

Setting up Authentication in Design Room ONE with Keycloak

This document describes how to setup and use authentication and user management in Design Room ONE by means of integrating with Keycloak.

Table of Contents

Keycloak Server Installation4
Downloading Keycloak4
Keycloak Server Configuration – Quarkus4
Configuring port and hostname4
Initial Startup of Keycloak Server5
Creating a Realm Administrator5
Starting Keycloak Server5
Importing Previous Configuration6
Configuring the Realm
Keycloak Server Configuration – Wildfly (Applicable only for DRONE 2.2.x Versions)
Configuring port and hostname12
Initial Startup of Keycloak Server12
Creating a Realm Administrator13
Starting Keycloak Server13
Importing Previous Configuration13
Configuring the Realm16
Setting up Users and Roles
Creating Users20
Managing Access with Roles23
Importing Users from Active Directory27
Starting the Design Room ONE Server
Logging into the Design Room ONE Server with the New User
Exporting Models with Design Room ONE Integration Plugin
Prerequisites:
Single Sign-On with Jazz Authorization Server via OpenID40
Prerequisites
Creating a New Identify Provider in Keycloak40
Setting up JAS Configuration Security41
Creating a Relying Party Application in JAS42

Creating a New Identify Provider in Keycloak Continued	44
Logging in with JAS Authentication	46
Known Limitations	

Keycloak Server Installation

The instructions below use the following variables that need to be replaced with their actual values DRONE_HOST_NAME e.g. drone.mycomp.any KEYCLOAK_HOST_NAME e.g. keycloakhost.mycomp.any KEYCLOAK_IP_ADDRESS e.g. 10.20.30.40 KEYCLOAK_INSTALL_DIR e.g. C:\Install\Keycloak If Keycloak and Design Room ONE are installed on different machines, these machines should be able to communicate with HTTP/HTTPS requests. This usually means adjusting firewall settings to allow such

communications and ensuring all host names can be successfully resolved on every machine.

Downloading Keycloak

Keycloak can be downloaded from the following site:

https://www.keycloak.org/downloads

Check system_requirements.pdf document for supported versions.

Unzip the downloaded file into an installation directory of your choice. We will refer to this installation directory as **KEYCLOAK_INSTALL_DIR**.

Keycloak Server Configuration – Quarkus

This section is only applicable to Quarkus distribution of Keycloak.

Configuring port and hostname

By default, Keycloak will use **8080** as http port and **8443** as https port and **localhost** as host. To use custom values, the following commands can be used.

To configure http port:

http-port= <port></port>	KEYCLOAK_INSTALL_DIR/conf/keycloak.conf
http-port <port></port>	command line
To configure https port:	
https-port= <port></port>	KEYCLOAK_INSTALL_DIR/conf/keycloak.conf
https-port <port></port>	command line

To configure hostname:

hostname= <keycloak.mycomp.any></keycloak.mycomp.any>	KEYCLOAK_INSTALL_DIR/conf/keycloak.conf
hostname <keycloak.mycomp.any></keycloak.mycomp.any>	command line

e.g.,

```
kc.bat start --hostname <keycloak.mycomp.any> --http-port 8051
Refer this link for more.
```

Initial Startup of Keycloak Server

Run the standalone version of the server in **KEYCLOAK_INSTALL_DIR/bin** For Linux

kc.sh start --auto-build

For Windows

kc.bat start --auto-build

Creating a Realm Administrator

Note: This step must be performed on a machine running Keycloak.

Open a browser and navigate to https://KEYCLOAK_HOST_NAME:8443/ (or HTTP	endpoint).
Note: the browser may show a warning if e.g., certificate does not match the host	: name
← → C (① 127.0.0.1:8080/auth/	☆ ♀ 🥊 :

Welcome to Keycloak		
Administration Console Please create an initial admin user to get started.	User Guide, Admin REST API and	G Keycloak Project >
Username	Javadocs	☑ Mailing List >
Password confirmation		

Specify the admin credentials and press Create.

This admin user is a super user with all full access to Keycloak (realm creation, update, deletion, user creation, update, deletion, etc.)

Starting Keycloak Server

Stop the Keycloak server and start it again with --hostname parameter. Run the standalone version of the server in KEYCLOAK_INSTALL_DIR/bin For Linux,

kc.sh start --auto-build --hostname KEYCLOAK_IP_ADDRESS
For Windows,

kc.bat start --auto-build --hostname KEYCLOAK_IP_ADDRESS It is possible to use 0.0.0.0 instead of **KEYCLOAK_IP_ADDRESS** to allow connection from any interface, by default only connections from the same machine will be accepted. See Keycloak <u>documentation</u>

corresponding to the version specified in system_requirements.pdf for details.

Importing Previous Configuration

If you configured drone realm in version earlier than 2.3 of Design Room ONE you need to perform the following steps to keep your configuration, i.e., users and roles. If you are doing a fresh installation of Design Room ONE proceed with the next section.

- 1. Export your current realm data
 - a. Ensure your keycloak server instance is stopped
 - b. Run the below command to export your current drone Keycloak realm data

Run the command below to export realm data to a directory:

For Linux	
	TNICTALL

KEYCLOAK_INSTALL_DIR/bin/kc.sh export --dir <directory>
For Windows
KEYCLOAK_INSTALL_DIR\bin\kc.bat export --dir <directory>

To export to a single file, use below command:

For Linux					
KEYCLOAK	INSTALL	_DIR/bin/kc.sh	export	file	<file></file>
For Window	vs				
KEYCLOAK	INSTALL	_DIR\bin\kc.bat	export	file	<file></file>

- 2. Delete existing drone realm
 - a. Start your Keycloak server instance
 - b. Choose the **Realm** (i.e. drone) in the dropdown on the left panel.
 - c. Navigate to "Realm Setting" and then click on **Actions** -> **Delete** to DRONE realm as shown below.

											0	kca	admin 👻 😩
drone •	drone											Enabled	Action 👻
Manage	Realm settings are set	tings that con	rol the optio	ns for use	rs, applica	tions, roles, and e	groups in the current re	alm. Learn r	nore 🗹				Partial import
Clients	General Log	in Email	Themes	Keys	Events	Localization	Security defenses	Sessions	Tokens	Client policies	User registration		Partial export
Client scopes													Delete
Realm roles	Realm ID *	drone								<u>i</u>			
Users	Display name	Design Roo	m ONF										
Groups	Display name	Designition	II ONL										
Sessions	HTML Display name												
Events	Frontend URL ③												
Configure	Require SSL ③	External req	uests							•			
Realm settings													
Authentication	ACR to LoA Mapping				No attrib	utes have been de udd attributes, key :	fined yet. Click the below	-					
Identity providers					Datton to c	key p	air.						
User federation						Add an a	ittribute						
	User-managed access	O Off											
	Endpoints ③	OpenID Endp SAML 2.0 Ide	ooint Configu Intity Provide	uration 🗹 er Metada	ita 🛃								
		Save	Revert										

							0	kc	admin 🝷 😫
drone 🔻	drone Realm settings are set	ings that control the options	for users, applications, roles, a	d groups in the current re	alm. Learn mo	Tokens Client polic	User registration	Enabled	Action
Clients									Partial export
Realm roles	Realm ID *	drone							Delete
Users Groups	Display name	Design Room ONE			-				
Sessions	HTML Display name	De	ete realm?		×				
Events	Frontend URL ③	If you	delete this realm, all associate	l data will be removed.					
Configure	Require SSL ③	External requests			_	•			
Realm settings Authentication Identity providers User federation	ACR to LoA Mapping		No attributes have been button to add attributes, k Add	defined yet. Click the below by and value are required for y pair. In attribute	a				
	User-managed access	Off							
	Endpoints ③	OpenID Endpoint Configur SAML 2.0 Identity Provider	tion 🖒 Metadata 🖒						

