

The Document Exchange Portal

Administrator Guide

v1.0
August 18, 2016

Contents

What is the Portal?	3
What is Keycloak?	3
Recommended internet browsers	3
Search for a specific user or view all users	4
Enable or Disable Users	5
Enable user.....	5
Disable user.....	6
Change User Password.....	6
Verify or Modify Role Mappings (permissions)	7
Manage Sessions at the user level.....	8
Manage Events.....	9
Service Accounts	12

What is the Portal?

The Portal is an online web application that provides Claims Administrators (CA), Utilization Review Organizations (URO), and the Independent Medical Review Organization (IMRO) a single, shared workspace to upload, view, and download documents associated with IMR cases.

What is Keycloak?

Keycloak is an open source Identity and Access Management Server for applications and services used to authenticate users accessing the Portal.

Recommended internet browsers

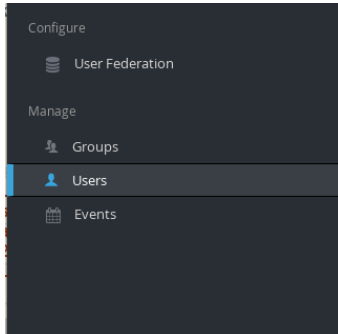
Chrome supports all functionality in the Portal.

The Portal will run in all browsers that support HTML5 including Firefox, Safari, Opera, IE 10, IE 11, and IE Edge with some limitations in functionality.

Browser	Description
Chrome, Opera	Only Chrome and Opera support named folder drag and drop.
IE Edge	Does not support drag and drop in Windows 10.
IE Edge	Very slow rendering of PDF images in PDF viewer.
IE v9 and older	Not supported.

Search for a specific user or view all users

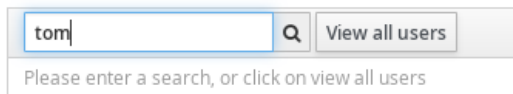
1. Login to the admin UI.
2. Select **Users** in the navigation pane.



Do one of the following:

- Search for a targeted user by entering their name in the search field and click the magnifying glass to begin the search.

Users

A screenshot of the 'Users' search interface. It features a search input field with the text 'tom' entered. To the right of the input field is a magnifying glass icon. Further right is a button labeled 'View all users'. Below the input field and button is a light gray box containing the text 'Please enter a search, or click on view all users'.


- View all users in the realm by clicking the **View all users** button and page through users with the **Next Page** / **Previous Page** buttons.

Enable or Disable Users

Enable user

1. Login to the admin UI.
 2. Search for a specific user or view all users.
 3. Select the **Edit** button to edit the targeted user.
- The **Details** tab will indicate **User Enabled OFF**.

Users » service.ca1only@maxird.com

Service.ca1only@maxird.com 

Details | Attributes | Credentials | Role Mappings | Groups | Consents | Sessions

ID: 5b5b6efd-1342-41cf-8b2c-e3b2ddc962f1


Created At: 8/10/16 4:47:36 AM


Username: service.ca1only@maxird.com


Email: service.ca1only@maxird.com


First Name: CA1ONLY

Last Name: Service

User Enabled : ☐ OFF

Email Verified : ☒ ON

Required User Actions : Select an action...

Impersonate user :

- Click **User Enabled OFF** to change the **User Enabled** state to **ON**.
 - Click the **Save** button to save the change.
 - Enter **Username, Email, First Name, Last Name**.
 - **Username** and **Email** should be the same.
 - Ensure **User Enabled** is **ON**.
 - Click the **Save** button.
5. Select the **Credentials** tab.
- For **Reset Actions**, add the following actions:
 - i. **Update Password**
 - ii. **Update Profile**

- Click the **Send email** button.
This will send a **time-sensitive** email to the user with a link that will bring them the user maintenance page.

6. Select the **Role Mappings** tab.

Available roles will be **group-admin**, **claimadmin-user**, and **claimadmin-super-user**

- Select the desired role and click the **Add selected** button.

Providing the role gives the new user access to the portal. The Send email step sends a time sensitive email to allow the user to provide their own initial password and verify their account details.

