digitalML

OIC API Catalog and Portal Admin Set Up Guide

7 steps to get your API Catalog and Portal set up

7 steps to getting started with the OIC API Catalog and Portal

1. OIC Instance DNS Setup
2. SSO Configuration
3. Connect your system to your OIC environment
4. Customize the branding of your API Catalog
5. Customize the branding of your Consumer Portal
6. Set up email notifications
7. Configure the Consumer Portal's Get API Access Form

Step 1 - Create a DNS A record

After the OIC API Catalog and Portal (also known as the ignite Suite for OIC) instance has been created, you must create a DNS A record for the hostname you specified as part of the configuration.

You will find the public IP address of the new instance in the output values of the newly created stack.

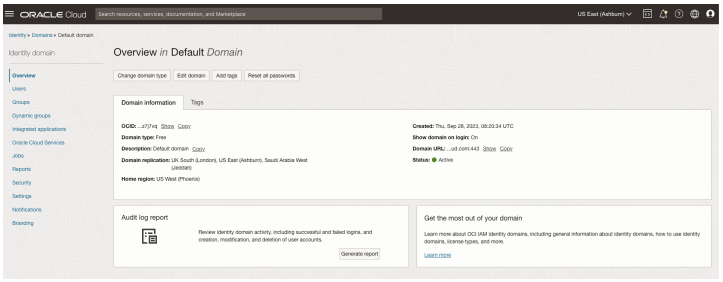
Step 2 - SSO Configuration

Your OIC environment's IAM domain can be coupled to your OIC API Catalog **and** your OIC Portal, so that users can access the portal using their existing OIC user details. There are two main steps, setup Keycloak as a client or application in the Oracle Identity Cloud Service/ IAM Domain and setup the IDCS/IAM domain as an identity provider in Keycloak. You'll have to do these for each the catalog and the portal.

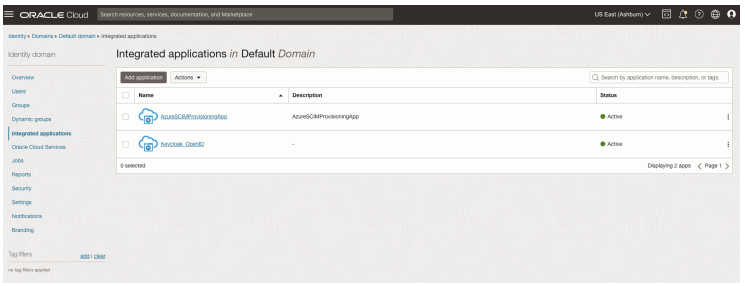
To configure SSO:

1. **Setup of Keycloak as client or application in Oracle Identity Cloud Service / IAM Domain**.

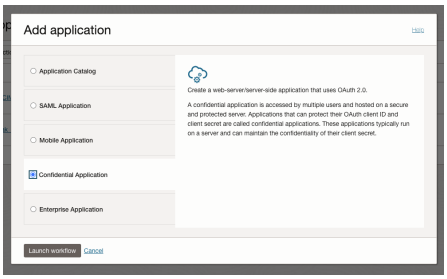
Log in to Oracle Cloud with a user who has enough privileges to set up the Identity Cloud Service or the newer IAM Domain designation, e.g. as an administrator of your cloud tenant. Then switch to the "Identity Domain" section. In the new interface for IAM domains, click "Identity → Domains → Default Domain"



2. Click on the "Integrated Applications" from the list on the left.



3. Click on the "+ Add Application" link , select "Confidential Application" from the list and click on "Launch Workflow"