3. Import Design Room ONE provided sample realm Run the following command

For Linux

KEYCLOAK_INSTALL_DIR/bin/kc.sh import --file
DR_ONE_INSTALL_DIR/DR_Install/Resources/Keycloak/drone-realmexport.json
For Windows
KEYCLOAK_INSTALL_DIR\bin\kc.bat import --file
DR_ONE_INSTALL_DIR/DR_Install/Resources/Keycloak/drone-realmexport.json
2022-07-06 18:14:15,665 INF0 [org.keycloak.exportimport.util.ImportUtils] (main) Realm 'drone' imported ◄
2022-07-06 18:14:15,701 INF0 [org.keycloak.services] (main) KC-SERVICES0032: Import finished successfully
2022-07-06 18:14:16,145 INF0 [io.quarkus] (main) Keycloak 18.0.0 on JVM (powered by Quarkus 2.7.5.Final) started in 9.666s

4. Import your exported realm

Run the command below to import from a directory: For Linux KEYCLOAK_INSTALL_DIR/bin/kc.sh import --dir <directory> For Windows KEYCLOAK_INSTALL_DIR\bin\kc.bat import --dir <directory>

Run the command below to import from a single file: For Linux KEYCLOAK_INSTALL_DIR/bin/kc.sh import --file <file> For Windows

KEYCLOAK_INSTALL_DIR\bin\kc.bat import --file <file>

- **5**. Start the Keycloak server, see <u>this section</u> for details.
- 6. Ensure that all previously created users have **view-realm** role as explained in <u>creating users</u> <u>section</u>
- **7.** Realm configuration is now complete, you should skip instructions in the next section and proceed with <u>Setting up Users and Roles</u>.

Refer Importing and Exporting Realms for more details.

Configuring the Realm

Note: this step is easier to do from the machine where Design Room ONE is installed

- 1. Import the realm data
 - a. Hover over **Realm** dropdown in top left corner and click on **Create Realm** and wait for it load to the below page.

= 🎯K	EYCLOAK			0	kcadmin 🝷	
Main Main master	•	Create realm A realm manages a set control.	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and au	henticate	the users that the	:y
Crea	ate Realm	Resource file	Drag a file here or browse to upload Browse Clear			
		Realm name *	Upload a JSON file			
		Enabled	On On			
			Create Cancel			
https://10.115.88.231:	:8443/admin/master/console,	/#/Main/add-realm				

- b. Click on Select File and point to drone-realm-export.json file. It can be found in machine where Design Room ONE is installed under following path: DR_ONE_INSTALL_DIR/DR_Install/Resources/Keycloak/drone-realm-export.json
- c. Then, click **Create**

			0	kcadmin 👻	
Main ← Main ✔ master	Create realm A realm manages a set control.	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manag	e and authenticate	the users that they	/
Create Realm	Resource file	Drag a file here or browse to upload Browse Clear 1 { 			
	Realm name *	drone			
	Enabled	C On			
		Create Cancel			

d. Your **Drone** realm should be created successfully as shown below:

		() kca	admin 👻 😩
drone 💌	drone		Enabled	Action 👻
Manage	Realm settings are set	go that control the options for users, applications, roles, and groups in the current realm. Learn more 🗠		Partial import
Clients	General Log	Email Themes Keys Events Localization Security defenses Sessions Tokens Client policies User registration		Partial export
Client scopes				Delete
Realm roles	Realm ID *	drone 🔮		
Users	Display name	Design Room ONE		
Groups	bispicy name	bulger room one		
Sessions	HTML Display name			
Events	Frontend URL ③			
Configure	Require SSL ③	External requests 🗸		
Realm settings				
Authentication	ACR to LoA Mapping	No attributes have been defined yet. Click the below button to add attributes, key and value are required for a		
Identity providers		key pair.		
User federation		O Add an attribute		
	User-managed access	Off Off		
	Endpoints ③	DpenID Endpoint Configuration 🛃		
		Save Revert		

- 2. Setup drone_client
 - a. Under **Clients** click on the drone_client link

					🕥 kcadmin 👻 🔔
drone Manage Clients	Clients Clients are applications and service Clients list Initial access t	es that can request authentication of a u	iser. Learn more 🗹		
Client scopes	Q Search for client →	Create client Import client			1-7 = < >
Realm roles Users	Client ID	Name	Туре	Description	Home URL
Groups	account	\${client_account}	OpenID Connect	-	https://10.115.88.231:8443/realms/drone/account/ 🗹
Sessions	account-console	\${client_account-console}	OpenID Connect	-	https://10.115.88.231:8443/realms/drone/account/ 🗹 🕴
Events	admin-cli	\${client_admin-cli}	OpenID Connect	-	- 1
	broker	\${client_broker}	OpenID Connect	-	- 1
Configure	drone client	Welcome to DR ONE	OpenID Connect	-	https://10.115.88.231:10101/dr/web 🗹
Realm settings	realm-management	\${client_realm-management}	OpenID Connect	-	- 1
Authentication	security-admin-console	\${client_security-admin-console}	OpenID Connect	-	https://10.115.88.231:8443/admin/drone/console/ 🗹
Identity providers					
User federation					1-7 - < >
https://10.115.88.231:8443/admin/master/console/	#/drone/clients/38b4bd0d-920e-4123-84eb-52	77961542ce/settings			4

Access settings

b. Click on the **Settings** top menu, scroll down and add **DRONE_HOST_NAME** (or ip address) accessible by other machines for the server Keycloak as valid redirect URIs as in example below. It is recommended to use lowercase letters.

Root URL ③	https://10.115.33.90:10101/dr/web	
Home URL ③		
Valid redirect URIs ③	http://10.115.33.90:*	•
	https://10.115.33.90:*	•
	http://localhost:*	٥
	https://localhost:*	•
	Add valid redirect URIs	
Valid post logout	+	0
redirect URIs 💿	• Add valid post logout redirect URIs	
Web origins ③	https://10.115.33.90:10101	٥
	• Add web origins	
Admin URL ③	https://10.115.33.90:10101/dr/web	

c. Make sure **Root URL**, **Admin URL**, and **Web Origins** fields are also updated with **DRONE_HOST_NAME** and hit **Save**

- d. On the top right Action dropdown, select Download adaptor config menu.
- e. In the **Download adaptor configs** popup, select **Keycloak OIDC JSON** in **format option** and click **Download**.

							0
drone 👻	Clients > Client details						
	drone_client	OpenID Connect			Enab	ed 🖲 Action	-
Manage	Clients are application	Download adapter configs			Do	wnload adapter c	onfig
Clients	Settings Role	Download adaptor configs	~		Ex	port	
Client scopes		Format option ③					
Realm roles	General Settings	Keycloak OIDC JSON	•	Jump to section	De	lete	
Users	Client ID * (2)	Details 💿					
Groups		ŧ		General Settings			
Sessions	Name ⑦	"realm": "drone", "auth-server-url": "https://10.115.88.231:8443/".		Access settings			
Events		"ssl-required": "external",					
	Description ③	"resource": "drone_client", "public-client": true.		Capability config			
Configure		"confidential-port": 0					
Realm settings	Always display in UI ③	3					
Authentication	Access settings			Logout settings			
Identity providere	j						
	Root URL ③		le				
User rederation	Harry HDL (C	Download Cancel					
	Home URL ()						
	Valid redirect URIs ③	https://drone.mycompany:*	•				
		http://drone.mycompany:*	•				
			-				
		Save Revert					

Note: Copy and paste **auth-server-url** and **ssl-required** properties in the file **DR_ONE_INSTALL_DIR/OnPrem_Design_Room/config/server-config.json**

under **dr_keycloak_config** object. Also change **"dr_auth"** attribute value to **"keycloak"**. Then the configuration file would look like this.

```
// Authentication (for accessing information stored in Design Room ONE)
```

// "none": Do not use any authentication. Everyone can access all designs.

// "jazz": Use Jazz authentication. User needs to be logged in to Jazz to acces
s designs.

// "keycloak": Use Keycloak authentication. User needs to be logged via keycloa
k to access designs.

"dr_auth": "keycloak",

```
//Keycloak configuration
"dr_keycloak_config": {
    "auth-server-url": "https://drone.mycomp.any:8443/",
    //Defines security level for Keycloak server
    //"none": HTTPS not required for any IP address
    //"external": Private IP and localhost can access without HTTPS
    //"all": HTTPS required for all IP addresses
    "ssl-required": "external"
```

```
}
```

Note: Make sure correct **KEYCLOAK_HOST_NAME** (or ip-address) specified in **auth-server-url** attribute, and the URL is accessible by machine where Design Room ONE server is installed and from user machines. It is recommended to use lowercase letters in the URLs.

