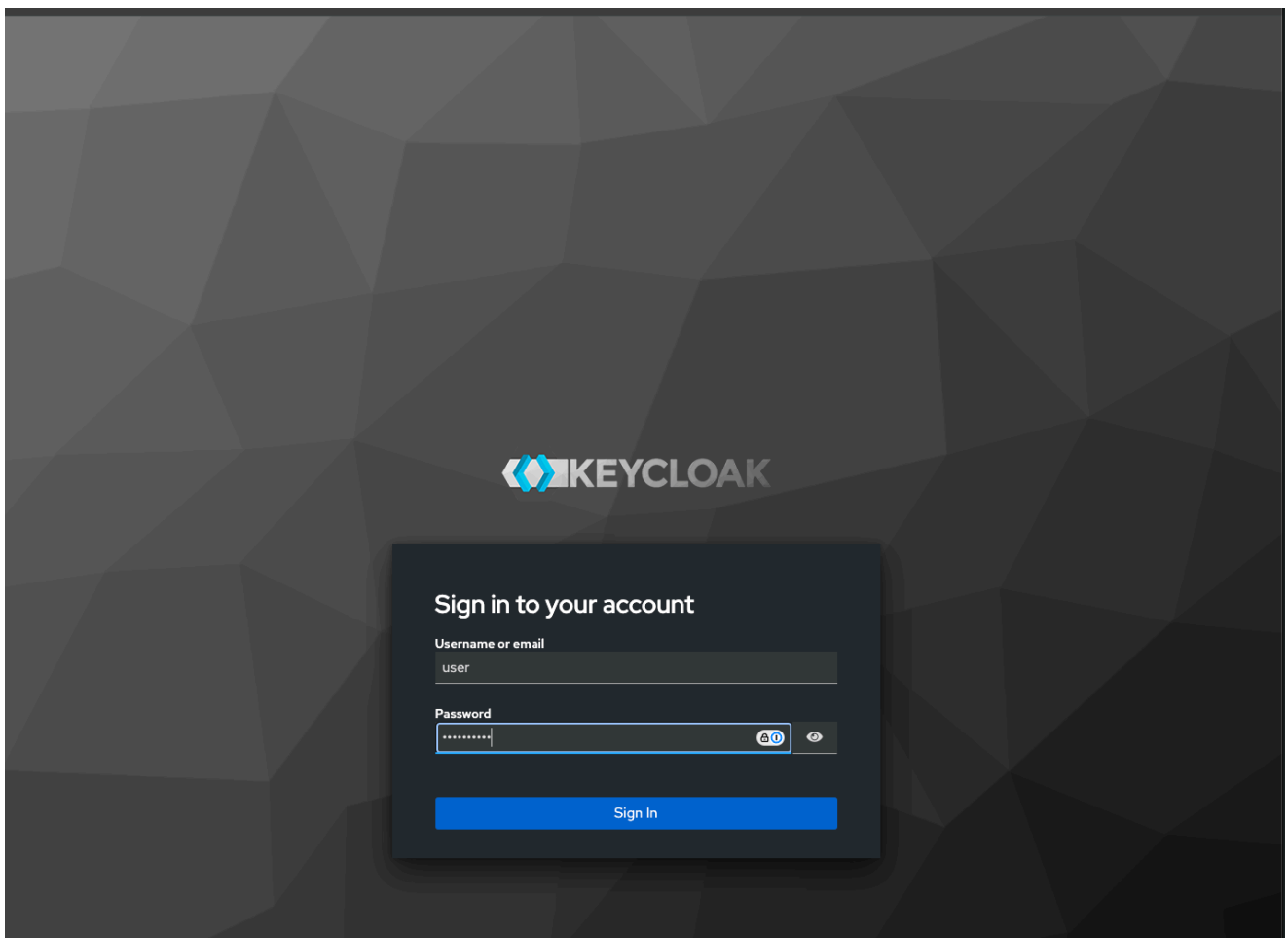


Keycloak Setup Instructions

Configuring Keycloak

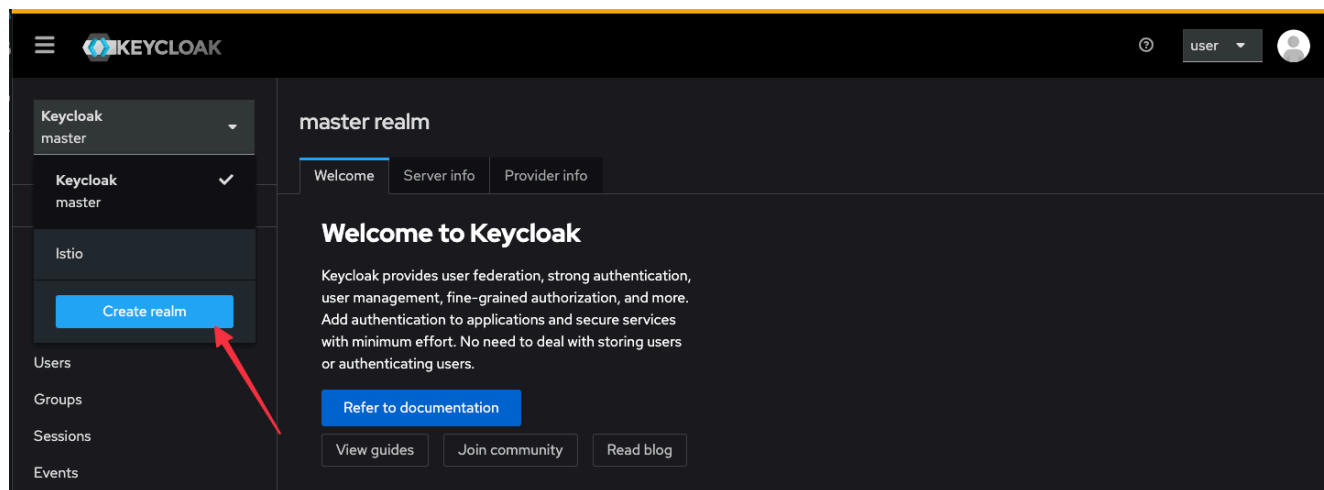
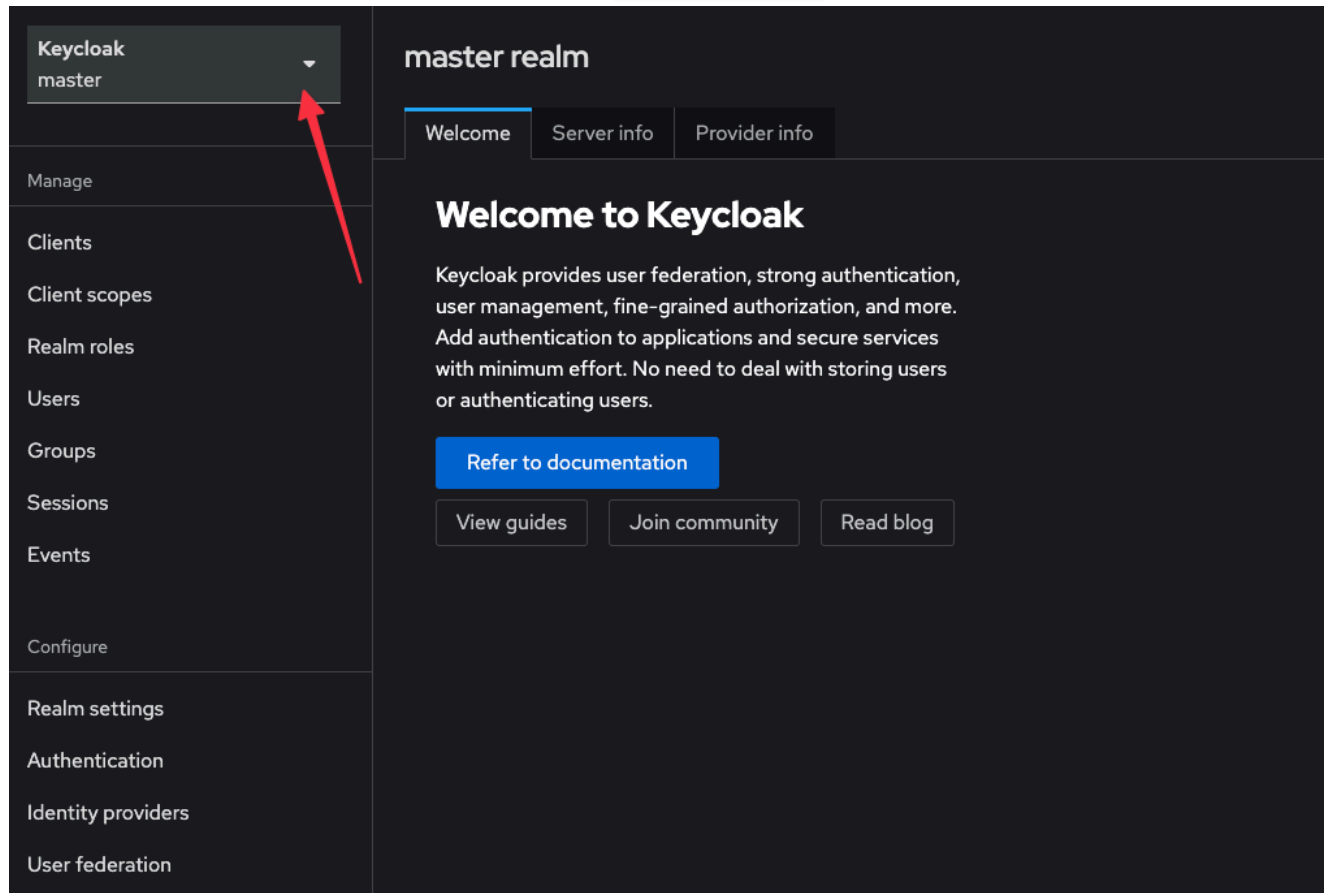
Once you have created a DNS entry, the next step will be to configure Keycloak as the OpenID Connect (OIDC) provider for the DPN software. Navigate to the admin console `keycloak-data-sharing.YOUR_DOMAIN/admin` or other DNS name forward slash to admin. The default username is `user` the password can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

```
kubect1 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` .