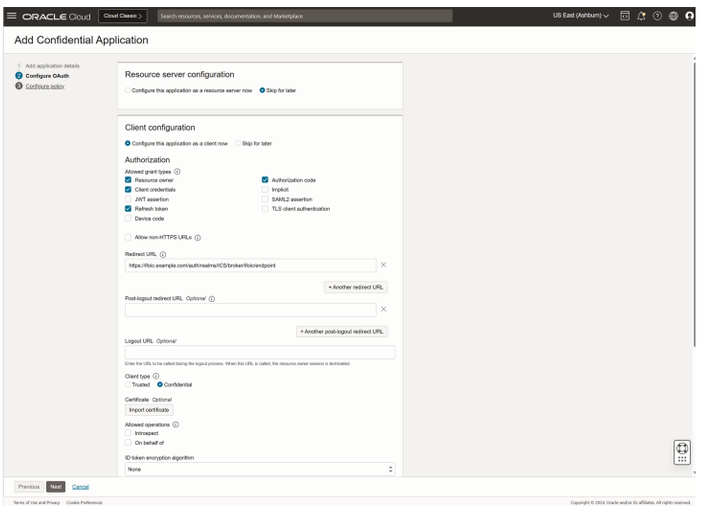
Give the application a name, (e.g. "IgniteForOICApp" for the Catalog and “IgniteforOICPortalApp” for the Portal), optionally add a description and icon. Leave all other fields empty for the time being and select "Next" at the bottom.

Select “Client configuration” and setup as below

- Under Authorization select "Client Credentials", "Authorization Code" “Resource Owner”, and “Refresh Token”. See screenshot below.
- Fill in the “Redirect URL” field with the following value https://hostname/auth/realms/ICS/broker/ifoic/endpoint. Replace hostname with your OIC API Catalog and Portal hostname.

Note: The value “ifoic” can vary but if you change it you must use the same value later when setting up keycloak.

- Select "Confidential" as client type.
- Select "Anywhere" for "Allowed Client IP Address".
- Leave all other entries at default.



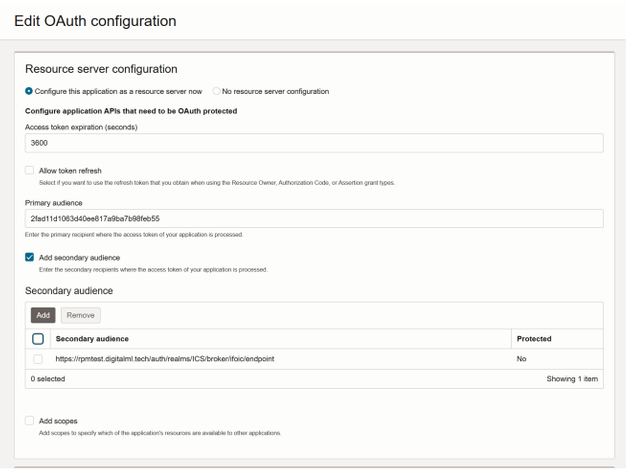
- Click on the "Next" button on the Bottom.
- For “Web Tier Policy” select “skip and do later”
- Click “Finish” a client ID and a client secret will be created for you. Make a copy of this value so it can be used in subsequent steps.

Now click on “Edit Oauth configuration” and at the top select “Configure this application as a resource server now”

- Primary audience will be Client ID you just copied.
- Select “Add secondary audience” and use the same URL as for the Redirect URL: https://hostname/auth/realms/ICS/broker/ifoic/endpoint. Remember to replace the hostname with the correct value.

Note: The value “ifoic” can vary but if you change it you must use the same value later when setting up keycloak.

- Optionally, select whether an auto-refresh of the token should be possible and change how long the token should be valid.
- Save Changes



Click “Activate” to enable the application.

Public access to the certificates used by IDCS is required. To enable this, navigate to the identity domain page, then click on "Settings", and activate the checkbox "Configure Client Access"

The IDCS/IAM domain part of the configuration is now complete.

Reminder: you must do Step 1 twice - once for the catalog and once for the portal.

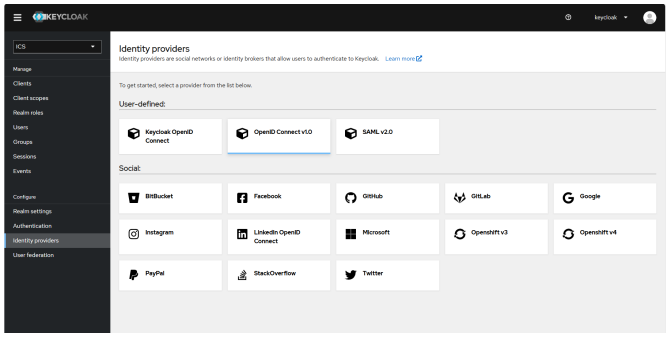
2. Set up the IDCS/ IAM domain as an identity provider in Keycloak.

