Red Hat Single Sign-On 7.0 Getting Started Guide

Getting Started Guide

Red Hat Customer Content Services

Getting Started Guide

Legal Notice

Abstract

This guide consist of basic information and instruction to get started with Red Hat Single Sign-On 7.0

Table of Contents

CHAPTER 1. OVERVIEW **3**

CHAPTER 2. INSTALL AND BOOT **4**
2.1. INSTALLING DISTRIBUTION FILES 4
2.2. BOOT THE SERVER 4
2.3. CREATE ADMIN ACCOUNT 5
2.4. LOGIN TO ADMIN CONSOLE 6

CHAPTER 3. CREATE A REALM AND USER **8**
3.1. BEFORE YOU START 8
3.2. CREATE A NEW REALM 8
3.3. CREATE A NEW USER 9
3.4. USER ACCOUNT SERVICE 11

CHAPTER 4. SECURING A JBOSS SERVLET APPLICATION **13**
4.1. BEFORE YOU START 13
4.2. INSTALL THE CLIENT ADAPTER 13
4.3. DOWNLOAD, BUILD, DEPLOY APPLICATION CODE 14
4.4. CREATE AND REGISTER CLIENT 16
4.5. CONFIGURE SUBSYSTEM 19

CHAPTER 1. OVERVIEW

The purpose of this guide is to get you up and running as quickly as possible so that you can play with and test drive various features that Red Hat Single Sign-On has. It relies heavily on the default database and server configuration that come out of the box and does not get into any complex deployment options. If you want a more in depth discussion of any features or configuration options, you should consult the various other reference guides available.

CHAPTER 2. INSTALL AND BOOT

This very short tutorial walks you through booting up the server in standalone mode, setting up the initial admin user, and logging into the Red Hat Single Sign-On admin console.

2.1. INSTALLING DISTRIBUTION FILES

The Red Hat Single Sign-On Server is contained in one distribution file:

- 'RH-SSO-7.0.0.[zip|tar.gz]'

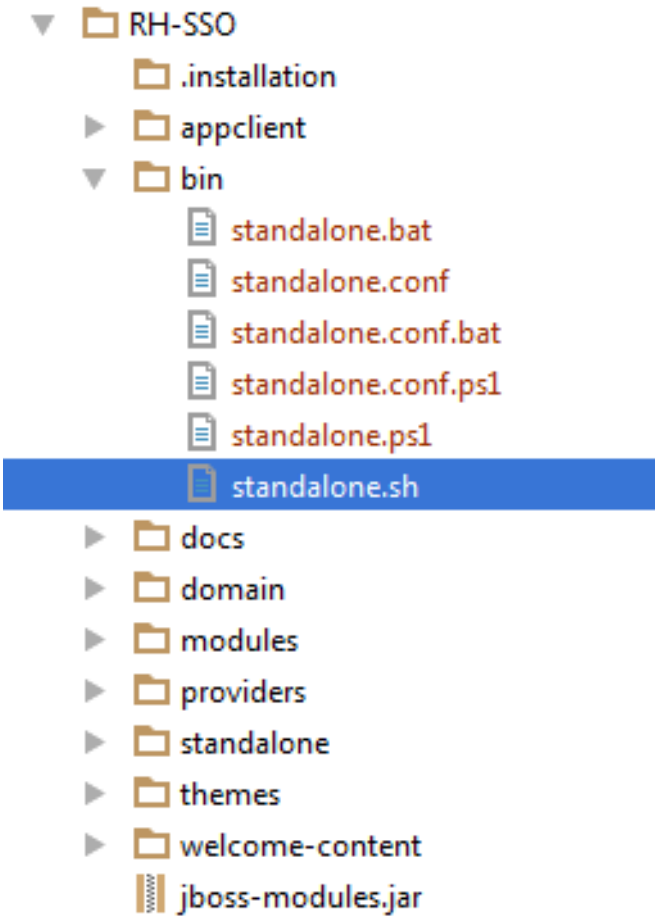
The 'RH-SSO-7.0.0.[zip|tar.gz]' file is the server only distribution. It contains nothing other than the scripts and binaries to run the Red Hat Single Sign-On server.

To unpack these files run the **`unzip`** or **`gunzip`** and **`tar`** utilities.

2.2. BOOT THE SERVER

To boot the Red Hat Single Sign-On server, go to the *bin/* directory of the server distribution.

Standalone Boot Scripts



To boot the server:

Linux/Unix

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

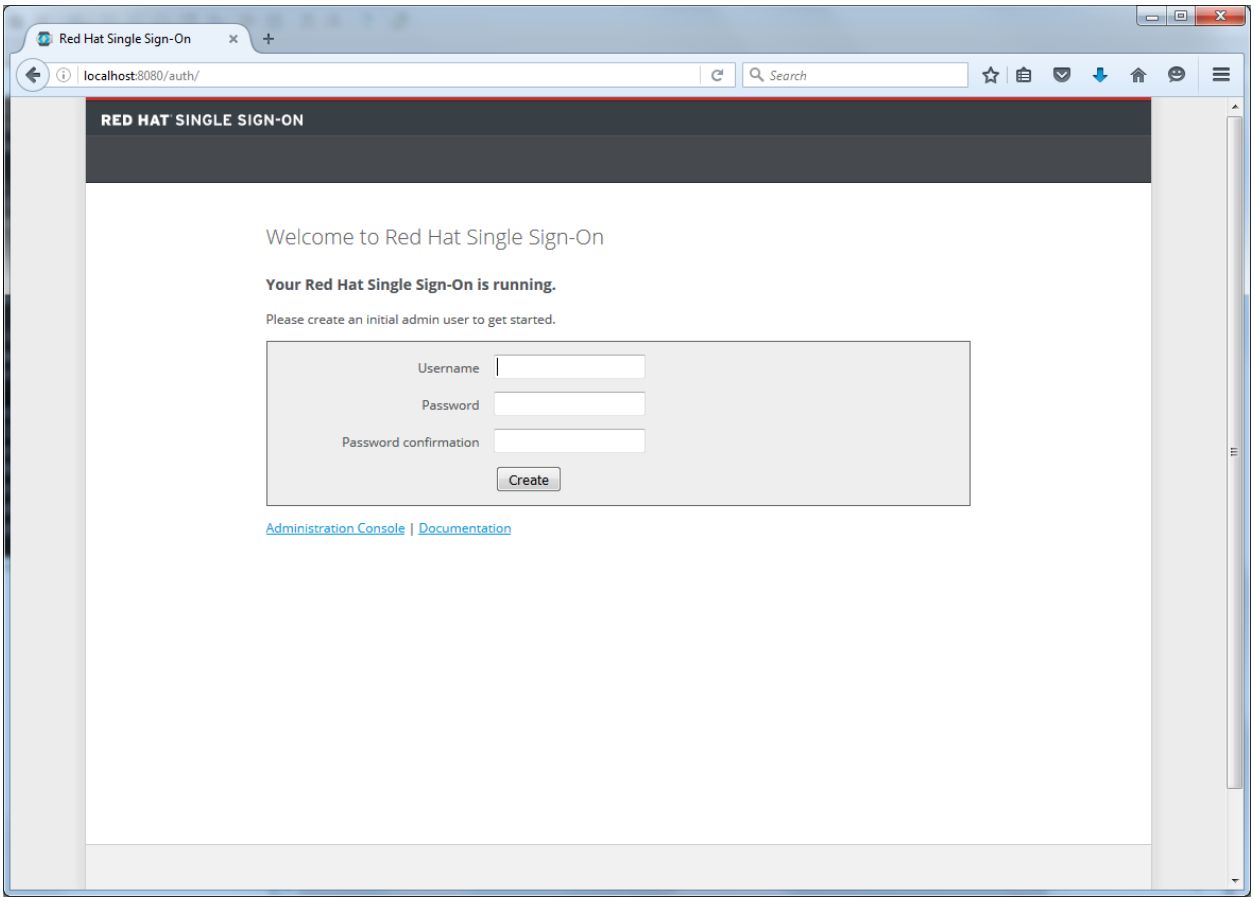
Windows

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

2.3. CREATE ADMIN ACCOUNT

After the server boots, open your browser and go to the http://localhost:8080/auth URL. The page should look like this:

Welcome Page



Red Hat Single Sign-On does not have any configured admin account out of the box. You must create one on the Welcome Page. This account will allow you to create an admin that can log into the *master* realm's administration console so that you can start creating realms, users and registering applications to be secured by Red Hat Single Sign-On.

