Oracle Fusion Cloud Student Financial Planning

How do I set up OCI Identity and Access Management for Student Financial Aid?

Oracle Fusion Cloud Student Financial Planning
How do I set up OCI Identity and Access Management for Student Financial Aid?

G26973-02

Author: Higher Education Information Development Team

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 How do I set up OCI Identity and Access Management for Student Financial Aid?

Overview of OCI Identity and Access Management

Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) enables enterprise grade identity and access management capabilities. Integrating with OCI IAM allows for a self-serviced, centralized approach with enhanced security and enforcement of credentials for your end users. You have greater control over what type of access a group of users has and to which specific permissions and roles they have access to.

Student Financial Aid (SFA)-specific configurations will be managed in the SFA application, and OCI IAM will be used to manage users, identity providers, and so on.

These are some of the key features included with IAM:

- Custom sign-in policies
- Password policies
- Self-service password management
- Custom notification management
- IAM interface branding
- Session timeouts controls
- Custom IdP policies
- Just in time provisioning
- Multifactor authentication
- Audit logging and reporting
- Increased user management capabilities
- Bulk management of users and groups

Here's documentation for features you may want to use if they align with your organization's requirements:

- *Adaptive security*
- *Branding*
- *Custom IdP policies*
- *Custom sign-in policies*
- *Custom terms of use documents*
- *End user account recovery*
- *End user credential management*
- *Multifactor authentication*
- *Network perimeters*
- *Notifications*

- *Passwordless authentication*
- *Password policies*
- *Session timeout controls*

Set Up Your OCI Cloud Account for Student Financial Aid

Student Financial Aid (SFA) integrates with OCI identity domain to enable you to manage users and groups who can then be allowed to access certain resources.

After provisioning your SFA environments, you need explore and understand the integration between SFA and OCI Identity and Access Management. Other configuration is required to grant access to SFA environments.

These tasks are a one-time required setup to provision your first SFA environment.

Note:

- The identity domain you select is used for all future SFA environments and can't be changed.
- To filter the permissions that SFA has in the identity domain you select, the domain must be in a compartment or subcompartment under the root compartment of your tenancy.

If you want to modify the identity domain you created, see *Managing Identity Domains* for more information.

1. *Create a compartment*.
   We suggest using **SFA-Resources** as the name of the compartment.
2. *Create an identity domain*. Create this domain in the compartment you just made.
   We suggest using **SFA-Domain** as the name and selecting **Free** as the domain type. SFA will upgrade the domain type to Oracle Apps.
   You also need to make sure these options are selected:
   - Make sure the selected region is **US East (Ashburn)** or **US West (Phoenix)**.
   - In **Remote region disaster recovery**, select **Enable remote region disaster recovery**.
3. Create a group in the identity domain you selected.
   This group will be granted permissions to manage the provisioning of SFA environments. We suggest using the name **SFA-OCI-App-Mgmt**.
4. Create an identity policy to grant SFA access to integrate with your selected identity domain. For information on identity policies, see *How Policies Work*.
   These policies are required:
   - Allow service sfpprodiam to manage domains in compartment SFA-Resources
   - Allow group SFA-Domain/SFA-OCI-App-Mgmt to read subscriptions in tenancy
   - Allow group SFA-Domain/SFA-OCI-App-Mgmt to read app-listing-environments in tenancy
   - Allow group SFA-Domain/SFA-OCI-App-Mgmt to read metrics in tenancy

- Allow group SFA-Domain/SFA-OCI-App-Mgmt to read domains in tenancy
- Allow group SFA-Domain/SFA-OCI-App-Mgmt to read announcements in tenancy
- Allow group SFA-Domain/SFA-OCI-App-Mgmt to manage organizations-family in tenancy
- Allow group SFA-Domain/SFA-OCI-App-Mgmt to manage OSFPCS-environment-family in tenancy

Note that if you used a different compartment name, use that instead of **SFA-Resources**. And if you used a different group name, use that name here instead of **SFA-OCI-App-Mgmt**.

5. In the identity domain you created:
   a. Allow clients to access the signing certificate for the identity domain in IAM without logging in to an identity domain. For instructions, see *Viewing SAML Certificate Metadata*.
   b. Verify that a primary email address is required to create user accounts in an identity domain in IAM. For instructions, see *Requiring User's Email Address for Account Creation*.
   c. Create the user account that becomes the default global administrator for your SFA environments. For instructions, see *Creating a User*.

      You can modify this later.
   d. Enable the user account to also manage SFA environment provisioning. To do this, add the user to the group you created earlier (step 3).

      If you used a different group name than the one we suggested (SFA-OCI-App-Mgmt), you will have to add the user to the group name you created. See *Adding Users to a Group* for more information.