Log into your Keycloak installation as the user "keycloak" using the password entered as part of the initial creation of your OIC API Catalog and Portal.

Select the ICS realm from the dropdown on the top left (this is the realm for the Catalog)

In your selected realm, click on "Identity Providers" on the left, then add a new "OpenId Connect v1.0".

5. Your OIC API Catalog is now connected and ready for use. - To learn more about importing **visit the documentation on importing into the Catalog**



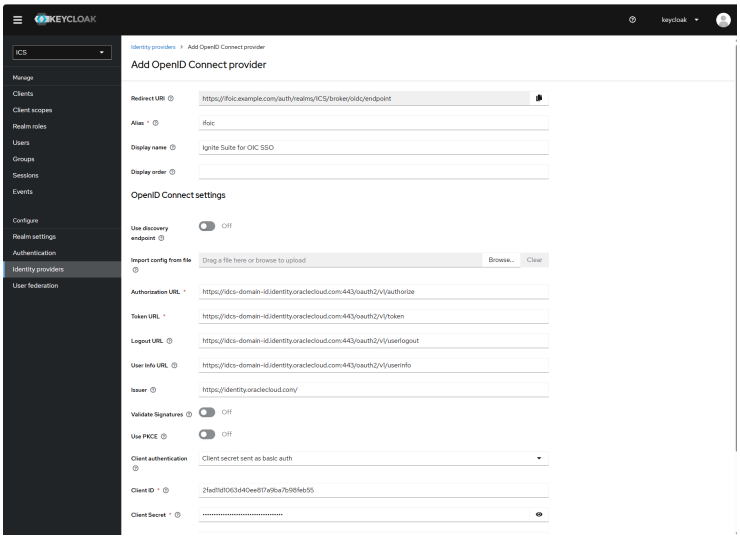
- Give the provider the alias "ifoic".

Note: If you used a different value in the “Redirect URL” when configuring the client on OCI you must use that value here as the alias.

At this point, instructions continue for the set up of the Catalog, you’ll have to repeat step 2 again for the portal which we detail later.

Catalog Configuration:

- Fill in a value for “Display name”. This is what will be displayed in the button on the login page for your OIC API Catalog.
- Disable the “Use Discovery Endpoint” option.
- You need to fill in the four URL values. These are formed using the Domain URL which can be found on the Overview page for your IDCS instance and adding a suffix:
- For “Authorization URL”: /oauth2/v1/authorize
- For “Token URL”: /oauth2/v1/token
- For “Logout URL”: /oauth2/v1/userlogout
- For “User Info URL”: /oauth2/v1/userinfo
- The “Issuer” must be https://identity.oraclecloud.com/ including the trailing slash.
- For “Client Authentication” select "Client Secret sent as Basic Auth".
- For “Client ID” and “Client Secret” add the values created for the IDCS application.
- For "Client Assertion Signature Algorithm" select “RS256”.
- Now click “Add” to create the provider.



We are not quite done yet - the transferred groups, or at least a relevant part of them, needs to be mapped to the "ROLE_ADMINISTRATOR" role defined in Keycloak.

To do this, switch to the "Mappers" tab at the very top of the form.

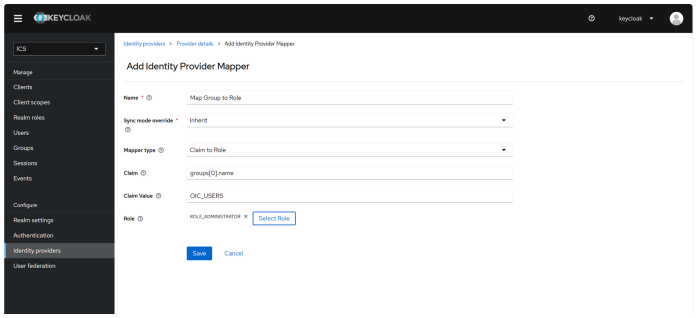
You will see an empty list, in our example you already see several defined mappers.

- In the newly created provider expand the Advanced settings section.
- For “Scopes” add the value "openid groups email".
- Leave all other entries as their defaults.
- Click the Save button at the very end of the form.

