Oracle Fusion Cloud Applications

Securing Applications

25B

Oracle Fusion Cloud Applications
Securing Applications

25B

G26727-01

Author: Dinesh Kumar Venugopal

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 Introduction

About This Guide

If you are a security manager or administrator, then this guide is for you. You can use this guide to learn about tasks such as setting up users, roles, and privileges, managing passwords, and defining access control.

The conceptual and procedural information in the guide is generic and applies to many or all product families. For product-specific information refer to the corresponding product-specific guides if available. You must have access to the Security Console to perform the tasks covered in this guide.

Role Types

Oracle Applications Cloud defines the following types of roles.

- Job roles
- Abstract roles
- Duty roles
- Aggregate privileges

Let's look at the role types in detail.

Job Roles

Job roles represent the jobs that users perform in an organization. You can also create job roles.

Examples: General Accountant and Accounts Receivables Manager

Abstract Roles

Abstract roles represent users in the enterprise independent of the jobs they perform. You can also create abstract roles.

All users are likely to have at least one abstract role that provides access to a set of standard functions. You may assign abstract roles directly to users.

Examples: Enterprise Resource Planning Self Service User and Project Team Member

Duty Roles

Duty roles represent a logical collection of privileges that grant access to tasks that someone performs as part of a job. You can also create duty roles. Here are some duty role characteristics:

- They group multiple function security privileges.
- They can inherit aggregate privileges and other duty roles.
- You can copy and edit them.

Job and abstract roles may inherit duty roles either directly or indirectly. You don't assign duty roles directly to users.

Examples: Budget Review and Account Balance Review

Aggregate Privileges

Aggregate privileges are roles that combine the functional privilege for an individual task or duty with the relevant data security policies. Functions that aggregate privileges might grant access to include task flows, application pages, work areas, dashboards, reports, batch programs, and so on.

Aggregate privileges differ from duty roles in these ways:

- All aggregate privileges are predefined. You can't create, modify, or copy them.
- They don't inherit any type of roles.

You can include the predefined aggregate privileges in your job and abstract roles. You assign aggregate privileges to these roles directly. You don't assign aggregate privileges directly to users.

Role Inheritance

Almost every role is a hierarchy or collection of other roles.

- Job and abstract roles inherit aggregate privileges. They may also inherit duty roles.

  > **Note:** In addition to aggregate privileges and duty roles, job and abstract roles are granted many function security privileges and data security policies directly. You can explore the complete structure of a job or abstract role in the Security Console.

- Duty roles can inherit other duty roles and aggregate privileges.

When you assign roles, users inherit all of the data and function security associated with those roles.

Duty Role Components

A typical duty role consists of function security privileges and data security policies. Duty roles may also inherit aggregate privileges and other duty roles.

Data Security Policies

For a given duty role, you may create any number of data security policies. Each policy selects a set of data required for the duty to be completed and actions that may be performed on that data. The duty role may also acquire data security policies indirectly from its aggregate privileges.

These are the components of a data security policy:

- A duty role, for example Expense Entry Duty.
- A business object that's being accessed, for example Expense Reports.

- The condition, if any, that controls access to specific instances of the business object. For example, a condition may allow access to data applying to users for whom a manager is responsible.
- A data security privilege, which defines what may be done with the specified data, for example Manage Expense Report.

Function Security Privileges

Many function security privileges are granted directly to a duty role. It also acquires function security privileges indirectly from its aggregate privileges.

Each function security privilege secures the code resources that make up the relevant pages, such as the Manage Grades and Manage Locations pages.

> **Tip:** The predefined duty roles represent logical groupings of privileges that you may want to manage as a group. They also represent real-world groups of tasks. For example, the predefined General Accountant job role inherits the General Ledger Reporting duty role. You can create a General Accountant job role with no access to reporting structures. To create such a job role, copy the job role and remove the General Ledger Reporting duty role from the role hierarchy.

Aggregate Privileges

Aggregate privileges are a type of role. Each aggregate privilege combines one function security privilege with related data security policies. All aggregate privileges are predefined. This topic describes how to name and use aggregate privileges.

Aggregate Privilege Names

An aggregate privilege takes its name from the function security privilege that it includes. For example, the Promote Worker aggregate privilege includes the Promote Worker function security privilege.

Aggregate Privileges in the Role Hierarchy

Job roles and abstract roles inherit aggregate privileges directly. Duty roles may also inherit aggregate privileges. However, aggregate privileges can't inherit other roles of any type. As most function and data security in job and abstract roles is provided by aggregate privileges, the role hierarchy has few levels. This flat hierarchy is easy to manage.

Aggregate Privileges in Custom Roles

You can include aggregate privileges in the role hierarchy of a custom role. Treat aggregate privileges as role building blocks.

Create, Edit, or Copy Aggregate Privileges

You can't create, edit, or copy aggregate privileges, nor can you grant the privileges from an aggregate privilege to another role. The purpose of an aggregate privilege is to grant a function security privilege only in combination with a specific data security policy. Therefore, you must use the aggregate privilege as a single entity.