Keycloak Server Configuration – Wildfly (Applicable only for DRONE 2.2.x Versions)

This section is only applicable to Wildfly distribution of Keycloak.

Configuring port and hostname

```
The script we will use by default is configured with the following file
KEYCLOAK_INSTALL_DIR/standalone/configuration/standalone.xml
<socket-binding-group name="standard-sockets" default-interface="public" port-</pre>
offset="${jboss.socket.binding.port-offset:0}">
        <socket-binding name="management-</pre>
http" interface="management" port="${jboss.management.http.port:9990}"/>
        <socket-binding name="management-</pre>
https" interface="management" port="${jboss.management.https.port:9993}"/>
        <socket-binding name="ajp" port="${jboss.ajp.port:8009}"/>
        <socket-binding name="http" port="${jboss.http.port:8080}"/>
        <socket-binding name="https" port="${jboss.https.port:8443}"/>
        <socket-binding name="txn-recovery-environment" port="4712"/>
        <socket-binding name="txn-status-manager" port="4713"/>
        <outbound-socket-binding name="mail-smtp">
            <remote-destination host="localhost" port="25"/>
        </outbound-socket-binding>
    </socket-binding-group>
```

By default, Keycloak will use **8080** as an http port, **8443** as an https port and **localhost** as host. If you decided to use custom **KEYCLOAK_HOST_NAME**, it should be specified as shown in bold below.

Initial Startup of Keycloak Server

Run the standalone version of the server in KEYCLOAK_INSTALL_DIR/bin For Linux standalone.sh

For Windows

standalone.bat

Creating a Realm Administrator

Note: This step must be performed on a machine running Keycloak.

Open a browser and navigate to <u>https://KEYCLOAK_HOST_NAME:8443/auth</u> (or HTTP endpoint). **Note:** the browser may show a warning if e.g. certificate does not match the host name

Welcome to Keycloak			
Administration Console Please create an initial admin user to get started.	Documentation > User Guide, Admin REST API and Javadocs	G Keycloak Project >	
Username Password		Mailing List >	
Password confirmation		濉 Report an issue >	
Create			
		Security CLOAK Welcome to Keycloak Please create an initial admin user to get started. User Guide, Admin REST API and Javadocs User Suide, Admin REST API and Javadocs Password confirmation Create	Comme to Keycloak Administration Console Plasse crate an initial admin user to get started. User Guide, Admin REST API and Javadocs User Guide, Admin REST API and Javadocs Mailing List > Mailing List > Mailing List >

Specify the admin credentials and press Create.

This admin user is a super user with all full access to Keycloak (realm creation, update, deletion, user creation, update, deletion, etc.)

Starting Keycloak Server

Stop the Keycloak server and start it again with -b parameter.

Run the standalone version of the server in KEYCLOAK_INSTALL_DIR/bin

For Linux

standalone.sh -b KEYCLOAK_IP_ADDRESS

For Windows

standalone.bat -b KEYCLOAK_IP_ADDRESS

It is possible to use 0.0.0.0 instead of **KEYCLOAK_IP_ADDRESS** to allow connection from any interface, by default only connections from the same machine will be accepted. See Keycloak <u>documentation</u> corresponding to the version specified in system_requirements.pdf for details.

Importing Previous Configuration

If you configured drone realm in version earlier than 2.3 of Design Room ONE you need to perform the following steps to keep your configuration, i.e., users and roles. If you are doing a fresh installation for Design Room ONE proceed with the next section.

- 1. Export your current realm data
 - c. Ensure your keycloak server instance is stopped
 - d. Run the below command to export your current drone Keycloak realm data

Run the command below:

For Linux
KEYCLOAK_INSTALL_DIR/bin/standalone.sh Dkeycloak.migration.action=export Dkeycloak.migration.provider=singleFile
-Dkeycloak.migration.file=/tmp/myOldRealm.json
For Windows
KEYCLOAK_INSTALL_DIR\bin\standalone.bat Dkeycloak.migration.action=export Dkeycloak.migration.provider=singleFile
-Dkeycloak.migration.file={path_to_temp_folder}\myOldRealm.json

- 2. Delete existing drone realm
 - a. Start your Keycloak server instance
 - b. Choose the **Realm** (i.e. drone) in the dropdown on the left panel.
 - c. Navigate to "Realm Setting" and then click on **Actions** -> **Delete** to DRONE realm as shown below.

											0	kca	admin 👻 😩
drone 💌	drone				P				-			Enabled	Action 👻
Manage	Realm settings are set	tings that con	troi the optio	ns tor use	rs, applica	tions, roles, and e	groups in the current re	aim. Learn r	nore 🔼				Partial import
Clients	General Log	in Email	Themes	Keys	Events	Localization	Security defenses	Sessions	Tokens	Client policies	User registration		Partial export
Client scopes													Delete
Realm roles	Realm ID *	drone								<u>i</u>			
Users	Display name	Design Roo	m ONF										
Groups	bispidy name	Designition	III OILE										
Sessions	HTML Display name												
Events	Frontend URL ③												
Configure	Require SSL 💿	External rec	uests							•			
Realm settings													
Authentication	ACR to LoA Mapping				No attrib	utes have been de dd attributes key :	fined yet. Click the below	2					
Identity providers					Dutton to a	key p	air.	-					
User federation						Add an a	ittribute						
	User-managed access	Off											
	Endpoints ③	OpenID End SAML 2.0 Id	point Configu entity Provide	ration 🗹 er Metada	ita 🗹								
		Save	Revert										

		٥	kca	admin 🝷 🕒
drone -	drone Realm settings are se General Log	tings that control the options for users, applications, roles, and groups in the current realm. Learn more 🕑	Enabled	Action 👻 Partial import Partial export
Client scopes				Delete
Realm roles Users	Realm ID *			
Groups	Display name	Design Room ONE Delete realm? ×		
Sessions	Frontend URL ③	If you delete this realm, all associated data will be removed.		
Configure	Require SSL ③	External requests		
Authentication Identity providers User federation	ACR to LoA Mapping	No attributes have been defined yet. Click the below button to add attributes, key and value are required for a key pair. C Add an attribute		
	User-managed access	Off		
	Endpoints 🕥	OpenID Endpoint Configuration 2 SAML 2.0 Identity Provider Metadata		

3. Import Design Room ONE provided sample realm

Run the following command

For Linux

KEYCLOAK_INSTALL_DIR/bin/standalone.sh -

Dkeycloak.migration.action=import -

Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.file= DR_ONE_INSTALL_DIR/DR_Install/Resources/Keycloak/drone-realmexport.json

For Windows

KEYCLOAK_INSTALL_DIR\bin\standalone.bat -

Dkeycloak.migration.action=import -

Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.file=

DR_ONE_INSTALL_DIR\DR_Install\Resources\Keycloak\drone-realm-

export.json

all/Resources/Keycloak/drone-realm-export.json 18:52:06,121 INFO [org.keycloak.exportimport.util.ImportUtils] (ServerService Thread Pool -- 68) Realm 'drone' imported 18:52:06,157 INFO [org.keycloak.services] (ServerService Thread Pool -- 68) KC-SERVICES0032: Import finished successfully 18:52:06,191 INFO [org.jboss.resteasy.resteasy_jaxrs.i18n] (ServerService Thread Pool -- 68) RESTEASY002225: Deploying javax.ws.rs.core.A

The Keycloak server will start, you should stop it again.

4. Import your exported realm

Run the command below:

For Linux

KEYCLOAK_INSTALL_DIR/bin/standalone.sh Dkeycloak.migration.action=import Dkeycloak.migration.provider=singleFile Dkeycloak.migration.file=/tmp/myOldRealm.json
For Windows

KEYCLOAK_INSTALL_DIR\bin\standalone.bat Dkeycloak.migration.action=import Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.file= {path_to_temp_folder}\myOldRealm.json

- 5. Start the Keycloak server, see this section for details.
- 6. Ensure that all previously created users have **view-realm** role as explained in <u>creating users</u> <u>section</u>
- **7.** Realm configuration is now complete, you should skip instructions in the next section and proceed with <u>Setting up Users and Roles</u>.