Manage Authentication for Administrators and Non-Administrators

After having provisioned your production and nonproduction environments, you can access your identity domain through *cloud.oracle.com* and log in using the same credentials you used during the provisioning of the Student Financial Aid (SFA) environments.

Note that:

- The OCI identity domain selected during the provisioning of your production SFA environment will be used for all your SFA environments.
- You'll need to know the OCI Cloud Account name and the OCI compartment and identity domain (if you're not using the values we suggested) that were selected during the provisioning process.

For each production and non-production environment, two Oracle Cloud Service applications are created: one for the administration UI and the APIs, and one for the Student/Parent Self-Service Portal. These applications serve as the integration point between your OCI identity domain and your SFA environments and enable SSO.

Production and Non-Production Environment URLs

Production Environment URLs	Non-Production Environment URLs
Financial Aid Application (Admin): `https://sfp.ocs.oraclecloud.com/<customer_shortname>/vm-ui/ui-auth`	Financial Aid Application (Admin): `https://sfp.ocs.oc-test.com/<customer_shortname-test>/vm-ui/ui-auth`

Production Environment URLs	Non-Production Environment URLs
Student Portal: `https://sfp.ocs.oraclecloud.com/<customer_shortname>/portal/ui-auth`	Student Portal: `https://sfp.ocs.oc-test.com/<customer_shortname-test>/portal/ui-auth`

Authentication for Administrators

If these groups haven't already been created, SFA creates two default SFA global administrator groups in your OCI identity domain. The user that initiated the provisioning of the SFA environments is also added to these groups.

- **Admin**. This group gives default administrator permissions to all your Student/Parent Self-Service Portal environments.
- **SYS_ADMIN**. This group gives default administrator permissions to all your administration UI environments.

To manage these groups, from the OCI console's navigation menu, go to **Identity & Security** > **Domains**, then select your identity domain, and then groups.

Users that are members of these groups can use the production and non-production environment URLs to authenticate themselves and access the administration UI and the APIs, and one for the Student/Parent Self-Service Portal.

Authentication for Non-Administrators

To successfully log in and access SFA, these conditions must be true:

- The user is a member of an identity domain group.
- The group must have a role in SFA. You assign this role in SFA itself.
- The role must have at least one permission assigned in SFA.

When you view role and group mappings in the administration UI and Student/Parent Self-Service Portal, you'll see all the groups in the identity domain that's integrated with your SFA environments. These groups can be those created by OCI, SFA, or the ones you created yourself. To avoid confusion, we recommend adopting a naming convention for all the groups you create that meets your organization's requirements. Here's an example of a naming convention: <environment>-<workload>-<purpose> (oracletest-portal-generaladmin).

Set up Access to REST API

The Oracle Cloud Service applications are used for API authentication and authorization. The applications add controls that enable you to issue tokens with READ (GET as an example) and ADMIN (POST as an example).

In OCI IAM, the controls are referred to as scopes. These scopes are available for each Student Financial Aid (SFA) environment:

- /audit.admin
- /audit.readonly
- /mpg.admin

- /mpg.readonly
- /ui.admin
- /ui.readonly
- /vug.admin
- /vug.readonly

Here are examples of when to use the different scopes:

- When you need to make a READ (GET) call to the Vocado US Department of Education Gateway (VUG) API, you would request a token with only the /vug.readonly scope for the corresponding SFA environment.
- When you need to make an ADMIN (POST) call to the Message Processing Gateway (MPG) API, you would request a token with only the /mpg.admin scope for the corresponding SFA environment.

Environment URLs and Endpoints

Here's the list of production and test environments as well as the endpoints.

Production and Test Environment Formats

Production Environment	Test Environment
Format: `https://sfp.ocs.oraclecloud.com/<environment>/<endpoint>` Example: `https://sfp.ocs.oraclecloud.com/oracleprod/<endpoint>`	Format: `https://sfp.ocs.oc-test.com/<environment>/<endpoint>` Example: `https://sfp.ocs.oc-test.com/oracletest/<endpoint>`

These are the endpoints in the production and test environments:

- API
  - /audit/v2
  - /mpg/v2
  - /portal/info
  - /vm-ui/rest
  - /vug/v2
- Financial Aid System and Self-Service Portal
  - /vm-ui/ui-auth
  - /portal/ui-auth

Add a Confidential Application

To access the APIs for all your SFA environments, you need to create a **Confidential Application** for which you can regenerate the credentials on an ongoing basis, and control who has access to it.

For the complete instructions, see *Adding a Confidential Application*. The steps outlined below provide some recommendations as you add a new application.

