How to add the Security Console in Oracle Fusion and manage users and roles

This guide shows you how to add the Security Console in Oracle Fusion to your administration workflow. You sign in with a user that has the right role, open the console from the **Tools** menu, and then manage user accounts, roles, and security settings. It also covers importing user and role data, reviewing each console area, querying user and role data with SQL, and troubleshooting user access.

Prerequisites

Before you begin, make sure you have the following:

- A browser and the URL of your Oracle Fusion ERP instance.
- A user account with the **IT Security Manager** role, which is required to access the Security Console. The example user in this guide is **FAS16 student**.
- Permission to schedule processes, so you can run **Import User and Role Application Security Data**.
- Access to a SQL query tool if you want to run the example queries in the user and role data sections.

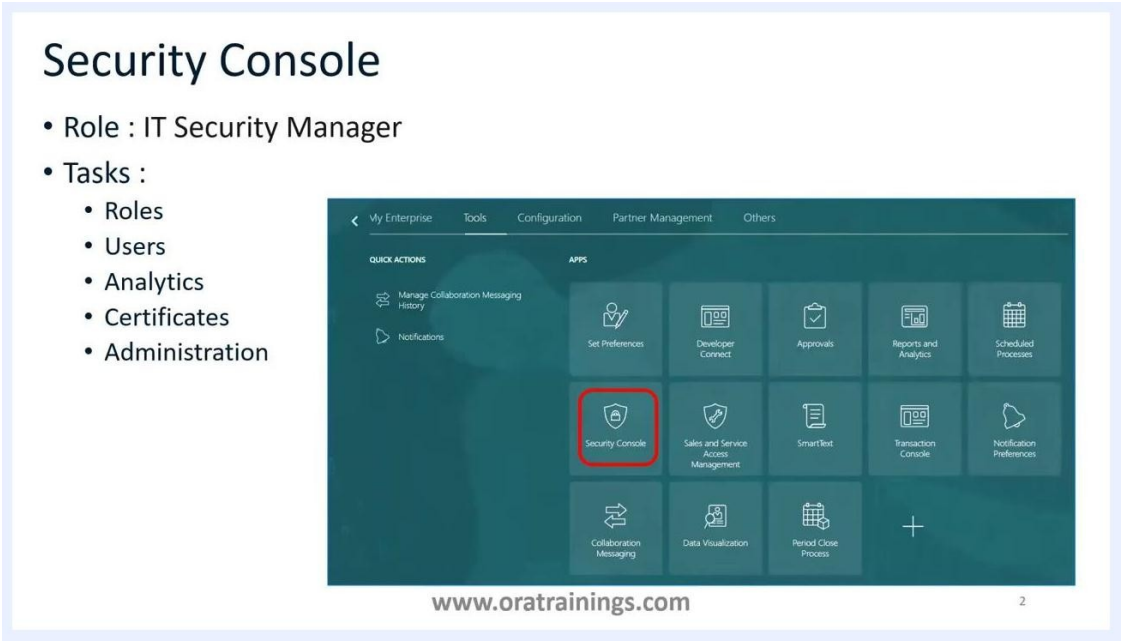
Understand role-based access control

Step 1: Understand what the Security Console controls

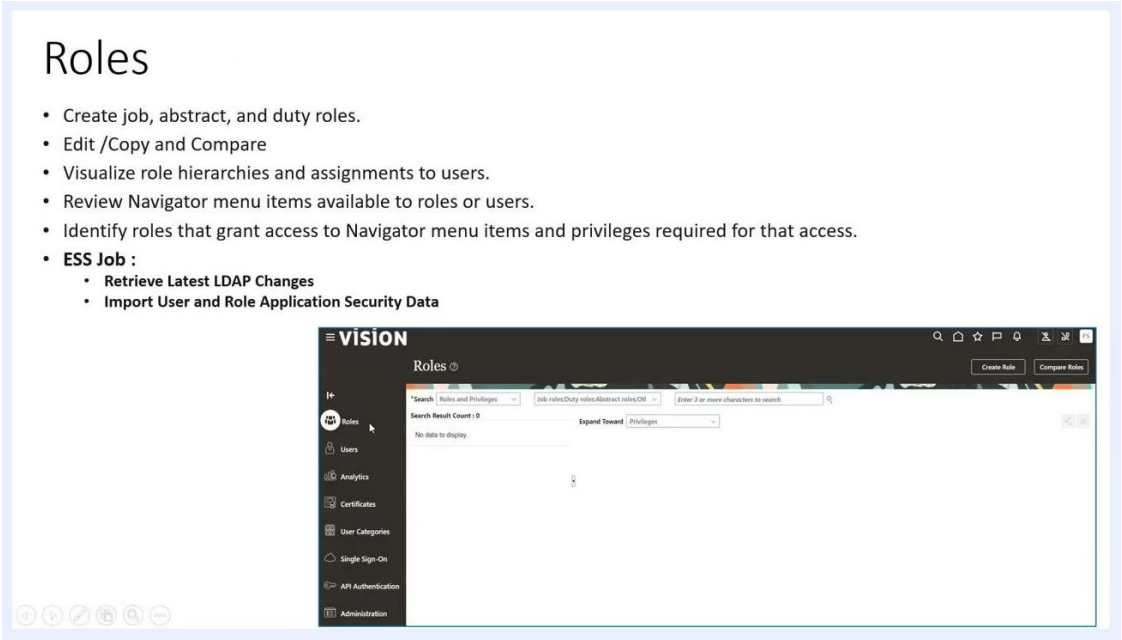
The Security Console is a key functionality within Oracle Fusion ERP. You use it to control:

- Creation and management of user roles
- API certification
- LDAP synchronization
- Other critical security and administrative tasks

All of these functions are governed by role-based access control (RBAC). Every action and page access in Oracle Fusion ERP is determined by the roles assigned to a user. Without the appropriate role, users cannot access specific pages or views.



Title slide showing "Security Console Oracle Cloud ERP (Fusion Apps)" and "Prepared by: Oratrainings.com"



Security Console dashboard with tasks and the Security Console icon highlighted to show role-based access

Step 2: Review what you can manage with the Security Console

Use the Security Console to manage roles, including:

- Creating job, abstract, and duty roles
- Editing, copying, and comparing roles
- Visualizing role hierarchies and assignments to users
- Reviewing Navigator menu items available to roles or users
- Identifying roles that grant access to specific Navigator menu items and the required privileges

Add the Security Console in Oracle Fusion: sign in and open it

Step 3: Sign in with Security Console access

1. Open your browser and go to your Oracle Fusion ERP instance.
2. Sign in with a user account that has the necessary role, such as **IT Security Manager**. The example user is **FAS16 student**.
3. Confirm that the user has the **IT Security Manager** role. This role is required to access the Security Console.

Step 4: Open the Security Console from the Tools menu

1. After you sign in, click the **Tools** menu.
2. Select **Security Console** from the available options.

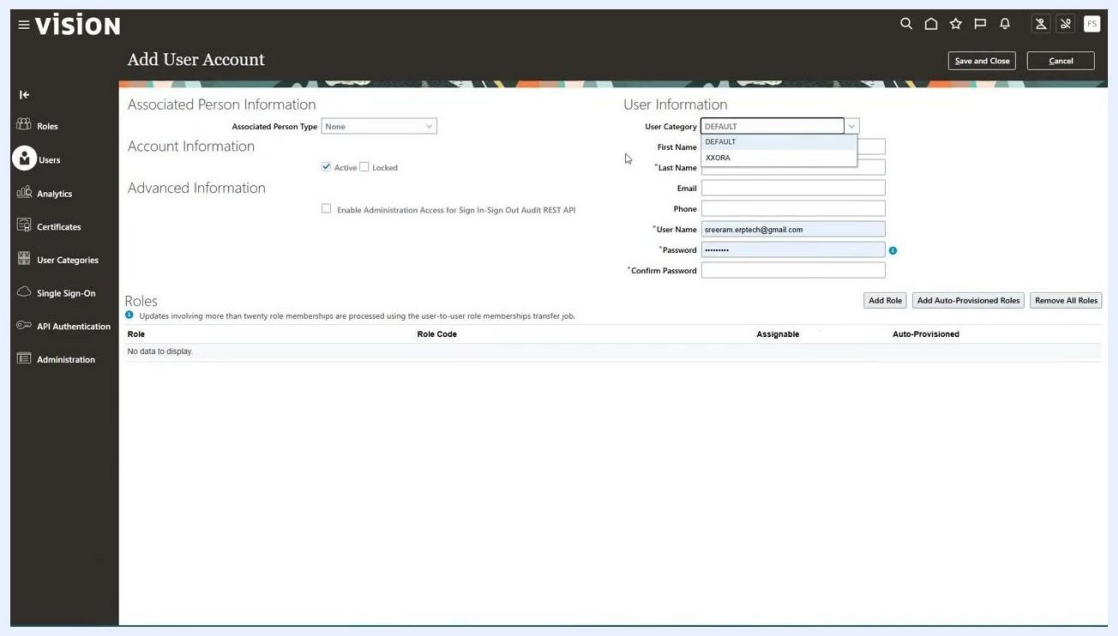
Only users with the **IT Security Manager** role see this option.

Manage user accounts in the Security Console

Step 5: Open the User Accounts screen

1. In the left sidebar, click **Users** to open the **User Accounts** screen.
2. To add a new user, click the **Add User Account** button in the upper right.

If users exist, the list appears under "Search Results". Otherwise, the screen shows "No data to display."



