Reporting Suite

Reporting and Dashboarding

Single Sign-On Guide

Version 5.6.0

1/22/2026

Enghouse Interactive

Contents

About this Guide

Audience

This Guide is for the developer responsible for integrating Single Sign On authentication of Reporting with their own applications. The developer or administrator must possess a working knowledge and skills related to this topic.

New in this release

Added information about the possibility of editing the shared secret when using Single Sign On via JSON Web Token (JWT).

Guide conventions

This Guide uses the following text formats and notation conventions.

Text format

Bold text indicates a button, field, link, option name, or similar function requiring an action.

Italicized text indicates new terms, directory paths, or references to external documents.

`Text in this font` indicates code.

Notes and cautions

Icons used throughout this Guide identify additional details or special conditions.

> **Note**
> Provides additional information or describes special circumstances.

> **Caution**
> Warns of user actions that may cause system failure or irreversible conditions.

> **Stop**
> Describes actions that you should only perform under the supervision of Enghouse Interactive Customer Support.

Legal disclaimer

This document is governed by the terms of the software license agreement and applicable contract (including addendums) entered into with Enghouse.

Contact information

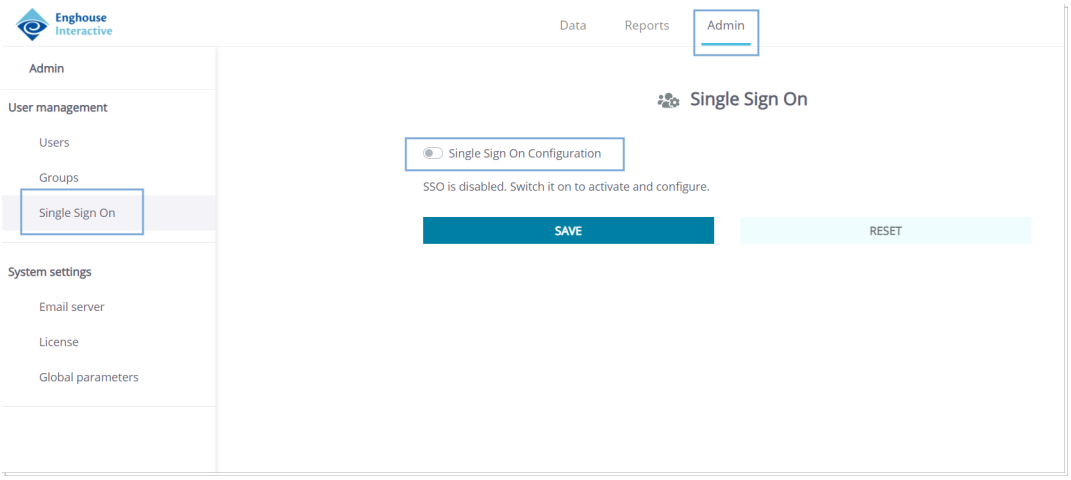
To submit comments or questions about the content in this Guide, please open a case in Support.

Single Sign On in Reporting

Single Sign On (SSO) is a mechanism that allows systems outside of Reporting to authenticate users and subsequently tell Reporting that the user is valid and has been successfully authenticated. This mechanism allows other systems to register and authenticate users in and for Reporting. SSO in Reporting can be done via the JWT and OpenID Connect protocols.

In order to use SSO via JWT or OpenID Connect, this first needs to be enabled and set up by an Administrator. To do this, follow these steps:

1. In the top section of the Reporting window, click the **Admin** tab. This takes you to the Admin panel.
2. In the **Admin** view, in the left-hand side of the window, click **Single Sign On** in the User management group.
3. Switch the **Single Sign On Configuration** toggle ON to enable SSO and its configuration.



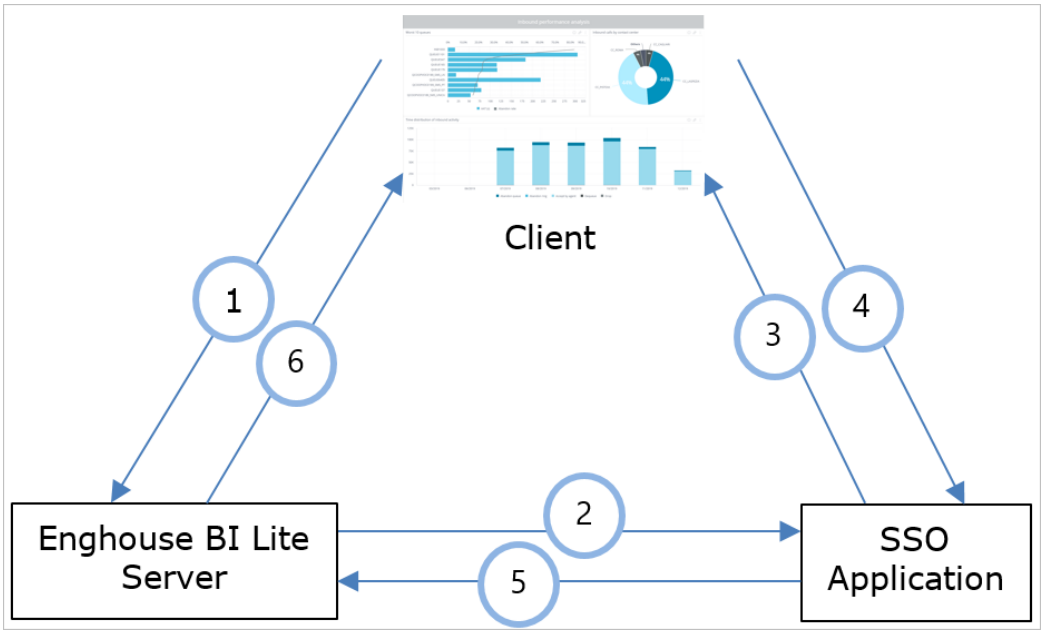
4. Select a method, i.e. a protocol for SSO:
   - To connect via JWT, see *SSO via JSON Web Token (JWT) below*.
   - To connect via OpenID Connect, see *SSO via OpenID Connect on page 8*.
5. Once you have entered all the relevant settings, click **Save** to preserve your settings.

SSO via JSON Web Token (JWT)

One of the ways Reporting uses **Single Sign On** is via JSON Web Token (JWT). JWT is a token that represents the users' credentials wrapped in a single query string. Reporting also uses additional parameters for security reasons.

Reporting SSO Authentication flow

The following schema describes the JWT authentication flow:



1. A user requests a resource from Reporting.
2. Reporting recognizes that no authenticated cookie is present. If SSO is enabled, the user is redirected to an SSO Endpoint defined by the admin in the Reporting web application.
3. The user must authenticate their account with the provided SSO Endpoint.
4. The application at the SSO Endpoint authenticates the user and generates a JWT.
5. The application at the SSO Endpoint redirects the user back to Reporting, with the encoded JWT in the query string. Reporting then sets a cookie that authenticates the user until the end of their session.
6. Reporting provides the user with the resource requested in the first step.