Configuring the Realm

Note: this step is easier to do from the machine where Design Room ONE is installed

- 1. Import the realm data
 - a. Hover over **Realm** dropdown in top left corner and click on **Create Realm** and wait for it load to the below page.

			0	kcadmin 🝷	
Main Main	Create realm A realm manages a set control.	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage an	d authenticate	the users that they	/
Create Realm	Resource file	Drag a file here or browse to upload Browse Clear			
	Realm name *	Upload a JSON file			
	Enabled	on On			
		Create Cancel			
https://10.115.88.231:8443/admin/master/console/#	/Main/add-realm				

- b. Click on Select File and point to drone-realm-export.json file. It can be found in machine where Design Room ONE is installed under following path: DR_ONE_INSTALL_DIR/DR_Install/Resources/Keycloak/drone-realm-export.json
- c. Then, click Create

			0	kcadmin 👻	
Main Main	Create realm A realm manages a set control.	of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only man	age and authenticate t	he users that they	,
Create Realm	Resource file	Drag a file here or browse to upload Browse Clear 1 { fifty: "drone", "realin": "drone", 4 "displayaeet: "besign Roon ONE", 5			
	Realm name *	drone			
	Enabled	On On			
		Create Cancel			

d. Your **Drone** realm should be created successfully as shown below:

		() kca	admin 👻 😩
drone 💌	drone		Enabled	Action 👻
Manage	Realm settings are set	go that control the options for users, applications, roles, and groups in the current realm. Learn more 🗠		Partial import
Clients	General Log	Email Themes Keys Events Localization Security defenses Sessions Tokens Client policies User registration		Partial export
Client scopes				Delete
Realm roles	Realm ID *	drone 🔮		
Users	Display name	Design Room ONE		
Groups	bispicy name	bulger room one		
Sessions	HTML Display name			
Events	Frontend URL ③			
Configure	Require SSL ③	External requests 🗸		
Realm settings				
Authentication	ACR to LoA Mapping	No attributes have been defined yet. Click the below button to add attributes, key and value are required for a		
Identity providers		key pair.		
User federation		O Add an attribute		
	User-managed access	Off		
	Endpoints ③	DpenID Endpoint Configuration 🛃		
		Save Revert		

- 2. Setup drone_client
 - a. Under **Clients** click on the drone_client link

					🕑 kcadmin 👻 🤮
drone Manage Clients Client scopes	Clients Clients are applications and service Clients list Initial access to Q. Search for client →	es that can request authentication of a to oken Client registration	user. Learn more 🗹		1-7 • < >
Realm roles	Client ID	Name	Туре	Description	Home URL
Groups	account	\${client_account}	OpenID Connect	-	https://10.115.88.231:8443/realms/drone/account/ 🗹
Sessions	account-console	\${client_account-console}	OpenID Connect	-	https://10.115.88.231:8443/realms/drone/account/ 🗹
Events	admin-cli	\${client_admin-cli}	OpenID Connect	-	- :
Lyong	broker	\${client_broker}	OpenID Connect	-	- 1
Configure	drone_client	Welcome to DR ONE	OpenID Connect	-	https://10.115.88.231:10101/dr/web 🗹
Realm settings	realm-management	\${client_realm-management}	OpenID Connect	-	- 1
Authentication	security-admin-console	\${client_security-admin-console}	OpenID Connect	-	https://10.115.88.231:8443/admin/drone/console/ 🗹
Identity providers User federation	7/dronycilanty/3854500-920a-4123-84ab-52	279815422e/nettings			1-7 + < >

b. Click on the **Settings** top menu, scroll down and add **DRONE_HOST_NAME** (or ip address) accessible by other machines for the server Keycloak as valid redirect URIs as shown in example below. It is recommended to use lowercase letters.

Access settings

Root URL ⑦	https://10.115.33.90:10101/dr/web	
Home URL ③		
Valid redirect URIs ③	http://10.115.33.90:*	•
	https://10.115.33.90:*	•
	http://localhost:*	•
	https://localhost:*	•
	Add valid redirect URIs	
Valid post logout	+	•
redirect URIs ③	Add valid post logout redirect URIs	
Web origins ③	https://10.115.33.90:10101	•
	• Add web origins	
Admin URL ③	https://10.115.33.90:10101/dr/web	

c. Make sure **Root URL**, **Admin URL**, and **Web Origins** fields are also updated with **DRONE_HOST_NAME** and hit **Save**

- d. On the top right Action dropdown, select Download adaptor config menu.
- e. In the **Download adaptor configs** popup, select **Keycloak OIDC JSON** in **format option** and click **Download**.

						0
drone 👻	Clients > Client details					
	drone_client	penID Connect			Enabled ③ Action	-
Manage	Clients are application	Developed adapter configs			Download adapter co	onfig
Clients	Settings Role	Download adaptor configs	×		Export	
Client scopes		Format option 💿	_			
Realm roles	General Settings	Keycloak OIDC JSON	- Jump to	section	Delete	
Users		Details 🗇				
Groups	Client ID - @	ł	Gene	ral Settings		
Sessions	Name ⑦	"realm": "drone",	Acces			
		auth-server-uni : https://10.115.88.231.8443/ , "ssl-required": "external",	P to be			
Events	Description ③	"resource": "drone_client",	Capal	bility config		
Carlinua		confidential-port": 0				
Configure	Always display in UI 💿	}	Login			
Realm settings			Logo	ut settings		
Authentication	Access settings					
Identity providers	Root URL ①		te.			
User federation		Download Cancel				
	Home URL ③	Connect				
	Valid redirect URIs ③	https://drone.mycompany:*	•			
		http://drone.mycompany:*	•			
			-			
	10	Save Revert				

Note : Copy and paste auth-server-url and ssl-required properties in the file DR_ONE_INSTALL_DIR/OnPrem_Design_Room/config/server-config.json

under **dr_keycloak_config** object. Also change **"dr_auth"** attribute value to **"keycloak"**. Then the configuration file would look like this.

```
// Authentication (for accessing information stored in Design Room ONE)
```

// "none": Do not use any authentication. Everyone can access all designs.

// "jazz": Use Jazz authentication. User needs to be logged in to Jazz to acces
s designs.

// "keycloak": Use Keycloak authentication. User needs to be logged via keycloa
k to access designs.

"dr_auth": "keycloak",

```
//Keycloak configuration
"dr_keycloak_config": {
    "auth-server-url": "https://keycloak.mycomp.any:8443/auth/",
    //Defines security level for Keycloak server
    //"none": HTTPS not required for any IP address
    //"external": Private IP and localhost can access without HTTPS
    //"all": HTTPS required for all IP addresses
    "ssl-required": "external"
```

```
}
```

Note: Make sure correct **KEYCLOAK_HOST_NAME** (or ip-address) specified in **auth-server-url** attribute and the URL is accessible by machine where Design Room ONE server is installed and from user machines. It is recommended to use lowercase letters in the URLs.

Setting up Users and Roles

Creating Users

Before we create a user, you can notice that some roles were created by default in Keycloak as below.

			0	kcadmin 👻 😩
Realm roles Realm roles are the roles that you define for use in	the current realm.	sam more 🖉		
,				
Q Search role by name → Create role	e			1-6 - >
Role name	Composite	Description		
default-roles-drone 👁	True	\${role_default-roles}		1
drone_user	False	A user in DRONE must have this role to login		:
offline_access	False	\${role_offline-access}		1
sample_all_access	False	This role gives read and write access to all designs.		:
sample_partial_access	False	This role will give read access to all design starting with traffic		:
uma_authorization	False	\${role_uma_authorization}		:
				1-6 👻 < >
	Realm roles Realm roles are the roles that you define for use in Q. Search role by name → Create rol Role name default-roles-drone O default-roles-drone O default-roles-droles-d	Realm roles Realm roles are the roles that you define for use in the current realm. Realm roles are the roles that you define for use in the current realm. Realm roles are the roles that you define for use in the current realm. Realm roles are the roles that you define for use in the current realm. Rele name Composite default-roles-drone O True default-roles-drone O True offline_access Palse sample_atl_access Palse uma_authorization Palse	Realm roles Realm roles are the roles that you define for use in the current realm. Learn more of the second sec	Fermine Caretorole by name Caretorole Caretorole Ture Specification Specification Caretorole Auser in DRONE must have this role to login Caretorole False Specification False Caretorole False This role gives read and write access to all design Caretorole False Caretorole Specification Caretorole False Specification Specification Caretorole False Caretorole Specification

Note: Under the **Realm Roles** tab, as shown below, you will notice that **drone_user** is a default role and is automatically assigned to newly created users. These roles are **required** by the Design Room ONE server normal operation.

