



HEAL

DOCUMENTATION

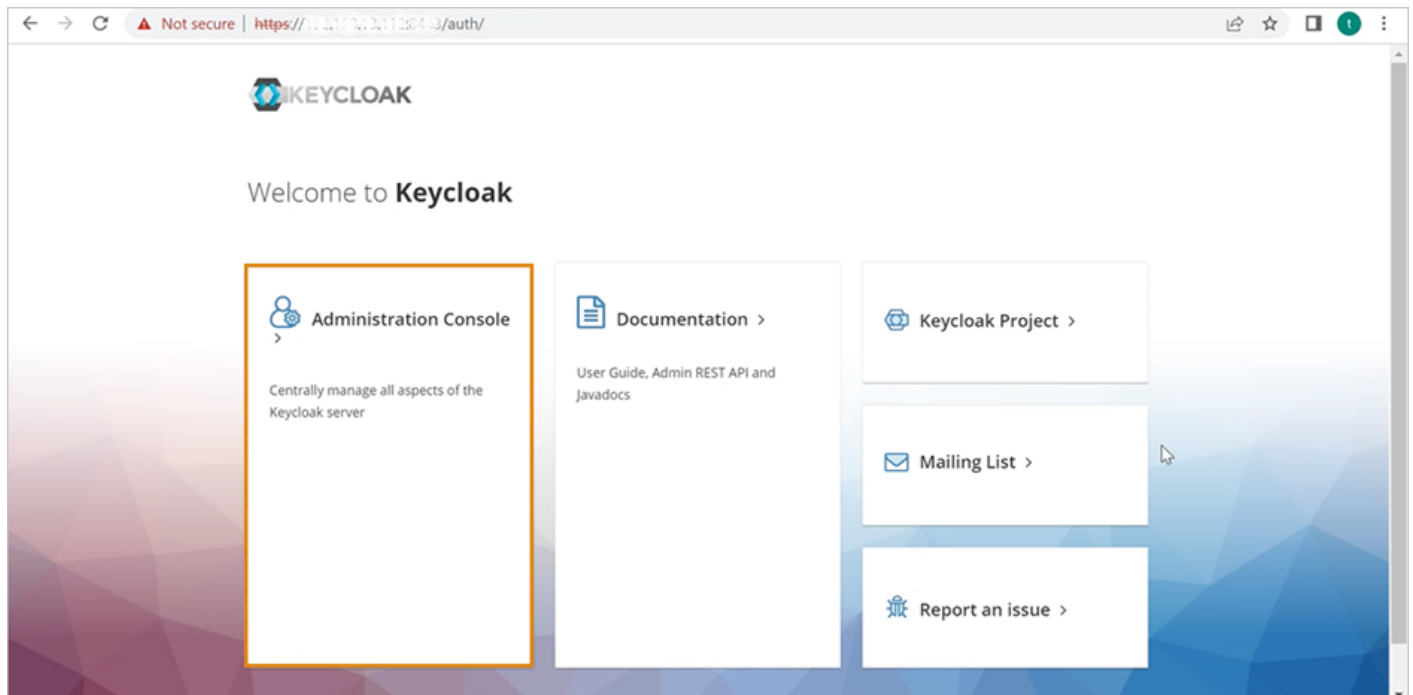
HEAL Software Inc.