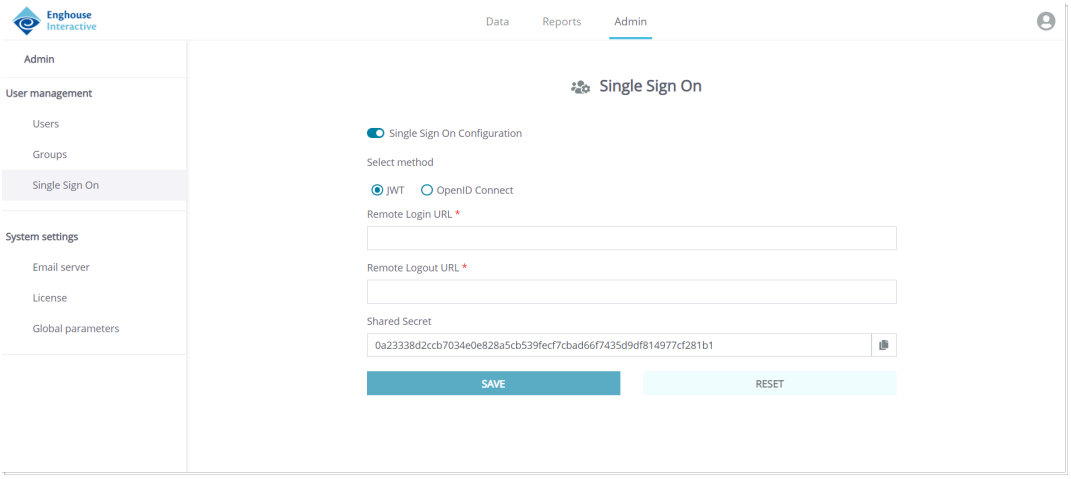
Setting up SSO via JWT

After SSO authentication is enabled on the Reporting server and JWT is the selected protocol, settings for this method of SSO become available. Required fields are marked with *.

A **Shared Secret** is generated and displayed on the SSO configuration page. The shared secret is the key used to sign the JWT payload. The JWT must be signed with the **Shared Secret**, so that it can later be verified in Reporting. You can copy the shared secret manually or by clicking the **Copy to clipboard** button at the right edge of the Shared Secret field. You can also edit the originally generated shared secret, but you must keep the 64-character hexadecimal string format.

Remote Login URL and **Remote Logout URL** endpoints must also be set in the Administrator settings in Reporting.

> **Note**
> The SSO configuration page and all its settings are accessible only to Administrator users.



JWT payload description

JSON Web Tokens consist of three parts separated by dots (.).

The parts are identified as:

- **Header**: Used to specify the token type and signature algorithm.
- **Payload**: The real content of the JWT, where the user is described.
- **Signature**: A checksum of the JWT that is used to verify it.

A typical JWT takes the following form: *xxxxx.yyyyy.zzzzz*, with *xxxxx* representing the header, *yyyyy* the payload, and *zzzzz* the signature part.

The following sections describe each part of the JWT in detail.

Header

The header consists of two parts: the type of the token, which is JWT, and the signing algorithm being used.

For example:

```
{
    "alg": "HS256",
    "typ": "JWT"
}
```

Next, this JSON is Base64Url encoded to form the first part of the JWT.

The following table sums up the fields included in the header:

Attribute	Description	Type	Value
typ	Type of token	string	JWT
alg	Algorithm of JWT signature	string	HS256

Payload

The second part of the token is the payload, which contains the claims. Claims are statements about a user, along with additional data.

Here is an example payload:

```
{
    "sub": "user@example.com",
    "firstName": "John Doe",
}
```

The payload is then Base64Url encoded to form the second part of the JSON Web Token.

The following table describes each field of the Reporting JWT payload:

Attribute	Description	Type	Value	Mandatory	Default value
iat	Time when the token was generated. Used to ensure that the given token gets used shortly after it was generated	integer	Number of seconds since UNIX epoch	Yes	
sub	Email of the user being signed in. Used to uniquely identify the user in Reporting.	string	e.g. 'John.Doe@example.com'	Yes	
jti	A unique string that is used to prevent replay attacks by making sure the token is used only once.	string	e.g.: generate a UUID	Yes	
userName	User name of the user being signed in. Used to uniquely identify the user in Reporting.	string	e.g. 'John.Doe'	No	Default value is set to the same as the `sub` attribute
firstName	First name of the user, later used in the registration process if the user is	string	e.g. 'John'	No	Default value is set to the same as

Attribute	Description	Type	Value	Mandatory	Default value
	accessing Reporting for the first time.				`sub` attribute
lastName	Last name of the user, later used in the registration process if the user is accessing Reporting for the first time.	string	e.g. 'Doe'	No	None
role	User role in Reporting.	string	Allowed values are: - Administrator - Viewer - Designer - DataDesigner - PowerViewer	No	'Viewer'
lang	Language of the Reporting user interface	string	If not specified, the default Reporting language is used at first login. After registering and logging in, the user can select a different language.	No	'en'

Signature

To create the signature part, the following elements are used to create a sign:

- the algorithm specified in the header,
- the encoded header,
- the encoded payload,
- a secret.

For example, using the HMAC SHA256 algorithm, the signature will be created in the following way:

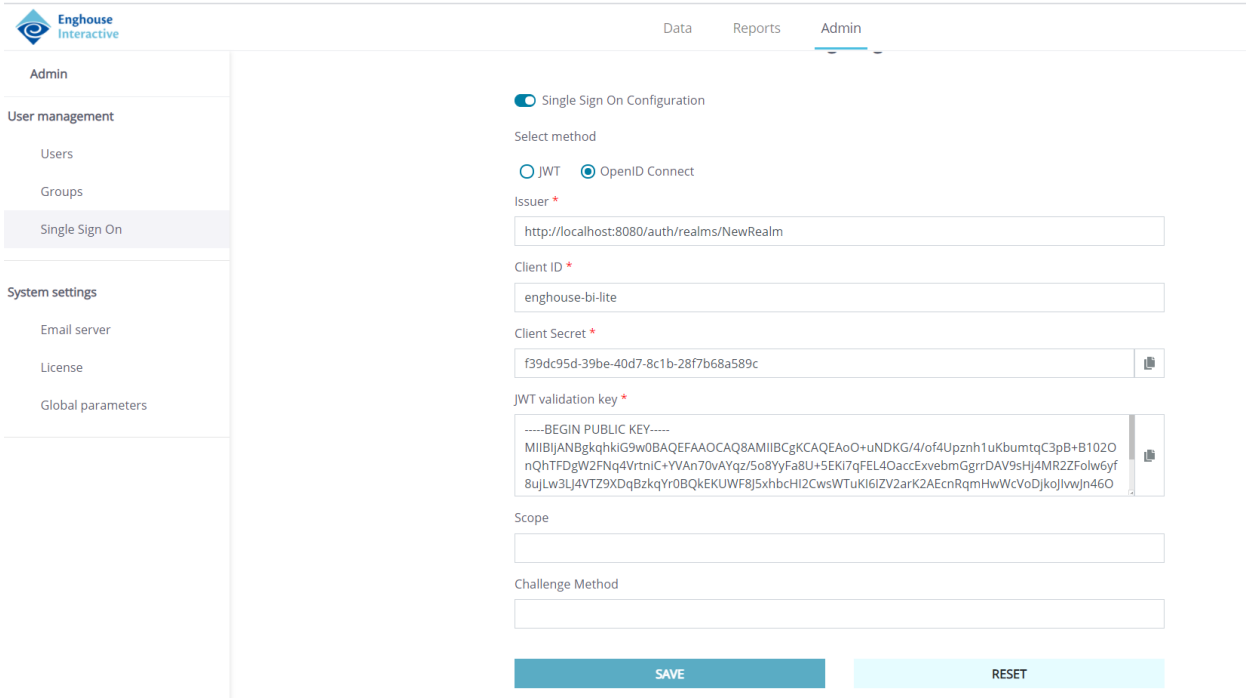
```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    secret)
```

The signature is used to verify the message was not modified along the way.

