Getting Started Guide

Table of Contents

1. Overview
2. Installing and Booting
   2.1. Installing Distribution Files
   2.2. Booting the Server
   2.3. Creating the Admin Account
   2.4. Logging in to the Admin Console
3. Creating a Realm and User
   3.1. Before You Start
   3.2. Creating a New Realm
   3.3. Creating a New User
   3.4. User Account Service
4. Securing a JBoss Servlet Application
   4.1. Before You Start
   4.2. Installing the Client Adapter
   4.3. Downloading, Building, and Deploying Application Code
   4.4. Creating and Registering the Client
   4.5. Configuring the Subsystem

1. Overview

This guide helps you get started with Keycloak. It covers server configuration and use of the default database. Advanced deployment options are not covered. For a deeper description of features or configuration options, consult the other reference guides.

2. Installing and Booting

This section describes how to boot a Keycloak server in standalone mode, set up the initial admin user, and log in to the Keycloak admin console.

2.1. Installing Distribution Files

Download the Keycloak Server:

- **keycloak-6.0.1.[zip|tar.gz]**

(https://www.keycloak.org/downloads.html).

The **keycloak-6.0.1.[zip|tar.gz]** file is the server-only distribution. It contains only the scripts and binaries to run the Keycloak server.

Place the file in a directory you choose and use either the `unzip` or `tar` utility to extract it.

Linux/Unix

BASH

```bash
$ unzip keycloak-6.0.1.zip

or

$ tar -xvzf keycloak-6.0.1.tar.gz
```

Windows

BASH

```bash
> unzip keycloak-6.0.1.zip
```

2.2. Booting the Server

To boot the Keycloak server, go to the `bin` directory of the server distribution and run the `standalone` boot script:

Linux/Unix

BASH

```bash
$ cd bin
$ ./standalone.sh
```

Windows

BASH

```bash
> ...\bin\standalone.bat
```

2.3. Creating the Admin Account

After the server boots, open http://localhost:8080/auth in your web browser. The welcome page will indicate that the server is running.

Enter a username and password to create an initial admin user.

This account will be permitted to log in to the `master` realm’s administration console, from which you will create realms and users and register applications to be secured by Keycloak.

using `localhost`. This is a security precaution. You can create the initial admin user at the command line with the `add-user-keycloak.sh` script. For more information, see the Server Installation and Configuration Guide (https://www.keycloak.org/docs/6.0/server_installation/) and the Server Administration Guide (https://www.keycloak.org/docs/6.0/server_admin/).