User Accounts screen with the search bar, the Add User Account button, and an empty user list

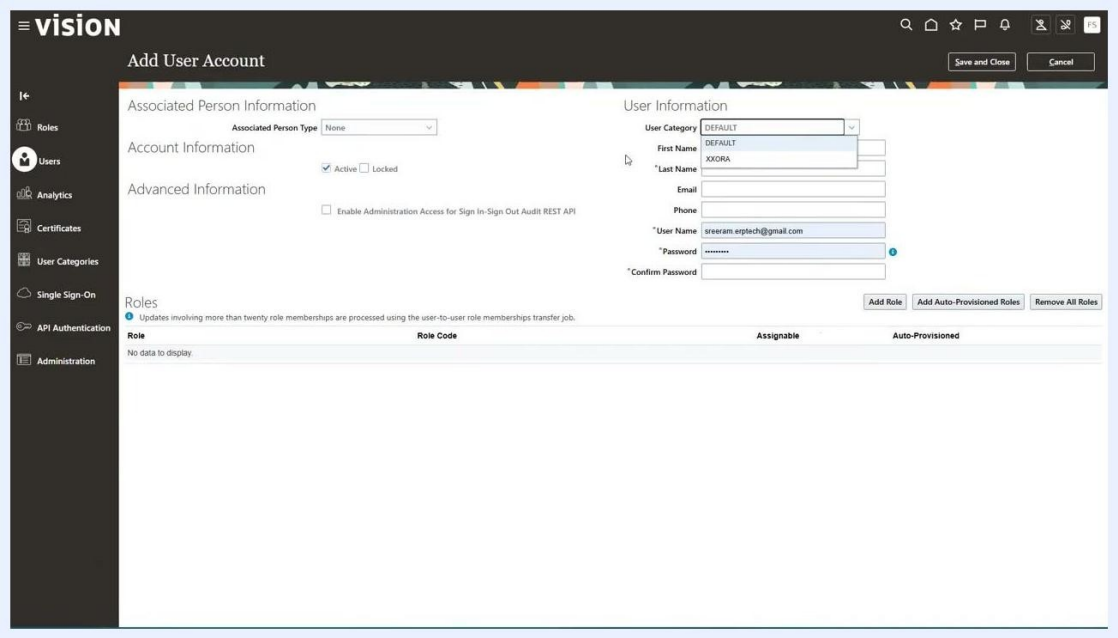
Step 6: Add a new user account

On the **Add User Account** screen, fill in the following details:

- **Associated Person Information**: Select the associated person type, if applicable.
- **Account Information**: Select **Active** to enable the account. Select **Locked** if you want to lock the account initially.
- **Advanced Information**: Optionally, enable administration access for the Sign In/Sign Out Audit REST API.
- **User Category**: Select a category from the dropdown, for example DEFAULT or XXORA.
- **First Name**: Enter the user's first name, for example erpuser.
- **Last Name**: Enter the user's last name, for example XXORA.
- **Email**: Enter the user's email address.
- **Phone**: Enter the user's phone number.
- **User Name**: Enter the username, for example sreeram.erptech@gmail.com.
- **Password**: Enter the password.
- **Confirm Password**: Re-enter the password.

In the **Roles** area, click **Add Role** or **Add Auto-Provisioned Roles** to assign roles. Use **Remove All Roles** to clear assigned roles.

Click **Save and Close** to create the user, or **Cancel** to discard your changes.

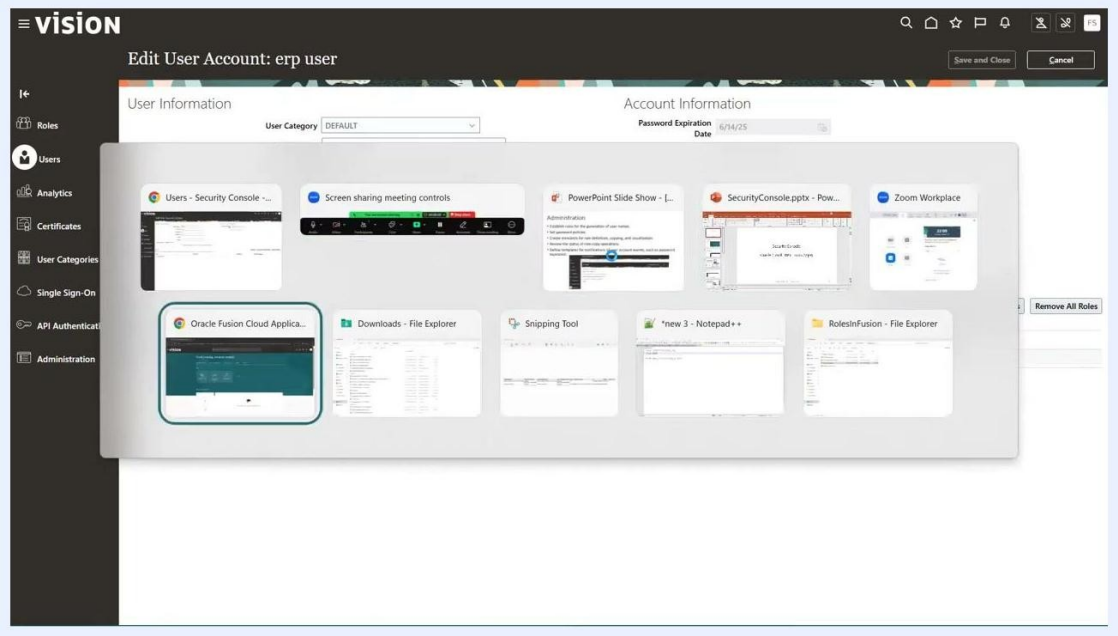


Add User Account screen with user information fields, the user category dropdown, and role assignment options

Step 7: Test the new user's sign-in in a separate browser

1. Open a new browser window or an incognito window.
2. A window switcher or application overview may appear as you prepare to sign in. You don't need to take any action in the Oracle interface for this.
3. On the Oracle Applications Cloud sign-in page, enter **erp.user** as the **User ID**.
4. Enter the password you set for the user.

5. Click **Sign In**.



Oracle Applications Cloud sign-in page with erp.user entered as the User ID and the password masked

Step 8: Assign roles to the user

To grant access to additional functionality, assign roles to **erp.user**:

1. On the **Edit User Account** screen, click **Add Role** or **Add Auto-Provisioned Roles**.
2. Select the appropriate roles from the available list.
3. Click **Save and Close** to apply the changes.

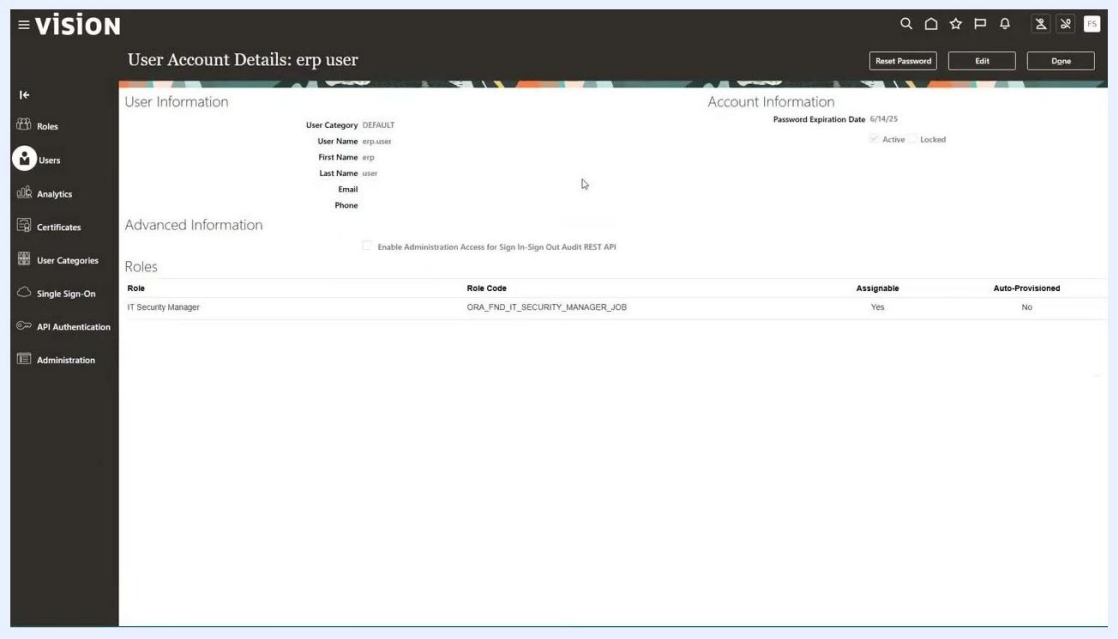
A user without assigned roles has minimal or no access to application features. Always assign at least one role to enable the necessary permissions.

Step 9: Review the user account details and role synchronization

After you assign a role, review the **User Account Details** screen for **erp.user**. This is a review step, so you don't need to change anything.

- **User Information**: User Category is DEFAULT, User Name is erp.user, First Name is erp, and Last Name is user. Email and Phone are not specified.

