# How To – Setup Keycloak

**Install and Configure Keycloak standalone**

1. Extract the contents of the file *keycloak-3.3.0.CR2.tar.gz*, and place in target location.
2. Execute …/bin/standalone.sh

You should now have an instance of Keycloak running.

**Creating the Admin Account**

1. Navigate to <http://localhost:8080/auth> where you will be prompted to create the admin account. Do this and note the credentials down.

**Binding the machine’s ip address**

1. Edit …/standalone/configuration/standalone.xml Find the interfaces block, find the inet-address tags. Edit the ip addresses of *jboss.bind.address.management* and *jboss.bind.address* to the machine’s correct IP address.
2. Restart the keycloak instance

**Login as Admin**

1. Navigate to <http://host-ip:8080/auth/admin/> where you will be prompted for your newly created admin account credentials.

**Create the CFG-Classification realm**

1. In the top left corner dropdown menu that is titled Master, click **Add Realm**.
2. For the required name field enter *cfg-classification* , click on create.

**Realm Roles**

1. Click Roles in the left hand menu.
2. Click Add Role on the right hand side.
3. Enter role name “user”. Click on Save.
4. Repeat above steps for user role “cfg-admin”
5. Repeat above steps for role “analyst”

**Create first user account in cfg-classification realm**

1. In the left menu bar click **Users**. The user list page opens.
2. On the right side of the empty user list, click **Add User**.
3. Enter a Username, a first name and a last name. When you are finished, click **Save**. The management page for your new user opens.
4. The next step is to define a temporary password for your new user. Click the **Credentials** tab. Set Temporary Password. Click on Reset Password.

**User Role Mappings**

1. In the left menu bar, click users.
2. Click the edit button action on the username you would like to add role privileges to.
3. Click on the Role Mappings tab.
4. Click on Add selected to promote the *user* Available role to Assigned Roles.

**Creating and Registering the cfg-classification-webapp Client**

1. Click Clients in the left side menu. The Clients page opens.
2. On the right click **Create**.
3. Set Client ID to cfg-classification-webapp
4. Set Root URL to cfg-classication-webapp machine IP
5. Set Valid Redirect URIs to cfg-classication-webapp machine IP as well as keycloak machine IP *e.g. https://keycloak-ip/\**
6. Set Web Origins to cfg-classication-webapp machine IP
7. Click on SAVE

**How to setup the CFG-Classification-webapp with Keycloak**

1. Verify the file *keycloak.json* Specifically verify auth-server-url is set to correct http://ipaddr:port/auth

**Securing Application Server Services**

The CFG Classification Application utilizes java services that are served from an Apache Tomcat 8 container. The following libraries must be deployed in the lib folder of the Tomcat installation.

\*\*\****The implementation’s WEB-INF/lib folder is not sufficient these libraries must be in Tomcat’s main /lib folder.***

1. **Install the following jar in the tomcat/lib folder**

*bcpkix-jdk15on-1.56.jar*

*bcprov-jdk15on-1.56.jar*

*commons-codec-1.9.jar*

*commons-logging-1.2.jar*

*httpclient-4.5.jar*

*httpcore-4.4.1.jar*

*jackson-annotations-2.5.4.jar*

*jackson-core-2.5.4.jar*

*jackson-databind-2.5.4.jar*

*jboss-logging-3.3.0.Final.jar*

*keycloak-adapter-core-3.3.0.CR1.jar*

*keycloak-adapter-spi-3.3.0.CR1.jar*

*keycloak-authz-client-3.3.0.CR1.jar*

*keycloak-common-3.3.0.CR1.jar*

*keycloak-core-3.3.0.CR1.jar*

*keycloak-tomcat8-adapter-3.3.0.CR1.jar*

*keycloak-tomcat-adapter-spi-3.3.0.CR1.jar*

*keycloak-tomcat-core-adapter-3.3.0.CR1.jar*

***How to disable Keycloak Authentication on the Tomcat server***

1. The following xml tag sections must be commented out in the web.xml file found in the deployed project under the *tomcat webapp/cfg-task-service/WEB-INF* folder.