Create realm

A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.

Resource file

Drag a file here or browse to upload

Browse...

Clear

```
{
  "id": "bb2b94a2-287a-476b-8f8f-9b855dfb08e8",
  "realm": "test",
  "notBefore": 0,
  "defaultSignatureAlgorithm": "RS256",
  "revokeRefreshToken": false,
  "refreshTokenMaxDance": 0
}
```

Upload a JSON file

Realm name *

Istio

Enabled



On

Create

Cancel

Step 3

Click on the **Clients** on the left-hand pane and on the highlighted screenshot click on the **telicent**. 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

Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list

Initial access token

Client registration

Search for client



Create client

Import client

Refresh

1 - 8



Client ID	Name	Type	Description	Home URL	
Istio	—	OpenID Connect	—	https://keycloak-YOUR_DOMAIN	⋮
account	client_account	OpenID Connect	—	http://localhost:8080/realms/test/account/	⋮
account-console	client_account-console	OpenID Connect	—	http://localhost:8080/realms/test/account/	⋮
admin-cli	client_admin-cli	OpenID Connect	—	—	⋮
broker	client_broker	OpenID Connect	—	—	⋮
realm-management	client_security-admin-console	OpenID Connect	—	—	⋮
security-admin-console	client_security-admin-cons...	OpenID Connect	—	http://localhost:8080/admin/test/console/	⋮
telicent	—	OpenID Connect	—	https://YOUR_DATA_SHARING_DOMAIN	⋮

1 - 8



[Clients](#) > Client details

telicent

OpenID Connect

Enabled

?

Action

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

General settings

Client ID * ?

telicent

Name ?

Description ?

Always display in UI ?

Off

Access settings

Root URL ?

Home URL ?

https://YOUR_DATA_SHARING_DOMAIN

Valid redirect URIs ?

https://YOUR_DATA_SHARING_DOMAIN/oauth2/callback

+ Add valid redirect URIs

Valid post logout redirect URIs ?

+ Add valid post logout redirect URIs

Web origins ?

/*

Jump to section

General settings

Access settings

Capability config

Login settings

Logout settings

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.

Clients > Client details

telicent OpenID Connect Enabled Action

Clients are applications and services that can request authentication of a user.

Settings Keys **Credentials** Roles Client scopes Sessions Advanced

Client Authenticator Client Id and Secret

Save

Client Secret Regenerate

Registration access token Regenerate

Step 5

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

[Users](#) > Create user

Create user

Required user actions ✕ ▼

Email verified ? ☐ Off

General

Jump to section

General

Username *

Email

First name

Last name

Groups ?

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**

Assign roles to test

Filter by clients Search by role name → Refresh 1 - 10 < >

Filter by realm roles

		Description
<input type="checkbox"/>	account delete-account	role_delete-account
<input type="checkbox"/>	account manage-account	role_manage-account
<input type="checkbox"/>	account manage-account-links	role_manage-account-links
<input type="checkbox"/>	account manage-consent	role_manage-consent
<input type="checkbox"/>	account view-applications	role_view-applications
<input type="checkbox"/>	account view-consent	role_view-consent
<input type="checkbox"/>	account view-groups	role_view-groups
<input type="checkbox"/>	account view-profile	role_view-profile
<input type="checkbox"/>	broker read-token	role_read-token
<input type="checkbox"/>	realm-management create-client	role_create-client

1 - 10 < >

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

Repeat this process for all users.