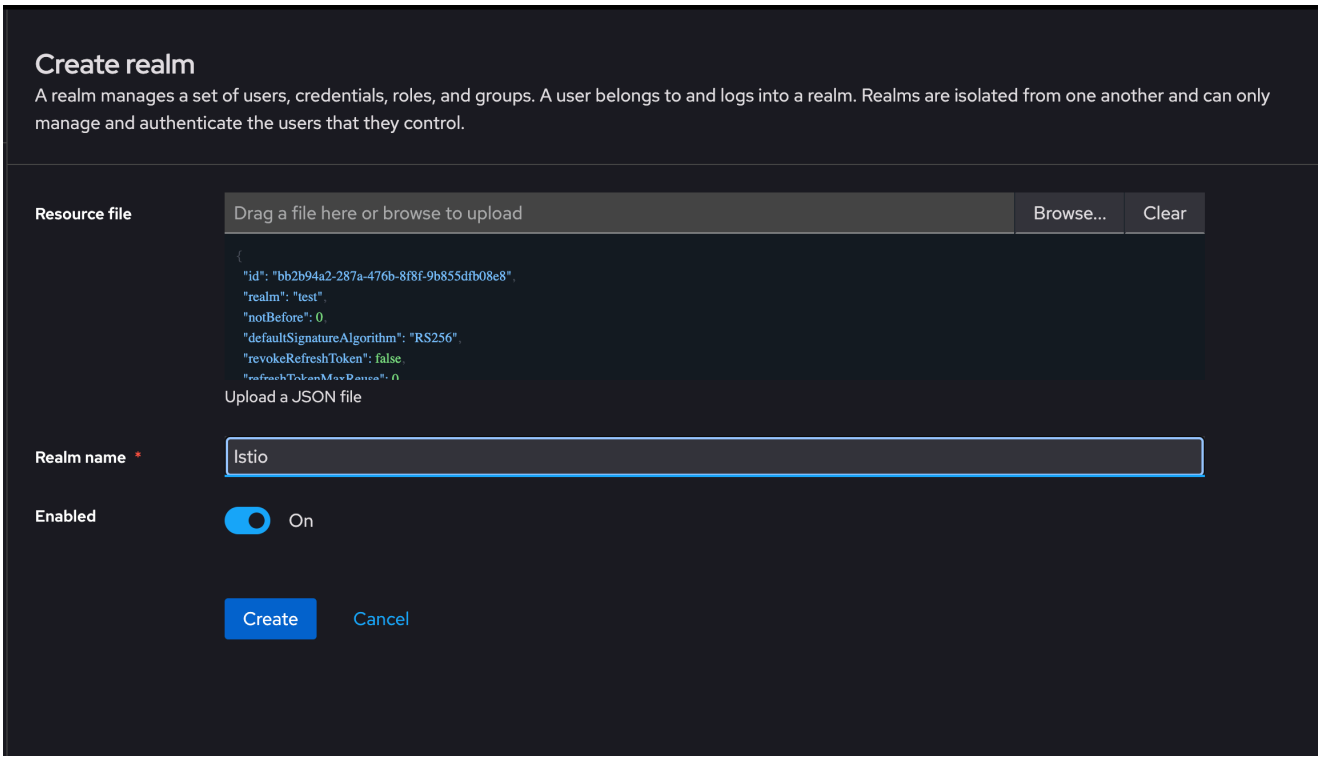
Create new realm drop-down and click on `Create Realm`