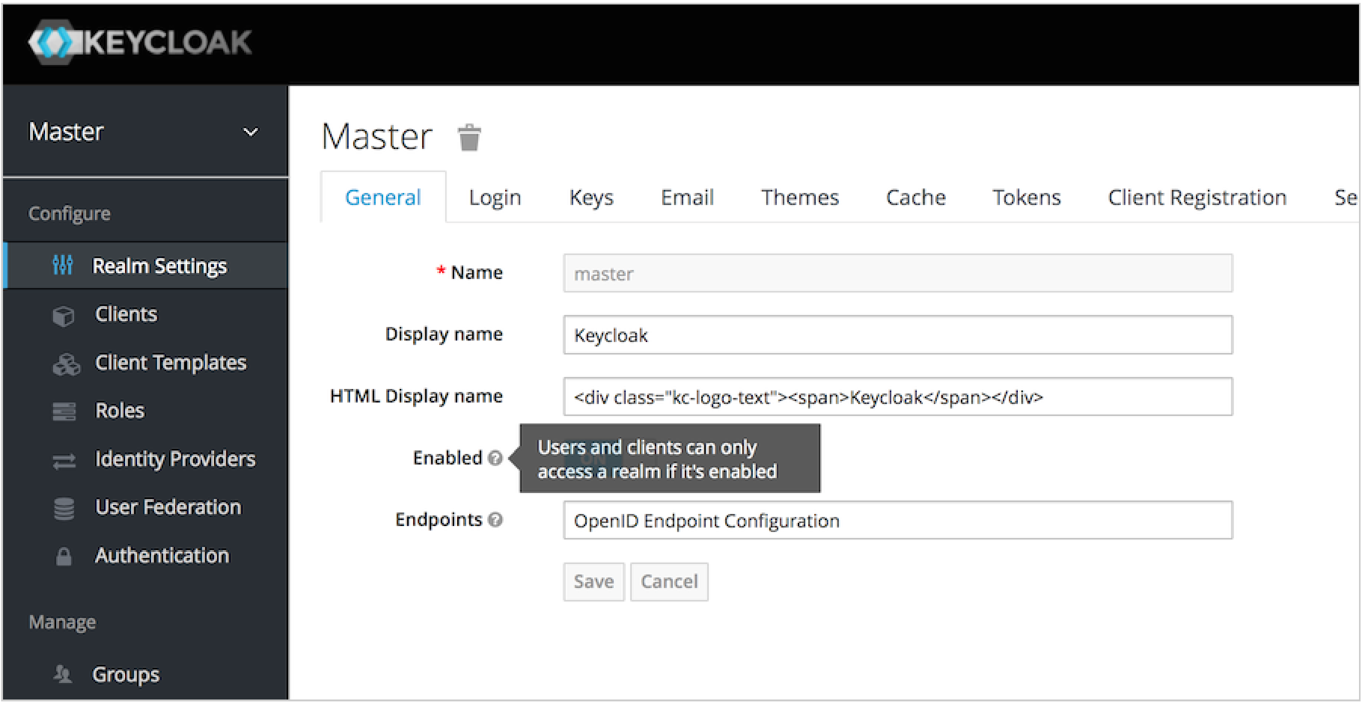
2.4. Logging in to the Admin Console

After you create the initial admin account, use the following steps to log in to the admin console:

1. Click the **Administration Console** link on the **Welcome** page or go directly to the console URL http://localhost:8080/auth/admin/

2. Type the username and password you created on the **Welcome** page to open the **Keycloak Admin Console**.

   Admin Console



* Name: master

Display name: Keycloak

HTML Display name: <div class="kc-logo-text"><span>Keycloak</span></div>

Enabled: Users and clients can only access a realm if it's enabled

Endpoints: OpenID Endpoint Configuration

3. Creating a Realm and User

In this section you will create a new realm within the Keycloak admin console and add a new user to that realm. You will use that new user to log in to your new realm and visit the built-in user account service that all users have access to.

3.1. Before You Start

Before you can create your first realm, complete the installation of Keycloak and create the initial admin user as shown in Installing and Booting.

To create a new realm, complete the following steps:

1. Go to http://localhost:8080/auth/admin/ and log in to the Keycloak Admin Console using the account you created in Install and Boot.
2. From the **Master** drop-down menu, click **Add Realm**. When you are logged in to the master realm this drop-down menu lists all existing realms.
3. Type `demo` in the **Name** field and click **Create**.

When the realm is created, the main admin console page opens. Notice the current realm is now set to `demo`. Switch between managing the `master` realm and the realm you just created by clicking entries in the **Select realm** drop-down menu.

3.3. Creating a New User

To create a new user in the `demo` realm, along with a temporary password for that new user, complete the following steps:

1. From the menu, click **Users** to open the user list page.
2. On the right side of the empty user list, click **Add User** to open the add user page.
3. Enter a name in the `Username` field; this is the only required field. Click **Save** to save the data and open the management page for the new user.
4. Click the **Credentials** tab to set a temporary password for the new user.
5. Type a new password and confirm it. Click **Reset Password** to set the user password to the new one you specified.

> This password is temporary and the user will be required to change it after the first login. To create a password that is persistent, flip the **Temporary** switch from **On** to **Off** before clicking **Reset Password**.

3.4. User Account Service

1. After you create the new user, log out of the management console by opening the user drop-down menu and selecting **Sign Out**.
2. Go to http://localhost:8080/auth/realms/demo/account and log in to the User Account Service of your `demo` realm with the user you just created.

password after you successfully log in, unless you changed the **Temporary** setting to **Off** when you created the password.

The user account service page will open. Every user in a realm has access to this account service by default. From this page, you can update profile information and change or add additional credentials. For more information on this service see the Server Administration Guide (https://www.keycloak.org/docs/6.0/server_admin/).

4. Securing a JBoss Servlet Application

This section describes how to secure a Java servlet application on the WildFly application server by:

- Installing the Keycloak client adapter on a WildFly application server distribution
- Creating and registering a client application in the Keycloak admin console
- Configuring the application to be secured by Keycloak

4.1. Before You Start

Before you can secure a Java servlet application, you must complete the installation of Keycloak and create the initial admin user as shown in Installing and Booting.

There is one caveat: Even though WildFly is bundled with Keycloak, you cannot use this as an application container. Instead, you must run a separate WildFly instance on the same machine as the Keycloak server to run your Java servlet application. Run the Keycloak using a different port than the WildFly, to avoid port conflicts.