Keycloak Administration Console

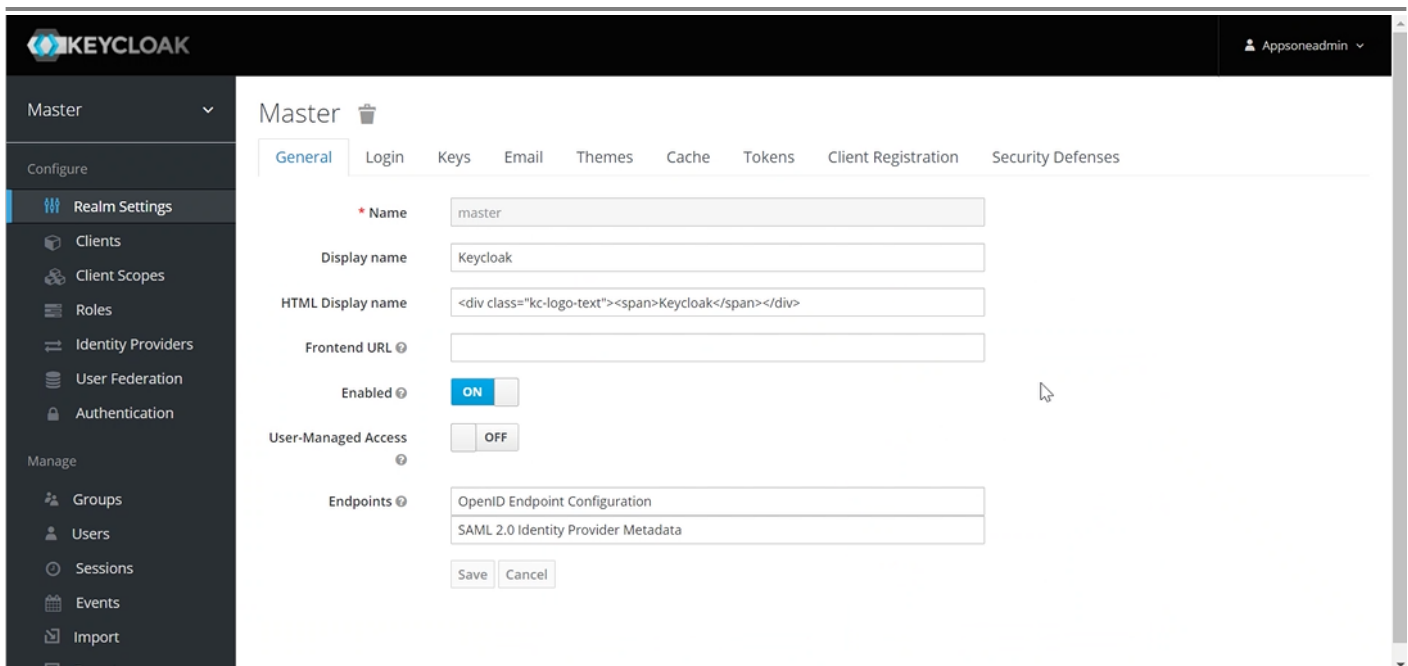
Keycloak Administration Console is a centralized administration and control of the keycloak identity and access management system, providing administrators with the necessary tools to manage user identities, configure security settings, and ensure a secure and seamless user experience.

Go to the Keycloak UI using the below URL and click on Administration console.

[box] <https://<Keycloak IP>:<Keycloak port>/auth/>[/box]



The Master page appears as below.



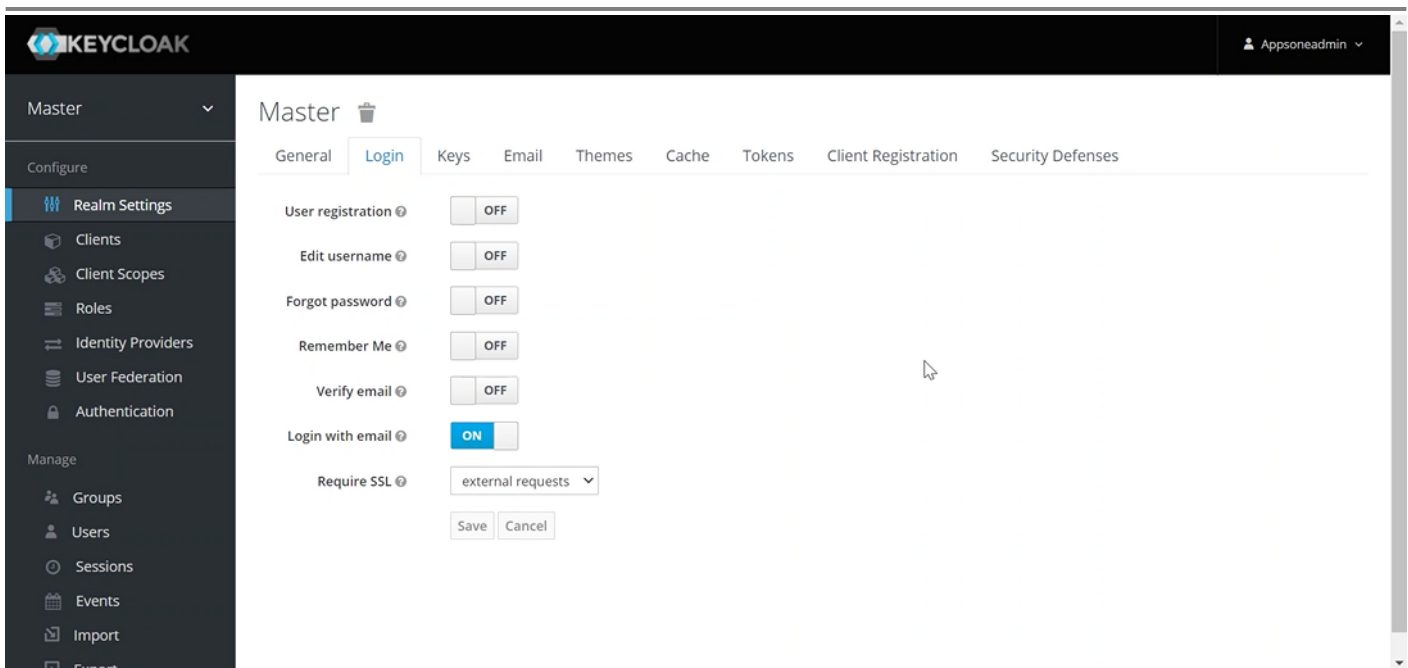
The below are the modified **Master Tabs** respectively.