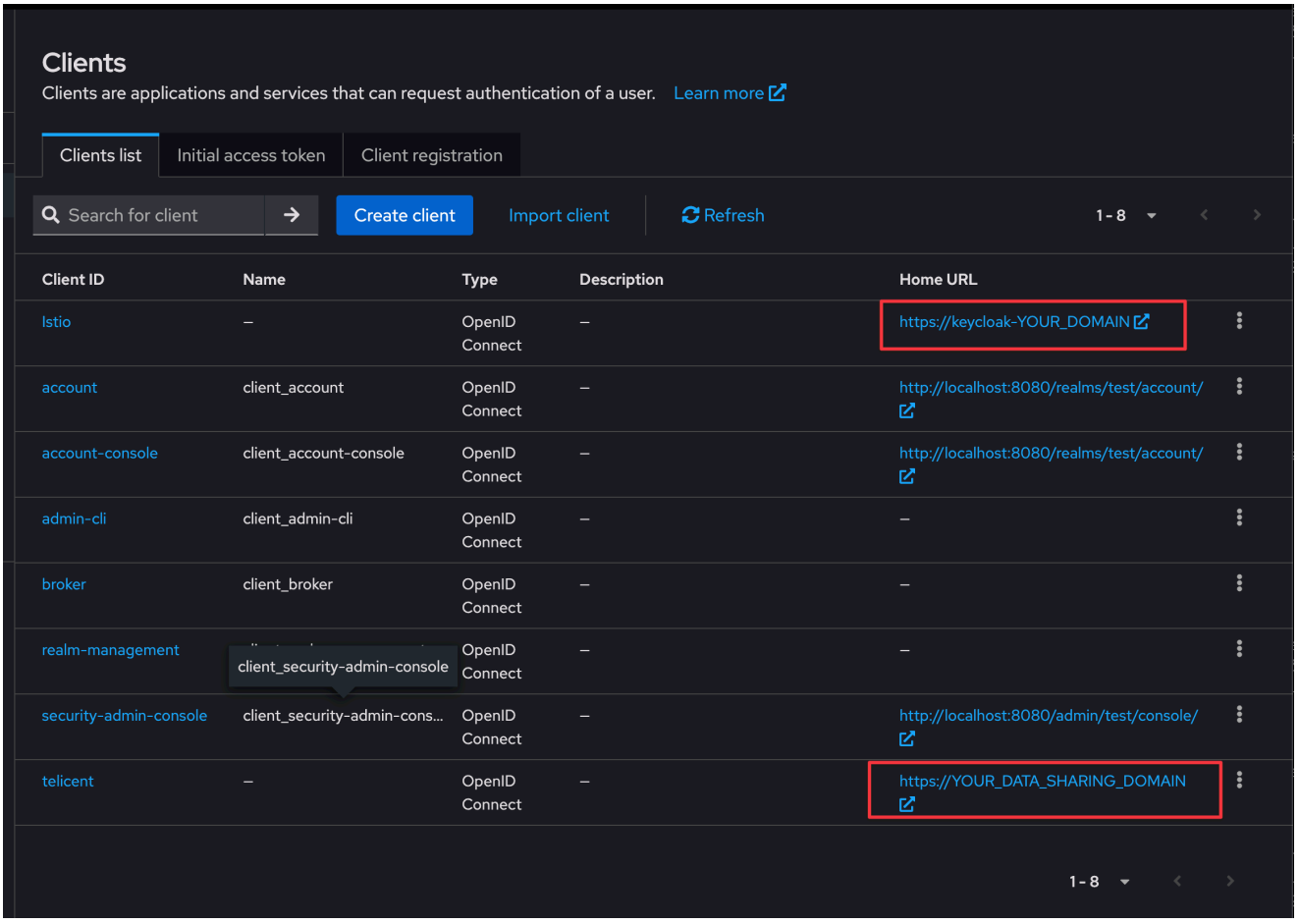
Step 2

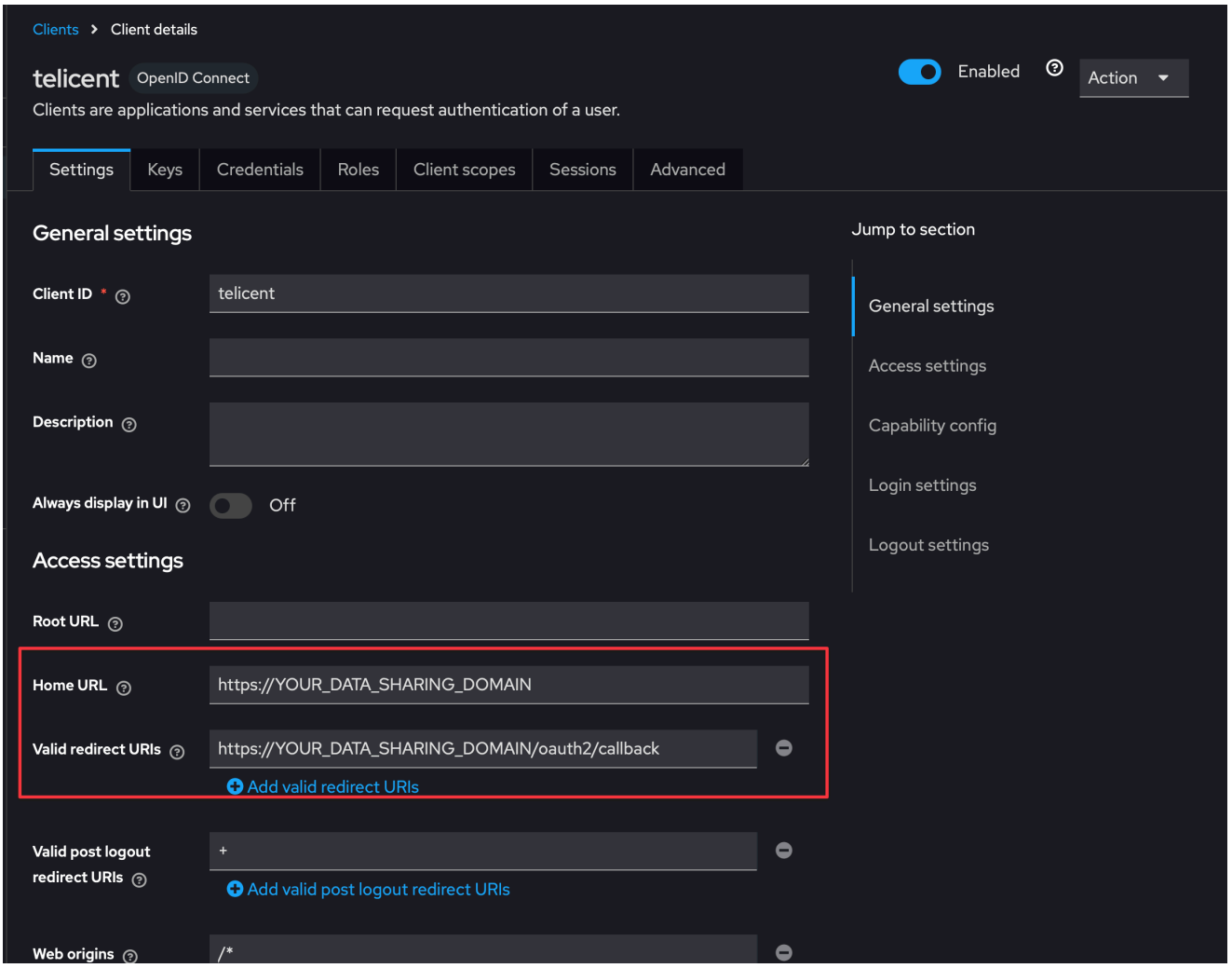
Click on Browse and upload the `template_realm.json` that is within the repository. Provide the Realm name as `Istio` Then click `Create`.