To adjust the port used, change the value of the `jboss.socket.binding.port-offset` system property when starting the server from the command line. The value of this property is a number that will be added to the base value of every port opened by the Keycloak server.

To start the Keycloak server while also adjusting the port:

Linux/Unix

BASH

```bash
$ cd bin
$ ./standalone.sh -Djboss.socket.binding.port-offset=100
```

Windows

BASH

```bash
> ...\bin\standalone.bat -Djboss.socket.binding.port-offset=100
```

4.2. Installing the Client Adapter

Download the WildFly distribution and extract it from the compressed file into a directory on your machine.

Download the WildFly OpenID Connect adapter distribution from keycloak.org (https://www.keycloak.org/downloads.html).

Extract the contents of this file into the root directory of your WildFly distribution.

Run the appropriate script for your platform:

WildFly 10 and Linux/Unix

BASH

```
$ cd bin
$ ./jboss-cli.sh --file=adapter-install-offline.cli
```

WildFly 10 and Windows

BASH

```
> cd bin
> jboss-cli.bat --file=adapter-install-offline.cli
```

Wildfly 11 and Linux/Unix

BASH

```
$ cd bin
$ ./jboss-cli.sh --file=adapter-elytron-install-offline.cli
```

Wildfly 11 and Windows

BASH

```
> cd bin
> jboss-cli.bat --file=adapter-elytron-install-offline.cli
```

This script will make the necessary edits to the `…/standalone/configuration/standalone.xml` file of your app server distribution and may take some time to complete.

Start the application server.

Linux/Unix

BASH

```
$ cd bin
$ ./standalone.sh
```

BASH

```
> ...\bin\standalone.bat
```

4.3. Downloading, Building, and Deploying Application Code

You must have the following installed on your machine and available in your PATH before you continue:

- Java JDK 8
- Apache Maven 3.1.1 or higher
- Git

> You can obtain the code by cloning the Keycloak Quickstarts Repository repository at https://github.com/keycloak/keycloak-quickstarts. The quickstarts are designed to work with the most recent Keycloak release.

Make sure your WildFly application server is started before you continue.

To download, build, and deploy the code, complete the following steps.

Clone Project

```
$ git clone https://github.com/keycloak/keycloak-quickstarts
$ cd keycloak-quickstarts/app-profile-jee-vanilla
$ mvn clean wildfly:deploy
```

During installation, you will see some text scroll by in the application server console window.

To confirm that the application is successfully deployed, go to http://localhost:8080/vanilla and a login page should appear.

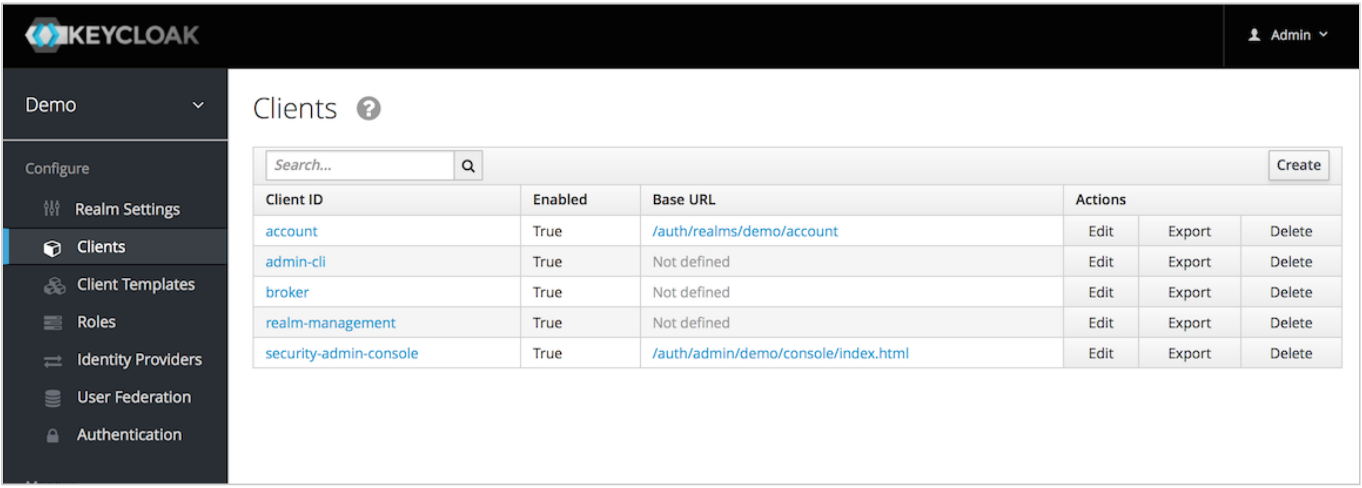
> If you click **Login**, the browser will pop up a BASIC auth login dialog. However, the application is not yet secured by any identity provider, so anything you enter in the dialog box will result in a `Forbidden` message being sent back by the server. You can confirm that the application is currently secured via `BASIC` authentication by finding the setting in the application's `web.xml` file.