Disable user

- The **Details** tab will indicate **User Enabled ON**.
- Click **User Enabled ON** to change the **User Enabled** state to **OFF**.
- Click the **Save** button to save the change.

Change User Password

1. Login to the admin UI.
2. Search for a specific user or view all users.
3. Click the **Edit** button to edit the targeted user.
4. Select the **Credentials** tab.

The screenshot shows the 'Users' management interface. At the top, it says 'Users » tomstockton@maximus.com'. Below this is the user's name 'Tomstockton@maximus.com' with a trash icon. There are several tabs: 'Details', 'Attributes', 'Credentials' (which is selected and highlighted in blue), 'Role Mappings', 'Groups', 'Consents', and 'Sessions'. Under the 'Credentials' tab, there are several form elements: a 'New Password' text field, a 'Password Confirmation' text field, a 'Temporary' toggle switch currently set to 'ON' (indicated by a blue bar), a 'Reset Actions' dropdown menu with the text 'Select an action...', and a 'Reset Actions Email' button labeled 'Send email'.

5. Enter a new password in the **New Password** field. It must conform to the password policy for the realm.
6. Reenter the password in the **Password Confirmation** field.

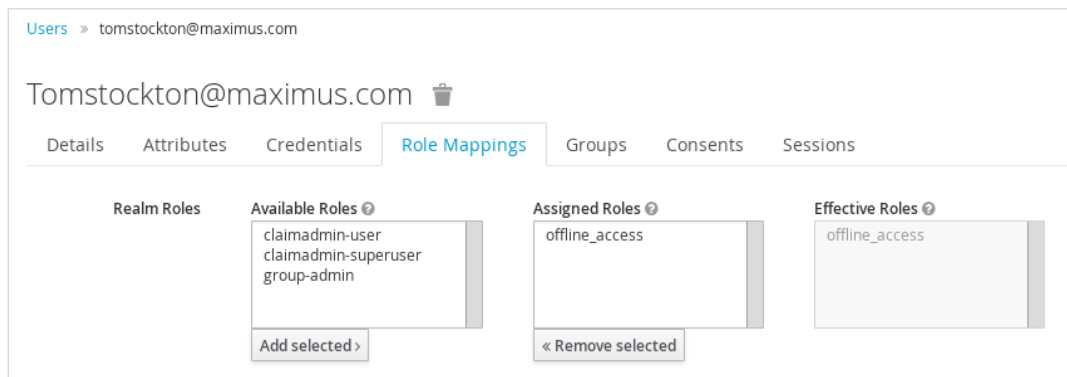
- **Temporary** can be set to **ON** or **OFF**
 - If set to **ON**, the user will be forced to reset the password at the first login.
 - If set to **OFF**, the user can use the password until it expires.

- **Reset Actions** can be one or all of the following:
 - **Configure Totp**
The user will need to configure a password through Google Authenticator in the next login sequence.
 - **Update Password**
The user will have to update their password in the next login sequence.
 - **Update Profile**
The user will have to update their profile (First name, Last name, email address) in the next login sequence.
 - **Verify Email**
A time-sensitive email will be sent to the user. The user can activate a link to initiate the Reset Actions. When the **Send email** button is clicked, an email will be sent to the user's configured email address.

Verify or Modify Role Mappings (permissions)

If a user is unable to perform the expected actions in the Portal, the role mappings for the user may need to be verified or modified.

1. Login to the admin UI.
2. Search for a specific user or view all users.
Select the **Edit** button to edit the targeted user.
3. Select the **Role Mappings** tab.



- Typically, a user will need to carry the **claimadmin-user** realm role. The desired roles should appear in the **Assigned Roles** list box. Having a role in the **Assigned Roles** list indicates the user has the set of privileges associated with the role. Existing roles are:
 - **claimadmin-user**
This role provides the user the ability to use the portal
 - **group-admin**
This role provides the user the ability to administer users within the realm.
 - **claimadmin-superuser**
This is a convenience role combining group-admin and claimadmin-user. The same privileges can be awarded by assigning the roles separately.