Step 3

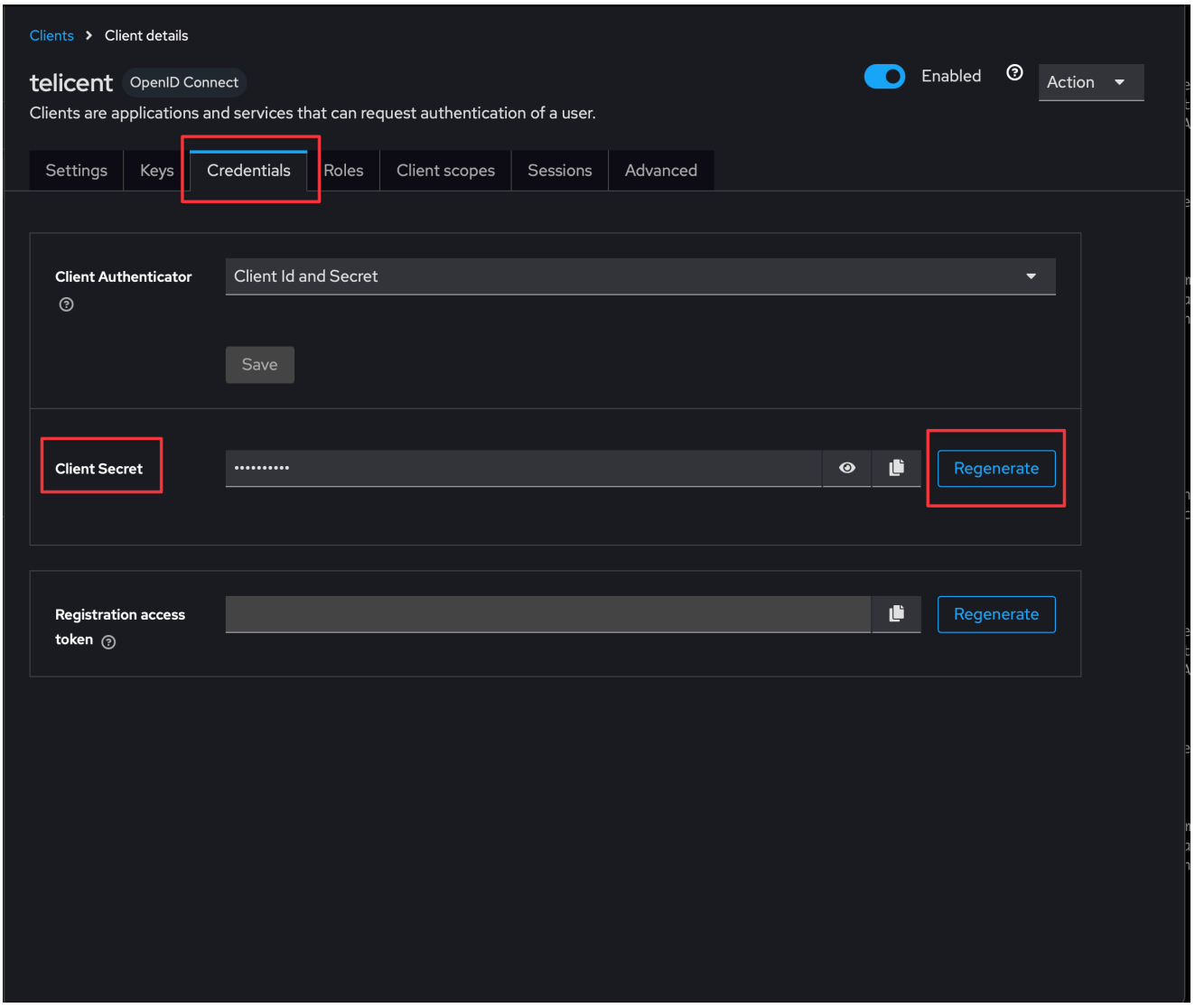
Click on the `Clients` on the left-hand pane and on the highlighted screenshot click on the Click on respective Client ID and update the domain to the specific domain you have created. Within the telicent Client ID update both the Home URL and Valid redirect URIs