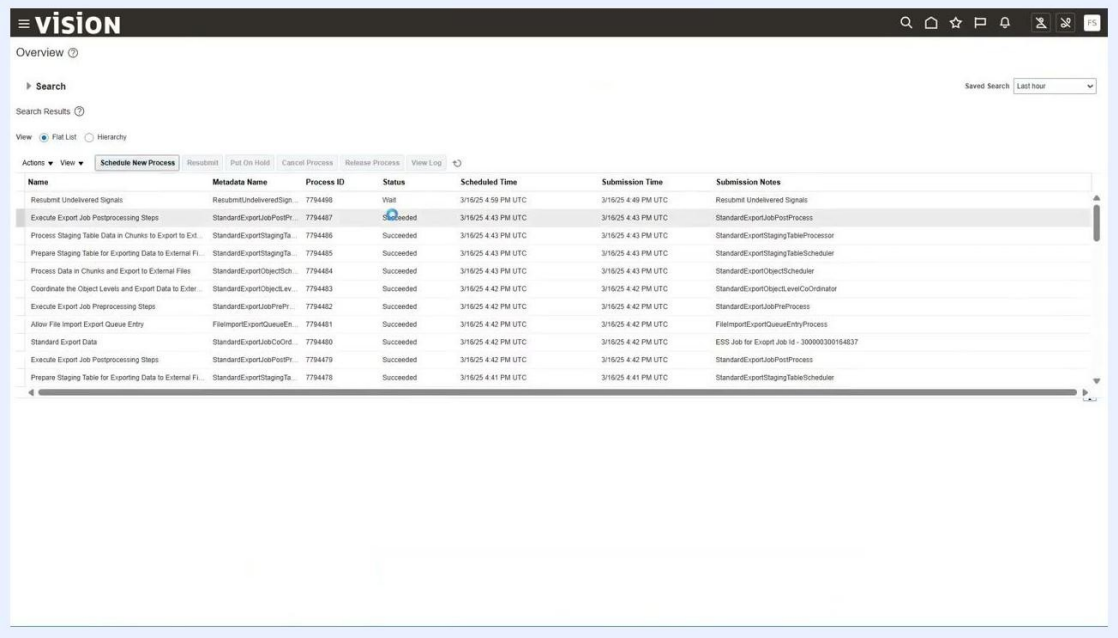
- **Account Information**: Password Expiration Date is 6/14/25, **Active** is checked, and **Locked** is not checked.
- **Roles**: The **IT Security Manager** role is now listed, with Role Code ORA_FND_IT_SECURITY_MANAGER_JOB, Assignable set to Yes, and Auto-Provisioned set to No.
- The top right of the screen offers **Reset Password**, **Edit**, and **Done**.



User Account Details screen for erp.user showing the IT Security Manager role assigned

If you refresh the user screen immediately after you assign a role, it may not show the updated roles. Synchronization delays in the instance cause this.

Click **Done** in the upper right to exit the user account details screen.



User Account Details screen for erp.user with the Done button highlighted

Import user and role application security data

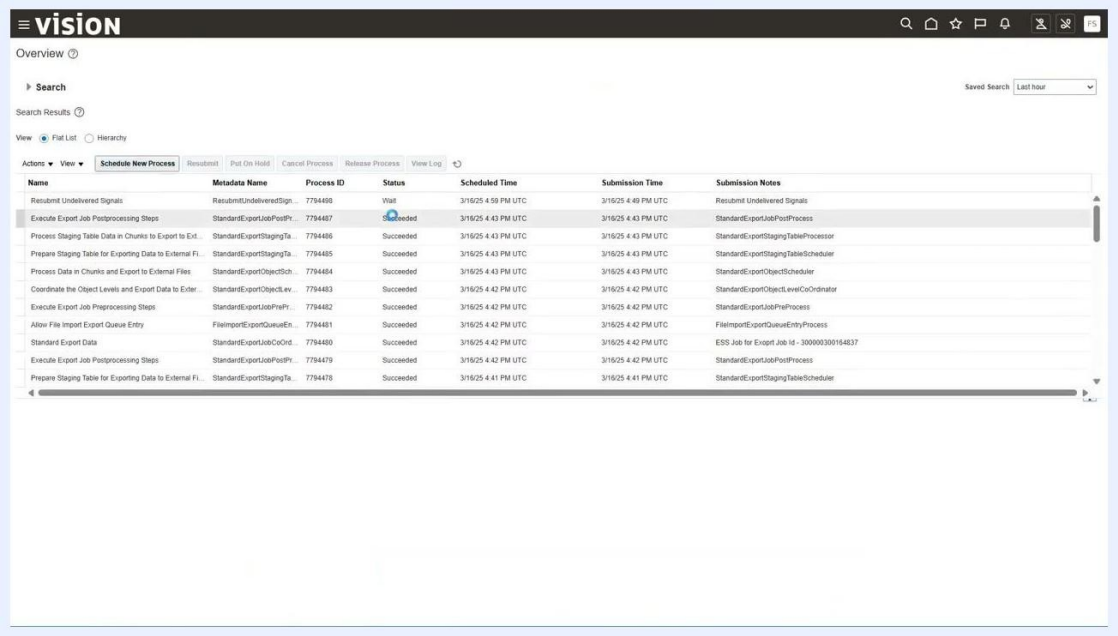
Step 10: Open the Scheduled Processes overview

Go to the **Overview** screen for scheduled processes. The screen lists processes with these columns: **Name**, **Metadata Name**, **Process ID**, **Status**, **Scheduled Time**, **Submission Time**, and **Submission Notes**.

Example processes include:

- "Execute Export Job Postprocessing Steps" (Status: Succeeded)
- "Process Staging Table Data in Chunks to Export to External Files" (Status: Succeeded)
- "Resubmit Undelivered Signals" (Status: Wait)

This is the process monitoring area, so you don't need to take any action yet.

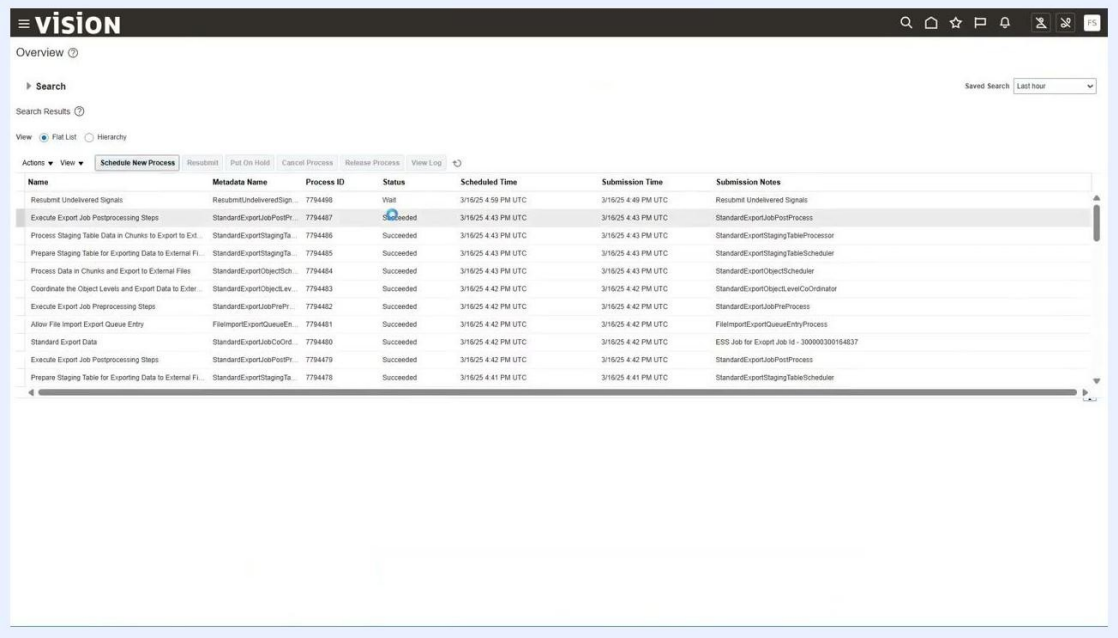


Scheduled Processes Overview screen showing a list of processes and their statuses

Step 11: Schedule the import process

1. Click **Schedule New Process**.
2. In the **Search and Select: Name** dialog, search for and select **Import User and Role Application Security Data**. Its description is "Import user and role data."

3. Click **OK** to proceed.

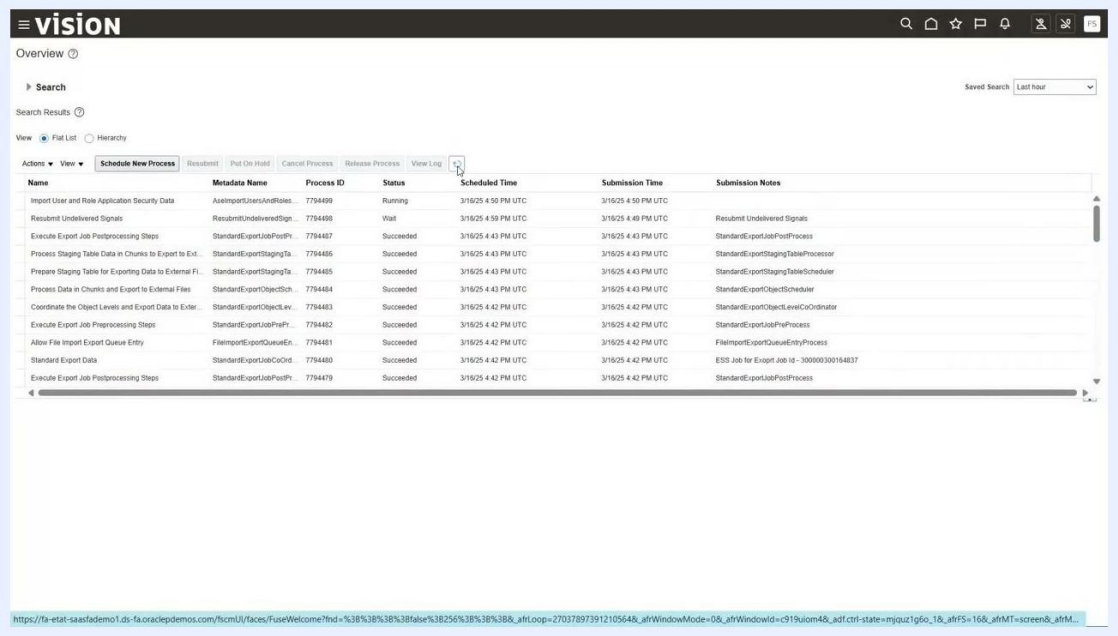


Search and Select dialog with Import User and Role Application Security Data highlighted

Step 12: Monitor the import process

1. Return to the **Overview** screen.
2. Find **Import User and Role Application Security Data** in the list. Its **Status** is Running at first. Other processes may show as Succeeded or Wait.
3. Click **View Log** if you want to monitor progress.