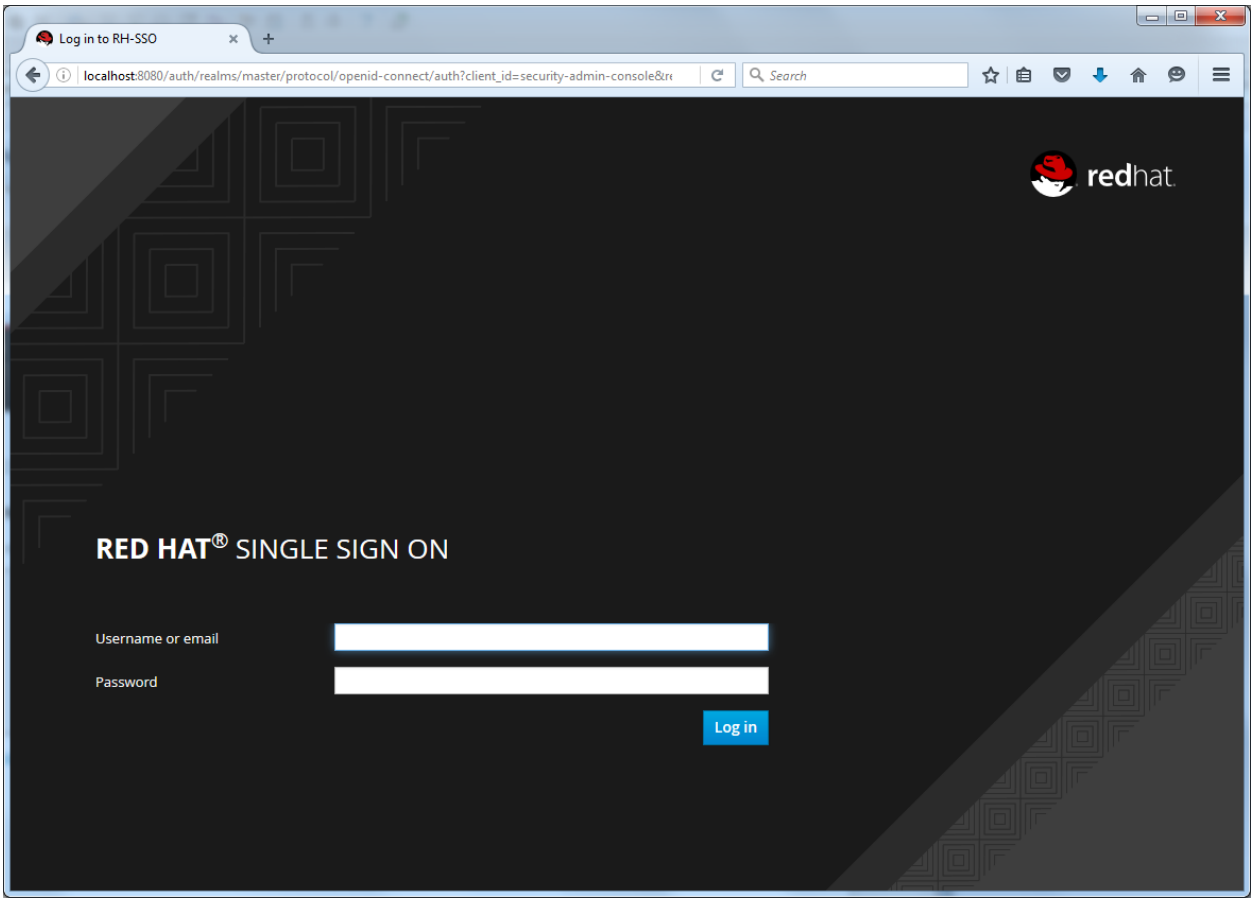
Note

You can only create an initial admin user on the Welcome Page if you connect via **`localhost`**. This is a security precaution. You can also create the initial admin user at the command line with the **`add-user-keycloak.sh`** script. This is discussed more in the Server Installation and Configuration Guide and Server Administration Guide.

2.4. LOGIN TO ADMIN CONSOLE

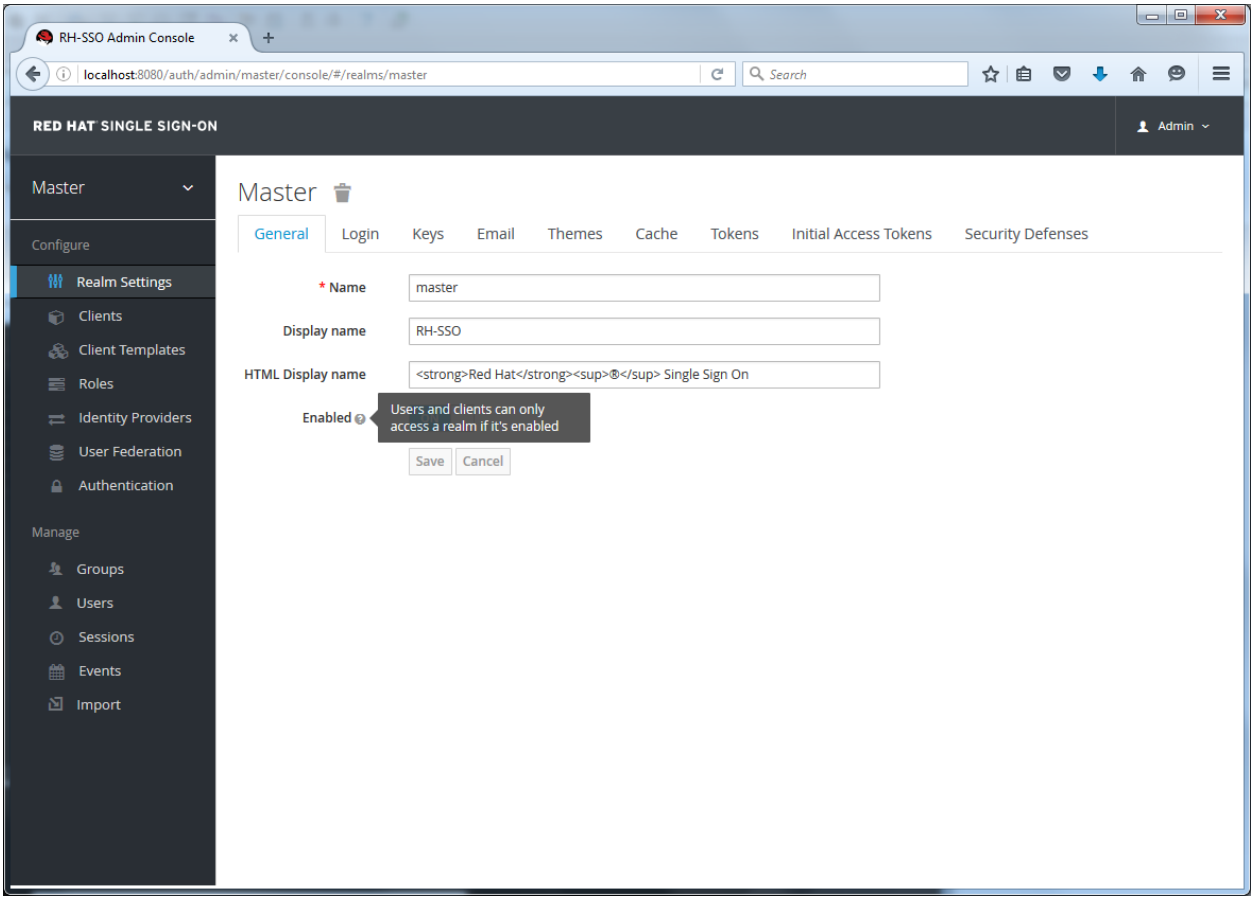
After you create the initial admin account, click on the *Administration Console* link on the bottom of the Welcome Page. Alternatively you can go to the console url directly at http://localhost:8080/auth/admin/

Login Page



Enter the username and password you created on the Welcome Page. This will bring you to the Red Hat Single Sign-On Admin Console.