		③ kcadmin 🕶 🕒
drone 👻	Users > User details	
Manage Clients	John Assign roles to john ×	Enabled Action •
Client scopes Realm roles	Q ▼ Filter by realm roles ▼ Q. Search by role name → 1-5 ▼ < >	1-1 - ← →
Users	Name Description	
Groups	drone_user A user in DRONE must have this role to login	:
Sessions	offline_access \${role_offline-access}	
Events	sample_all_access This role gives read and write access to all designs.	1-1 ▼ 〈 >
	Sample_partial_access This role will give read access to all design starting with traffic	
Configure	uma_authorization \${role_uma_authorization}	
Realm settings Authentication	1-5 • 〈 →	
User federation	Assign Cancel	

1. Create a user by clicking **Add user**.

					0	kcadmin 👻 😩
drone 🔹	Users Users are the users in the current realm.	Learn more 🕻				
Clients Client scopes Realm roles	▼ Default search ▼ Q. Search user	→ Add user	Delete user			1-1 ∗ < →
Users	Username	Email	Last name	First name	Status	
Groups	dradmin	0 -	-	-	-	1
Sessions						Delete
Events						1-1 * <
Configure Realm settings Authentication Identity providers						
User federation						

2. Fill in the necessary user information and click on **Create**.

			0	kcadmin 🝷	
drone 🗸	Users > Create user		 		
	Create user				
Manage					
Clients	1				
Client scopes	Required user actions	Select action •			
Realm roles	Ű				
Users	Username *	john			
Groups	Email	inhn@test.com			
Sessions		la und season			
Events	Email verified ⑦	No No			
	First name	John			
Configure					
Realm settings	Last name	Williams			
Authentication	Groups (2)				
Identity providers	Storbs ()	a an a sa a a a a a a a a a a a a a a a			
User federation	1				
	1	Create Cancel			
	1				
	1				
	1				
	1				L.

3. Verify the details in **User details** page.

								0	kcad	min 👻	
master 🔹	Users > User details	Users > User details				The user has been of the us	rreated	Enabled	Action	ĸ	
Manage									Lindbled	Action	
Clients	Details Attrit	outes Credentials	Role mapping	Groups	Consents	Identity provider links	Sessions				
Client scopes											
Realm roles	ID *	38659f18-350e-46	8c-b146-03e039c	1b5c4							
Users	Created at *	10/4/2023, 2:22:12 F	M								
Groups											
Sessions	Required user actions	Select action					•				
Events	Ū										
Confirme	Username *	dradmin									
Realm settings	Email										
Authentication		No									
Identity providers	Email verified ③										
User federation	First name										
	Last name										
		Save Revert									

4. Switch to **Credentials** tab and click on **Set password.**

		3 kcadmin 👻 📒
drone 👻	Users > User details	
Manage	john	Enabled Action •
Clients	Details Attributes Credentials Role mapping Groups Consents Identity provider links Sessions	
Client scopes	•	
Realm roles		
Users	No credentials	
Groups	This user does not have any credentials. You can set assessmed for this user	
Sessions	This user under the name any creations. The car passion in this user.	
Events	Set password	
	Credential Reset	
Configure		
Realm settings		
Authentication		
Identity providers		
User federation		

5. Enter the **Password** details, select **Temporary** preference toggle and click on **Save**.

		💿 kcadmin 🕶
drone 👻	Users > User details	Frahled Action
Manage		
Clients	Details Attributes Credentials Role mapping Groups Consents Identity provider links Sessions	
Client scopes	•	
Realm roles		
Users	Set password for john ×	
Groups	Password *	
Sessions		
Events	Password confirmation *	
	Temporary 🕐 💽 On	
Configure		
Realm settings	Save Cancel	
Authentication		
Identity providers		
User federation		

Managing Access with Roles

Access to designs in Design Room ONE is controlled with special attributes that can be specified for a role in Keycloak. The **dr_can_read** and **dr_can_write** attributes of roles give users respectively read and write access to specific designs. These attributes support wildcard as shown in the picture below.

 Under Realm Roles > sample_partial_access > Attributes, you can see that the dr_can_read and dr_can_write attributes are both set to "traffic*" which means that users or groups with this role will be able to read and write to all designs with names starting with "traffic".

				⑦ kcadmin ▾	
drone 👻	Realm roles > Role details				
	sample_partial_access			Action	•
Manage					
Clients	Details Attributes Users in role				
Client scopes	Key	Value			
Realm roles	dr_can_write	traffic*	•		
Users	dr. con rood	traffic#	•		
Groups	u_cai_leau	uame	•		
Sessions	Add an attribute				
Events					
Configure	Save Revert				
Realm settings					
Authentication					
Identity providers					
User federation					

Note: It is possible to specify several alternatives by using pipe (|) character.e.g., the following value **traffic* |*_secretproject |*alice*** will give read or write access (depending on the attribute it is specified in) to designs, which name either starts with **traffic**, or ends with **_secretproject** or contains the word **alice**. Note that design names are case sensitive.



2. To explicitly assign a role to a user, **Users** > Select the user > **Role Mapping**, click on Assign role.

3. Select the roles to be assigned for the user and click Assign.

				③ kcadmin ▾ 🎴
drone 👻	Users > User details			Enabled Action •
Manage Clients	Assign roles to john		×	
Client scopes Realm roles	Q Filter by realm roles Q Search by rol	e name	1-5 👻 < >	1-1 - ← ← →
Users	Name Desc	ption		
Groups	drone_user A use	in DRONE must have this role to login		:
Sessions	offline_access \${role	_offline-access}		
Events	sample_all_access This r	le gives read and write access to all designs.		1-1 ▼ < >
	sample_partial_access This r	le will give read access to all design starting with traffic		
Configure	uma_authorization \${role	_uma_authorization}		
Realm settings				
Authentication			1-5 - < >	
Identity providers				
User federation	Assign Cancel			

4. A user can implicitly get roles from the groups they belong to. To assign a role to a group, navigate to **Groups** > Select the group.

		🗿 kcadmin 🕶 🤐
master 👻		¢
	Q Search for groups →	Groups
Manage	Exact search	A group is a set of attributes and role mappings that can be applied to a user. You can create, edit, and delete groups and manage their child-
Clients	1-1 - ← →	parent organization. Learn more 🗹
Client scopes		
Realm roles	drone-test-group #	Q Filter groups → Create group 1-1 -
Users		Group name
Groups	1-1 + < >	drone-test-group
Sessions		
Events		1-1 < >
Configure		
Realm settings		
Authentication		
Identity providers		
User federation		

5. Under Role Mapping, click on **Assign role.**

							0	kcadmin 👻 😩
master -	Q. Search for groups	÷	< Groups > G	roup details				
Manage	Exact search		drone-tes	t-group				Action 🝷
Clients	_	1-1 - ← →	Child gro	ips Members	Attributes	Role mapping	1	
Client scopes								
Realm roles	drone-test-group	:					0	
Users								
Groups		1-1 -				No role	s for this group	
Sessions					You haven't c	reated any roles fo	or this group. Create a role to get started.	
Events								
			Ш				asigniture	
Configure								
Realm settings								
Authentication								
Identity providers								
User federation								

6. Select the role to be assigned and click on Assign.

						kcadmin 🝷 🙁
master 👻	0 Search for ground	< Gro	oups > Group details			
Manage	Assign roles to drone-	-test-group	toot group	×		Action 🝷
Client scopes	▼ Filter by realm roles ▼	Q Search by role name	\rightarrow	1-5 * < >		
Vsers	Name		Description			
Groups	admin		\${role_admin}			
Sessions	create-realm		\${role_create-realm}		t started.	
Events	default-roles-master		\${role_default-roles}			
	offline_access		\${role_offline-access}			
Configure	uma_authorization		{role_uma_authorization}			
Realm settings Authentication Identity providers				1-5 ▼ 〈 〉		
User federation	Assign Cancel					