Finally you must create a role mapper. Select the mapper tab and click on the "Add mapper" button then fill in the first form as follows:

- For “Name” set an appropriate name, e.g., “Map Group to role”
- For “Sync Mode Override” leave the default value of "inherit".
- For “Mapper Type” set to "Claim to Role
- For “Claim” set the value "groups[0].name". Explanation: the groups come from IDCS as an object array, not as an array of strings. In the object array, there is a field "name" that contains the name of the group among other fields like id and type. The selected mapper can only handle string arrays, so in multiple mappers we have to iterate through all the groups transferred and check if the selected group is the one we want to map.

- For “Claim Value” set the name of one of the groups in IDCS that your cloud user belongs to. In our example "OIC_USERS", for you it will probably be different.
- For “Role” choose "ROLE_ADMINISTRATOR". Do not select any other role.
- Finally save the role mapper.



You should now be able to log in to you OIC API Catalog using your Oracle IDCS users.

Now it’s time to do the same for the portal set up. Follow step 2 up until the catalog configuration point and repeat the steps for the portal configuration as follows:

Portal Configuration:

- Fill in a value for “Display name”. This is what will be displayed in the button on the login page for your OIC Portal.
- Disable the “Use Discovery Endpoint” option.
- You need to fill in the four URL values. These are formed using the Domain URL which can be found on the Overview page for your IDCS instance and adding a suffix:
  - For “Authorization URL”: /oauth2/v1/authorize
  - For “Token URL”: /oauth2/v1/token
  - For “Logout URL”: /oauth2/v1/userlogout
  - For “User Info URL”: /oauth2/v1/userinfo
- The “Issuer” must be https://identity.oraclecloud.com/ including the trailing slash.
- For “Client Authentication” select "Client Secret sent as Basic Auth".
- For “Client ID” and “Client Secret” add the values created for the IDCS application.
- For "Client Assertion Signature Algorithm" select “RS256”.
- Now click “Add” to create the provider.

We are not quite done yet - the transferred groups, or at least a relevant part of them, needs to be mapped to the "ROLE_STORE_USER" role defined in Keycloak.

To do this, switch to the "Mappers" tab at the very top of the form.

You will see an empty list, in our example you already see several defined mappers.

- In the newly created provider expand the Advanced settings section.
- For “Scopes” add the value "openid groups email".
- Leave all other entries as their defaults.
- Click the Save button at the very end of the form.

Finally you must create a role mapper. Select the mapper tab and click on the "Add mapper" button then fill in the first form as follows:

- For “Name” set an appropriate name, e.g., “Map Group to role”
- For “Sync Mode Override” leave the default value of "inherit".
- For “Mapper Type” set to "Claim to Role
- For “Claim” set the value "groups[0].name". Explanation: the groups come from IDCS as an object array, not as an array of strings. In the object array, there is a field "name" that contains the name of the group among other fields like id and type. The selected mapper can only handle string arrays, so in multiple mappers we have to iterate through all the groups transferred and check if the selected group is the one we want to map.
- For “Claim Value” set the name of one of the groups in IDCS that your cloud user belongs to. In our example "OIC_USERS", for you it will probably be different.
- For “Role” choose "ROLE_STORE_USER". Do not select any other role.
- Finally save the role mapper.

You should now be able to log in to your OIC Portal using your Oracle IDCS users.

Step 3 - Connect your system to your OIC environment

Before you can import OIC Projects and their integrations into your OIC API catalog, you must first configure the system to connect to your Integration Instance and set-up authentication for it.

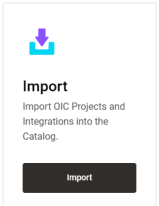
You will need to following information to complete the configuration:

OIC Integration Instance identifier: ID that uniquely identifies the OIC Service Instance you want to connect to an import content from into the OIC catalog.
For example: aaaa-amaa-amaaaaaacxr-am
Note that you can find this value on the About box of your OIC instance:

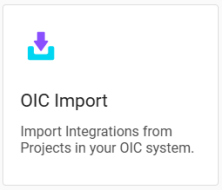
- OIC URL: Base-URL of the OIC instance you want to connect to.
  For example: https://design.integration.us-phoenix-1.ocp.oraclecloud.com
- Token URL: Location of the OAuth2 authorization server.
  For example: https://idcs-10809f41179d4b6982340a8220a8558c.identity.oraclecloud.com/oauth2/v1/token
- Client ID: OAuth2 client identifier of the OIC application.
  For example: d0beacfcd601f4ec2a8ad415cab24b60
- Client Secret: OAuth2 application client secret.
- Scopes: A list of OAuth2 scopes required for the OIC application access.