Admin Console



Note

If you are curious about a certain feature, button, or field within the Admin Console, simply hover your mouse over any question mark **?** icon. This will pop up tooltip text to describe the area of the console you are interested in. The image above shows the tooltip in action.

CHAPTER 3. CREATE A REALM AND USER

This short tutorial walks you through creating a new realm within the Red Hat Single Sign-On Admin Console and adding a new user to that realm. With that new user you will log into 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 participate in this tutorial, you need to complete the installation of Red Hat Single Sign-On and create the initial admin user as shown in the Install and Boot tutorial.

3.2. CREATE A NEW REALM

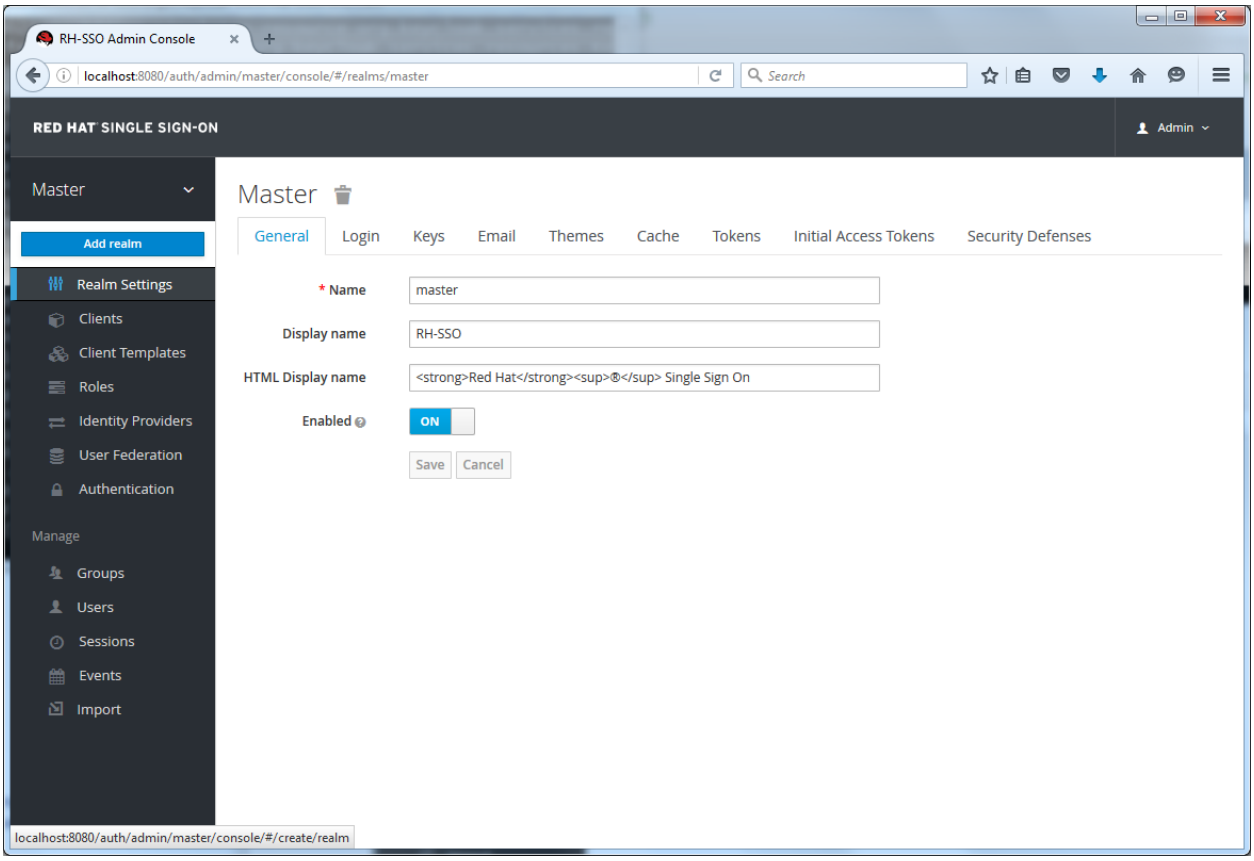
Login to the Red Hat Single Sign-On Admin Console using the account you created in the Install and Boot tutorial.

Admin Console Link

http://localhost:8080/auth/admin/

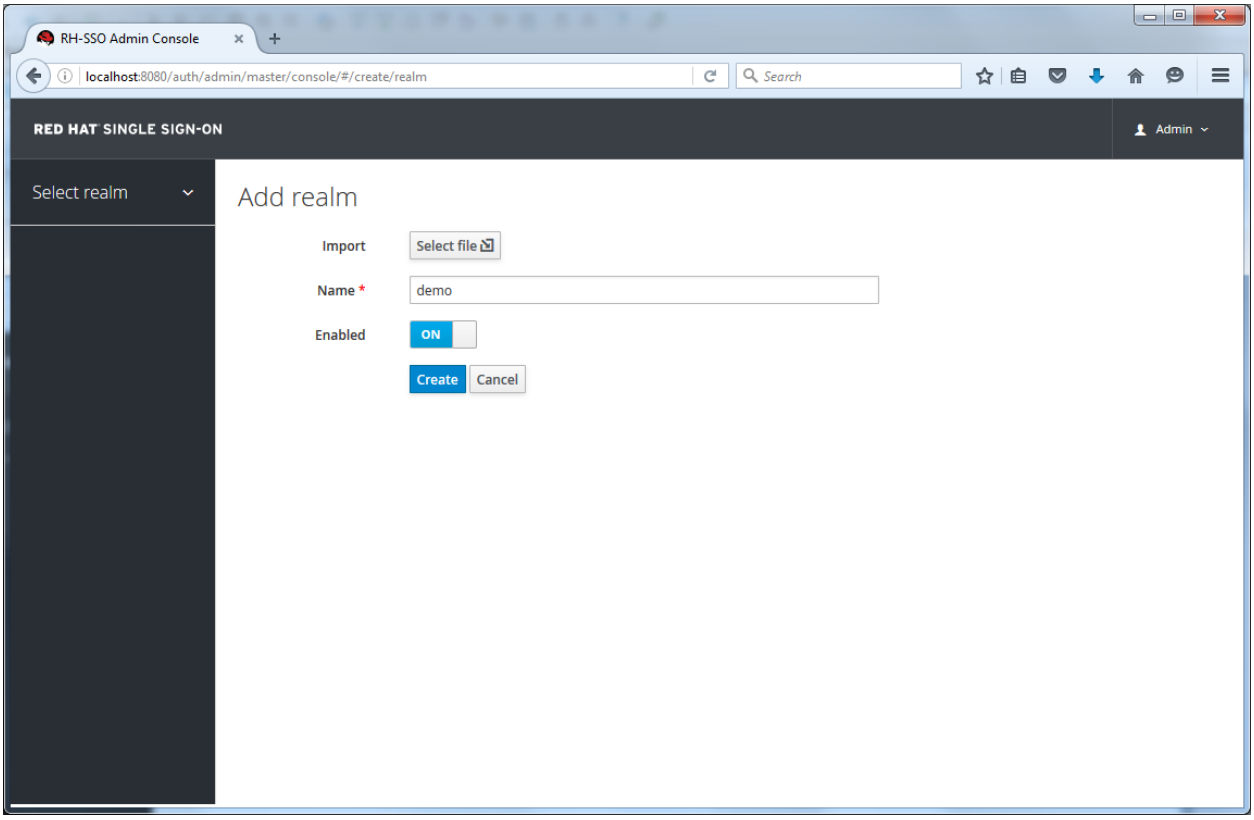
Place the mouse over the top left corner drop down menu that is titled with **`Master`**. If you are logged in the master realm this drop down menu lists all the realms created. The last entry of this drop down menu is always **`Add Realm`**. Click this to add a realm.