7. Verify the changes below.

				0	kcadmin 👻 🧕
master •	Q. Search for groups →	< Groups > Group details drone-test-group	Role mapping updat	ted	Action 👻
Clients	1-1 • < >	Child groups Members Attribu	utes Role mapping		
Client scopes Realm roles	drone-test-group *	Q Search by name → ✔ H	ide inherited roles Assign role	Unassign	1-1 • < >
Users		Name	Inherited	Description	
Groups	1-1 - >	admin	False	\${role_admin}	:
Sessions					
Events					1-1 👻 < >
Configure		П			
Realm settings					
Authentication					
Identity providers					
User federation					

			🔊 kcadmin 👻 🦲
master	Users > User details dradmin		Enabled Action
Manage			
Clients	Details Attributes Credentials Role mapping Groups Conse	Identity provider links Sessions	
Client scopes	Q Search group → Join Group ✓ Direct membership	Leave	1-1 - ← →
Realm roles			
Users	Group membership	Path	
Groups	drone-test-group	/drone-test-group	Leave
Sessions			
Events			1-1 - 🗸 🔿
Configure			
Realm settings			
Authentication			
Identity providers			
User federation			

Note:

- a) A user will inherit all the roles from the groups they belong to. In the example below user **dradmin** belongs to **drone-test-group.**
- b) This means user **dradmin** automatically inherits **admin** role because it is assigned to the group.
- c) This results in any **my_partial_access_group** member including user **Steven** being able to read and write all designs with names starting with "traffic" because of the group membership.

Importing Users from Active Directory

Note: The Active Directory server reference is at the end of this section

1. Ensure you are in the **Drone** realm and click on **User Federation** left menu item Then select **Idap** from the dropdown

		0	kcadmin 👻	
drone 💌	User federation			
Manage				
Clients	To get started, select a provider from the list below.			
Client scopes	Add providers			
Realm roles				
Users	Add Kerberos providers Add Ldap providers			
Groups				
Sessions				
Events				
Carling				
Realm settings				
Authentication				
Identity providers				
User federation				

Note: Basic Active Directory configuration will be covered in this section. Additional configuration options are available in Keycloak with context sensitive help.

2. Set Vendor to Active Directory

			💿 kcadmin 🕶 🥘
drone •	User federation > Add	LDAP provider	
	Add LDAP pro	vider	
Manage			
Clients	General options		Jump to section
Client scopes	e chief al options		
Realm roles	UI display name 📩 💿	Idap	General options
Users			
Groups	Vendor * ③	Active Directory	Connection and authentication settings
Sessions		Active Directory 🗸	LDAP searching and updating
Events		Red Hat Directory Server	
	Connection and a	Tivoli	Synchronization settings
Configure		Novell eDirectory	Kerberos integration
Realm settings	Connection URL * 💿	Other	· · · · · · · · · · · · · · · · · · ·
Authentication	Enable StartTLS ③	Off	Cache settings
Identity providers			Advanced settings
User federation	Use Truststore SPI 💿	Always 🔹	rarenee eetange
	Connection pooling ③	Off Off	
	© Connection timeout		
	Saus Carrol		
	Save Cancel		

You should see some fields pre-filled with default values as shown below:

			🔊 kcadmin 🕶 🌏
drone 💌	LDAP searching a	and updating	Jump to section
Manage	Edit mode * 💿	•	General options
Clients Client scopes	Users DN * 🗇		Connection and authentication settings
Realm roles	Licemente L DAD		LDAP searching and updating
Users	attribute * ⑦	ui	Synchronization settings
Groups	RDN LDAP attribute	cn	Kerberos integration
Sessions	0		Reibelos integration
Events	UUID LDAP attribute	objectGUID	Cache settings
Configure	- 0		Advanced settings
Realm settings	User object classes *	person, organizationalPerson, user	
Authentication	-		
Identity providers	User LDAP filter 💿		
User federation	Search scope ③	One Level 🗸	
	Read timeout ⑦		
	Pagination ③	Off Off	
	Save Cancel		

3. Set the connection url and test the connection via the **Test connection** button as shown below:

Import Users 😡	ON Successi LDAP connection successful.	
Edit Mode 😡	\$	
Sync Registrations @	OFF	
* Vendor 😡	Active Directory \$	
* Username LDAP attribute @	cn	
* RDN LDAP attribute ©	cn	
* UUID LDAP attribute 😔	objectGUID	
* User Object Classes 🖗	organizationalPerson	
* Connection URL ©	Idap://steven.ad	Test connection
* Users DN ©	LDAP Users DN	
* Bind Type 😡	simple ¢	
Enable StartTLS 😡	OFF	

4. Set the active directory users database here.

* Users DN 🖗	ou=users,dc=hcl,dc=com	
* Bind Type 😡	simple	\$
Enable StartTLS 🔞	OFF	

5. Set the Active Directory (AD) admin credentials and test authentication to the AD server as shown below:

	1 · M· · · · · · · · · · · · · · · · · ·	
* Connection URL 😡	Idap://steven.ad Success! LDAP authentication successful.	Test connection
* Users DN @	ou=users,dc=hcl,dc=com	
* Bind Type 😡	simple \$	
Enable StartTLS ©	OFF	
* Bind DN Ø	cn=admin,dc=hcl,dc=com	
* Bind Credential @	•••••	Test authentication
Custom User LDAP Filter 🖗	LDAP Filter	

6. Leave the rest as is and scroll down and click **Save**, then click on **Synchronize all users** to import all existing users from AD to Keycloak

Connection Timeout 😡	Surcess! Sync of users finished surcessfully 1 imported users 0 undated users
Read Timeout 🖗	Read Timeout
Pagination @	ON
Kerberos Integration	
Allow Kerberos authentication @	OFF
Use Kerberos For Password Authentication Ø	OFF
Sync Settings	
Batch Size 😡	1000
Periodic Full Sync 😡	OFF
Periodic Changed Users Sync 😡	OFF
Cache Settings	
Cache Policy @	DEFAULT \$
	Save Cancel Synchronize changed users Synchronize all users Remove imported Unlink users

In our case 1, the user was imported from our active directory server.

7. If we now click on the Users menu, we see our imported user.

E WEYCLOAK					0	kcadmin 👻 😩
master 🗸	Users	ealm Learn more 🕫				
Manage						
Clients	User list					
Client scopes	▼Default search ▼ Q. Searc	h user Add user Delete user				1-3 -
Realm roles						
Users	Username	Email	Last name	First name	Status	
Groups	dradmin	0 -	-	-	-	:
Sessions	kcadmin	0 -	-	-	-	
Events	steven	● steven@test.com	Williams	Steven	-	ŧ
Configure						1-3 👻 < >
Realm settings						
Authentication						
Identity providers						
User federation						

8. Click on the user and observe the role mappings. The user should inherit all default roles (including **drone_user** and **view-realm**) to have access to the Design Room ONE server

				③ kcadmin ▾ 🥘
master 👻	Users > User details			
Manage	steven	_		Enabled Action •
Clients	Details Attributes Credentials Role mapping	Groups Consents Identity pre	ovider links Sessions	
Client scopes	Q. Search by name → ✓ Hide inherited roles	Assign role Unassign		1-1 - >
Realm roles				
Users	Name	Inherited	Description	
Groups	default-roles-master	False	\${role_default-roles}	:
Sessions				
Events				1-1 👻 < >
Configure				
Realm settings				
Authentication				
Identity providers				
User federation				

9. You can now login into Design Room ONE with the newly created user.

LDAP Directory Information Tree data reference

```
LDAPv3
  base <dc=hcl,dc=com> (default) with scope subtree
  filter: (objectclass=*)
  requesting: ALL
# hcl.com
dn: dc=hcl,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: hcl
dc: hcl
# admin, hcl.com
dn: cn=admin,dc=hcl,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
# users, hcl.com
dn: ou=users,dc=hcl,dc=com
objectClass: organizationalUnit
ou: users
# steven, users, hcl.com
dn: cn=steven,ou=users,dc=hcl,dc=com
cn: steven
sn: US
objectClass: organizationalPerson
# search result
search: 2
result: 0 Success
# numResponses: 5
# numEntries: 4
```

Summary: Hcl.com(organization)->users(organization unit or OU)->steven(Member of OU)

Starting the Design Room ONE Server

Ensure Design Room ONE server is started. Navigate to your Design Room ONE installation and launch the dr-deploy.js script.