The import process may take some time to complete, so don't expect immediate results.



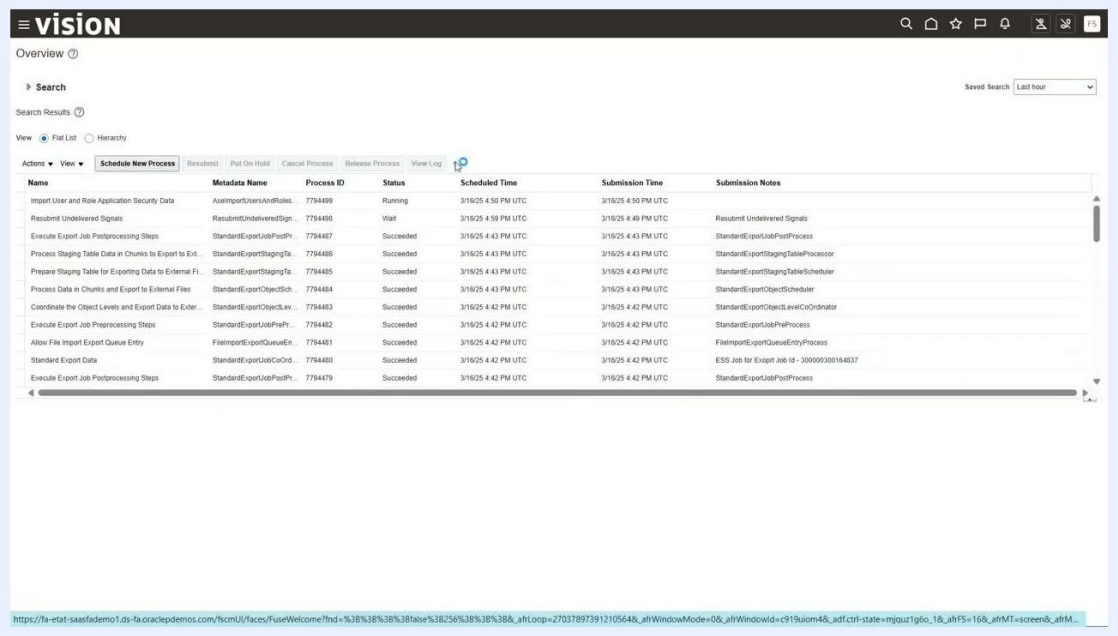
Scheduled Processes Overview with the Import User and Role Application Security Data process running

Step 13: Verify user access in Oracle Fusion Cloud Applications

Switch to the browser window where you are signed in as **erp.user**, and check the dashboard:

- The greeting reads "Good evening, erp user".
- The available apps are **Set Preferences**, **Approvals**, and **Reports and Analytics**.
- There are no open notifications or assigned tasks.

This confirms that the user can now access modules based on the assigned role.



Oracle Fusion Cloud Applications dashboard for erp.user showing available apps and no notifications

After you assign roles, always run **Import User and Role Application Security Data** to synchronize permissions. Allow time for the process to complete before you expect new roles to be reflected in user access.

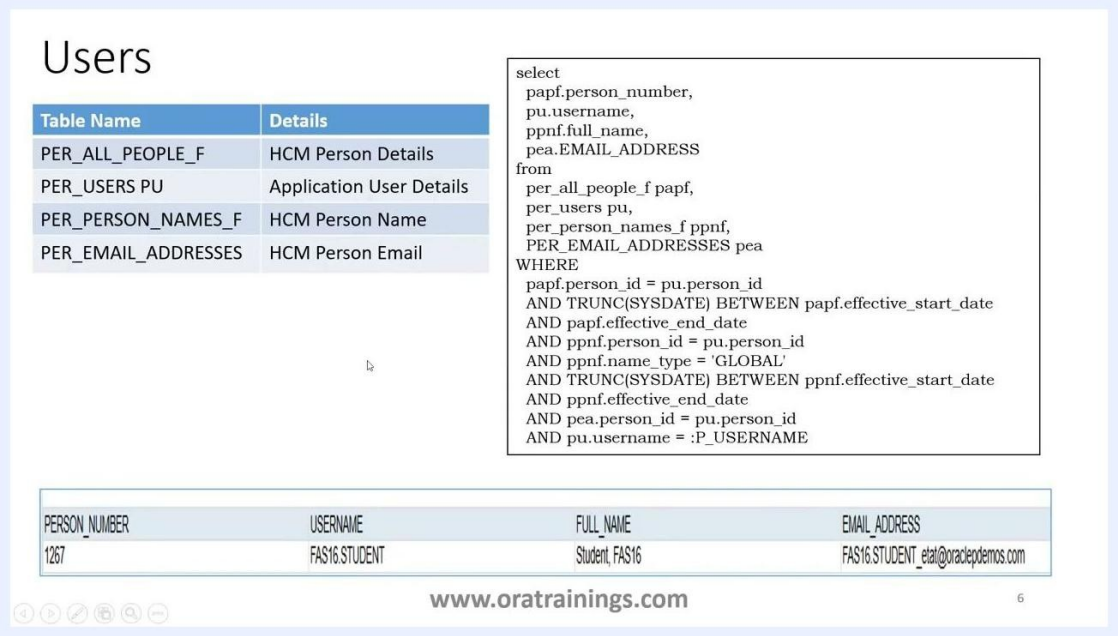
Explore the other Security Console areas

Step 14: Review role statistics in Analytics

Open the **Analytics** section in the Security Console to review statistics about roles and their categories. Use this screen to:

- View the number of roles in each category.
- Visualize the hierarchy and distribution of roles using graphical representations, such as pie charts.
- Review data security policies, roles, and users associated with each data resource.

This section is primarily for system administrators and doesn't provide backend table details.



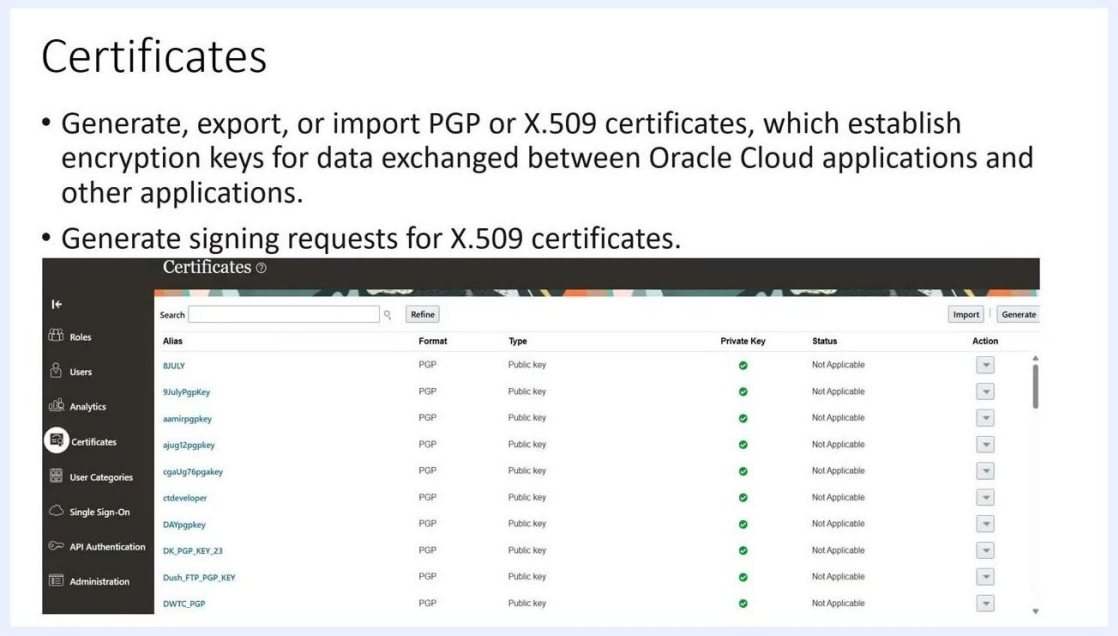
Analytics screen showing role categories, the number of roles per category, and a pie chart of role distribution, with the sidebar menu visible

Step 15: Manage encryption keys in Certificates

Use the **Certificates** section to manage encryption keys for integrating Oracle Fusion ERP with third-party systems. You can:

- Generate, export, or import PGP or X.509 certificates.
- Establish encryption keys for secure data exchange between Oracle Cloud applications and external applications.
- Generate signing requests for X.509 certificates.
- Upload the required security keys for integration scenarios.

