



[Home](#) / [Admin](#) / [Identity Providers](#) / Keycloak SSO

SSO With Keycloak

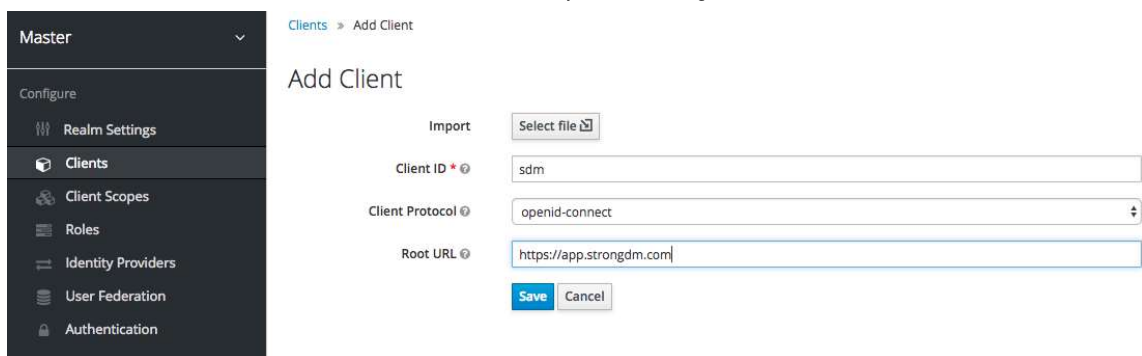
 Last modified on July 2, 2024

On this page 

This guide provides step-by-step instructions on how to configure single sign-on (SSO) with Keycloak. You already use Keycloak to conveniently manage permissions to applications. After SSO configuration is complete, you'll also be able to use Keycloak to manage permissions to your Datasources.

Steps

1. In your Keycloak admin console, go to the **Clients** section and click **Create** to add a client.
2. On the **Add Client** page, enter basic information and then save:
 1. **Client ID:** Enter a name like **StrongDM**.
 2. **Client Protocol:** Select **openid-connect**.
 3. **Root URL:** Enter `https://app.strongdm.com`.



Master ▾

Configure

- Realm Settings
- Clients**
- Client Scopes
- Roles
- Identity Providers
- User Federation
- Authentication

Clients > Add Client

Add Client

Import

Client ID *

Client Protocol

Root URL

Configure credentials

3. On the **Settings** tab, do the following:

1. Ensure that **Client Protocol** is **openid-connect**.
2. Set **Access Type** to **confidential**.
3. Under **Valid Redirect URIs**, add the following URLs:
`https://app.strongdm.com/auth/return` and
`https://app.strongdm.com/auth/return` .
4. Other fields are optional and can be set as you prefer. When done, click **Save**.

Master

Configure

- Realm Settings
- Clients**
 - Client Scopes
 - Roles
 - Identity Providers
 - User Federation
 - Authentication
- Manage
 - Groups
 - Users
 - Sessions
 - Events
 - Import
 - Export

Clients > sdm

Sdm

Settings Credentials Roles Client Scopes Mappers Scope Revocation Sessions Offline Acce

Permissions

Client ID sdm

Name strongDM

Description

Enabled **ON**

Consent Required **OFF**

Login Theme

Client Protocol openid-connect

Access Type confidential

Standard Flow Enabled **ON**

Implicit Flow Enabled **OFF**

Direct Access Grants Enabled **ON**

Service Accounts Enabled **OFF**

Authorization Enabled **OFF**

Root URL https://app.strongdm.com

Valid Redirect URIs

- https://app.strongdm.com/auth/return/
- https://app.strongdm.com/auth/return

Enter details

4. On the **Credentials** tab, copy the **Secret** value. You will need this in the next step.

Sdm

Settings **Credentials** Roles Client Scopes Mappers Scope Revocation Sessions

Permissions

Client Authenticator Client Id and Secret

Secret b88...

Regenerate Secret

Registration access token

Regenerate registration access token

Record client secret

5. Next, enter the account details in the StrongDM Admin UI. Go to **Settings** > [User Management](#). In the **Single Sign-on** section, set the following:

1. **Provider:** Select **Keycloak**.

2. **Single sign-on URL:** Add your URL (add `/auth/realms/<REALM_NAME>` to your Keycloak base URL).
 3. **Client ID:** Enter your client ID.
 4. **Client Secret:** Paste the secret that you copied previously.
6. Select your desired [general SSO settings](#) and click **activate**.

Single Sign-on

Click to prevent further changes

Enable single sign-on?
☒ Yes ☐ No

Provider

Keycloak

Single sign-on URL

http://localhost:8080/auth/admin/auth/realms/master

Client ID

StrongDM

Client Secret

.....

Allow password login for admins?
☒ Yes ☐ No

Send a welcome email to users?
☒ Yes ☐ No

Allow non-SSO users?
☐ Yes ☒ No

Reset

Save

What this means for you:

Users login with Keycloak.

Users will receive a welcome email with instructions.

Admins may login with email and password.

Admins may invite users without Keycloak accounts.

Setup Guides

- [Active Directory](#)
- [Azure](#)
- [Google](#)
- [Keycloak](#)
- [Okta](#)
- [OneLogin](#)
- [Auth0](#)

Configure Keycloak in StrongDM

7. Verify that all users in StrongDM exist in Keycloak.

Want to see StrongDM's capabilities beyond SSO with Keycloak? Learn more about [how it works](#) or [get a demo](#) to see it in action.