- In the **Realm Roles** section, modify the user's assigned role by selecting an item in the **Available Roles** list box and click on the **Add selected** button. To remove roles, select an item in the **Assigned Roles** list box and click on the **Remove selected** button. The item will return to the **Available Roles** list.
 - Each operation will be individually persisted and confirmed.

Note: Portal permissions are organized as **Realm Roles**. There should be no reason to manipulate **Client Roles**.

Manage Sessions at the user level

1. Login to the admin UI.
2. Search for a specific user or view all users.
3. Select the **Edit** button to edit the targeted user.
4. Select the **Sessions** tab.

[Users](#) > tomstockton@maximus.com

Tomstockton@maximus.com 

[Details](#) [Attributes](#) [Credentials](#) [Role Mappings](#) [Groups](#) [Consents](#) [Sessions](#)

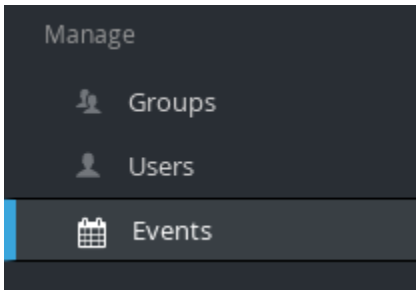
Logout all sessions				
IP Address	Started	Last Access	Clients	Action
10.160.93.62	Aug 3, 2016 8:34:15 AM	Aug 3, 2016 8:34:16 AM	account	Logout

- All active sessions will be shown and each will show as a different line.
- To logout sessions, do one of the following:
 - To logout a single session, click the **Logout** button associated with the session.
 - To logout all sessions, click the **Logout all sessions** button.

Manage Events

Note: Keycloak events should not be confused with Portal events. Keycloak events are confined to capturing actions related to user administration, authentication, and realm management.

1. Login to the admin UI.
2. Select **Events** in the navigation pane.



3. The **Login Events** tab allows an Administrator to view user and system actions related to authentication.

[Login Events](#) [Admin Events](#) [Config](#)

Event Type

Client

User

Date (From)

Date (To)

Filter Update Reset

Time	Event Type	Details								
8/3/16 8:52:28 AM	CODE_TO_TOKEN	<table><tr><td>Client</td><td>security-admin-console</td></tr><tr><td>User</td><td>feba1dc4-70eb-47ec-9644-e45dcd950eaf</td></tr><tr><td>IP Address</td><td>0:0:0:0:0:0:1</td></tr><tr><td>Details</td><td>+</td></tr></table>	Client	security-admin-console	User	feba1dc4-70eb-47ec-9644-e45dcd950eaf	IP Address	0:0:0:0:0:0:1	Details	+
Client	security-admin-console									
User	feba1dc4-70eb-47ec-9644-e45dcd950eaf									
IP Address	0:0:0:0:0:0:1									
Details	+									
8/3/16 8:52:28 AM	LOGIN	<table><tr><td>Client</td><td>security-admin-console</td></tr><tr><td>User</td><td>feba1dc4-70eb-47ec-9644-e45dcd950eaf</td></tr><tr><td>IP Address</td><td>0:0:0:0:0:0:1</td></tr><tr><td>Details</td><td>+</td></tr></table>	Client	security-admin-console	User	feba1dc4-70eb-47ec-9644-e45dcd950eaf	IP Address	0:0:0:0:0:0:1	Details	+
Client	security-admin-console									
User	feba1dc4-70eb-47ec-9644-e45dcd950eaf									
IP Address	0:0:0:0:0:0:1									
Details	+									

[<<](#) [<](#) [>](#) [>>](#)

- To filter events, click the **Filter** button.
- Events can be confined by **Event Type**, **Client**, **User**, or **Date**. Clicking in the **Event Type** field presents a multi-select list that will populate the field.
- To refresh the list with filter parameters, click the **Update** button.
- The **Reset** button clears all search parameters and updates the result list.

4. Admin Events

The **Admin Events** tab provides a view to the administrative actions (CREATE, DELETE, UPDATE, ACTION) performed against realm resources (users and clients). Filtering on this tab works on two levels:

- operation level
- details level

If filter parameters are set under **Authentication Details**, the list will be filtered to show only entries with conforming **Auth Details**. To view **Details**, click the **Auth** button for the associated line.