Add Realm Menu



This menu option will bring you to the **`Add Realm`** page. You will be creating a brand new realm from scratch so enter in **`demo`** for the realm name and click **`Create`**.

Create Realm

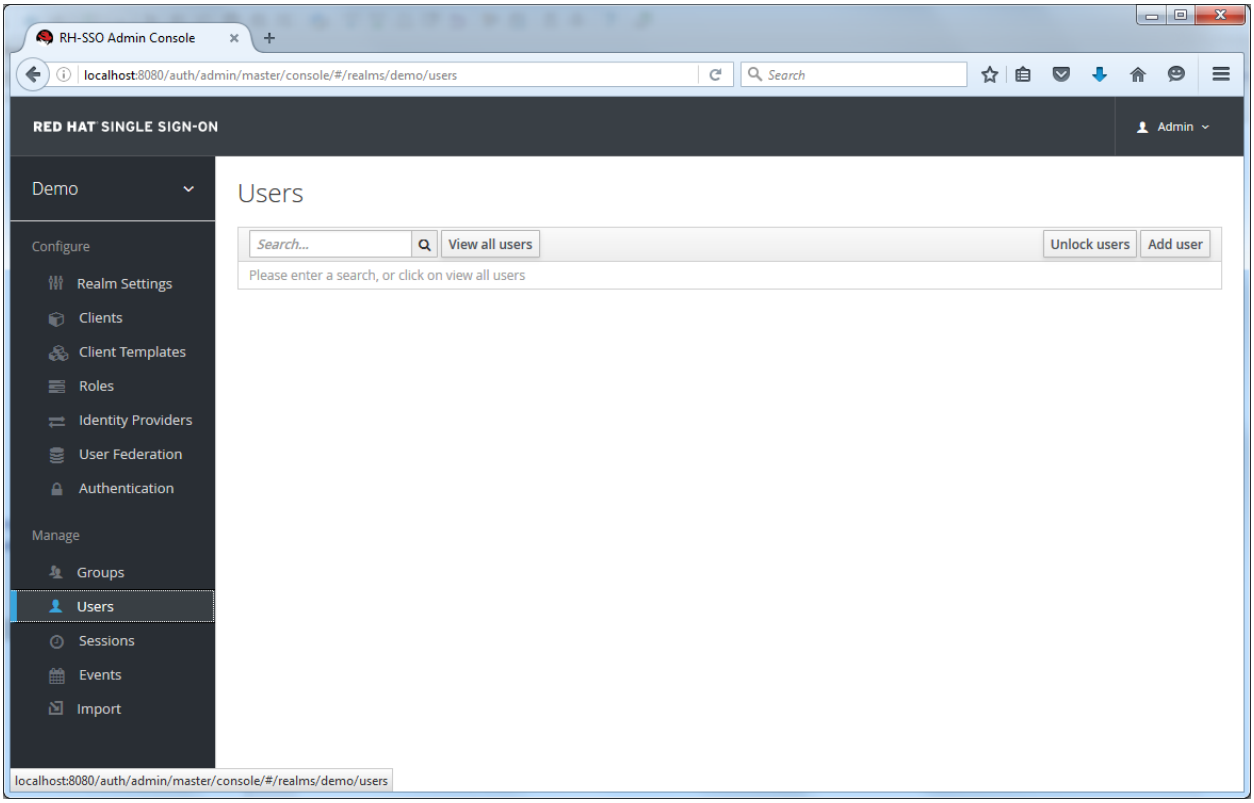


After creating the realm you are brought back to the main Admin Console page. The current realm will now be set to **`demo`**. You can switch between managing the **`master`** realm and the realm you just created by doing a mouseover on the top left corner drop down menu.

3.3. CREATE A NEW USER

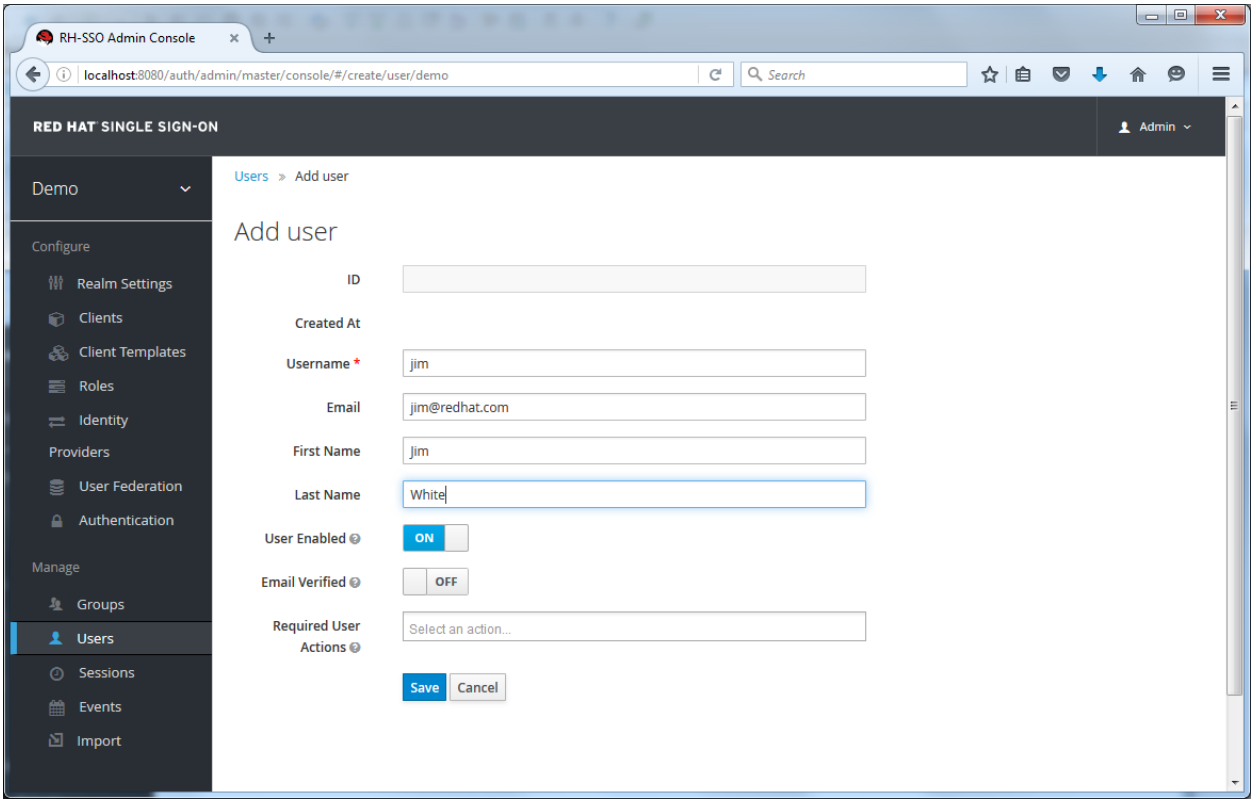
In this section you are going to create a new user in the **`demo`** realm as well as a temporary password for that account. The first step is to click on the **`Users`** in the left menu bar.