Logging into the Design Room ONE Server with the New User

Users will be redirected to login page when they try to access Design Room ONE resources for the first time

\leftrightarrow \rightarrow C (i) localhost:8080/auth/realms/drone/	protocol/openid-connect/auth?client_id=drone_client&state=165267e5-6400-49d3-8531-8	o• ☆	0	🕐 :
				1
	DESIGN ROOM ONE			24
	Log In			
	Lisername or email			
	liphn			
	Password			
				L
	Log In			
A A				-4/

To log out of Design Room ONE click on the username in the top right corner of the page or press SHIFT + L on the keyboard and then click on **Log Out** menu item or hit Enter.

🕑 Desig	n Room ONE	CoffeeMachine	Ø Connect to Jazz	💄 john -
🛃 Designs 🗸	📰 Window -	★ Favorites -	⑦ Help <i></i> -	Log Out
🖺 Explorer 🗙			$\triangle \triangle \Delta $	داس
Coffee	Machine			U

Exporting Models with Design Room ONE Integration Plugin

Below, we will highlight the steps to login in the eclipse client once Keycloak is enabled on the Design Room ONE server.

Prerequisites:

- 1. Install the Design Room ONE Integration feature in your modeling software by following the steps in the Design Room ONE installation document
- 2. Then ensure that the Design Room ONE server is started successfully.

Right click on a project you want to export and select Export



Under the Modeling folder, select Design Room Model

a: =: ?: ??	: 🗊 🗂 : 💑 . : 🛖 . : 🛲 . I	A. : A: N	Sere the Ander			QUICK ACCESS
Explorer 🖾			Export			
🖻 🕏 🖫 •	Select					
ple Model odels	Export models to Desig	n Room Server			25	
Blank Packag	Select an export wizard	:				
	type filter text				8	
o active editor t	 Constall Java Java Modeling Design Room N Ecore Model Localized Model Themes - Skete Themes - UML UML 2.2 Mode UML 2.2 XMI Ir UML 2.4.1 XMI Plug-in Developm Run/Debug Tasks Team 	Nodel el ch I hterchange Model I Interchange Model lent				the second se
	?	< Back	Next >	Cancel	Finish	Path

Then enter the server URL for your Design Room ONE server.



If authentication is enabled on the server and the URL is valid, you will see the message with a link to login.

9: Y : Ø		•••		친 • 인 • 산 산 • 너) * 	Qu	ICK AC
plorer 🖾				Export			
3 🕸 🖫 🗸	Design Room	Model					
Model els	Step 1: Setu	ip a server c	onnection				
ank Package	Server URL						
	https://local	host:10101/a	ir				
	E.g https://se	ervername:10)101/dr				
	Allow ins	ecure conne	ection	-			
	You are not I	ogged in. Clic	ck <u>here</u> to login				
	Design name:	Sample Des	ign			Browse	
	Local Configu	ration					
	Export lo	cal configur	ation				
	Name of bra	nch, stream,	etc.				
🗐 Task L							
tive editor t							
						1	-
						1	
							Path
odel							1
ie P2 repos ibase	?		< Back	Next >	Cancel	Finish	ip

Note: If using RSAD with IBM Java sometimes users can get errors when connecting to Design Room ONE servers, for example if only TLS 1.2 is enabled on the server. To address this, it is recommended to make sure java version is at least **1.8_201** and add the following line in the end of **eclipse.ini** file in RSAD installation folder:

```
-Dcom.ibm.jsse2.overrideDefaultTLS=true
```

If Java version update cannot be performed an alternative solution could be adding the root certificate used to sign sandbox connection in the trust store of the JVM used by RSAD in addition to the change of **eclipse.ini** described above.

Once you click on hyperlink here, you will be redirected to the native browser to login

C O localhost:8080/auth/realms/drone/protocol/openid-connect/auth?response_type=code&client_id=drone_client&redirect_uri \$	0 🌒 i
DESIGN ROOM ONE	
Log In	
Username or email	
Password	
Log In	

After a successful login, you will see the message.

$\leftrightarrow \rightarrow C$ (i) localhost:8080/auth/realm:	s/drone/protocol/openid-connect/delegated	아 ☆ 😡 🛛 👔 🗄
	DESIGN ROOM ONE	
	Login Successful	
$\langle / /$	You may close this browser window and go back to your console application.	

Note: Refer <u>Known Limitations</u> for Quarkus distribution.

Once you go back to your modeling tool, you will see that you are logged in and can proceed to make your export



To logout, you can click on the **here** link again and the window below will open in your native browser.

← → C	A Not secure	https://localhost:8443/realms/drone/protocol/openid-connect/auth?client_id=drone_client&stat	A® ĉa Ĉ≞	ع ک)
		DESIGN ROOM ONE			
		Sign in to your account			
		Username or email			
		Password			
		Sign in			

Single Sign-On with Jazz Authorization Server via OpenID

Prerequisites

- 1. Jazz Authorization Server (JAS) is installed
- 2. Keycloak Server is installed

Creating a New Identify Provider in Keycloak

- 1. Login into Keycloak server as admin
- 2. Click on DRONE realm on the top left
- 3. Click on Identity Providers left menu open
- 4. Under the dropdown, select **OpenID Connect v1.0** as shown below

	KEYCLOAK							1 Admin Y
Dron		Identity	Providers					
								[]
	Realm Settings	Name	Brouidar	Eashlad	Hiddon	Link only	CI II ordor	Add provider Add provider
6	Clients	Name IAConvor	Provider	True	False	Elikoniy	Golorder	User-defined
	Client Scones	JAServer	olde	Inde	False	Faise		OpenID Connect v1.0
	Client scopes							Keycloak OpenID Connect
	Roles	_						GitHub
≓	Identity Providers							Twitter
								Facebook
	User Federation							Openshift v3 Google
	Authentication							GitLab
								LinkedIn
								Instagram
								BitBucket
	Groups							PayPal
	Users							StackOverflow
	Sessions							
	Events							
	Import							

5. Create the alias name of your choice and use the redirect URI below to proceed in the next steps

-		Identity Providers > Add Identity prov	vider
Dror	e ~		
Config	ure	Add identity provide	r
\$ \$\$	Realm Settings	Redirect URI 😡	http://iocalhost:8080/auth/realms/drone/broker/oldc/endpoint
Ð	Clients	* Alias 😡	oidc
æ	Client Scopes	Display Name 😡	IAServer
=	Roles	Enabled @	
1	Identity Providers	Lindoled ip	
8	User Federation	Store Tokens 😡	OFF
A	Authentication	Stored Tokens Readable 😡	OFF
Mana	îe	Trust Email 😡	OFF
łł,	Groups	Account Linking Only	OFF
1	Users	Hide on Login Bage O	
Ø	Sessions	Hide on Login Page ()	OFF
Ċ	Events	GUI order 😡	
2	Import	First Login Flow 😡	Tirst broker login
R	Export	Post Login Flow 😡	Y
		v OpenID Connect Config	0
		openio connect com	×
		* Authorization URL 😡	
		Pass login_hint @	OFF
		Pass current locale @	OFF
		* Token URL 😡	*
		Logout URL 😡	
		Backchannel Logout 😡	OFF
		Disable User Info 😡	OFF
		User Info URL 😡	
		* Client ID 😡	
		* Client Secret @	
		ireure O	

6. You will notice that you are missing a few required fields such as "Authorization URL", "Token URL", "Client ID" and "Client Secret". We will get these values from the jazz authorization server and complete the form later. Make note of the "Redirect URI" as we will need it in the next step.

Setting up JAS Configuration Security

If the JAS server is started with a self-signed certificate or no certificate at all, modify the **oauthProvider** element in the **appConfig.xml** file as shown below. Change the **httpsRequired** attribute to false.