The screenshot displays the 'Admin Events' interface. At the top, there's a 'Login Events' tab. Below it, a modal window is open, showing a table with the following data:

Realm	master
Client	bfc4979e-fb3c-4a19-aa56-4ed39fcca895
User	ce1c96c6-d2a8-4f02-b15c-ef98e0cf93c
IP Address	0:0:0:0:0:0:1

The main interface includes a 'Filter' button and a 'Reset' button. Below these, there are input fields for 'Operation Types' (a dropdown menu), 'Resource Path', 'Date (From)', and 'Date (To)'. The 'Authentication Details' section contains input fields for 'Realm', 'Client', 'User', and 'IP Address'. At the bottom, there is a table listing events:

Time	Operation Type	Resource Path	Details
8/3/16 8:51:41 AM	CREATE	users/feba1dc4-70eb-47ec-9644-e45dcd950eaf/role-mappings/realm	Auth
8/3/16 8:51:36 AM	ACTION	users/feba1dc4-70eb-47ec-9644-e45dcd950eaf/reset-password	Auth
8/3/16 8:51:14 AM	CREATE	users/feba1dc4-70eb-47ec-9644-e45dcd950eaf	Auth
7/11/16 11:09:58 AM	UPDATE	clients/a6cf5d18-aab6-47ac-b8c6-e04b23c983d1	Auth
6/17/16 11:06:13 AM	CREATE	users/90b6b60c-1931-4faf-a57a-4b6fe0880263/role-mappings/realm	Auth

Config

There are a limited set of actions that can be performed on the **Config** tab.

- Control whether **Login Events** are saved to the database for your realm. This makes the event data available on the **Login Events** tab.
 - Set **Save Events** to **ON**. If set to **OFF**, data will not be available to filter and view.
- Control whether **Admin Events** are saved to the database for your realm. This makes the event data associated with administrative actions available on the **Admin Events** tab.
 - Set **Save Events** to **ON**. If set to **OFF**, data will not be available to filter and view.
- Set **Include Representation** to **ON** to include the JSON representation for **CREATE** and **UPDATE** requests in the log entry.

Events Config ?

Login EventsAdmin EventsConfig

Events Config

Event Listenersjboss-logging

Login Events Settings

Save EventsON

Saved Types

LOGINLOGIN_ERRORREGISTERREGISTER_ERRORLOGOUT
LOGOUT_ERRORCODE_TO_TOKENCODE_TO_TOKEN_ERRORCLIENT_LOGIN
CLIENT_LOGIN_ERRORFEDERATED_IDENTITY_LINK
FEDERATED_IDENTITY_LINK_ERRORREMOVE_FEDERATED_IDENTITY
REMOVE_FEDERATED_IDENTITY_ERRORUPDATE_EMAILUPDATE_EMAIL_ERROR
UPDATE_PROFILEUPDATE_PROFILE_ERRORUPDATE_PASSWORD
UPDATE_PASSWORD_ERRORUPDATE_TOTPUPDATE_TOTP_ERROR
VERIFY_EMAILVERIFY_EMAIL_ERRORREMOVE_TOTPREMOVE_TOTP_ERROR
REVOKE_GRANTSEND_VERIFY_EMAILSEND_VERIFY_EMAIL_ERROR
SEND_RESET_PASSWORDSEND_RESET_PASSWORD_ERROR
SEND_IDENTITY_PROVIDER_LINKSEND_IDENTITY_PROVIDER_LINK_ERROR
RESET_PASSWORDRESET_PASSWORD_ERRORIDENTITY_PROVIDER_FIRST_LOGIN
IDENTITY_PROVIDER_FIRST_LOGIN_ERRORIDENTITY_PROVIDER_POST_LOGIN
IDENTITY_PROVIDER_POST_LOGIN_ERRORIMPERSONATE
CUSTOM_REQUIRED_ACTIONCUSTOM_REQUIRED_ACTION_ERROR
EXECUTE_ACTIONSEXECUTE_ACTIONS_ERRORCLIENT_REGISTER
CLIENT_REGISTER_ERRORCLIENT_UPDATECLIENT_UPDATE_ERROR
CLIENT_DELETECLIENT_DELETE_ERROR

ExpirationHours

Admin Events Settings

Save EventsON

Include RepresentationON

Service Accounts

Note: Along with the realm, first and last name, and email addresses we requested to create user accounts, we would also like you to submit an email address for a service account.