1. From OCI's navigation menu, go to **Identity & Security** > **Domains** > **<your OCI identity domain>** > **Integrated applications**.
2. Add a new application.
3. Select **Confidential Application**.
    a. Enter the required information.
    b. Select **Enforce grants as authorization**.
4. On the **Configure OAuth** pane, select **Configure this application as a client now**.
5. Select **Client Credentials**.
6. Select **Add resources**.
    a. Expand the **. . ._ADMIN** app that corresponds to the SFA environment you want to interact with via REST API.
    b. Select the corresponding scope for the activity.

        You can select the checkbox next to all **. . ._ADMIN** apps that correspond to your SFA environments to add all scopes for those environments. But it's good practice to include *only* the SFA environments and specific scopes in the "Resources" of the Integrated application that are needed at the time, and to keep the "Resources" empty when not in use.

        By default, any scopes for newly provisioned SFA environments will not be included in "Resources."

    c. Select **Add**.
7. Select **Add app roles**.
    a. Select **Signin**.
    b. Select **Add**.
8. Finish creating the app. You don't need the other options.
9. Activate the application.

Request a Token

To access the REST APIs, you also need to request a token. This token can't be shared, but you can configure when the token expires. This period depends on your organization's requirements and whether you're comfortable allowing a token to be used for a certain period.

1. From OCI's navigation menu, go to **Identity & Security** > **Domains** > **<your OCI identity domain>** > **Integrated applications**.
2. Browse to the confidential application you created, then select it.
3. Select **OAuth Configuration**
    a. Locate **Client ID** and **Client secret**.

        We recommend routinely regenerating the Client Secret for the confidential application you created because this allows for READ and ADMIN access to the APIs for your SFA environments.

        We also recommend restricting who has access to the Client ID and Client Secret within OCI IAM.

    b. Encode the values to Base64.

        Here's an example in Windows Powershell:

        ```
        $stringToEncode = "id:secret"
        ```

```
# $bytes = [System.Text.Encoding]::UTF8.GetBytes($stringToEncode)
# $encodedString = [System.Convert]::ToBase64String($bytes)
# $encodedString
```

Make sure to note the value for use in token requests.

c. In your preferred software client, make an API call to request and retrieve a token.

When you need to make a READ (GET) call to the MPG API, you would request a token with only the /mpg.readonly scope for the SFA environment you need to interact with.

Example scope:

```
curl -H "Authorization: Basic <base64 string created from client id and client secret" -H "Content-Type: application/x-www-form-urlencoded;charset=UTF-8" --request POST https://<identity domain url>/oauth2/v1/token-d "grant_type=client_credentials&scope=https://sfp.ocs.oc-test.com/oracletest/mpg.readonly"
```

When you need to make an ADMIN (POST) call to the VUG API you would request a token with only the /vug.admin scope for the SFA environment you need to interact with.

Example scope:

```
curl -H "Authorization: Basic <base64 string created from client id and client secret" -H "Content-Type: application/x-www-form-urlencoded;charset=UTF-8" --request POST https://<identity domain url>/oauth2/v1/token -d "grant_type=client_credentials&scope=https://sfp.ocs.oc-test.com/oracletest/vug.admin"
```

d. To make an API call to interact with an SFA environment, use the token retrieved in the previous step.

```
curl -kv -X POST -H "Authorization: Bearer <token value>" -F "file=@demotest.dat" https://sfp.ocs.oc-test.com/oracletest/vug/v2/in/publish
```

Manage Users and Groups in OCI IAM

For users to access the Administration interface and Student/Parent Self-Service portal, they must exist in your OCI identity domain.

Manage Users

If you're going to use OCI IAM as your primary identity provider, we recommend reviewing the following documentation.

- *Creating a User*
- *Importing and Exporting Users, Groups, and AppRoles*
- *Editing a User*
- *Deleting a User*
- *Adding a User to a Group*
- *Removing Users from Groups*

Manage Federated Users

If you're going to use an external identity provider (IDP), the user accounts must still exist in OCI IAM with the federated attribute set to true so that they don't need to have a local OCI console password. When using an external IDP, you can assign the Oracle Cloud Service application directly to the identity provider policy. For information, see *Adding Apps to the Policy*.

To use an external IDP, we recommend you set up a SAML external IDP for authentication and authorization while using the System for Cross-Domain Identity Management (SCIM) protocol for user life cycle management. Review this documentation as well:

- *Adding a SAML Identity Provider*
- *Creating an Identity Provider Policy*
    - *SSO Between OCI and Microsoft Entra ID*
    - *Identity Lifecycle Management Between OCI IAM and Entra ID*
    - *SSO With OCI and Okta*
    - *Identity Lifecycle Management Between OCI and Okta*

  To provision other IDPs into your identity domain, you can set up a confidential application within the identity domain, and then configure the integration on your IDP's side. Consult your IDP support team as needed.