To configure the OIC connection and authentication:

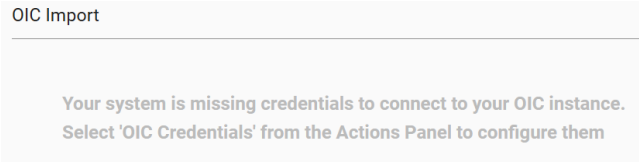
1. Login to the catalog and from the home screen, click the **Import** tile:



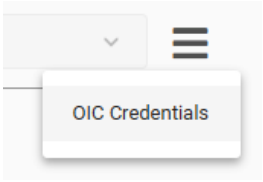
2. On the import screen, click OIC Import:



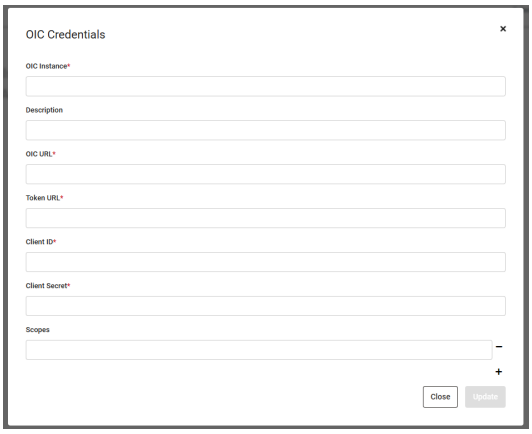
The following message should appear, indicating that the system is not configured:



3. From the hamburger **Actions menu** on the right, select **OIC Credentials**:



The following screen should appear:



4. Enter all the relevant values and click Update. If the configuration is not successful, a message will appear indicating the problem. Once successful, after update, the credentials screen will close and you should find a list of Projects in your OIC instance displayed on the page:

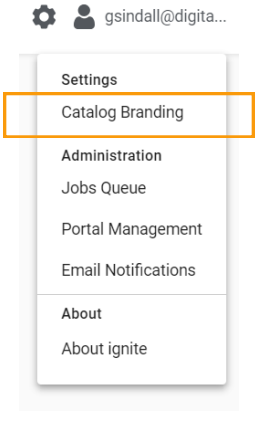
5. Your OIC API Catalog is now connected and ready for use. - To learn more about importing **visit the documentation on importing into the Catalog**

Step 4 - Customize the branding of your API Catalog

Configurable branding is available within your OIC catalog, ensuring that your brand's identity is maintained, helping you drive adoption of the platform within your end user base.

To configure the catalog branding:

1. Navigate to Catalog Branding, click on the cog wheel in the top right of the catalog screen and click **'Catalog Branding.'**



2. Upload your logo - To upload your logo either drag and drop it into the space provided or click for a file explorer type view where you can make your selection.

   Logos should be in .PNG format and have a maximum file size of 200kb.

   Your selected logo will then be previewed in the pane to the right, once you are happy simply click the upload button. If you refresh the UI of the catalog you should now see the updated logo.

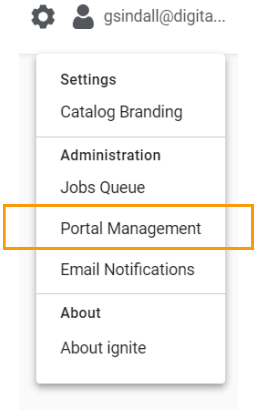
2. Update your brand colors and additional settings to further customize the look and feel of your API catalog. To view full instructions **visit the documentation on Catalog Branding**

Step 5 - Customize the branding of your Consumer Portal

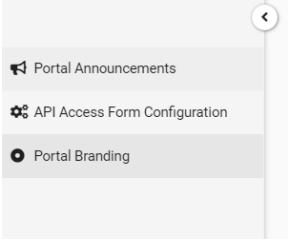
Configurable branding is available for your OIC portals, ensuring that your brand's identity is maintained and you can drive increased adoption within your end users.