No backend table details are provided for certificates.



Certificates screen showing certificate aliases, formats (PGP), types (Public key), private key status, and actions

Step 16: Use User Categories

Use **User Categories** to assign specific categories or naming conventions to users during account creation.

Step 17: Retrieve user category details

The data for user categories is stored in the ASE_USER_CATEGORY_B table. Retrieve the details with this SQL query:

```
SELECT * FROM ASE_USER_CATEGORY_B
```

The example output has these columns: CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATE_DATE, LAST_UPDATE_LOGIN, ID, CODE, NEXT_URL. Example values are CREATED_BY: FAS16.STUDENT and CODE: DEFAULT, XXORA.

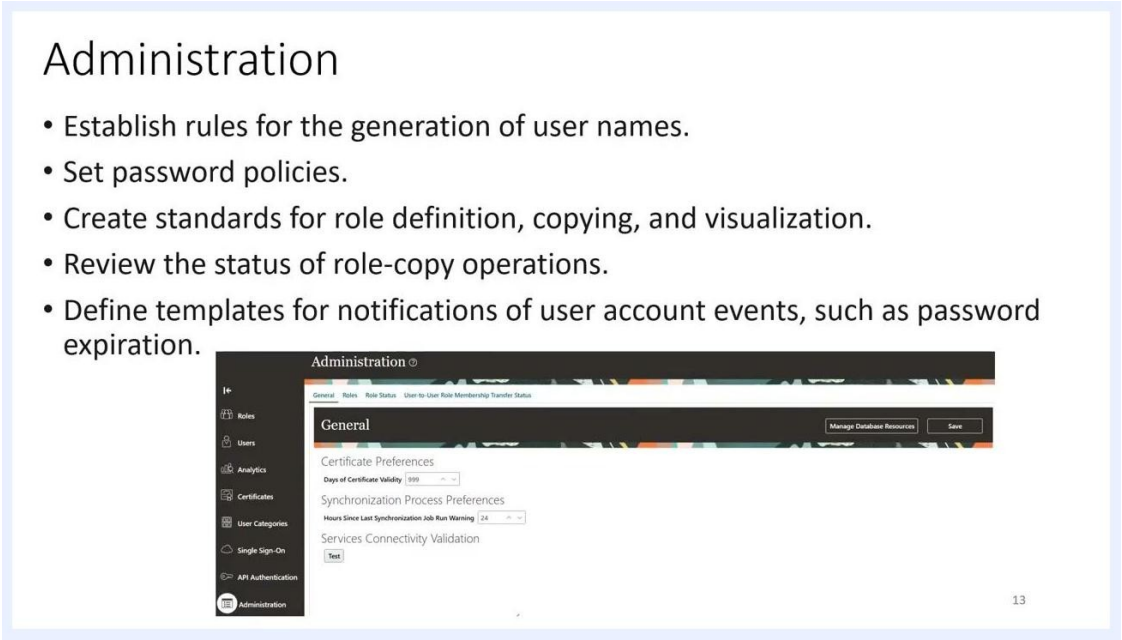


User Categories screen showing the ASE_USER_CATEGORY_B table, the sample SQL query, and output rows with columns such as CREATED_BY, CREATION_DATE, CODE, and NEXT_URL

Step 18: Configure Single Sign-On

1. Select **Single Sign-On** from the left sidebar menu.
2. In the **Single Sign-On Configuration** panel, locate the **Sign Out URL**, **Enable Chooser Login Page**, and **Single Sign-On Enabled** fields.
3. Under **Service Provider Details**, note the **Federation Metadata** value: https://login-etat-saassfademo1.ds-fa.oracledemos.com:443/oamfed/sp/metadata?signid=osts_signing_sha256&encid=osts_encryption_sha256&sigalgm=SHA-256
4. Download the **Signing Certificate** and **Encryption Certificate** from the links provided.
5. To make changes, click **Edit** in the upper right of the configuration panel.
6. To add a new identity provider, click **+ Create Identity Provider**.

If the table shows "No data to display.", no identity providers are currently listed.

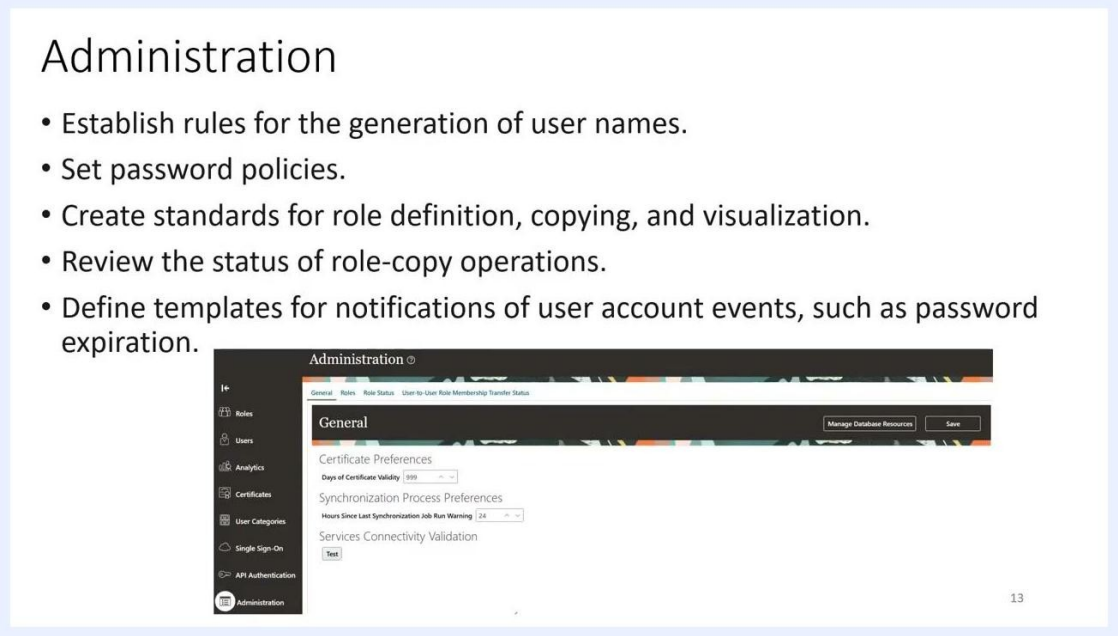


Single Sign-On configuration screen with service provider details, the federation metadata URL, certificate download links, and the option to create an identity provider

Step 19: Configure API Authentication

1. Select **API Authentication** from the left sidebar.
2. Review the list of existing API authentication providers. Each entry shows the provider URL (for example, https://identity.oraclecloud.com), the provider type (for example, Oracle API Authentication Provider), and the certificate common name (CN).
3. To add a new provider, click **Create External Client Application** or **Create Oracle API Authentication Provider** at the top.
4. To view logs or certificates, click **View Diagnostic Logs** or **Oracle Public Certificate**.

5. Use the **Sort By** dropdown to organize providers by type or name.



API Authentication screen showing provider URLs, types, certificate CNs, and options to create new providers or view logs

Step 20: Use Administration for user and role management

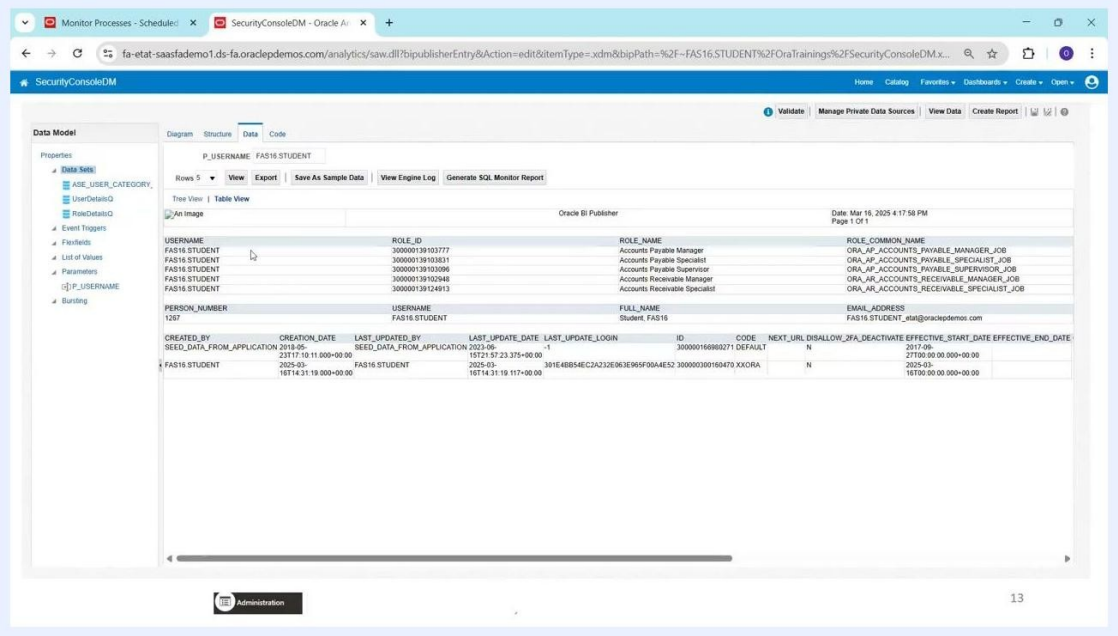
Go to **Administration** from the sidebar. You can perform these administrative tasks:

- Establish rules for the generation of user names.
- Set password policies.
- Create standards for role definition, copying, and visualization.
- Review the status of role-copy operations.
- Define templates for notifications of user account events, such as password expiration.