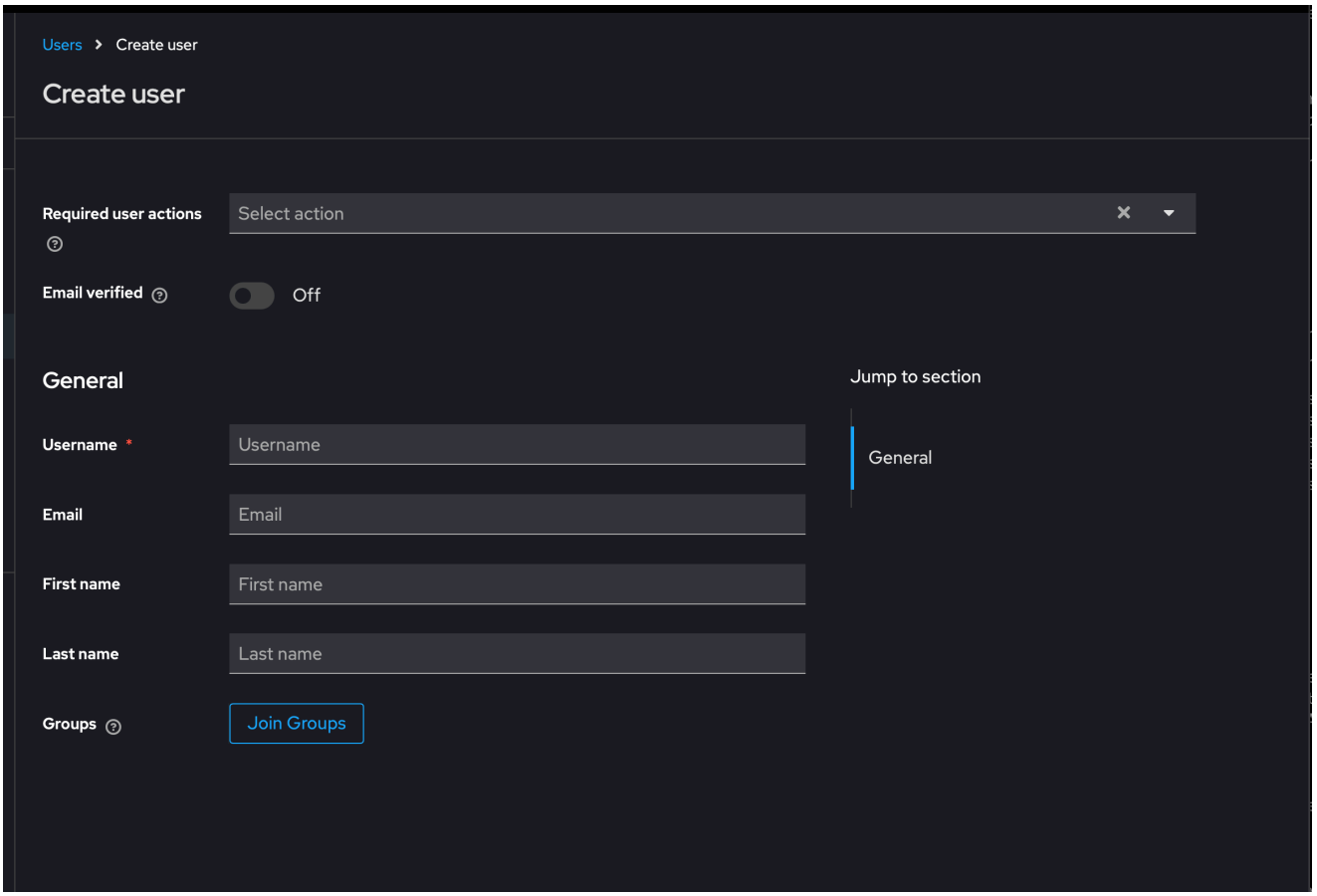
Step 4

Click on `telicent` Client ID within the `Clients` and Regnerate the Client Secret. Make a note of the secret as that will be required as part of the Oauth Proxy in the kubernetes manifest.