SSO via OpenID Connect

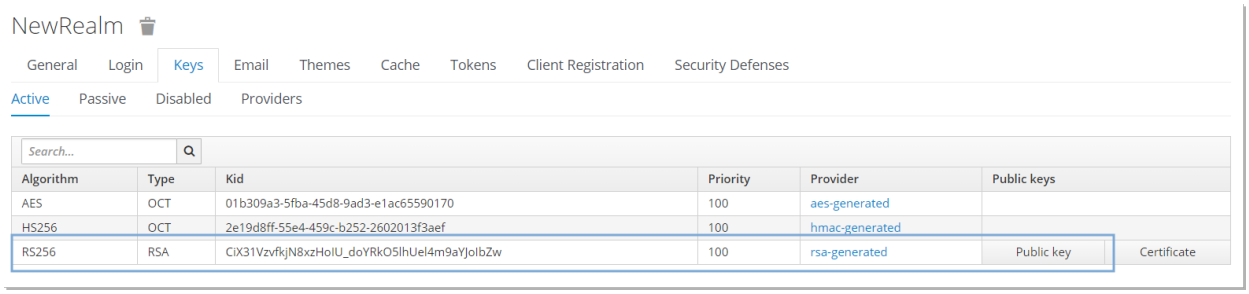
> **Note**
>
> For the purposes of this Guide, the used OpenID Connect provider is Keycloak. However, Reporting is agnostic of the provider, and can be integrated with any other provider that supports the OpenID Connect protocol. The following steps apply for all such cases. For further information on the Keycloak configuration used in this specific OpenID Connect example, see *Keycloak Configuration on page 11*.

Another way Reporting uses **Single Sign On** is via OpenID Connect. To access its configuration, select **OpenID Connect**. The settings for this method of SSO are now available. Required fields are marked with *.



To configure OpenID Connect, fill the following fields:

- **Issuer**: For the purposes of this Guide, the issuer is Keycloak and the URL needs to be set to `<keycloak_base_url>/auth/realms/<RealmName>`. For more information, see *Keycloak Configuration on page 11*.
- **Client ID**: Client ID of this application in Keycloak.
- **Client Secret**: The secret generated in the "Credentials" tab of the Client settings.
- **JWT validation key**: The RSA public key from the Realm Settings, found in the Keys tab in Keycloak (may vary based on which issuer you use).

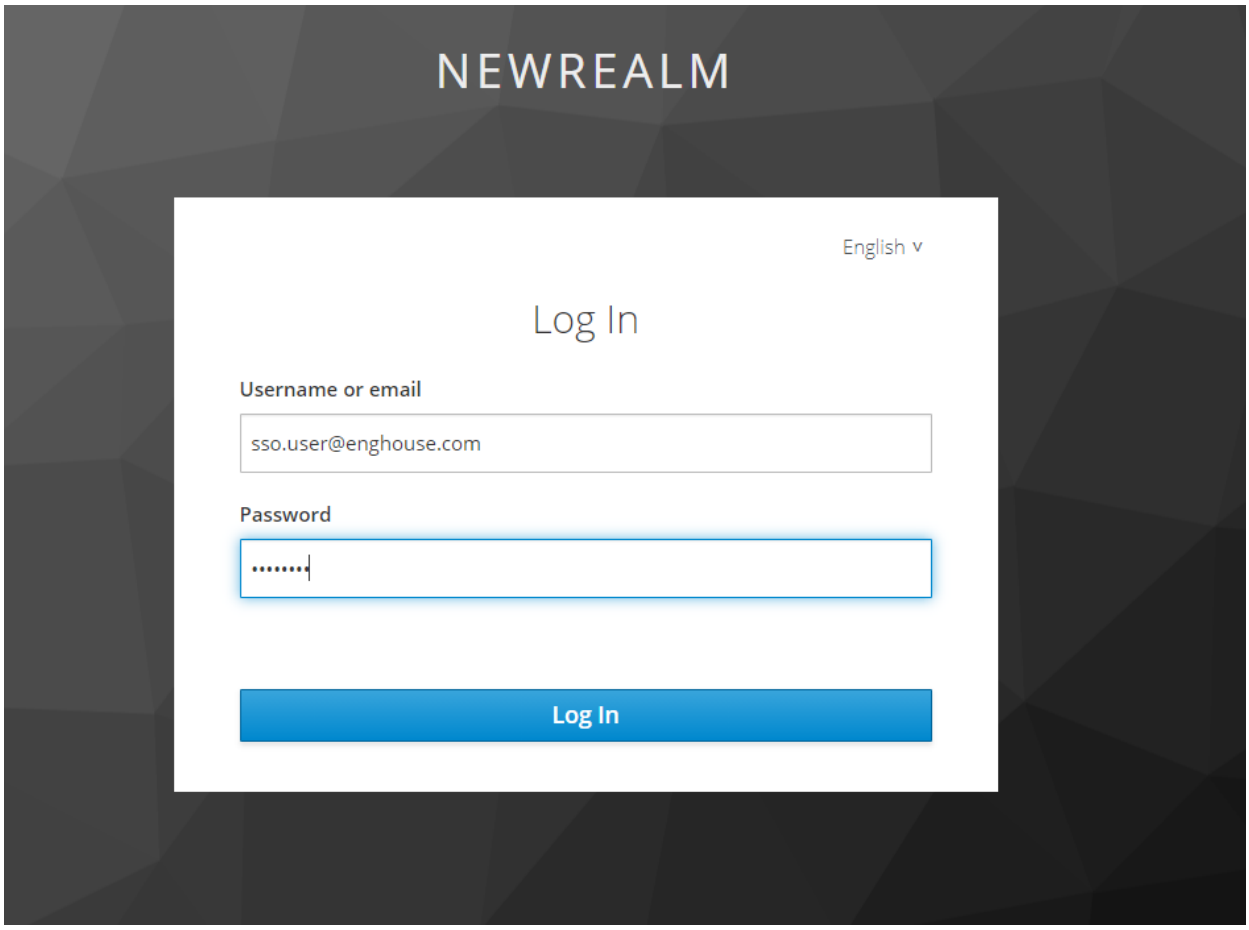


> **Note**
>
> When pasting a public key from Keycloak into the Reporting configuration, the key needs to be formatted as follows (the new line before and after the public key pasted from Keycloak is required!):
>
> ```
> -----BEGIN PUBLIC KEY-----
> <public key pasted from Keycloak>
> -----END PUBLIC KEY-----
> ```