*<security-constraint>*

*<security-role>*

1. The *<valve>* xml tag section must be commented out of the context.xml file found in the deployed project under the tomcat *webapp/cfg-task-service/META-INF* folder
2. Restart Tomcat server

**How to setup Keycloak as a service using Systemd**

1. Create a wildfly user

*sudo groupadd –r wildfly*

*sudo useradd –r –g wildfly –d /opt/keycloak-3.3.0 –s /sbin/nologin wildfly*

1. Install Keycloak Standalone

*tar xvzf keycloak-3.3.0.CR2.tar.gz –C /opt*

*sudo ln –s /opt/keycloak-3.3.0.CR2 /opt/wildfly*

*sudo chown –R wildfly:wildfly /opt/keycloak-3.3.0.CR2*

*sudo chown –R wildfly:wildfly /opt/wildfly*

1. Configure systemd (copy files from /opt/wildfly/docs/contrib/scripts/systemd)

*sudo mkdir /etc/wildfly*

*sudo cp wildfly.conf /etc/wildfly/*

*sudo cp wildfly.service /etc/systemd/system/*

*sudo cp launch.sh /opt/wildfly/bin/*

*sudo chmod +x /opt/wildfly/bin/launch.sh*

1. Start and enable

*systemctl start wildfly.service*

*systemctl enable wildfly.service*

# Troubleshooting

|  |  |
| --- | --- |
| ***Reported Error*** | ***Cause*** |
| ***WE'RE SORRY ...***  ***Invalid parameter: redirect\_uri*** | ***The redirect\_uri you are trying to redirect to is not included in the list of valid Redirect URIs. Check Keycloak admin console under clients->Cfg-classification-webapp->Settings*** |
| ***Failed to load resource: the server responded with a status of 504 (Gateway Timeout)*** |  |
| ***GET http://ipaddr:port/auth/realms/cfg-classification/protocol/openid-connect/login-status-iframe.html net::ERR\_CONNECTION\_TIMED\_OUT*** | ***-ensure keycloak instance is up and running*** |
| ***Failed to load http://ipaddress/auth/realms/cfg-classification/protocol/openid-connect/token: No 'Access-Control-Allow-Origin' header is present on the requested resource. Origin 'http://ipaddress' is therefore not allowed access.*** | ***You need to add your ip address and port to the WebOrigins(Allowed CORS origins). In the Keycloak admin console add it under Clients->Cfg-classification-webapp->Settings->Web Origins*** |
| ***From cfg-task-service: This request requires HTTP authentication.*** | ***Check auth-server-url in keycloak.json in webapps/cfg-task-service/WEB-INF/*** |
| ***GET*** [***http://ipaddress:8080/cfg-task-service/service/datasets?env=prod***](http://ipaddress:8080/cfg-task-service/service/datasets?env=prod)***: No ‘Access-control-Allow-Origin’ header is present on the requested resource. Origin ‘http://clienthost:port’ is therefore not allowed access. The response had HTTP status code 403*** | ***Ensure <role-name>cfg-admin</role-name> and <role-name>user</role-name> are present in cfg-task-service web.xml under <auth-constraint>*** |

# How to setup custom Login page

1. Create the folder /keycloak-3.3.0.CR2/themes/cfg-classification/login
2. In the above folder drop the theme.properties and login.ftl files from the Keycloak source repository.
3. Create the */keycloak-3.3.0.CR2/themes/cfg-classification/login/resources/css* folder
4. In the above folder, copy in the corresponding theme.css file from the Keycloak repository.
5. From the Keycloak repository copy the following file and replace the existing one:

*/themes/base/login/messages/messages\_en.properties*

1. Login to Keycloak Admin console
2. Verify that you are in Cfg-classification realm. Click on *Themes*. For *Login Theme* select *cfg-classification* and click *Save*.
3. Restart Keycloak server instance.

# How to setup Keycloak for SSL encryption

Setting up Keycloak for ssl involves changing all ip address specifications to correct protocol and port values (i.e.verify steps 24 Set Root URL through 26 Set Web Origins). Next you must configure all the certificates on the web server, application server and Keycloak server. Instructions and sample scripts used in dev can be found at <https://github.com/hres/cfg-classification-keycloak/tree/master/scripts/ssl>