Users



This menu option brings you to the user list page. On the right side of the empty user list, you should see an **`Add User`** button. Click that to start creating your new user.

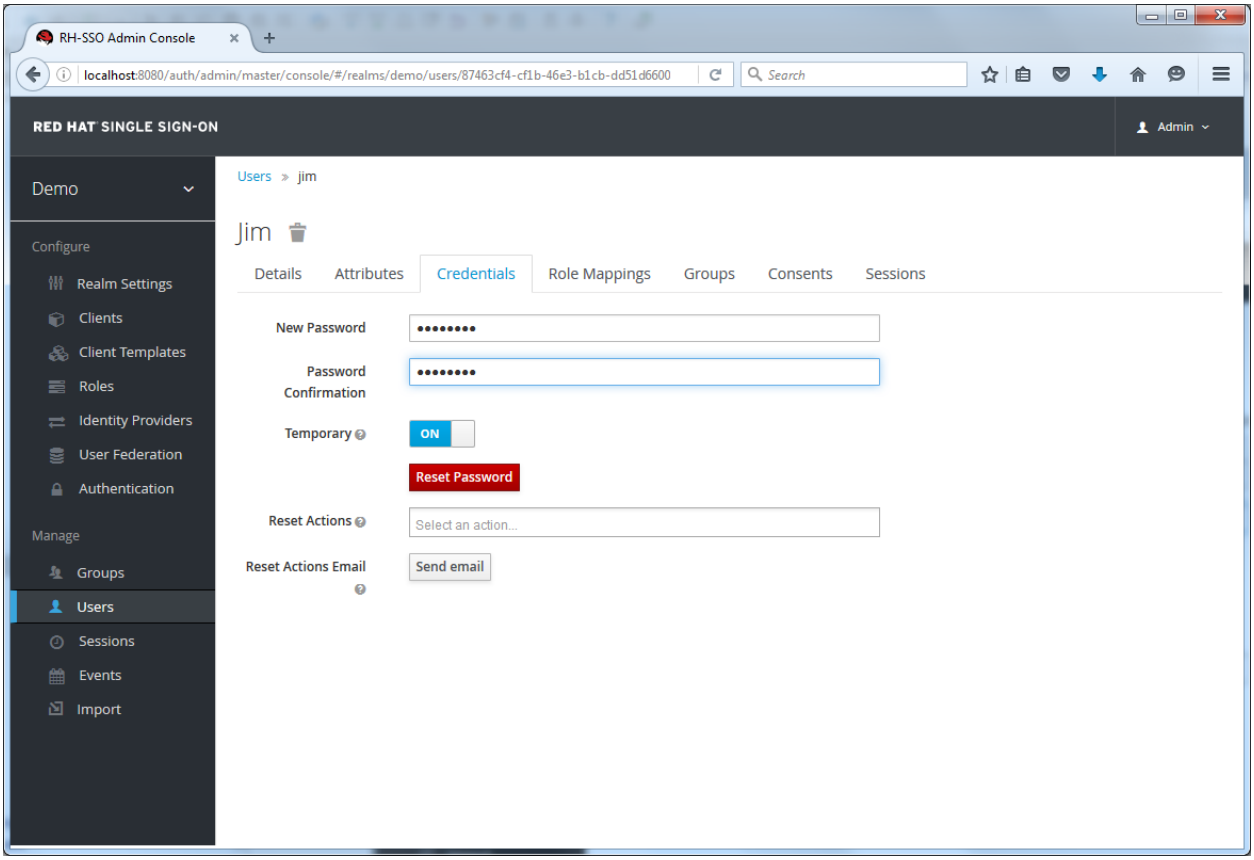
Add User



The only required field is **`Username`**. Click save. This will bring you to the management page for your new user.

The next step is to define a temporary password for your new user. Click on the **`Credentials`** tab to bring you to the page that will allow you to do this.

Set Temporary Password



Enter a new password and retype it within the **`Password Confirmation`** field. Once you do this a red **`Reset Password`** button should reappear. Clicking on that will reset the user's password to the new one you specified. Please note that this is a temporary password and the user will be required to change it after they first log in. You can make it permanent by flipping the **`Temporary`** switch from **`On`** to **`Off`** before you click the **`Reset Password`** button.

3.4. USER ACCOUNT SERVICE

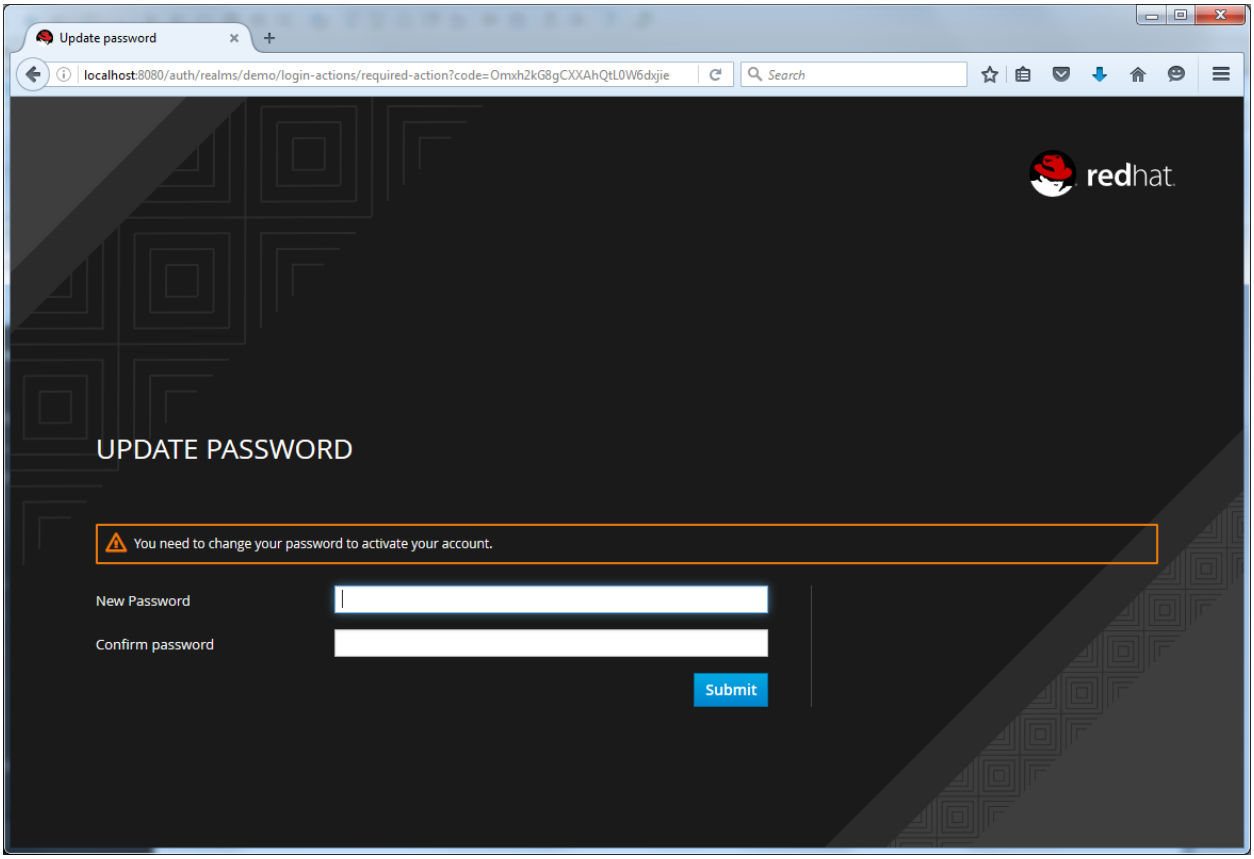
After creating the user, logout of the management console by clicking the right hand drop down menu and selecting **`Sign Off`**. Next, login to the User Account Service of your **`demo`** realm with the user you just created by clicking this link:

User Account Link

http://localhost:8080/auth/realms/demo/account

Enter the username and temporary password you created. You will be asked to change and create a permanent password after you successfully login.