In the **General** tab, configure the following:

- **Certificate Preferences**: Set "Days of Certificate Validity", for example 999.
- **Synchronization Process Preferences**: Set "Hours Since Last Synchronization Job Run Warning", for example 24.
- **Services Connectivity Validation**: Use the **Test** button to validate.

Click **Save** to apply your changes.



Administration screen with rules, password policies, certificate preferences, and synchronization settings

Query user and role data

Step 21: Understand role assignment tables

Four primary tables determine whether a role is assigned to a user:

- per_user_roles: Stores role assignments for users.
- per_users (alias pu): Contains user details.
- per_roles_dn_tl (alias prdt): Holds translated role details.
- pr_roles_dn (alias prd): Contains role details.

The tables relate to each other as follows:

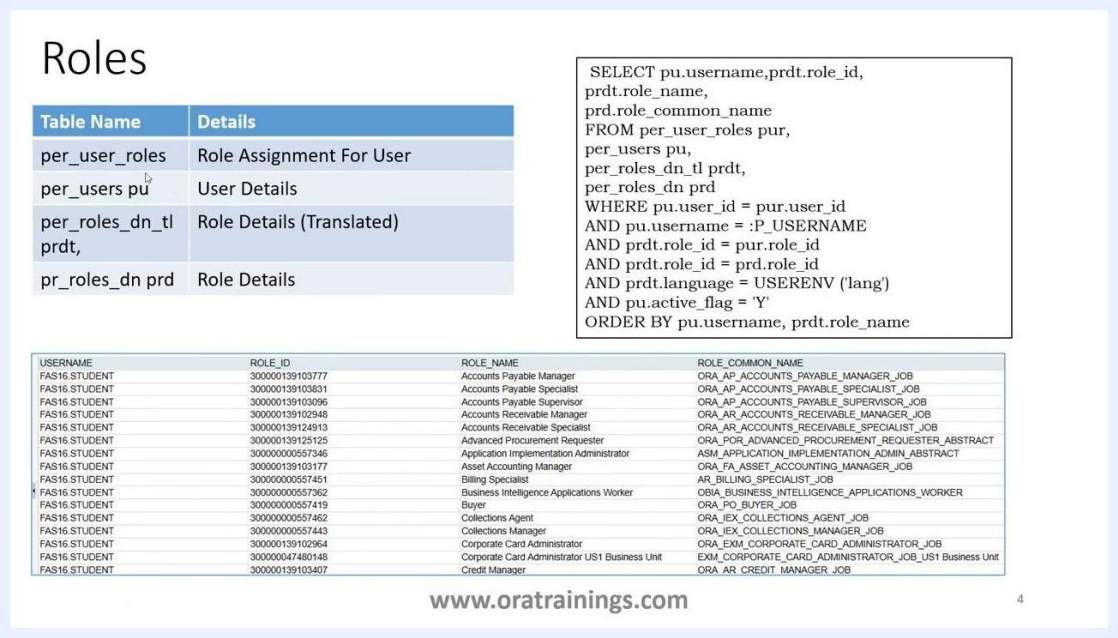
- The pu.user_id field is joined with pur.user_id to link user details with their role assignments.
- The pur.role_id field is joined with prdt.role_id and prd.role_id to retrieve role names and details.
- When a role is assigned to a user, the assignment is recorded in per_user_roles with both user_id and role_id.

Step 22: Retrieve user roles and details

Use the following SQL query to retrieve user roles and details:

```
SELECT pu.username, prdt.role_id, prdt.role_name, prd.role_common_name
FROM per_user_roles pur,
     per_users pu,
     per_roles_dn_tl prdt,
     pr_roles_dn prd
WHERE pu.user_id = pur.user_id
  AND pu.username = :P_USERNAME
  AND prdt.role_id = pur.role_id
  AND prdt.role_id = prd.role_id
  AND prdt.language = USERENV('lang')
  AND pu.active_flag = 'Y'
ORDER BY pu.username, prdt.role_name
```

The query returns the username, role ID, role name, and role common name for each assigned role.



The four key role tables, the SQL query, and a sample output table listing usernames, role IDs, role names, and role common names

Step 23: Verify role assignments in the output

Review the sample output to verify role assignments. The example output columns are USERNAME, ROLE_ID, ROLE_NAME, and ROLE_COMMON_NAME. Each row shows a user and their assigned roles.

Step 24: Understand application users and HCM persons

A "user" in Fusion ERP is an application login account, not necessarily an HCM (Human Capital Management) person. When you create a user, you can optionally link that user to an HCM person by associating the user account with a person ID.

The mapping works like this:

- Application user: Username from PER_USERS.
- HCM person: Person number, full name, and email from HCM tables.

Step 25: Identify the user and HCM person tables

The main tables for user and HCM person data are:

- PER_ALL_PEOPLE_F: HCM person details.
- PER_USERS (alias PU): Application user details.
- PER_PERSON_NAMES_F: HCM person names.
- PER_EMAIL_ADDRESSES: HCM person email addresses.

To obtain the username and email address for an application user, join the tables using the person_id field:

- Join PER_USERS with PER_ALL_PEOPLE_F on person_id.
- Join PER_PERSON_NAMES_F and PER_EMAIL_ADDRESSES using person_id.

This lets you retrieve the application username, HCM person number, full name, and email address for a given user.

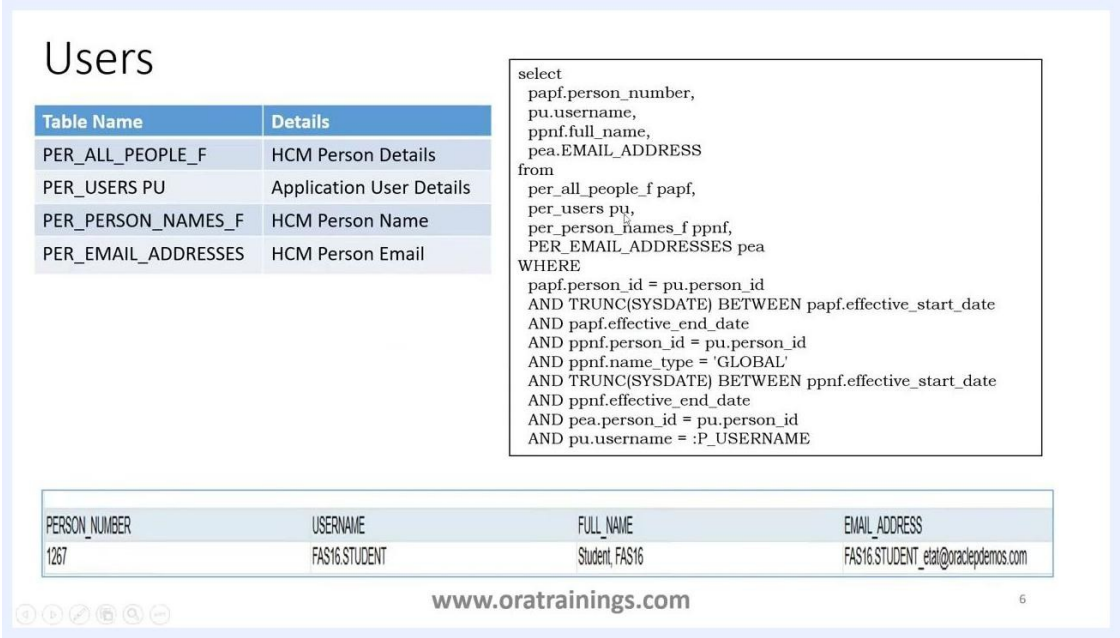
Step 26: Retrieve user and HCM person details

Use the following SQL query to retrieve these details:

```
SELECT papf.person_number,
       pu.username,
       ppnf.full_name,
       pea.EMAIL_ADDRESS
FROM   per_all_people_f papf,
       per_users pu,
       per_person_names_f ppnf,
       PER_EMAIL_ADDRESSES pea
```

```
WHERE  papf.person_id = pu.person_id
  AND TRUNC(SYSDATE) BETWEEN papf.effective_start_date AND
papf.effective_end_date
  AND ppnf.person_id = pu.person_id
  AND ppnf.name_type = 'GLOBAL'
  AND TRUNC(SYSDATE) BETWEEN ppnf.effective_start_date AND
ppnf.effective_end_date
  AND pea.person_id = pu.person_id
  AND pu.username = :P_USERNAME
```

The query returns these columns: PERSON_NUMBER, USERNAME, FULL_NAME, EMAIL_ADDRESS. With these queries, you can retrieve both user and role data in Oracle Fusion ERP and check user access and identity information.