If your IDP supports sending the studentID attribute as a string array data type, another option is to use just-in-time provisioning with a SAML IDP.

If you'll be using just-in-time provisioning for scenarios where only one value is in the studentID attribute in the SAML assertion from your IDP, then take one of these actions:

- Open a service request with Oracle Support to enable support of this scenario:
    - Product: Identity Cloud Service (IDCS)
    - Category: Applications
    - Subcategory: SAML Federation

  Make a request to have this feature enabled on the identity domain saml.jit.user.attribute.provisioning to support Student Financial Aid's custom schema attribute - studentID (string array) - in scenarios where only one value is sent in a SAML assertion.
- Modify the assertion sent to OCI IAM such that the studentID value is enclosed in brackets `[12345]`.

  For example: `<saml:Attribute Name="studentID"> <saml:AttributeValue xsi:type="xs:string">["123456789"]</saml:AttributeValue> </saml:Attribute>`

When configuring just-in-time provisioning in the OCI Console, the assertion attribute from your IDP must be mapped to `urn:ietf:params:scim:schemas:idcs:extension:custom:User:studentID`. You'd need to manually enter and then select this value.

We recommend reviewing the following documentation for just-in-time provisioning:

- *Adding a SAML Just-in-Time Identity Provider*

- *Creating an Identity Provider Policy*
  - *JIT Provisioning from Entra ID to OCI IAM*
  - *JIT Provisioning from Okta to OCI IAM*

Do note that:

- If you don't use SCIM or just-in-time provisioning to automate user account creation, you'll be responsible for creating the accounts in OCI. If you use a combination of external identity providers and OCI IAM users, you'll need to create the OCI IAM users before the users sign in.
- You can bulk create the OCI IAM users via OCI tools.

  You can also bulk create the OCI IAM federated users and set the federated attribute value to true. You can then set up SCIM or just-in-time provisioning so that the accounts are updated going forward.

Manage Groups

Groups must exist in OCI before assigning a user to the group either natively in OCI IAM or via just-in-time provisioning. Review the following documentation for more information:

- *Creating a Group*
- *Importing and Exporting Users, Groups, and AppRoles*
- *Deleting Groups*
- *Adding Users to a Group*
- *Removing Users from a Group*

Create a Direct Link to Student Financial Aid for Guest Users

To make it easier for guest users to authenticate and access Student Financial Aid, you can create a direct link that redirects guest users to the application.

By default, when a new OCI IAM user account is created, the user receives an email notification to activate their account. The link in the email takes the user to the OCI Cloud Console and, when complete, redirects the user to the OCI Cloud Console My Apps page.

On the My Apps page, you can add a link that lets guest users immediately access Financial Aid System (administrative interface) or the Self-Service Portal. To do this, see *Adding an Enterprise Application*. Make sure you select the checkbox **Display in My Apps**.

To control who can see this link, you'll have to manage the groups that are assigned to this application. For information, see *Assigning Applications to a Group*.

Related Topics

- Manage Authentication for Administrators and Non-Administrators

SAML Attributes Required for Authentication

When users log in to Student Financial Aid (SFA), OCI IAM sends attributes in the SAML assertion to authenticate users.

If you're using an external identity provider, you'd need to populate these attributes so that users can log in.

This table lists the attributes that OCI IAM sends in the SAML assertion to authenticate users accessing the administration UI.

OCI IAM attributes sent in the SAML assertion for the administration UI

Name	Format	Type	Type Value	Condition
firstName	Basic	User Attribute	First name	None
lastName	Basic	User Attribute	Last name	None
emailAddress	Basic	User Attribute	Primary email	None
roles	Basic	User Attribute	Group membership	All groups

This table lists the attributes that OCI IAM sends in the SAML assertion to authenticate users accessing the Student/Parent Self-Service Portal.

OCI IAM attributes sent in the SAML assertion for the Student/Parent Self-Service Portal

Name	Format	Type	Type Value	Condition
studentID	Basic	Expression/Literal	urn:ietf:params:scim:schema	None
firstName	Basic	User Attribute	First name	None
lastName	Basic	User Attribute	Last name	None
roles	Basic	User Attribute	Group membership	All groups
emailAddress	Basic	User Attribute	Primary email	None

studentID

The studentID attribute is a custom schema attribute that SFA adds to your identity domain schema when you provision the SFA environment for the first time. Make sure that this attribute:

- Is populated with a student's ID so that a student can successfully log in to Student Portal.
- Is populated with at least one student ID so that a guest user can successfully log in.
- Is of type `String Array` and must be of this type when included in the assertion from an IDP.
- Is presented in a comma-separated format: <studentID1>,<studentID2>, and so on.