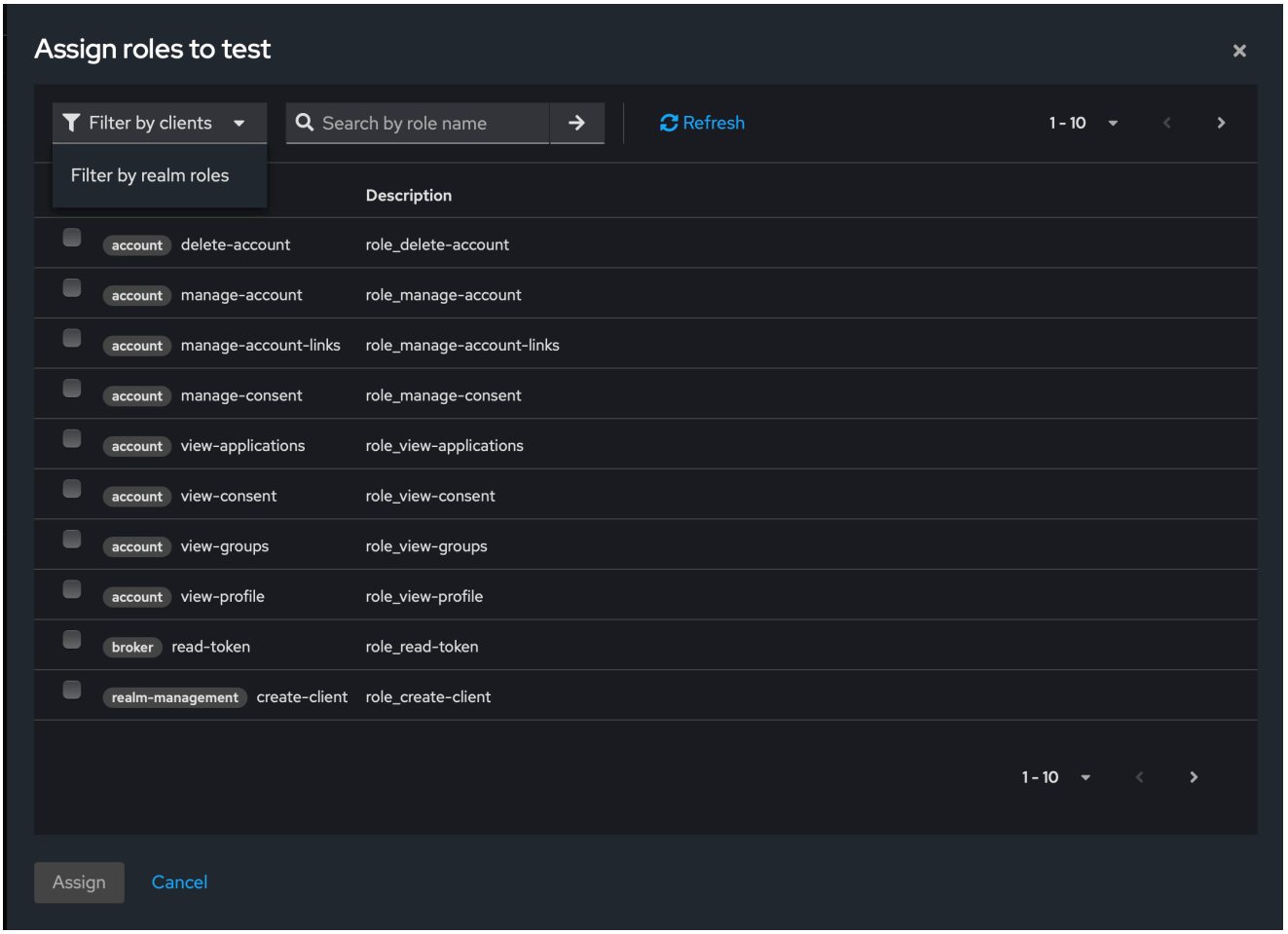


Step 5

On left-hand pane click on Users and click on `Create new user`



Create required users ensure you toggle on `Email verified`
Once the user has been, click on the `Role Mapping` tab and click on `Assign role`



Choose Filter by realm role and assign `tc_admin`, `tc_read`, `tc_write`.

Repeat this process for all users.