SQL query joining user and HCM person tables, with a sample output row showing PERSON_NUMBER 1267, USERNAME FAS16.STUDENT, FULL_NAME Student, FAS16, and EMAIL_ADDRESS FAS16.STUDENT_etat@oracledemos.com

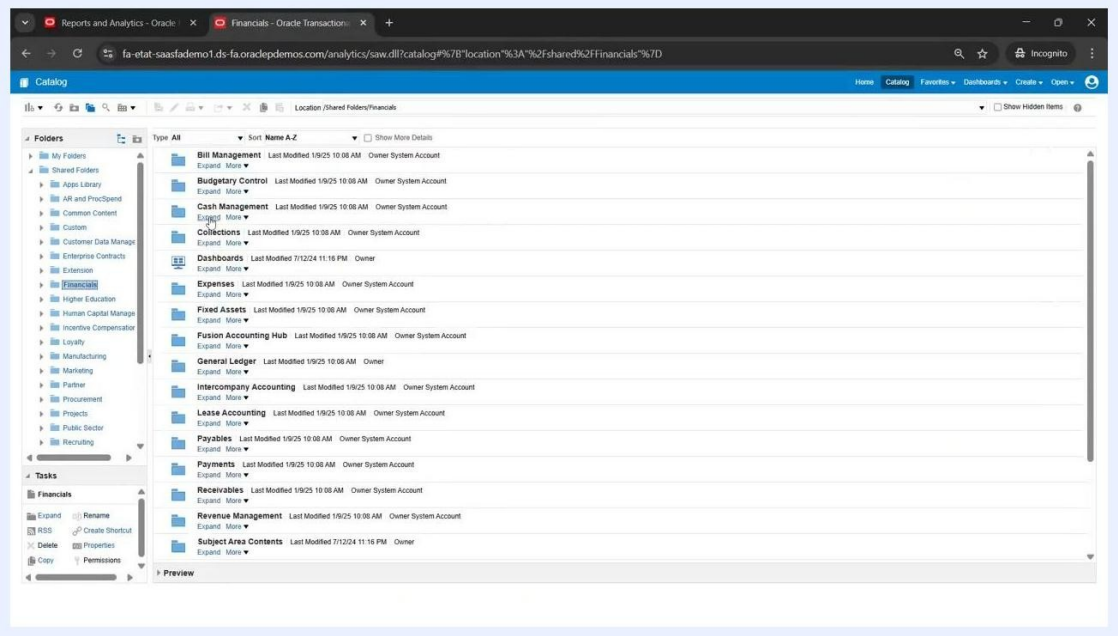
Troubleshoot user access

Step 27: Verify user access to Reports and Analytics

1. Open the Oracle Fusion Cloud application and go to the **Reports and Analytics** section.
2. Expand the **Financials** folder in the left navigation pane.

3. Review the available subfolders: Bill Management, Budgetary Control, Cash Management, Collections, Dashboards, Expenses, Fixed Assets, Fusion Accounting Hub, General Ledger, Intercompany Accounting, Lease Accounting, Payables, Payments, Receivables, Revenue Management, and Subject Area Contents.

If you don't see the expected reports or folders, you may not have the proper functionality or permissions for execution.

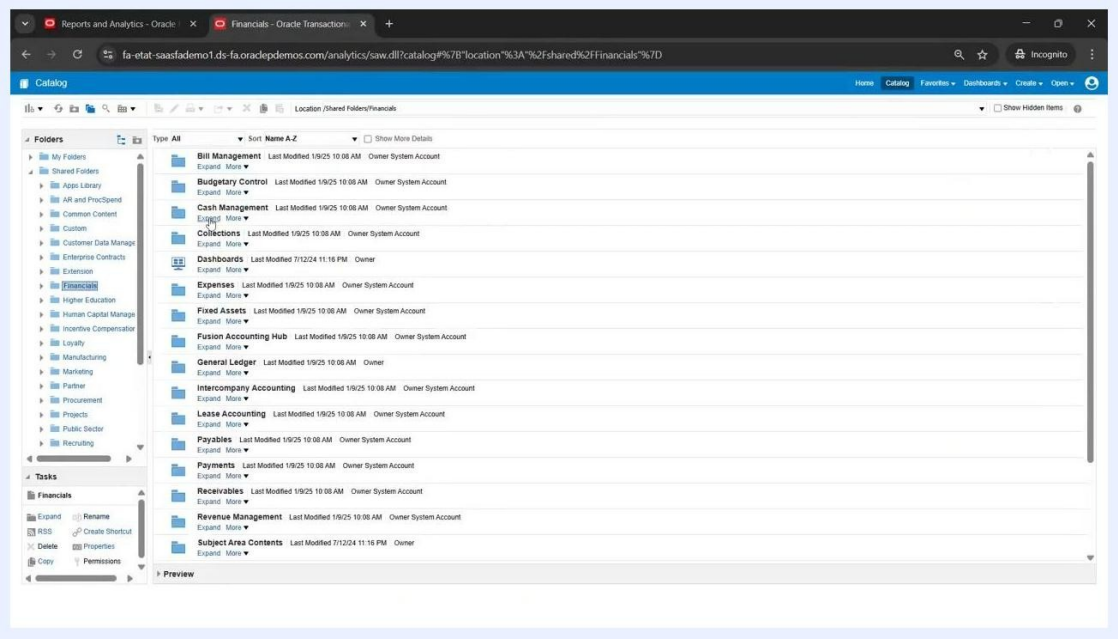


Catalog view showing the Financials folders and subfolders

Step 28: Check for missing reports

1. Select the **Collections** folder under **Financials**.

2. Observe the contents. If you see only subfolders such as "Aging" and "Correspondence" and no reports, access or permissions are missing.

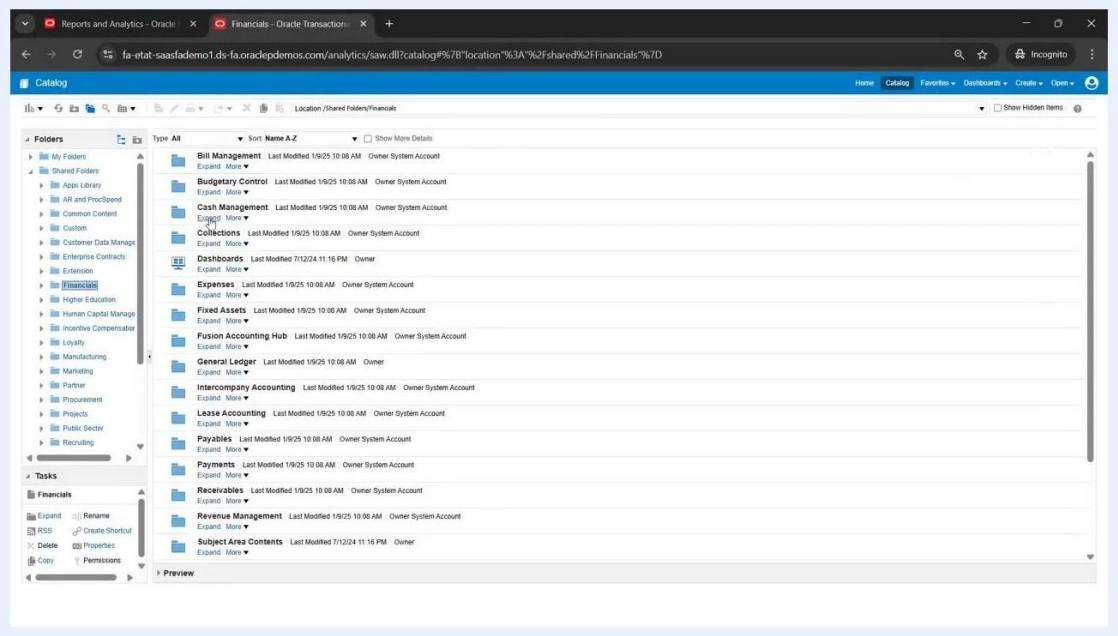


Collections folder selected, showing only the Aging and Correspondence subfolders and no reports

Step 29: Validate Workflow Reports access

1. In the folder structure, go to **Workflow Reports** > **Payables**.
2. Check for subfolders such as "Invoices" and "Payments".

If these folders contain no reports or only minimal content, the user likely lacks the proper functionality.



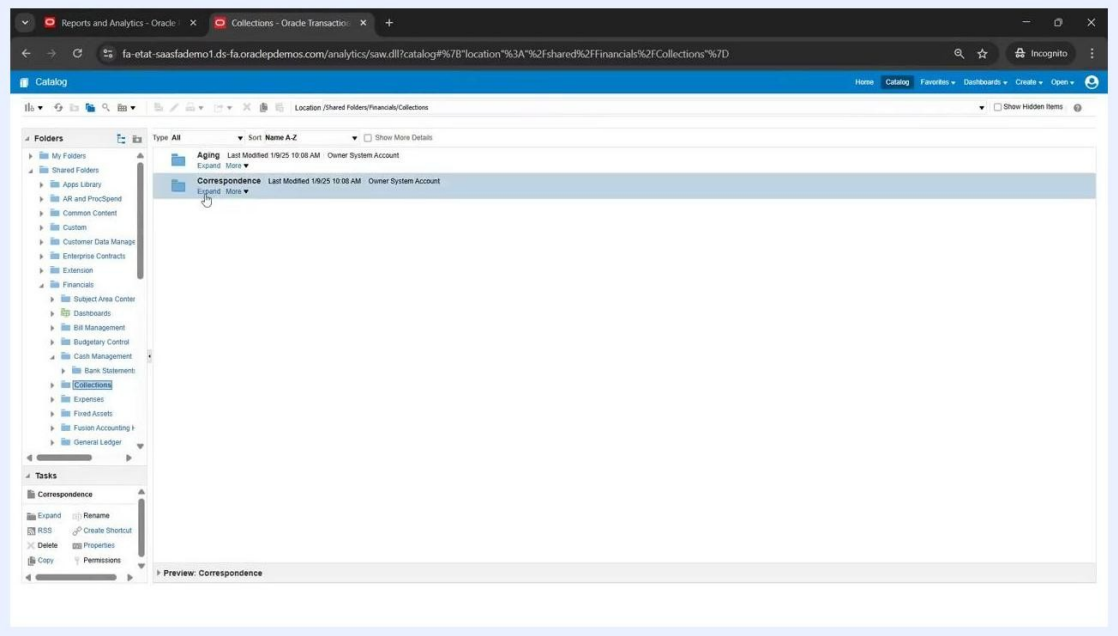
Workflow Reports > Payables folder selected, showing the Invoices and Payments subfolders

Step 30: Sign out and sign in to refresh permissions

If you recently updated user roles or permissions, sign out of the Oracle Fusion Cloud application:

1. Click your user icon (for example, "EU" in the top right corner).
2. Select **Sign Out** from the **Settings and Actions** menu.