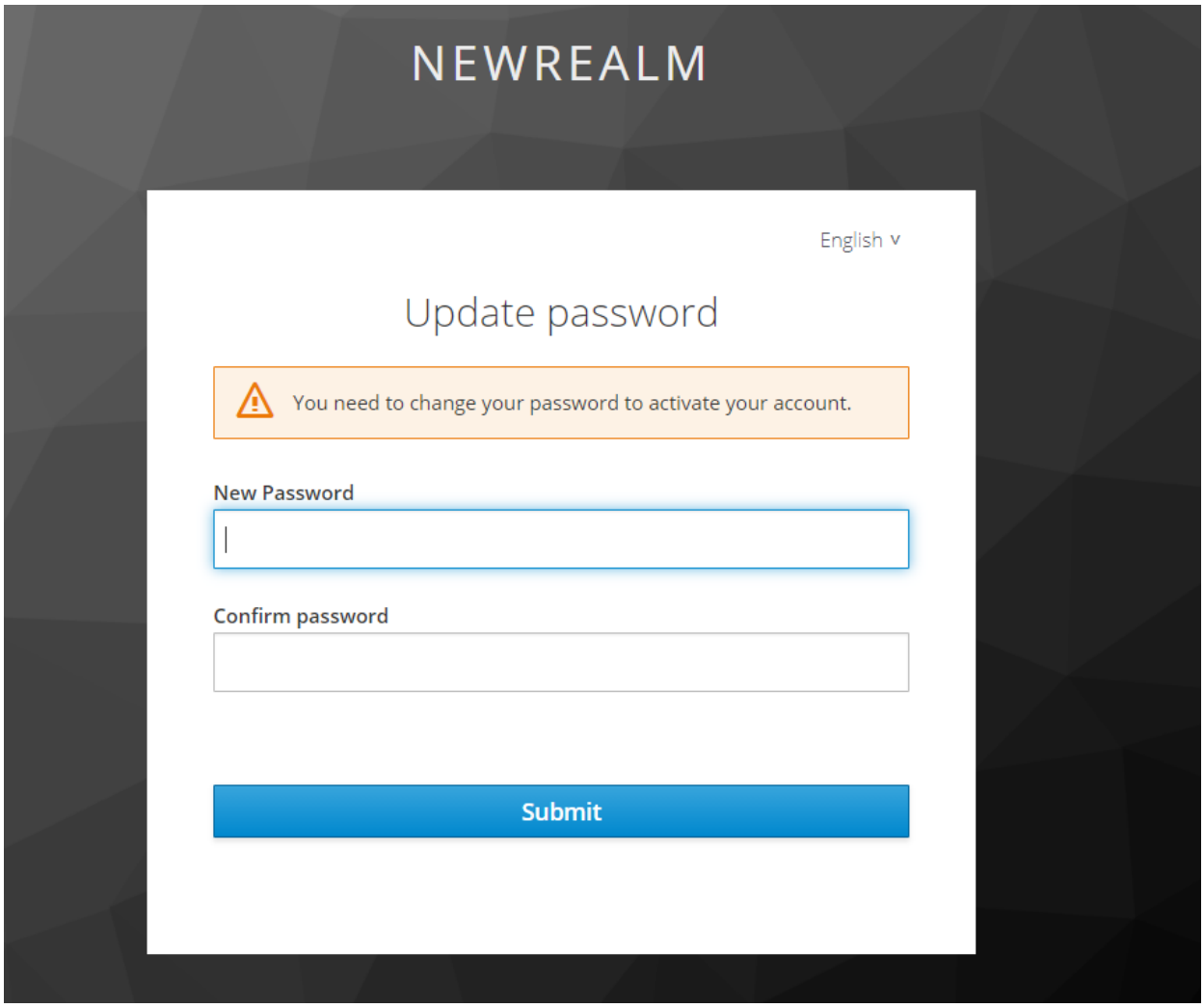
- **Scope**: This field not required. By default it is set to *openid*, which means full scope. If advanced scoping settings are needed, you can set it to a different value here.
- **Challenge Methods**: This field is not required. By default it is set to *S256*. You can set a different challenging method here.

> **Note**
>
> To use SSO via **EIS** in Reporting, you have to set the **Client ID** to "`ei_enghousebi_ers`", and the **Scope** needs to include "`all-roles`", for example, "`openid all-roles`". For information on EIS, see the *Reporting Administrator Guide* or *System Administrator Guide*.

Click **Save** after entering all the needed settings. If all the settings are configured correctly, all users are redirected to the Keycloak login page upon their next login:



If their password was set as temporary, the user is immediately asked to change the password.



After a successful login, and a password change, the user is redirected back to Reporting with the corresponding role rights assigned. This user can continue using the system as intended.

Keycloak Configuration

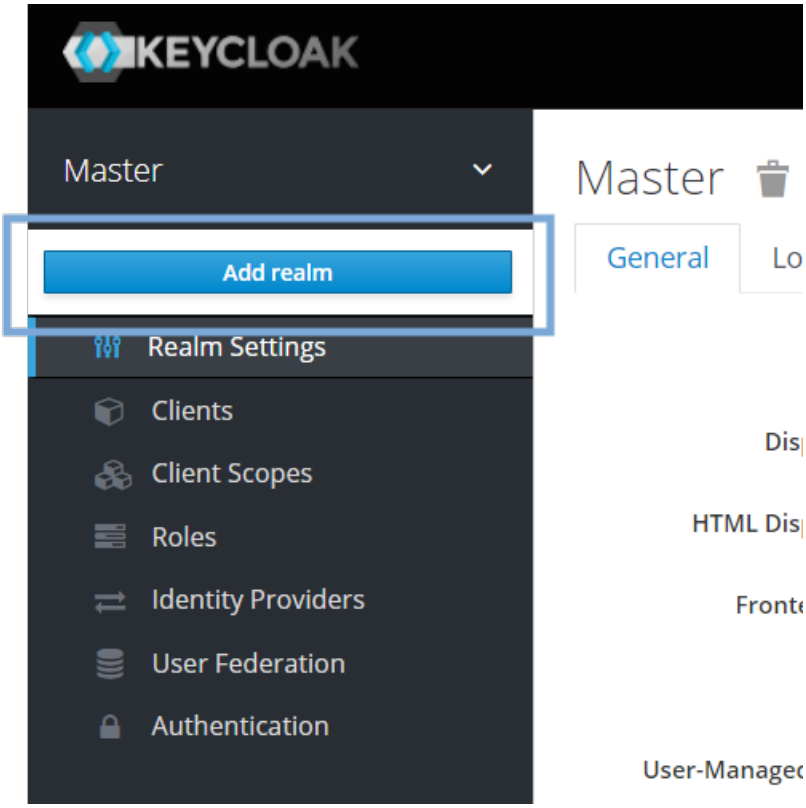
> **Note**
> The following sections of this Guide are an example of how SSO can be configured via OpenID Connect by using Keycloak. However, Reporting is agnostic of the service you use. These steps are not obligatory and can be otherwise done through any similar service or system of your choice.