Service accounts are created to allow organizations to automate services. In this scenario, an email will be sent to the email address associated with the service account as part of account creation. The email content will vary, but will look similar to the following:

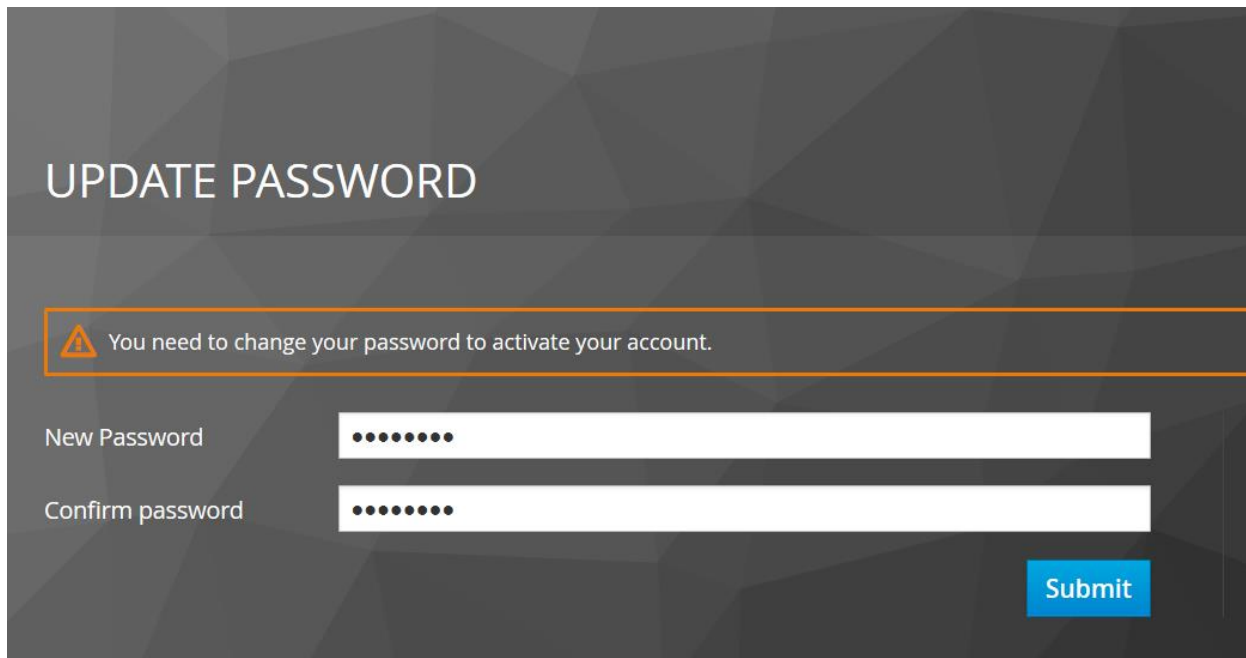
Your administrator has just requested that you update your `REALM NAME` account. Click on the link below to start this process.

[http://10.160.233.3:8180/auth/realms/REALM NAME/login-actions/execute-actions?key=4pc_iB0taWUG44m4uaYL73FUv6Q_NKUj_behEZanD8Y.c526a398-b854-4460-86dc-215bd4d59be7](http://10.160.233.3:8180/auth/realms/REALM%20NAME/login-actions/execute-actions?key=4pc_iB0taWUG44m4uaYL73FUv6Q_NKUj_behEZanD8Y.c526a398-b854-4460-86dc-215bd4d59be7)


This link will expire within `N` minutes.

If you are unaware that your admin has requested this, just ignore this message and nothing will be changed.

Activating the link will bring you to a password change dialog that is the final step in activating the service account.



UPDATE PASSWORD

 You need to change your password to activate your account.

New Password

Confirm password

Once the account is activated, the credentials and realm name will be used to access the automated services.