

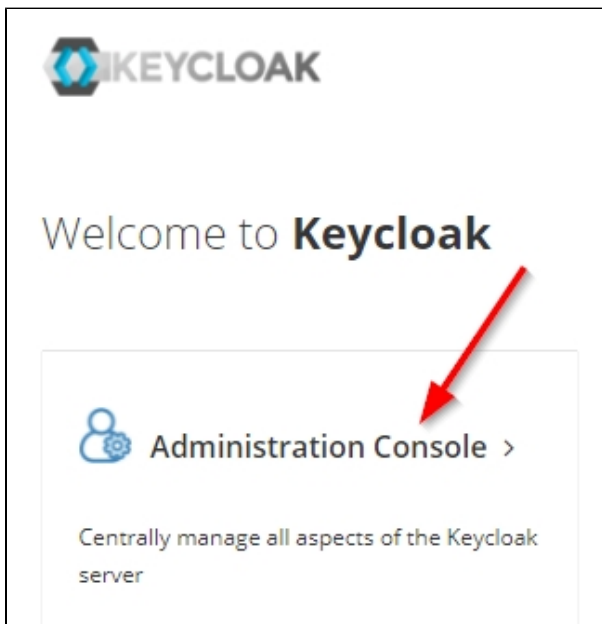
Initial login to Keycloak and configure a redirect - v. 2.x

i Summary: this page explains how to login to Keycloak for the first time and configure a redirect URI to ensure Console front-end can be accessed from wherever required.

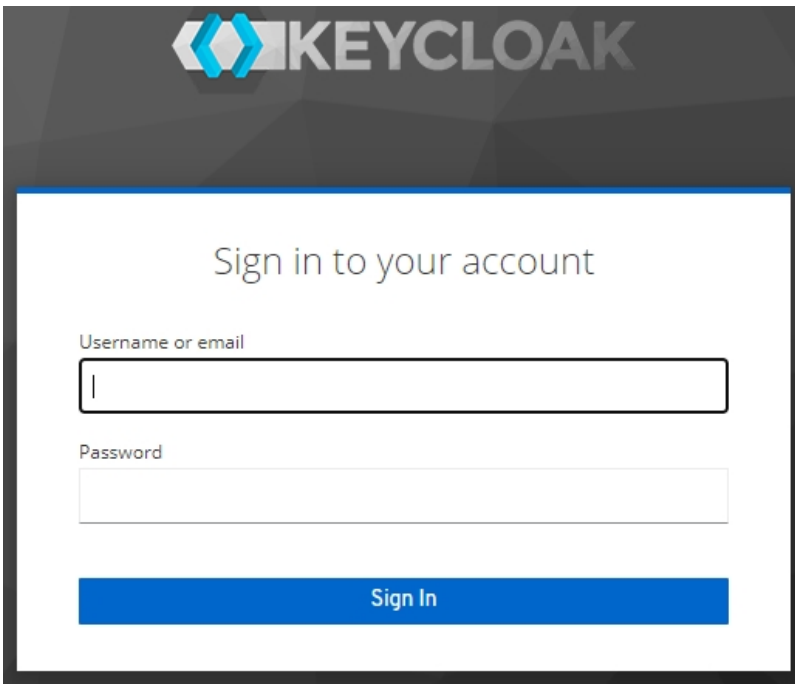
The Console **authentication provider** has been totally restructured in **2.x** and uses the open-source OAuth2 compatible **Keycloak** system. Keycloak provides local authentication, and can also interact with other enterprise authentication systems such as LDAP and SAML. Before you start using Console, you should configure a **redirect** in Keycloak to allow access to Console using the Console host name or IP address in addition to localhost (which is pre-configured). **If you do not, users will not be able to login to Console correctly.** To do so, connect to Keycloak **from any machine on the local network**:

```
http://localhost:8086  
or  
http://<ip_address>:8086  
or  
http://<host_name>:8086
```

Click the **Administration Console** option:



The default login credentials specified in the **docker-compose.yml** file are **admin/admin** - use these unless you have modified them as described in [AIP Console - front-end installation](#):