4.4. Creating and Registering the Client

To define and register the client in the Keycloak admin console, complete the following steps:

2. In the top left drop-down menu select and manage the `Demo` realm. Click `Clients` in the left side menu to open the Clients page.

Clients

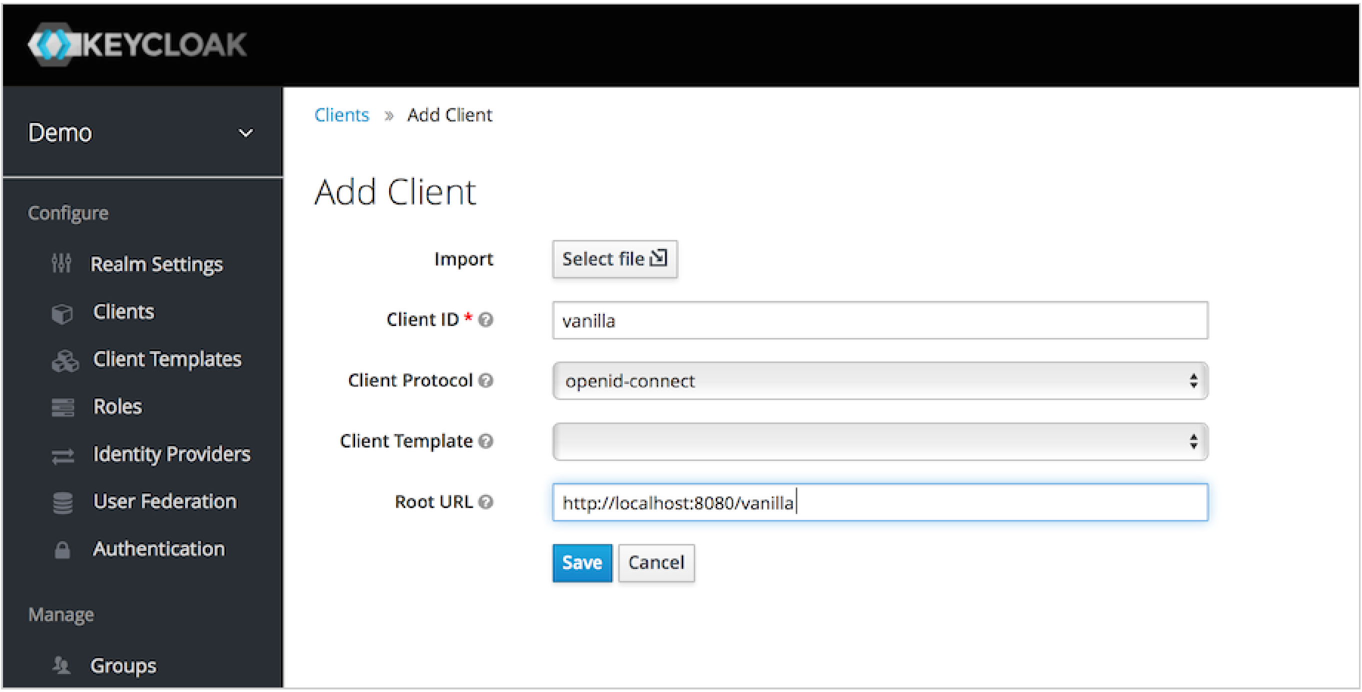


Client ID	Enabled	Base URL	Actions		
account	True	/auth/realms/demo/account	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	/auth/admin/demo/console/index.html	Edit	Export	Delete

3. On the right side, click **Create**.

4. Complete the fields as shown here:

Add Client



Import: Select file

Client ID *: vanilla

Client Protocol: openid-connect

Client Template:

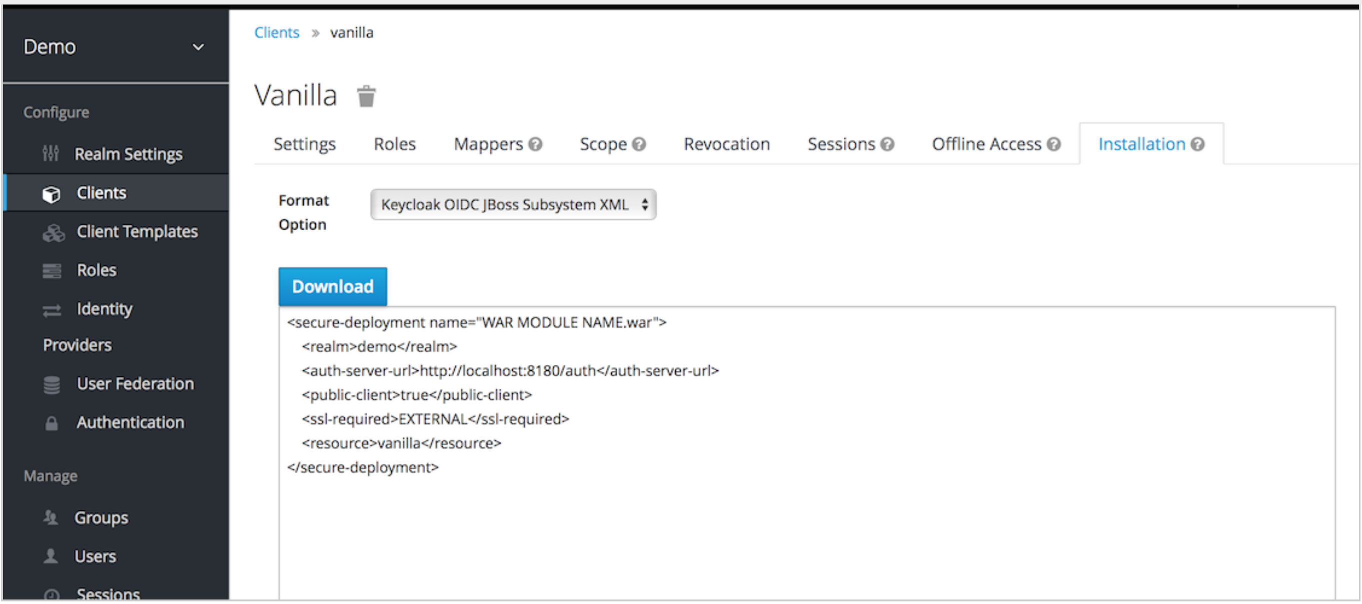
Root URL: http://localhost:8080/vanilla

5. Click **Save** to create the client application entry.

6. Click the **Installation** tab in the Keycloak admin console to obtain a configuration template.

7. Select **Keycloak OIDC JBoss Subsystem XML** to generate an XML template. Copy the contents for use in the next section.

Template XML



Format Option: Keycloak OIDC JBoss Subsystem XML

```
<secure-deployment name="WAR MODULE NAME.war">
   <realm>demo</realm>
   <auth-server-url>http://localhost:8180/auth</auth-server-url>
   <public-client>true</public-client>
   <ssl-required>EXTERNAL</ssl-required>
   <resource>vanilla</resource>
</secure-deployment>
```

4.5. Configuring the Subsystem

To configure the WildFly instance that the application is deployed on so that this app is secured by Keycloak, complete the following steps.

1. Open the `standalone/configuration/standalone.xml` file in the WildFly instance that the application is deployed on and search for the following text:

```xml
<subsystem xmlns="urn:jboss:domain:keycloak:1.1"/>
```

2. Modify this text to prepare the file for pasting in contents from the **Keycloak OIDC JBoss Subsystem XML** template we obtained Keycloak admin console **Installation** tab by changing the XML entry from self-closing to using a pair of opening and closing tags:

```xml
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
</subsystem>
```

3. Paste the contents of the template within the `<subsystem>` element, as shown in this example:

```xml
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="WAR MODULE NAME.war">
    <realm>demo</realm>
    <auth-server-url>http://localhost:8180/auth</auth-server-url>
    <public-client>true</public-client>
    <ssl-required>EXTERNAL</ssl-required>
    <resource>vanilla</resource>
  </secure-deployment>
</subsystem>
```

XML

```xml
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="vanilla.war">
  ...
</subsystem>
```

5. Reboot the application server.
6. Go to http://localhost:8080/vanilla and click **Login**. When the Keycloak login page opens, log in using the user you created in Creating a New User.

Last updated 2019-04-24 08:49:45 UTC