Update Password



Finally, you will be brought to the User Account Service. Every user in a realm has access to this Account Service by default. It allows you to update profile information and change or add additional credentials. More information on this service is provided in the Server Administration Guide.

CHAPTER 4. SECURING A JBOSS SERVLET APPLICATION

In this section you will learn how to secure a Java Servlet application on the JBoss EAP 7 application server. You will learn how to install the Red Hat Single Sign-On Client Adapter onto a JBoss EAP 7 application server distribution. You will create and register a client application in the Red Hat Single Sign-On Admin Console. Finally, you will configure the application to be secured by Red Hat Single Sign-On.

4.1. BEFORE YOU START

Before you can participate in this tutorial, you need to complete the installation of Red Hat Single Sign-On and create the initial admin user as shown in the Install and Boot tutorial. There is one caveat to this. You have to run a separate JBoss EAP 7 instance on the same machine as the Red Hat Single Sign-On server. This separate instance will run your Java Servlet application. Because of this you will have to run the Red Hat Single Sign-On under a different port so that there are no port conflicts when running on the same machine. Use the **`jboss.socket.binding.port-offset`** system property on 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 Red Hat Single Sign-On server.

To boot the Red Hat Single Sign-On server:

Linux/Unix

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

Windows

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

After booting up Red Hat Single Sign-On, you can then access the admin console at http://localhost:8180/auth/admin/

4.2. INSTALL THE CLIENT ADAPTER

Download the JBoss EAP 7 distribution and unzip it into a directory on your machine.

Next download the RH-SSO-7.0.0-eap7-adapter.zip distribution.

Unzip this file into the root directory of your JBoss EAP 7 distribution.

Next perform the following actions:

Linux/Unix

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

Windows

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

This script will make the appropriate edits to the *…/standalone/configuration/standalone.xml* file of your app server distribution. Finally, just boot the application server.

Linux/Unix

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

Windows

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

4.3. DOWNLOAD, BUILD, DEPLOY APPLICATION CODE

The project and code for the application you are going to secure is available in Red Hat Developers GitHub. You will need the following installed on your machine and available in your PATH before you can continue:

- Java JDK 8
- Apache Maven 3.1.1 or higher

You can obtain the code by cloning the repository at https://github.com/redhat-developer/redhat-sso-quickstarts. Follow these steps to download the code, build it, and deploy it. Make sure your JBoss EAP 7 application server is started before you run these steps.

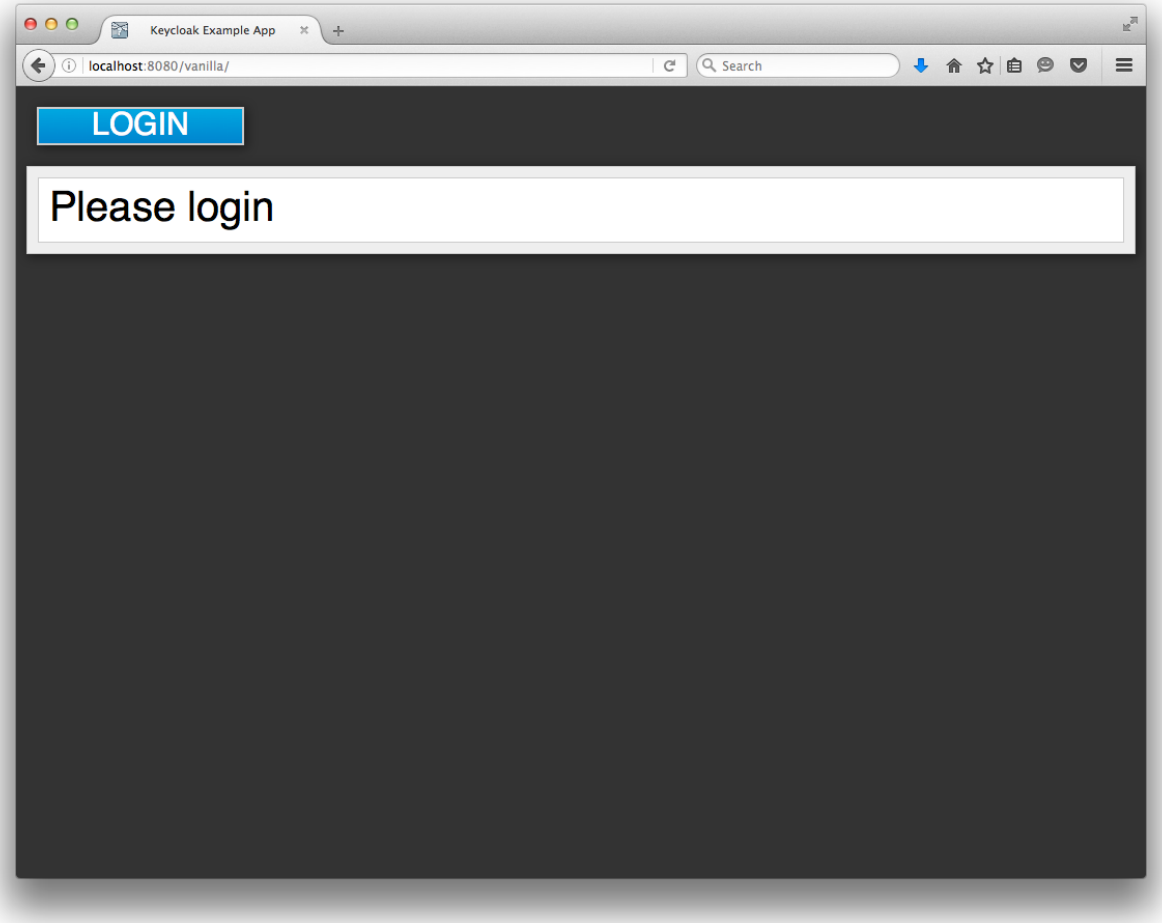
Clone Project

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

You should see some text scroll down in the application server console window. After the application is successfully deployed go to:

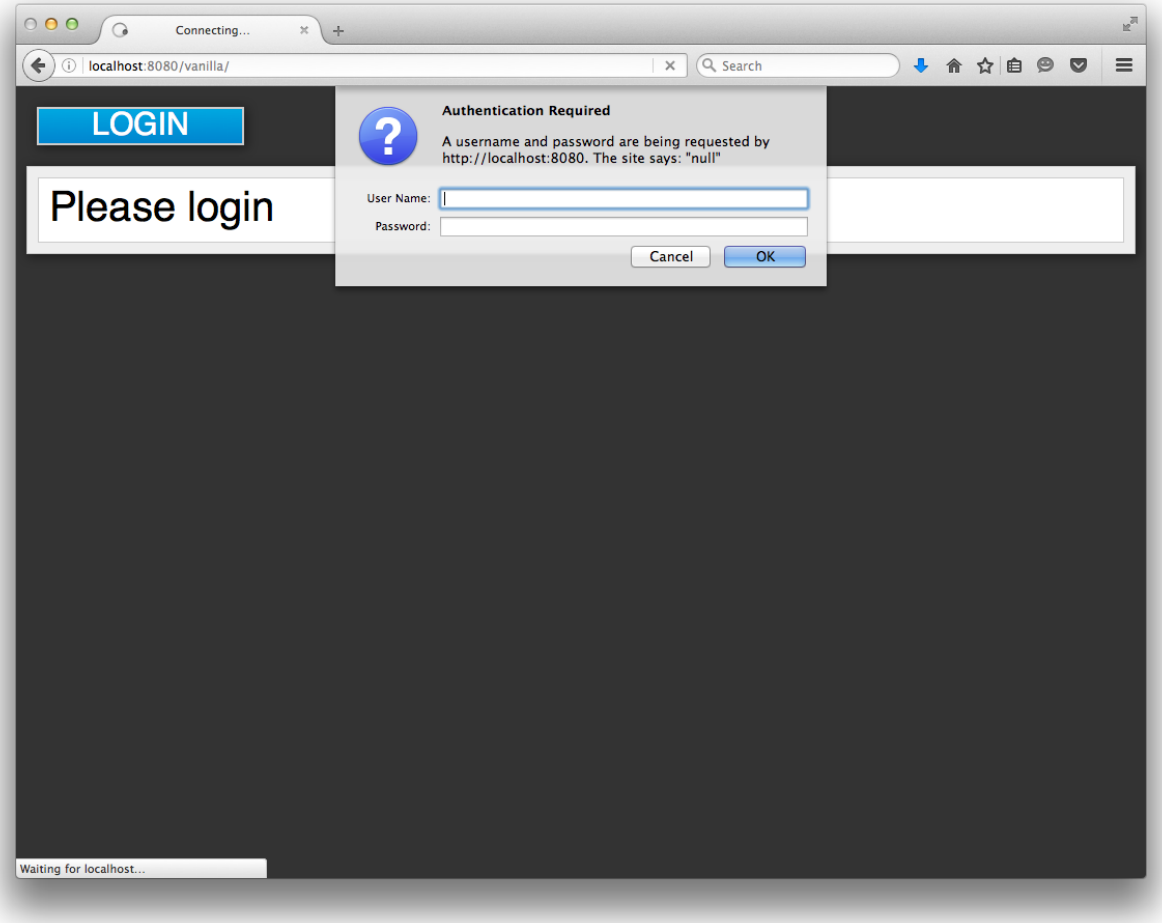
http://localhost:8080/vanilla

Application Login Page



If you open up the application's *web.xml* file you would see that the application is secured via **`BASIC`** authentication. If you click on the login button on the login page, the browser will pop up a BASIC auth login dialog.

Application Login Dialog

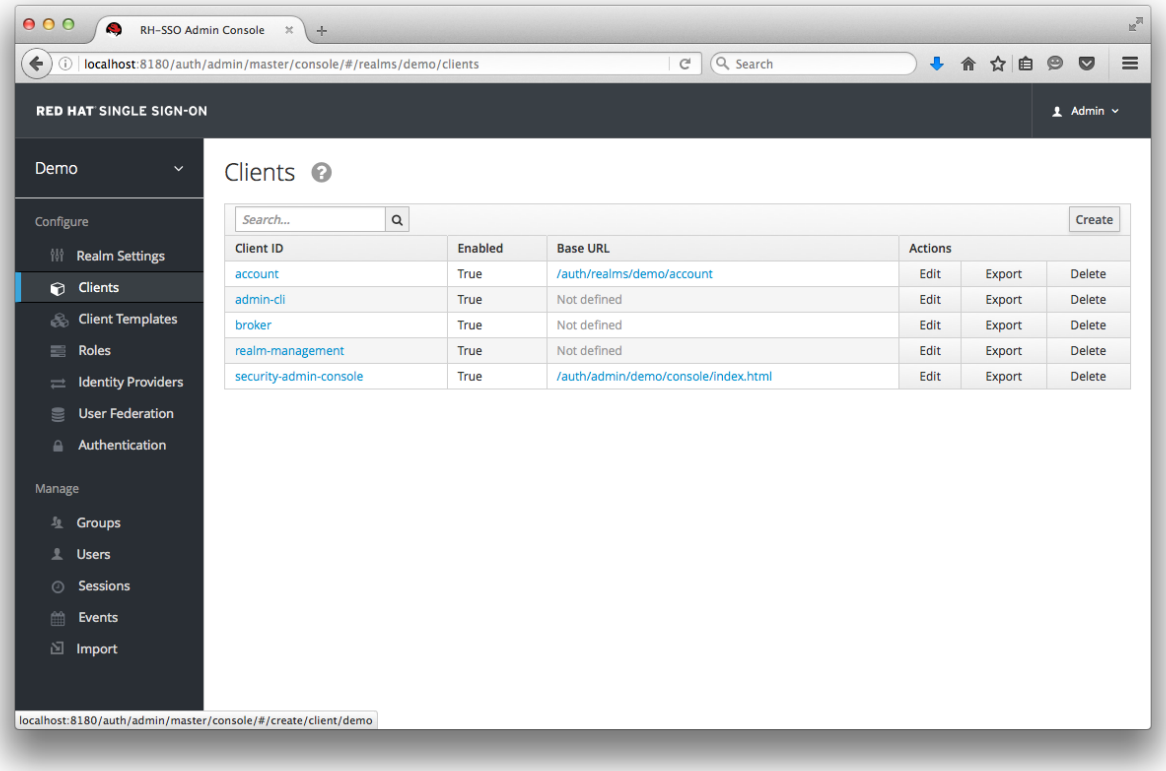


The application is not secured by any identity provider, so anything you enter in the dialog box will result in a **`Forbidden`** message being sent back by the server. The next section describes how you can take this deployed application and secure it.

4.4. CREATE AND REGISTER CLIENT

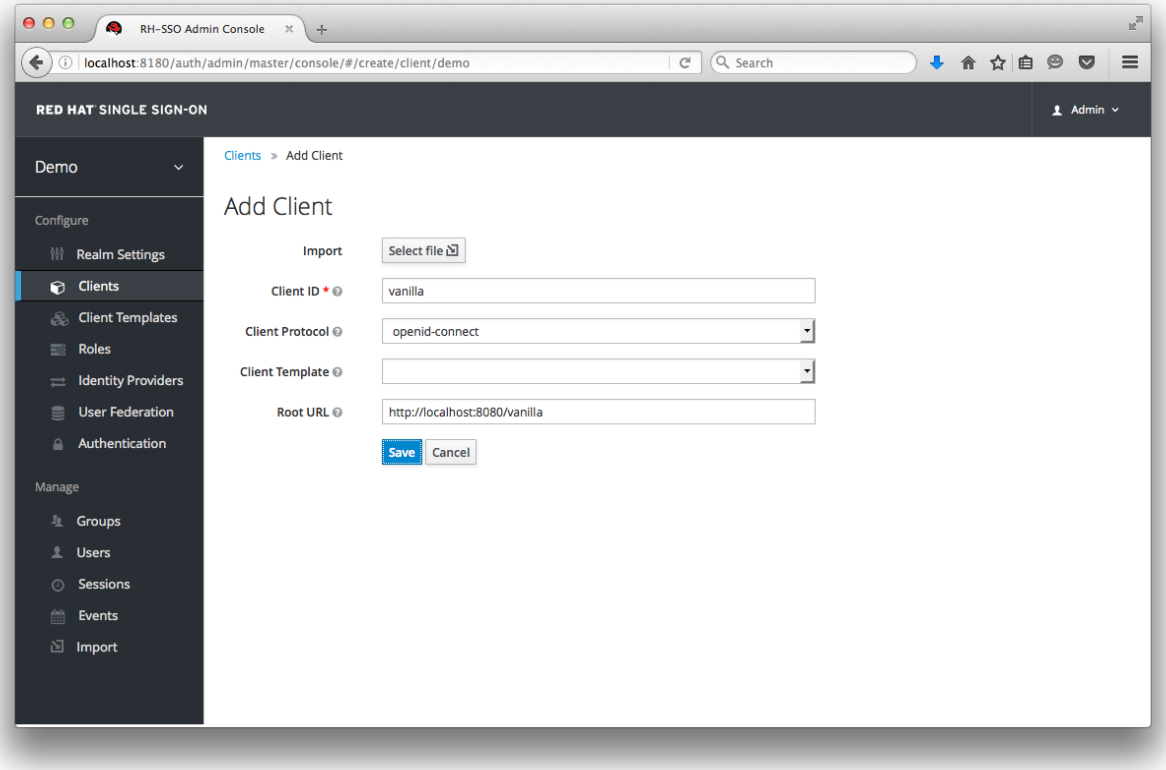
The next step you have to do is to define and register the client in the Red Hat Single Sign-On Admin Console. Log into the Admin Console with your admin account as you did in previous tutorials. In the top left hand drop down menu select and manage the **`demo`** realm. Click **`Clients`** in the left side menu. This will bring you to the **`Clients`** page.