To enable SSO for multiple applications through Keycloak and via OpenID Connect, a realm for these applications needs to be created. After realm creation, each client application needs to be registered in the realm. Finally, individual users need to be created, or imported from an external system, such as Active Directory.

Realm creation

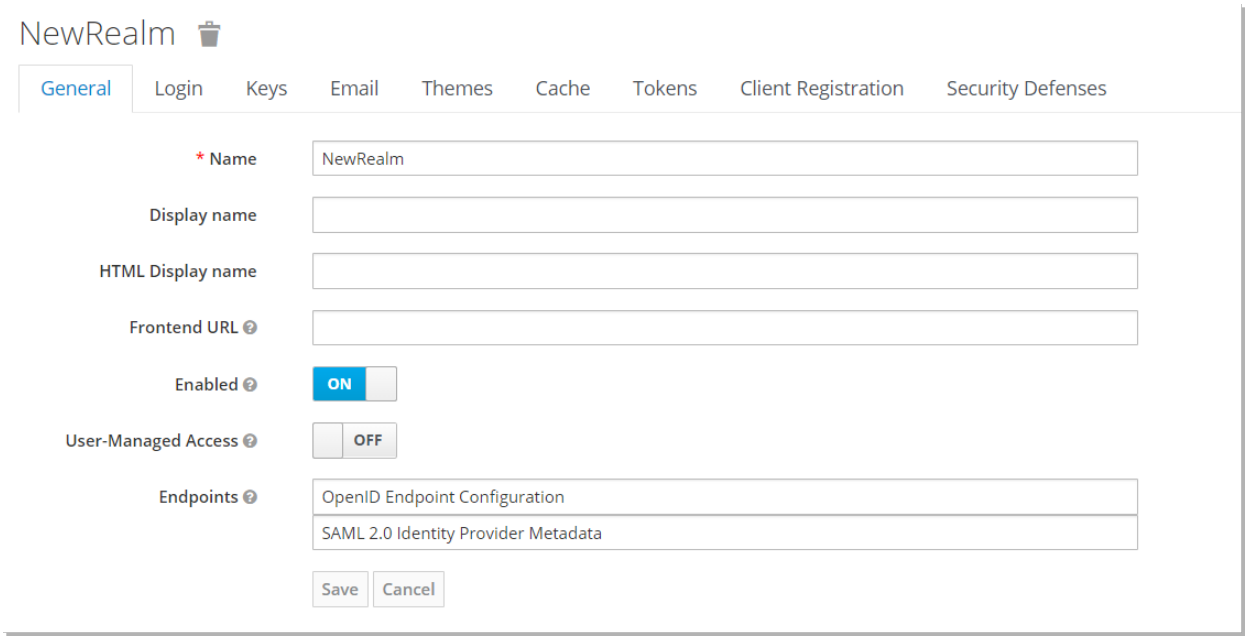
> **Note**
> In order to follow the steps described below, you need to have access to an Administrator account for your Keycloak system. This is an account unrelated to Reporting and needs to be made and maintained by you, independently of your (future or existing) Reporting account(s).

After logging into the Administration Console of Keycloak as an Administrator, the default realm is Master realm. Open the drop-down menu in the upper left corner of the screen, then click **Add realm** to add a new realm to the system.

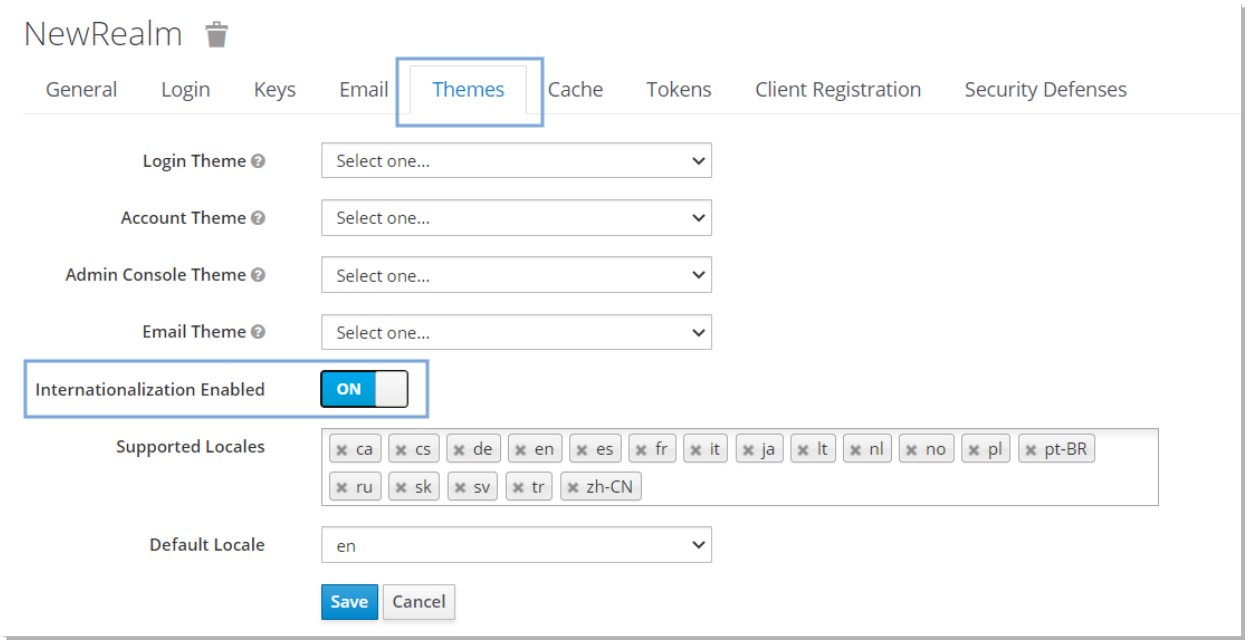


In the following window, you can import an existing realm or create a new one. To create a new realm, enter the realm name in **Name**. This field is required.

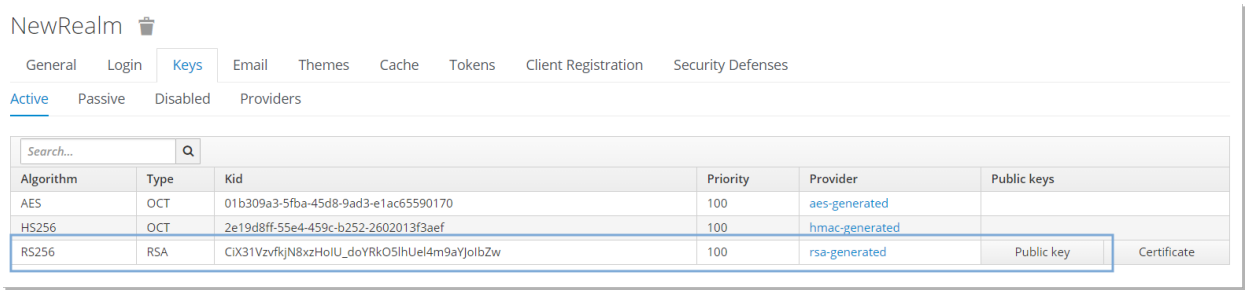
Once the realm is created, new tabs and fields become available for further configuration.