3. Wait for the sign-in screen to appear.

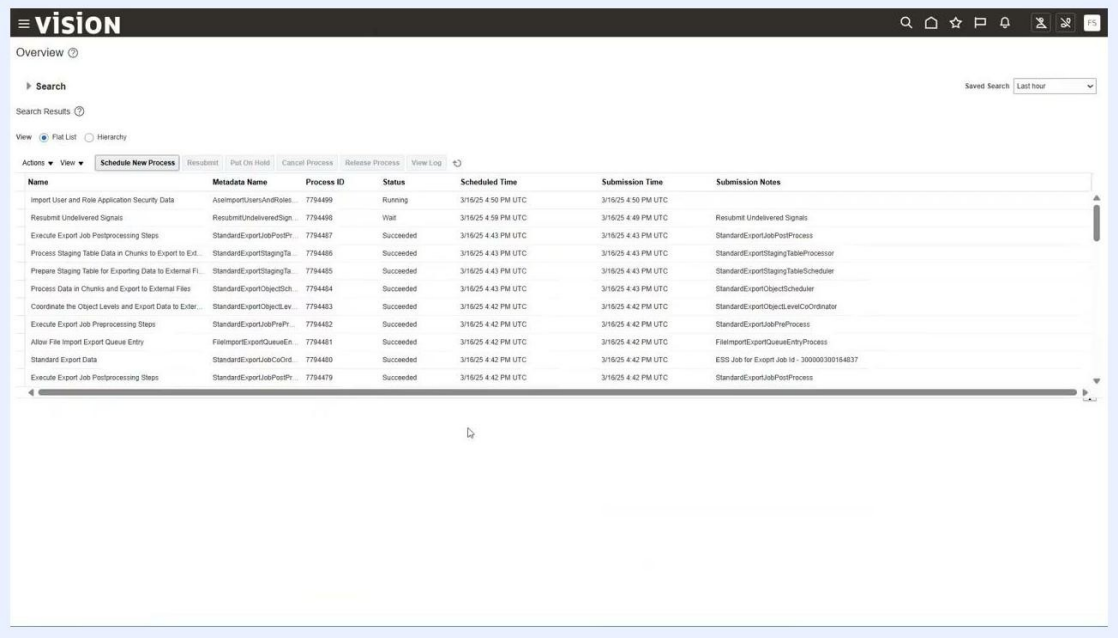


User profile menu open with the Sign Out option highlighted in Oracle Fusion Cloud

Then sign in again to Oracle Applications Cloud:

4. On the sign-in page, enter your User ID (for example, erp.user) and password.
5. Select your preferred language, for example English.

6. Click **Sign In** to log back into the system.



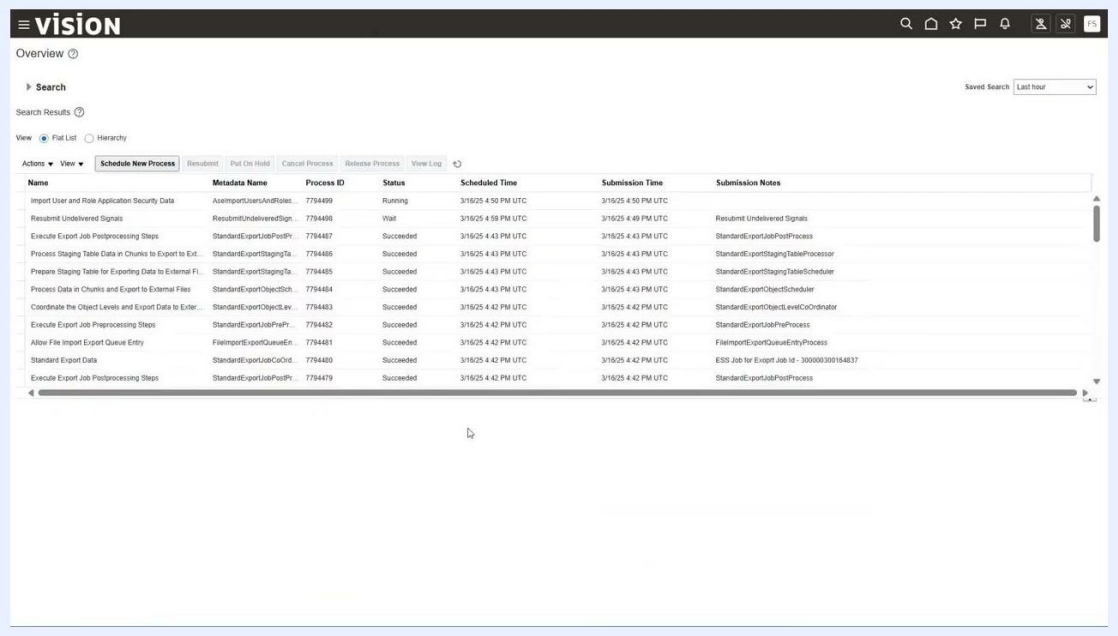
Oracle Applications Cloud sign-in screen with the User ID, Password, and Sign In button

Step 31: Verify updated access

After you sign in, confirm that your dashboard displays the correct set of applications and tools:

- Look for modules such as **Set Preferences**, **Approvals**, **Reports and Analytics**, **Scheduled Processes**, **Security Console**, and **Sales and Service Access Management**.

- Make sure the **Tools** tab is selected and that all expected applications are visible.



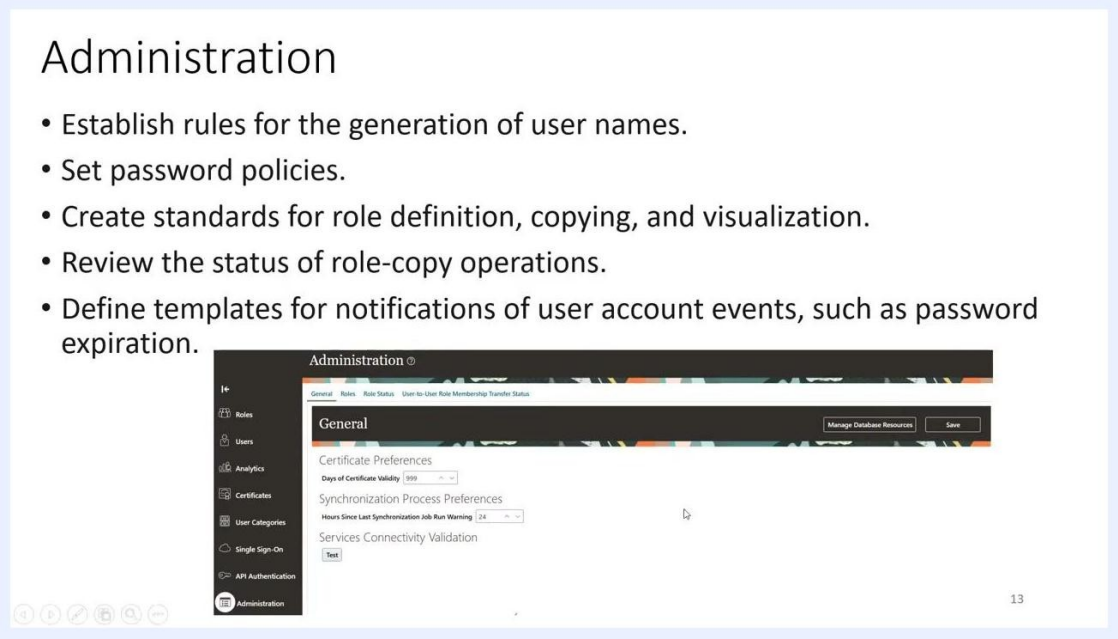
Oracle Fusion Cloud dashboard showing updated access with multiple application tiles

Step 32: Use APIs for roles and users management

Use the available APIs to automate and streamline the management of roles and users within Oracle Fusion Cloud. You can use APIs to:

- Create, update, or delete user accounts programmatically.
- Assign or revoke roles for users in bulk.
- Retrieve current user and role configurations for auditing or reporting purposes.
- Integrate user and role management with external systems or identity providers.

Make sure API access is secured and follows your organization's governance and compliance requirements. Refer to the Oracle Fusion Cloud documentation for detailed API endpoints and usage examples.



Administration screen showing user and role management policies, the Administration > General tab, and the API Authentication option in the navigation menu

Summary and what's next

You now know how to add the Security Console in Oracle Fusion to your workflow. You sign in with the **IT Security Manager** role and open **Security Console** from the **Tools** menu. From there you can create users, assign roles, and run **Import User and Role Application Security Data** to synchronize permissions. You can also review Analytics, Certificates, User Categories, Single Sign-On, API Authentication, and Administration, and query user and role data.

As next steps, you can automate user and role management with the Oracle APIs. Always validate your changes and make sure they comply with your organization's security standards. For further automation or integration needs, consult the official Oracle API documentation.