Clients



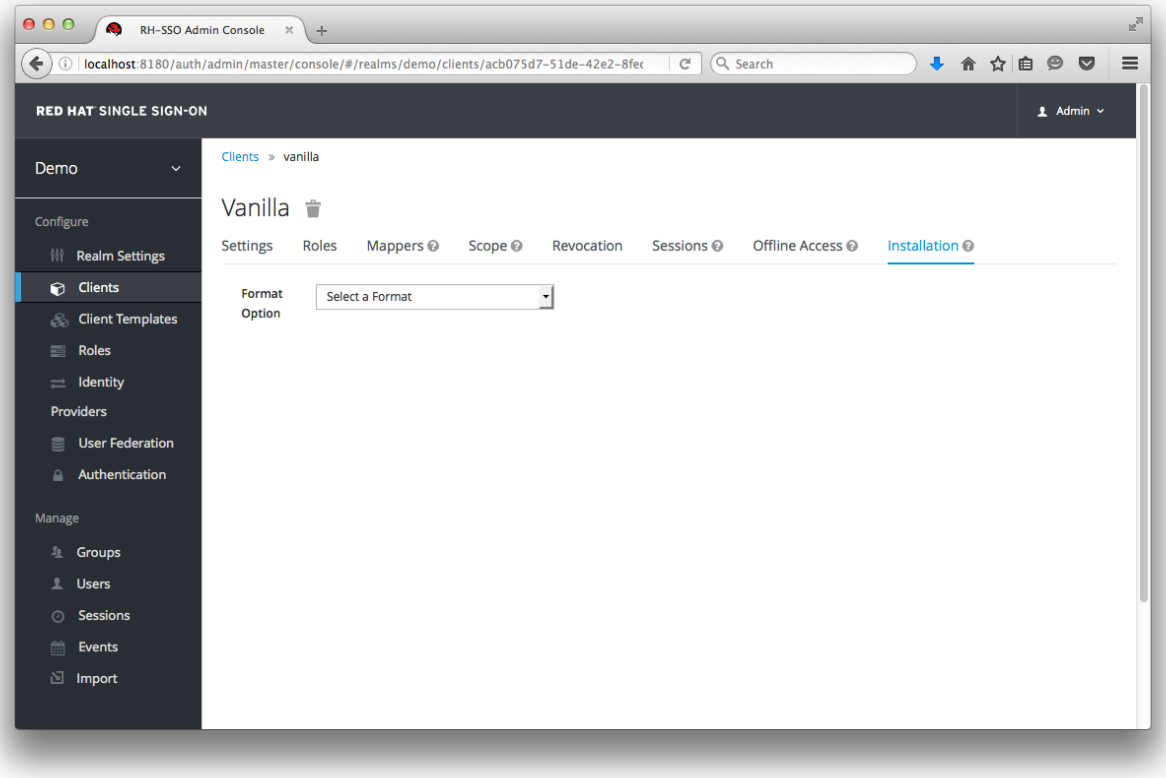
On the right hand side you should see a button named **`Create`**. Click this button and fill in the fields as shown below:

Add Client



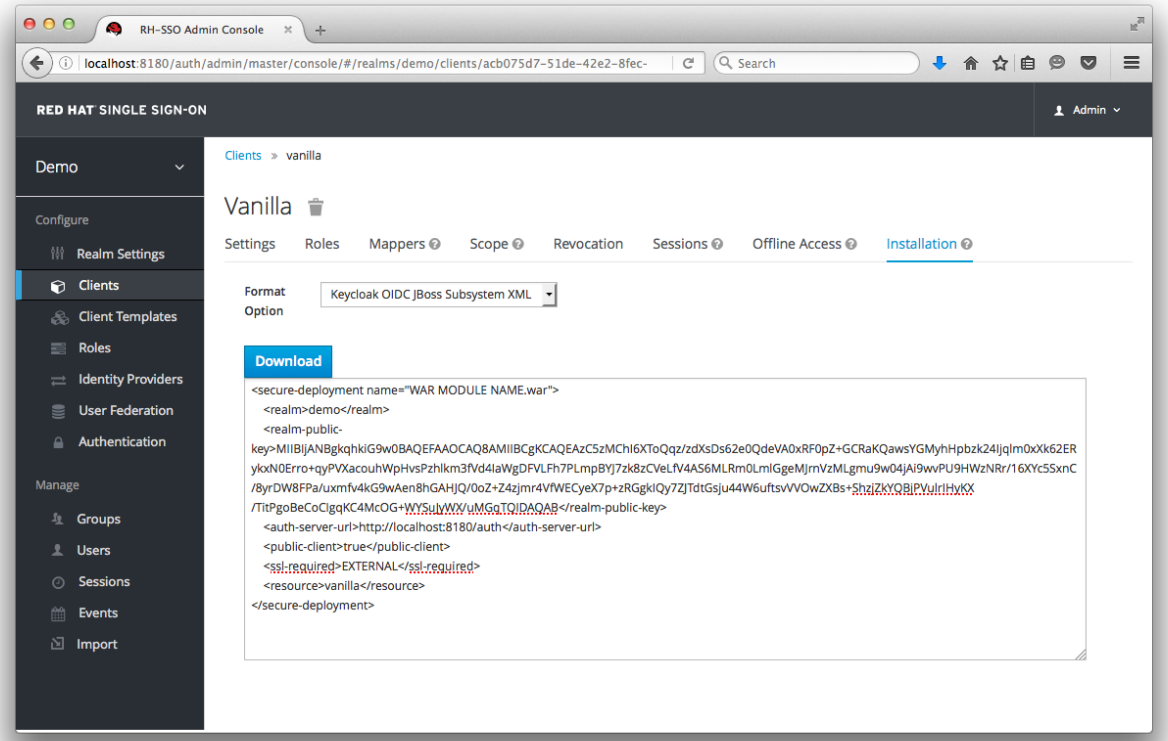
After clicking the **Save** button your client application entry will be created. You now have to go back to the JBoss EAP 7 instance that the application is deployed on and configure it so that this app is secured by Red Hat Single Sign-On. You can obtain a template for the configuration you need by going to the **Installation** tab in the client entry in the Red Hat Single Sign-On Admin Console.

Installation Tab



Select the **Keycloak OIDC JBoss Subsystem XML** option. This will generate an XML template that you'll need to cut and paste.

Template XML



4.5. CONFIGURE SUBSYSTEM

Now that you have copied the XML template from the **`Installation`** tab, you need to paste this into the *standalone.xml* file that lives in the *standalone/configuration* directory of the application server instance your application is deployed on. Open this file and search for the following text:

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

Modify this a little bit to prepare it for pasting in your template from the **`Installation`** tab.

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

Within the **`subsystem`** element, paste in the template. It will look something like this:

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="WAR MODULE NAME.war">
    <realm>demo</realm>
    <realm-public-key>MIIBIjANBgkqhkiG9B</realm-public-key>
    <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>
```

Change the **`WAR MODULE NAME`** text to be **`vanilla`** as follows:

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

Reboot your application's server and now when you visit http://localhost:8080/vanilla and hit the login button, you should get the Red Hat Single Sign-On login page. You can log in using the user you created in the Create New User chapter.