To configure the portal branding:

1. Navigate to Portal Branding, click on the cog wheel in the top right of the catalog screen and click **'Portal Management**.'



2. Click on **Portal Branding** in the left hand pane.



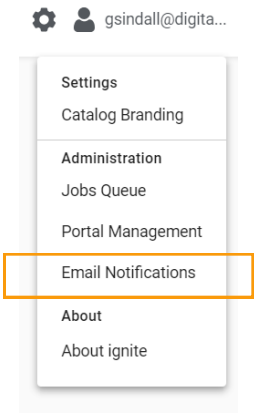
3. Upload your logo, customize the landing page title, message, brand colors and additional settings. To view full instructions **visit the documentation on Portal Branding**

Step 6 - Set up email notifications

Your OIC catalog and portal can send emails to your Integration owners and consumers (respectively) to notify them directly when questions and requests have been made and answered.

To configure the email notifications:

1. To set up the email notifications capability access this functionality area, select the **Email Notifications** option from the cog menu in the catalog UI.



The first **Email Notifications tab** allows you to select which email types you would like to go out in your catalog and portal instance:

- New portal request/question: will notify the Integration owner when a request or question comes in from a user in the Portal
- Portal replies: will notify the Integration owner when a user in the Portal has replied to a question answer or request response
- Catalog replies: will enable notifications to be sent out to the consumer when the Integration owner replies to their question or request

The second **Email Groups tab** allows you to define the email addresses that notifications should be sent to (i.e. your Integration owner(s)). To do this, click the Add New button and select the one option from the dropdown (most likely Oracle Integration Team or [Your Company] Integration Team). Input the appropriate email addresses to receive notifications. Note that these should be separated by commas.

The third **Email Server Configuration tab** connects to your OIC instance to use its email server to send the notifications. Fill out the details as per your instance. You can also test that the connection has been configured correctly using the Test button at the bottom of the page.

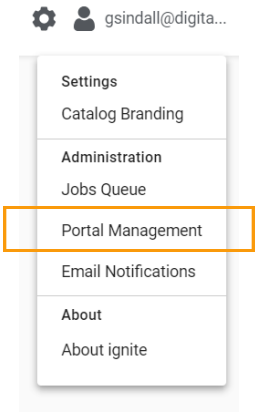
To view additional details as well as learn about subscribing to email notifications **visit the documentation on Email Notifications**

Step 7 - Configure the Consumer Portal's Get API Access Form

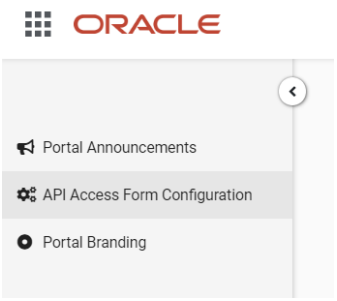
It's possible to configure the "Get API Access" which consumers use in your portal, ensuring that you are able to collect relevant data from your end users when they request access to your OIC Integrations.

To configure the access form:

1. Navigate to the API Access Form Configuration, click on the cog wheel in the top right of the catalog header and click **Portal Management**



2. Click on the '**API Access Form Configuration**' option in the left hand pane.



3. Edit the form configuration and click **Save.** To view full details on the form configuration **visit the documentation on Configuring the Get API Access Form**

Finally, you'll need to manually upgrade your OIC API Catalog and Portal when new updates are available (quarterly).

How to Upgrade:

1. Use your preferred SSH client to open a terminal to the OIC API Catalog and Portal VM. The username is opc. You will require the private key paired with the public key provided when initially deploying the VM from the marketplace.
2. Determine if there is an updated version of the OIC API Catalog and Portal available:

sudo yum check-update IgniteSuiteForOIC

This command will list available updates if there are any. If there is an update available install it using:

sudo yum update IgniteSuiteForOIC

Be aware your OIC API Catalog and Portal will not be available during this process and the process may take a long time. Even after the update appears to be finished there may be some time before the system is available.