DauthProvider id= JazzoP	
httpsRequired="false"	
autoAuthorize="true"	
customLoginURL="/jazzop	/form/login"
accessTokenLifetime="72	01"
authorizationGrantLifet	ime="604801">
<autoauthorizeclient>cl</autoauthorizeclient>	ient01
<databasestore dataso<="" td=""><td>urceRef="0AuthFvtDataSource" /></td></databasestore>	urceRef="0AuthFvtDataSource" />
/oauthProvider>	

Creating a Relying Party Application in JAS

1. Create a **body.json** file as shown below and make sure that you also add the above Keycloak redirect URI to the list of redirect_uris

```
"token endpoint auth method":"client secret basic",
"scope":"openid profile email general",
"grant types":[
 "authorization code",
 "client credentials",
 "implicit",
 "refresh token",
 "urn:ietf:params:oauth:grant-type:jwt-bearer"
],
"response types":[
 "code",
 "token",
 "id token token"
],
"application type":"web",
"subject type":"public",
"preauthorized scope":"openid profile email general",
"introspect tokens":true,
"trusted uri prefixes":[
 "https://keycloak.mycomp.any:*"
],
"redirect uris":[
 "http://keycloak.mycomp.any:8080/auth/realms/drone/broker/oidc/endpoint",
 "https://keycloak.mycomp.any:8443/auth/realms/drone/broker/oidc/endpoint"
]
```

Open command line and run the below command to create an application in the JAS server

```
curl --insecure --user admin:password --data @"./body.json"
http://jas.mycomp.any:9280/oidc/endpoint/jazzop/registration --header
"Content-Type: application/json"
```

2. If successful, the JAS server will respond with a response as shown below

"client_id_issued_at":1583359157,
"registration_client_uri":"https://localhost:9643/oidc/endpoint/jazzop/registration/d5852705ab4f4204ae29812373537277",
"client_secret_expires_at":0,
"token_endpoint_auth_method":"client_secret_basic",
"scope":"openid profile email general",
"grant_types":[
"authorization_code",
"client_credentials",
"implicit",
"refresh_token",
"urn:ietf:params:oauth:grant-type:jwt-bearer"
"response types":[
"code",
"token",
"id token token"
"application_type":"web",
"subject type":"public",
"preauthorized_scope":"openid profile email general",
"introspect tokens":true,
"trusted uri prefixes":[
"https://localhost:*/"
1,
"resource ids":[
1.
"client_id":"d5852705ab4f4204ae29812373537277",
"client_secret":"p7Da1WpAxs0ujm80mFn9pN2HDVXxtDEWXJy3pIa792TNgfUyGbU7tyKXPGSd",
"client_name":"d5852705ab4f4204ae29812373537277",
"redirect_uris":[
"http://localhost:8080/auth/realms/drone/broker/oidc/endpoint",
"https://localhost:8443/auth/realms/drone/broker/oidc/endpoint"
"allow_regexp_redirects":false

- 3. Note that we now have a valid **client_id** and **client_secret** to complete the creation of our identity provider application in Keycloak. Please make a note of that **client_id** and **client_secret**.
- Browsing to the public endpoint <u>http://jas.mycomp.any:9280/oidc/endpoint/jazzop/.well-known/openid-configuration</u> will provide the remaining Authorization and token URLs of the JAS server assuming the JAS http server is started locally and on port 9280. A sample response is shown below.

"introspection_endpoint":" <u>http://localhost:9280/oidc/endpoint/jazzop/introspect</u> "	
<pre>"coverage_map_endpoint":"<u>http://localhost:9280/oidc/endpoint/jazzop/coverage_map</u></pre>	<u>)</u> ",
"issuer":" <u>http://localhost:9280/oidc/endpoint/jazzop</u> ",	
"authorization_endpoint":" <u>http://localhost:9280/oidc/endpoint/jazzop/authoriz</u> e",	
"token_endpoint":" <u>http://localhost:9280/oidc/endpoint/jazzop/token</u> ",	
"jwks_uri":" <u>http://localhost:9280/oidc/endpoint/jazzop/jwk</u> ",	
"response_types_supported":[
"code",	
"token",	
"id_token token"	
],	
"subject_types_supported":[
"public"	
],	
"id_token_signing_alg_values_supported":[
"HS256"	
],	
"userinfo_endpoint":" <u>http://localhost:9280/oidc/endpoint/jazzop/userinfo</u> ",	
"registration_endpoint":" <u>http://localhost:9280/oidc/endpoint/jazzop/registration</u>	<u>1</u> ",
"scopes_supported":[
"openid",	
"general",	
"profile",	
"email",	
"address",	
"phone"	
],	
"claims supported":[
"sub",	
"groupIds",	
"name",	
"preferred username",	
"picture",	
"locale".	

5. We can now proceed back to Keycloak admin web page and finalize the identity provider form.

Creating a New Identify Provider in Keycloak Continued

6. Fill in the Client ID, Client Secret and other fields as shown in the picture below.

✓ OpenID Connect Config ②

* Authorization URL 😮	http://jas.mycomp.any:9280/oidc/endpoint/jazzop/authorize	
Pass login_hint 🕑	OFF	
Pass current locale 😧	OFF	
* Token URL 🕑	http://jas.mycomp.any:9280/oidc/endpoint/jazzop/token	
Logout URL 😧	http://jas.mycomp.any:9280/oidc/endpoint/jazzop/end_session	
Backchannel Logout 🕢	OFF	
Disable User Info 🚱	OFF	
User Info URL 🔞		
* Client Authentication 🕑	Client secret sent as post	~
* Client ID 🕝	4d94c7c76fd541ab8d6248a276e40400	
* Client Secret 🕑	•••••	۲
Issuer 😧		
Default Scopes 🕑		
Prompt 🕑	unspecified	~
Accepts prompt=none forward from client @	OFF	
Validate Signatures 🚱	OFF	

- 7. Make sure **Backchannel Logout** setting is off. After all required fields are completed, click the **Save** button.
- 8. Copy Logout URL and add it as the value "clm_end_session" property of DR_ONE_INSTALL_DIR/OnPrem_Design_Room/config/server-config.json

The property should be placed inside "dr_keycloak_config" object

```
//Keycloak configuration
```

```
"dr_keycloak_config": {
    "auth-server-url": "https://localhost:8443/auth",
    //Defines security level for Keycloak server
    //"none": HTTPS not required for any IP address
    //"external": Private IP and localhost can access without HTTPS
    //"all" : HTTPS required for all IP addresses
    "ssl-required": "external",
    "clm_end_session": https://jas.mycomp.any:9280/oidc/endpoint/jazzop/end sessi
on
```

9. Restart Design Room ONE server to apply the configuration changes.

Logging in with JAS Authentication

 Ensure that Keycloak is enabled in your Design Room ONE server (i.e., server-config.json) file. Start your Design Room ONE server and navigate to some URL e.g. <u>https://drone.mycomp.any:10101/dr/web</u> You should see the new identify provider option (JAServer) as shown here.

Log In Username or email JAServer	D	ESIGN ROOM	1 ONE	
Username or email JAServer Jassword		Log In		
Password	Username or email		JAServer	
	Password			

2. Click on JAServer option and you will be redirected to the JAS server to login

AUTHORIZATION The Jazz Authorization Serve	r at localhost requires a user ID and password:
000	User ID:
	Password:
	Log In
-	
Icensed Material - Property of IBM Corp. © Cop go, Jazz, and Rational are trademarks of IBM O cippes is a trademark of Echaer Foundation, inc rademarks of Dracle and/or its attiliance in the U	yright IBM Corp. and its licensors 2008, 2018. All Rights Reserved. IBM, the IBM Corporation, in the United States, other countries and regions, or both. Built on 2. Jowa and all Jowa-based trademarks and logon are trademarks or registered rited States, other countries and regions, or both.
	Rational software

3. After a successful login you will be redirected back to the Keycloak server to add additional details for the user.

Upo	late Account	Information	
Username			
ADMIN			
Email			
First name			
Last name			

After a successful completion of the form, you will be directed back to the Design Room ONE page you navigated.

Known Limitations

 In case of Quarkus distribution, after clicking on login link in the exporting wizard in a modeling tool a web browser with a message "We are sorry... Page not found" appears, the message should say "Login Successful".