Email - To Enable the “Forgot Password” Feature

Enabling the “Forgot Password” feature allows users to regain access to their accounts in case they forget their password. This feature enhances user experience by providing a convenient and secure way to reset their passwords without needing to contact support or create a new account.

To enable the ‘Forgot Password’ function, perform the following steps in the Keycloak Administration Console:

1. Navigate to **Realm Settings > Login**.



Click on the **Login with email** tab, to **Enable** the feature.

[box] Enabling this feature adds a 'Forgot Password' option in HEAL UI and also sends and receives password reset emails.[/box]

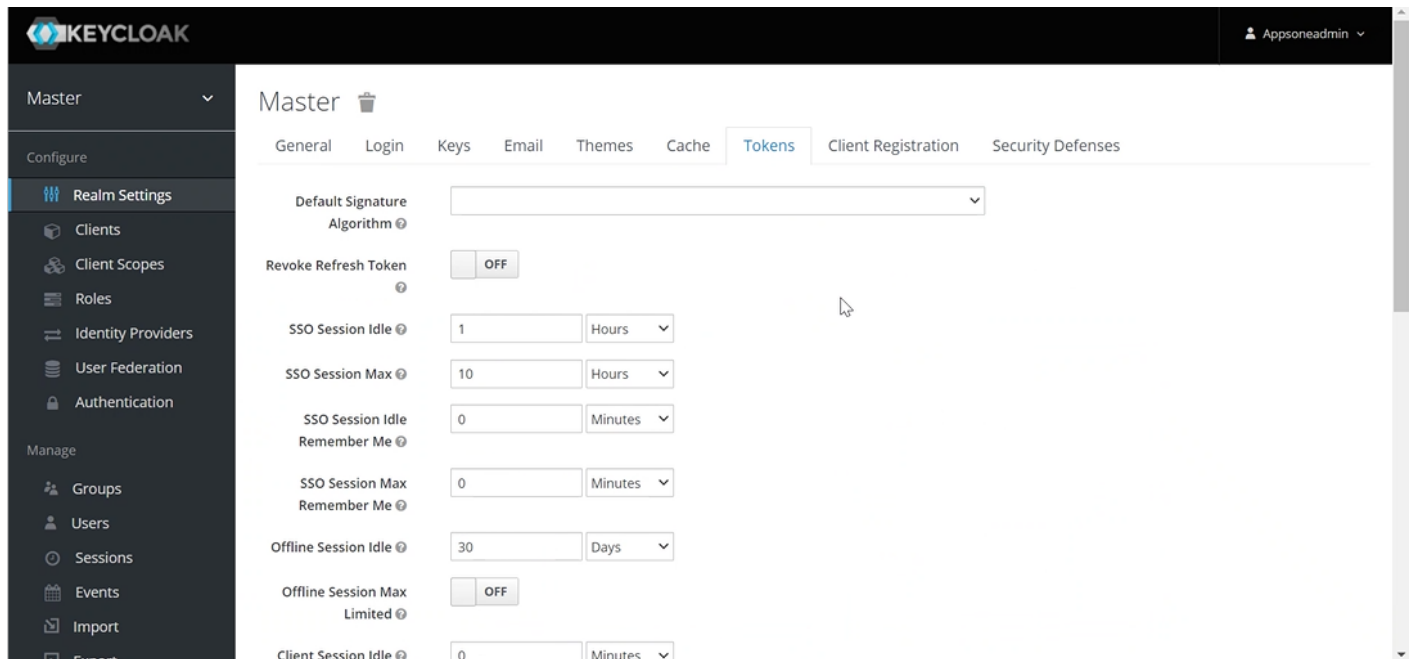
When the "Forgot Password" feature is enabled, users can initiate the password reset process by clicking on a designated link or button. They are typically prompted to provide their registered email address or username. Once submitted, the system sends a password reset email containing a unique link to the user's email address.