Click the **Themes** tab. Switch the **Internationalization Enabled** toggle ON to allow users to select their preferred language on the login screen. Add supported and default Locales as necessary.

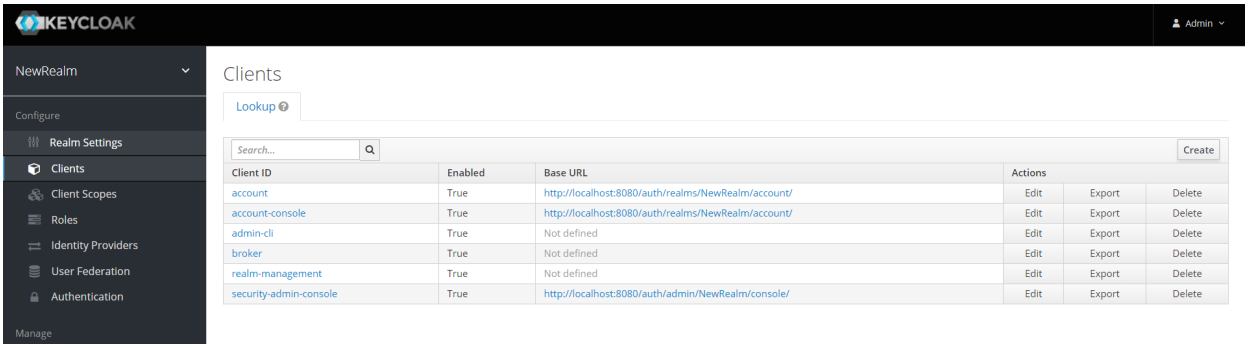


Click the **Keys** tab. The RSA key needed for the Reporting SSO configuration process is located here.



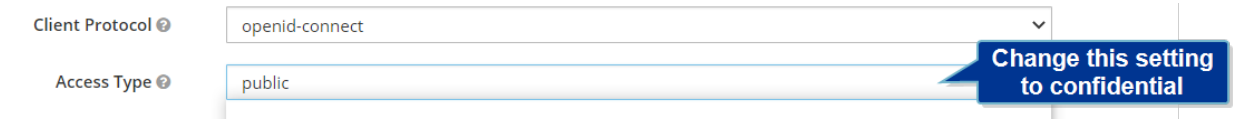
Client registration

To register a new client, click **Clients** in the menu on the left-hand side of the window, then click **Create** in the upper-right corner of the clients table. In this case, Reporting is going to be the client.

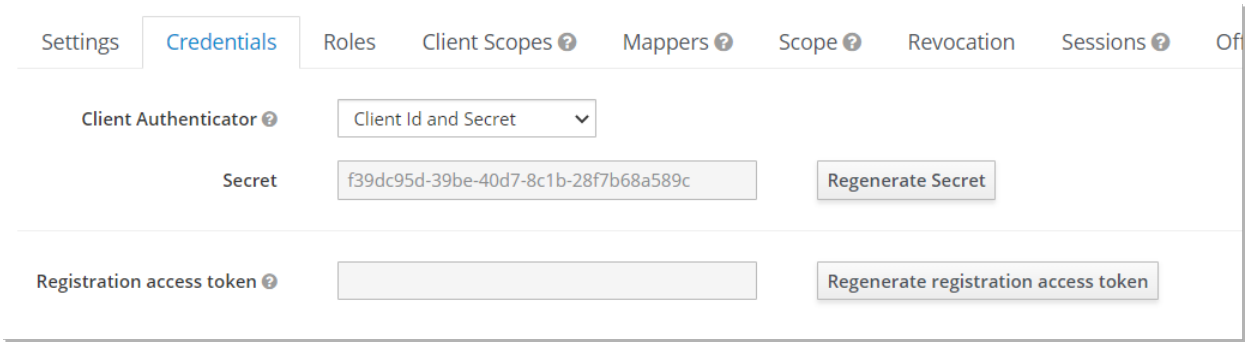


A unique **Client ID** must be defined, together with the **Client Protocol** (openid-connect in this case), and with the client application **Root URL**. A new client can also be imported.

Once the client is created, new tabs and fields appear. Change the **Access Type** from **public** to **confidential** via the drop-down menu. Save these changes by clicking **Save**.



After saving these changes, the **Credentials** tab appears for this client. Click the **Credentials** tab, then navigate to the **Client Authenticator** drop-down menu. By default, the selected option here is **Client Id and Secret**, and the client **Secret** is generated. The Secret can also be regenerated here.



Click the **Roles** tab. Here you can create and define new user roles. To create a role, it is sufficient to specify its name.

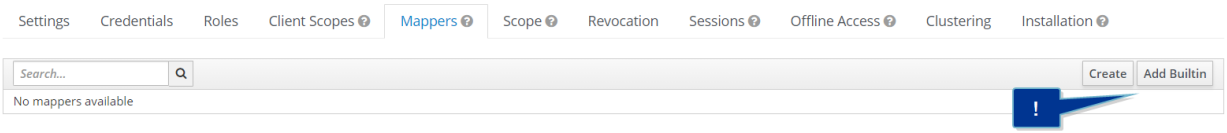
For Reporting, the following roles are available: Viewer, PowerViewer, Designer, DataDesigner, and Administrator. You can specify the actions each role can do by clicking **Edit** in the **Actions** column.

Once you have done so, click **Save** to continue.

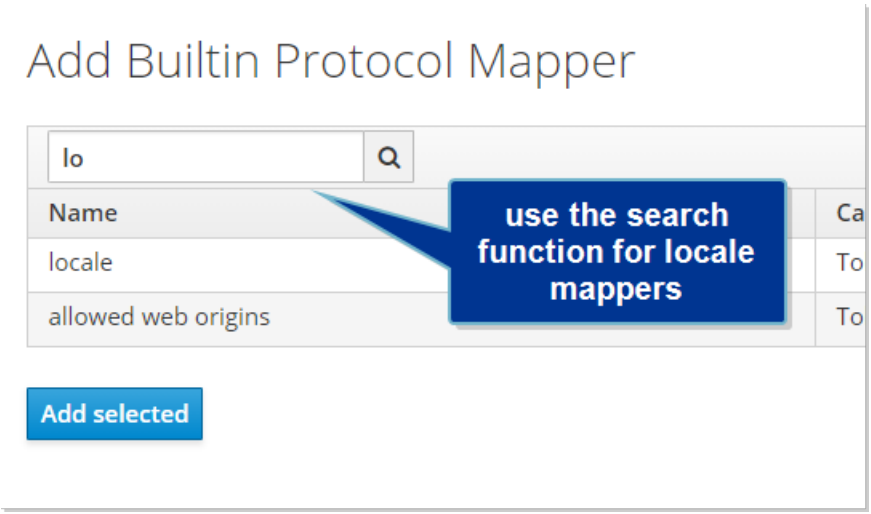
After all the necessary roles are created, navigate to the **Mappers** tab. Here, client mappers need to be specified. Two mappers are required for Reporting:

1. Localization mapper for property “locale”
2. Role mapper for Client user roles

The localization mapper is added by clicking on **Add Builtin** in the upper-right corner of the **Mappers** tab.