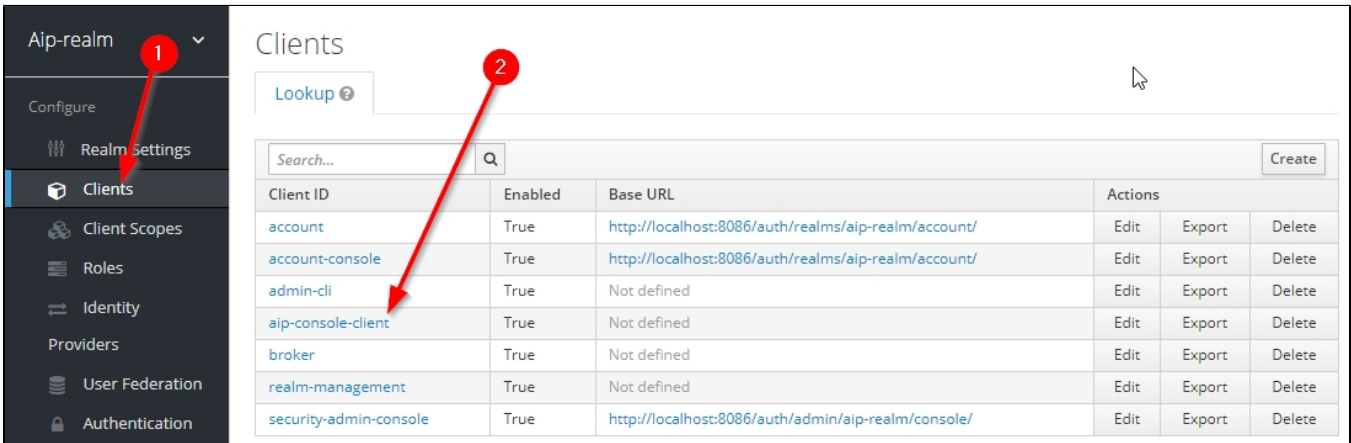


i These credentials are **specific to Keycloak and not Console**. You can change the default password if required, post installation, using the following URL:

```
http://localhost:8086/auth/realms/master/account/#/security/signingin
```

Now click the **Clients** option and then click **aip-console-client**:

Click to enlarge






The image shows the Keycloak administration console. On the left is a sidebar with navigation options: "Aip-realm", "Configure", "Realm Settings", "Clients", "Client Scopes", "Roles", "Identity", "Providers", "User Federation", and "Authentication". The "Clients" option is selected and highlighted with a red circle and arrow labeled "1". The main area is titled "Clients" and contains a "Lookup" button and a search bar. Below is a table of clients. The "aip-console-client" row is highlighted with a red circle and arrow labeled "2".


Client ID	Enabled	Base URL	Actions
account	True	http://localhost:8086/auth/realms/aip-realm/account/	Edit Export Delete
account-console	True	http://localhost:8086/auth/realms/aip-realm/account/	Edit Export Delete
admin-cli	True	Not defined	Edit Export Delete
aip-console-client	True	Not defined	Edit Export Delete
broker	True	Not defined	Edit Export Delete
realm-management	True	Not defined	Edit Export Delete
security-admin-console	True	http://localhost:8086/auth/admin/aip-realm/console/	Edit Export Delete


Now add a new redirect:

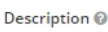
Clients > aip-console-client


Aip-console-client

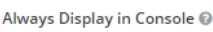
Settings | Credentials | Keys | Roles | Client Scopes  | Mappers  | Scope  | Revocation | Sessions  | Offline Access  | Clust


Client ID : aip-console-client


Name :


Description :

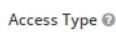
Enabled : ON

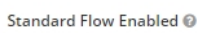
Always Display in Console : OFF


Consent Required : OFF


Login Theme :


Client Protocol : openid-connect

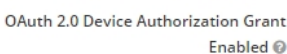
Access Type : confidential


Standard Flow Enabled : ON


Implicit Flow Enabled : OFF

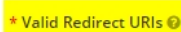


Direct Access Grants Enabled : ON


Service Accounts Enabled : OFF

OAuth 2.0 Device Authorization Grant Enabled : OFF

Authorization Enabled : OFF


Root URL :


* Valid Redirect URIs :  

Base URL :

You should add a redirect for **each** URL you want Console to be accessible on. For example:

- `http://<aip_console_server_hostname>:8081/*`
- `http://<aip_console_server_ip_address>:8081/*`

Root URL :

* Valid Redirect URIs :

Ensure you save the changes:

Backchannel Logout Session Required



ON

Backchannel Logout Revoke Offline


Sessions



OFF

> Fine Grain OpenID Connect Configuration 

> OpenID Connect Compatibility Modes 

> Advanced Settings 

> Authentication Flow Overrides 