Tokens - Application Session Timeout

The session timeout is a security feature within HEAL, that automatically terminates a user's session following a certain period of inactivity. It enhances security by preventing unauthorized access and protects user data from potential breaches.

In the HEAL software, which includes the Control Center and HEAL UI applications, session timeouts are managed via Keycloak. By adjusting the session timeout settings in Keycloak, administrators can modify the inactivity period before the session termination for both applications.

1. Click on the **Tokens** tab and the below details will be available.



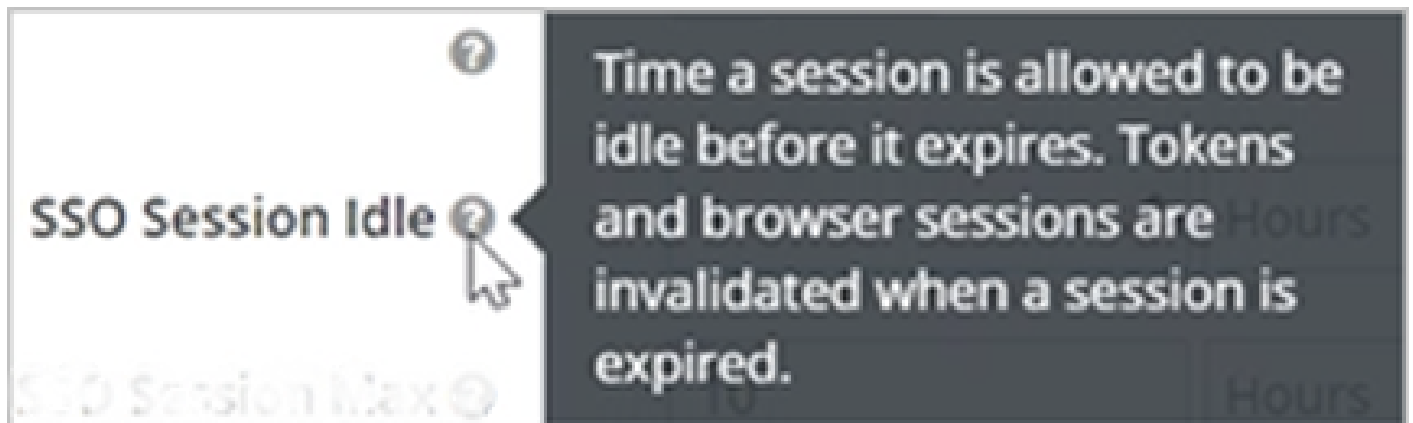
The screenshot shows the Keycloak administration interface. The left sidebar contains a 'Master' menu with options like 'Configure', 'Realm Settings', 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', 'Authentication', 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The main content area is titled 'Master' and has several tabs: 'General', 'Login', 'Keys', 'Email', 'Themes', 'Cache', 'Tokens' (which is selected), 'Client Registration', and 'Security Defenses'. The 'Tokens' tab displays various session settings:

- Default Signature Algorithm: A dropdown menu.
- Revoke Refresh Token: A toggle switch set to 'OFF'.
- SSO Session Idle: A text input with '1' and a dropdown menu set to 'Hours'.
- SSO Session Max: A text input with '10' and a dropdown menu set to 'Hours'.
- SSO Session Idle Remember Me: A text input with '0' and a dropdown menu set to 'Minutes'.
- SSO Session Max Remember Me: A text input with '0' and a dropdown menu set to 'Minutes'.
- Offline Session Idle: A text input with '30' and a dropdown menu set to 'Days'.
- Offline Session Max Limited: A toggle switch set to 'OFF'.
- Client Session Idle: A text input with '0' and a dropdown menu set to 'Minutes'.

2. Set the required duration in “**SSO Session Idle**”.

SSO: Single Sign-On

For information: Hover over the SSO Session Idle and the below information is displayed:



3. Click on the drop-down and select the required duration as below.

KEYCLOAK

Apponeadmin

Master

Configure

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

Manage

- Groups
- Users
- Sessions
- Events
- Import
- Export

Master

General Login Keys Email Themes Cache Tokens Client Registration Security Defenses

Default Signature Algorithm

Revoke Refresh Token OFF

SSO Session Idle 1 Hours

SSO Session Max 10 Days

SSO Session Idle Remember Me 0 Minutes

SSO Session Max Remember Me 0 Minutes

Offline Session Idle 30 Days

Offline Session Max Limited OFF

Client Session Idle 0 Minutes