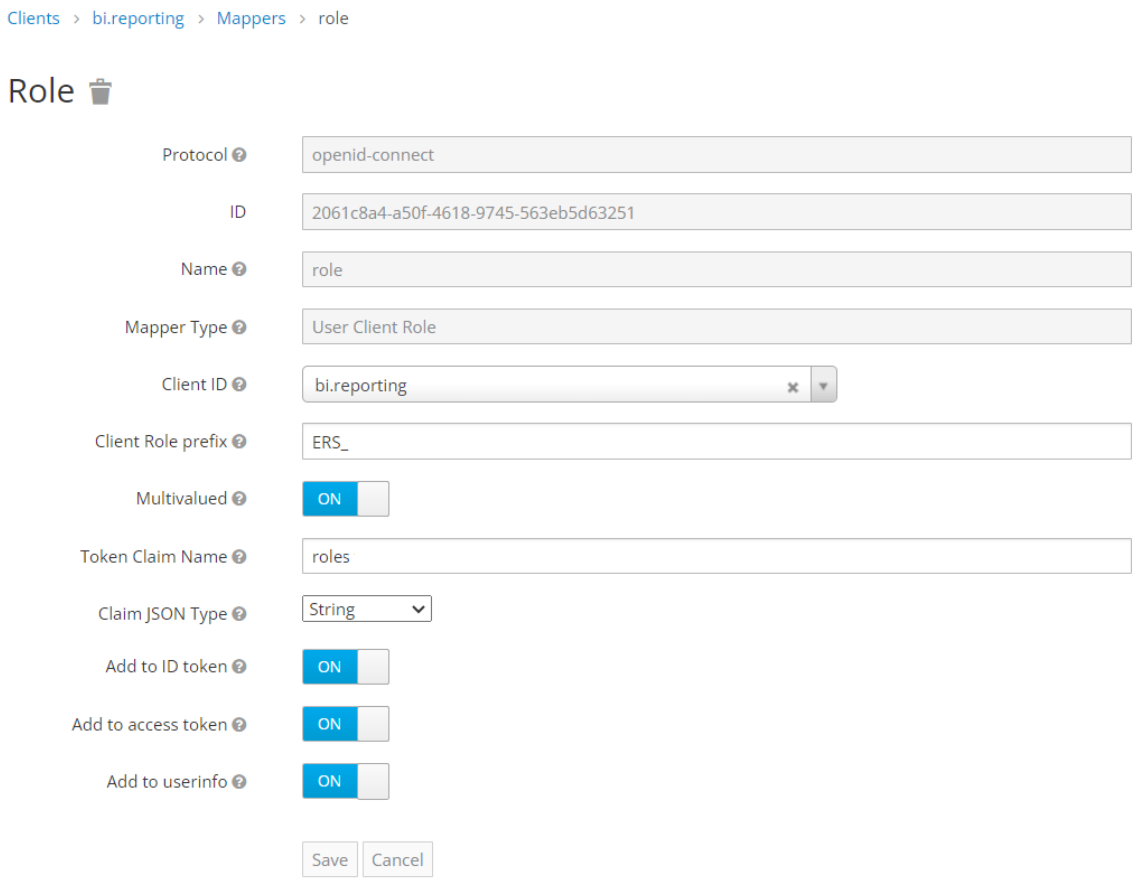


When adding a locale mapper, you can search built-in mappers by name, and then select and add the locale mapper.



> **Note**
>
> This locale value is populated after user login based on the selected language of the user, if Internationalization is enabled for the realm.

To create role mapping, click **Create** in the upper-right corner of the **Mappers** tab. When creating a role mapper, enter the settings as shown in the following image:

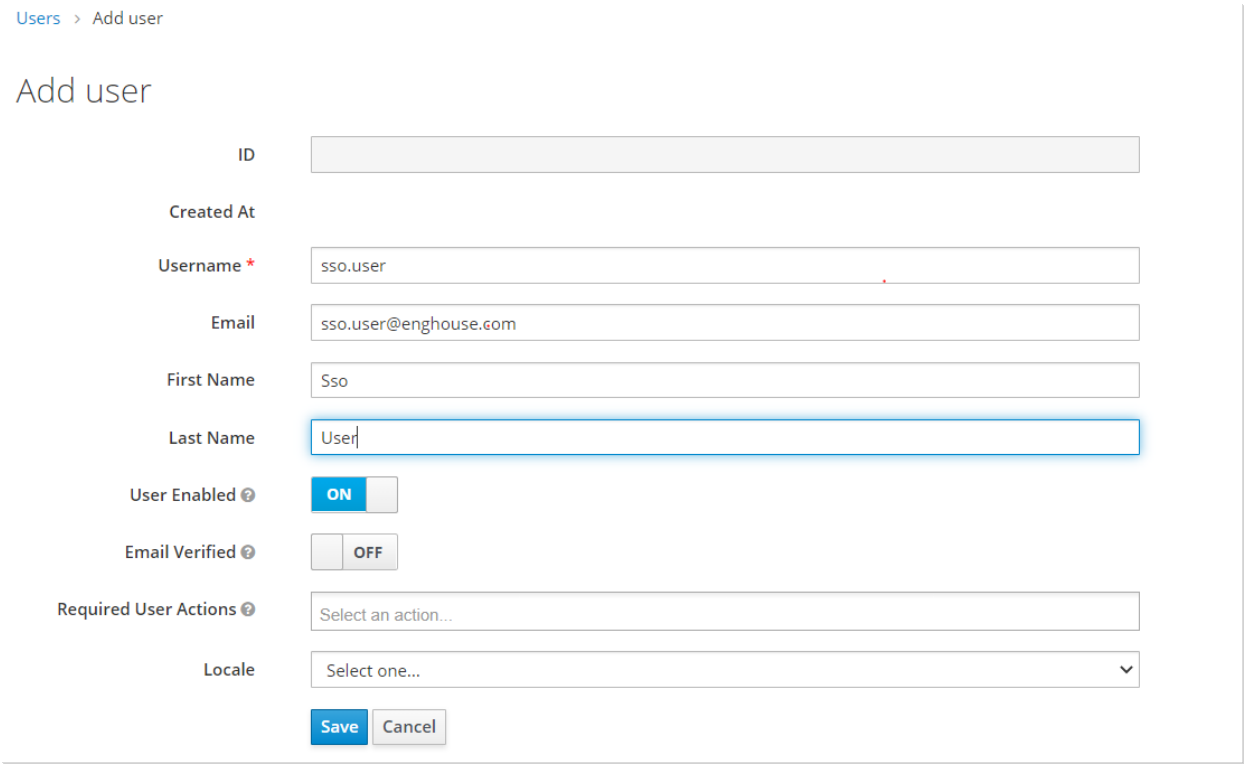


> **Caution**
>
> The "EnghouseBILite_" prefix is currently still supported, but is deprecated and is expected to be removed in upcoming versions of Reporting.

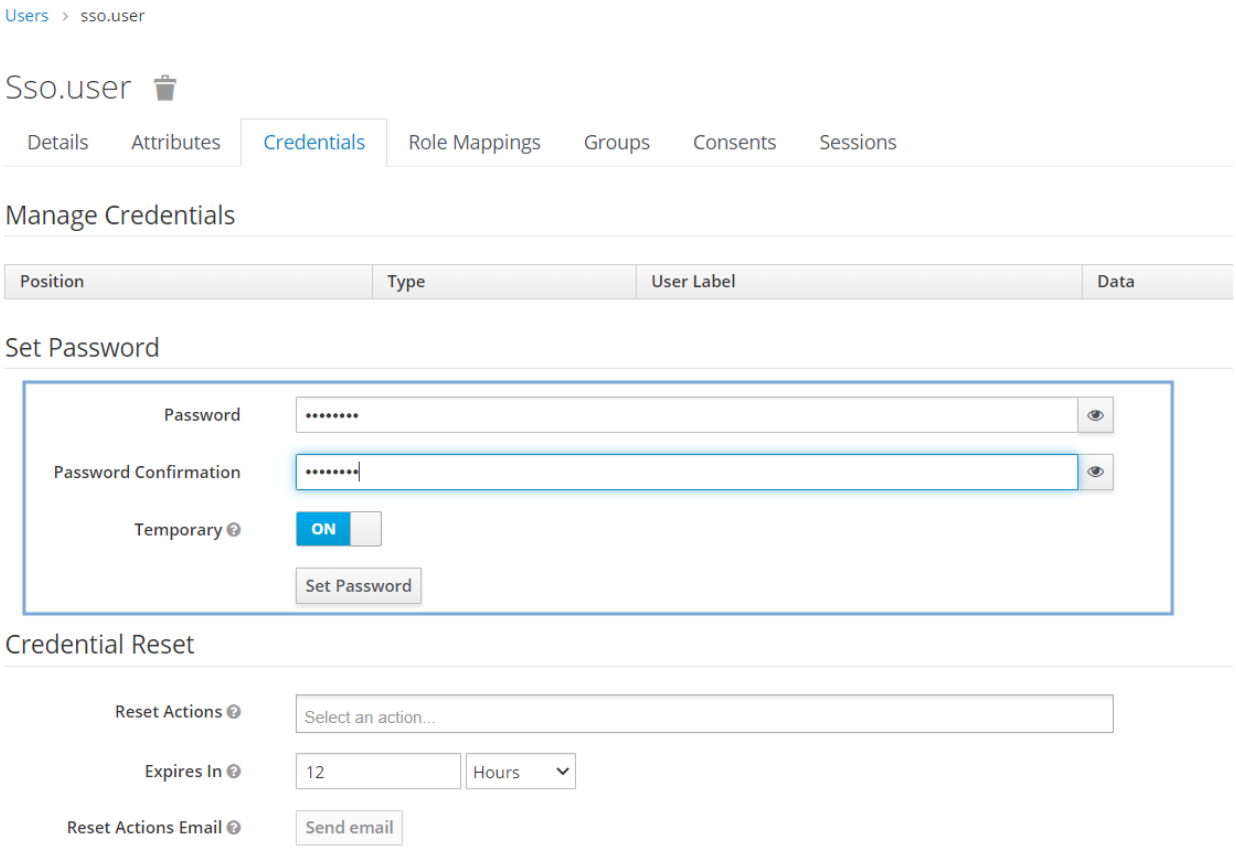
User creation

To create a user, click **User** in the menu on the left side of the window, and then click **Add user**.

To create a user, enter a **Username** and **Email**. **First Name** and **Last Name** are not required. Click **Save** to create the user.



After a user is created, navigate to the **Credentials** tab at the top of the window, and then define the user's password. Switch the **Temporary** toggle ON to make the password last only for a limited amount of time. The user will be prompted to change their password on first login if this setting is toggled on.



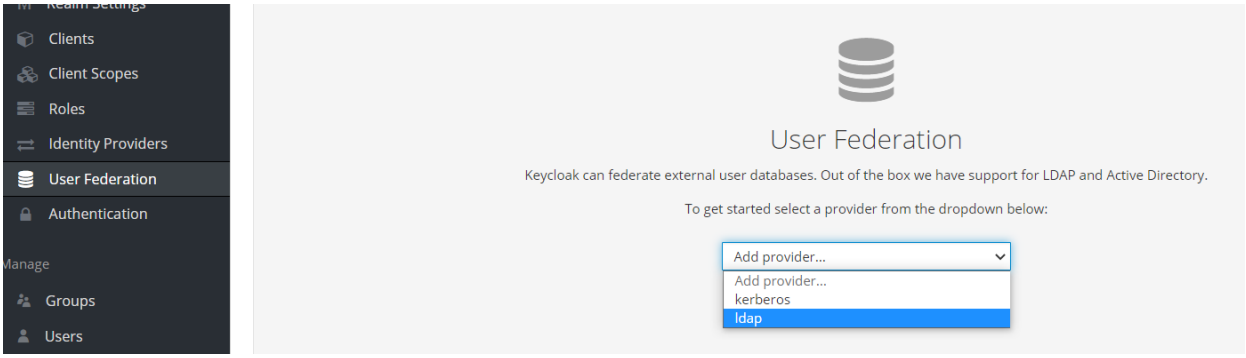
In the **Role Mappings tab**, a user's role can be specified.

To specify a Client User role, click the relevant the client in **Client Roles** dropdown menu. Click the necessary role in the **Available Roles** box, then click **Add selected** to add this role to the **Assigned Roles** box.

> **Note**
>
> - If a user with the same credentials existed in the Reporting app prior to the user logging in via SSO, the existing user is then updated with the SSO info upon successfully logging in via SSO.
> - If no role is specified for a new user for Reporting, the user is automatically assigned the Viewer role on successful login.
> - If no role is specified for a new user via SSO, but the user with the same credentials already exists in Reporting, the user's existing role is kept after a successful login via SSO. For example, if no user role is specified via KeyCloak, but the user already exists as a Designer in the Reporting web app, upon logging in via SSO, the user will preserve the Designer role.
> - Keycloak allows multiple roles to be assigned to one user, but Reporting does not. Therefore, only one role is applied to the user. This is the role with highest privileges among available roles. In Reporting, Administrator is considered to have highest privileges, followed by Data Designer, then Designer, then Power Viewer. Finally, Viewer has the lowest level privileges.

Keycloak – Active Directory Integration

Integration of Active Directory users with a Keycloak realm and related applications can be done by clicking **User Federation** in the left-hand menu. In this window, select **ldap** in the **Add provider** drop-down menu.



Once user federation is created, the Active Directory integration configuration needs to be entered. After the parameters are entered, and the connection and authentication are tested successfully, you can save the settings.

Once the settings are saved, click **Synchronize all users** at the bottom of the page. This imports all users from Active Directory to Keycloak. All of these users are immediately able to log into Reporting with their Active Directory credentials. Until they are assigned a different role by a Keycloak Administrator, the default role for these imported users is Viewer.