If you copy a job or abstract role, then the source role's aggregate privileges are never copied. Instead, role membership is added automatically to the aggregate privilege for the copied role.

Guidelines for Configuring Security in Oracle Applications Cloud

If the predefined security reference implementation doesn't fully represent your enterprise, then you can make changes.

For example, the predefined Line Manager abstract role includes compensation management privileges. If some of your line managers don't handle compensation, then you can create a line manager role without those privileges. To create a role, you can either copy an existing role or create a role from scratch.

During implementation, you evaluate the predefined roles and decide whether changes are needed. You can identify predefined application roles easily by their role codes, which all have the prefix *ORA_*. For example, the role code of the Payroll Manager application job role *is ORA_PAY_PAYROLL_MANAGER_JOB*. All predefined roles are granted many function security privileges and data security policies. They also inherit aggregate privileges and duty roles. To make minor changes to a role, copying and editing the predefined role is the more efficient approach. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren't represented in the security reference implementation, then you can create your own job roles. Add privileges, aggregate privileges, or duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges

If the privileges for a predefined job role don't match the corresponding job in your enterprise, then you can create your own version of the role. You can copy the predefined role and edit it to add or remove aggregate privileges, duty roles, function security privileges, and data security policies, as appropriate.

Predefined Roles with Missing Privileges

If the privileges for a job aren't defined in the security reference implementation, then you can create your own duty roles. However, a typical implementation doesn't use custom duty roles. You can't create aggregate privileges.

Related Topics

- Options for Reviewing Predefined Roles

2 Security Console

Overview

Use the Security Console to manage application security in your Oracle Applications Cloud service. You can do tasks related to role management, role analysis, user account management, and certificate management.

Security Console Access

You must have the IT Security Manager role to use the Security Console. This role inherits the Security Management and Security Reporting duty roles.

Security Console Tasks

You can do these tasks on the Security Console:

- Roles
  - Create job, abstract, and duty roles.
  - Edit custom roles.
  - Copy roles.
  - Compare roles.
  - Visualize role hierarchies and assignments to users.
  - Review Navigator menu items available to roles or users.
  - Identify roles that grant access to Navigator menu items and privileges required for that access.
- Users
  - Create user accounts.
  - Review, edit, lock, or delete existing user accounts.
  - Assign roles to user accounts.
  - Reset users' passwords.
- Analytics
  - Review statistics of role categories, the roles belonging to each category, and the components of each role.
  - View the data security policies, roles, and users associated with each data resource.
- Certificates
  - Generate, export, or import PGP or X.509 certificates, which establish encryption keys for data exchanged between Oracle Cloud applications and other applications.
  - Generate signing requests for X.509 certificates.
- Administration

- 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.

Configure the Security Console

Before you start using the Security Console, ensure that you run the background processes that refresh security data. You can use the Security Console Administration pages to select the general options, role-oriented options, and track the status of role-copy jobs.

You can also select, edit, or add notification templates.

Run the Background Processes

Here are the background processes you must run:

- **Retrieve Latest LDAP Changes** - This process copies data from the LDAP directory to the Oracle Cloud Applications Security tables. Run this process once, before you start the implementation.
- **Import User and Role Application Security Data** - This process imports users, roles, privileges, and data security policies from the identity store, policy store, and Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables.

To run the **Retrieve Latest LDAP Changes** process:

1. In the Setup and Maintenance work area, go to the **Run User and Roles Synchronization Process** task in the Initial Users functional area.
2. If you want to be notified when this process ends select the corresponding option.
3. Click **Submit**.
4. Review the confirmation message and click **OK**.

To run the **Import User and Role Application Security Data** process:

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User and Role Application Security Data** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set Run to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Days Between Runs** to **1**.
8. Enter start and end dates and times. The start time should be after any daily run of the **Send Pending LDAP Requests** process completes.
9. Click **Submit**.
10. Click **OK** to close the confirmation message.

Configure the General Administration Options

1. On the Security Console, click **Administration**.
2. In the Certificate Preferences section, set the default number of days for which a certificate remains valid. Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications.
3. In the Synchronization Process Preferences section, specify the number of hours since the last run of the **Import User and Role Application Security Data** process. When you select the Roles tab, a warning message appears if the process hasn't been run in this period.

Configure the Role Administration Options

1. On the Security Console, click **Administration**.
2. On the Roles tab, specify the prefix and suffix that you want to add to the name and code of role copies. Each role has a Role Name (a display name) and a Role Code (an internal name). A role copy takes up the name and code of the source role, with this prefix or suffix (or both) added. The addition distinguishes the copy from its source. By default, there is no prefix, the suffix for a role name is "Custom," and the suffix for a role code is "_CUSTOM."
3. In the **Graph Node Limit** field, set the maximum number of nodes a visualization graph can display. When a visualization graph contains a greater number of nodes, the visualizer recommends the table view.
4. Deselect **Enable default table view**, if you want the visualizations generated from the Roles tab to have the radial graph view.

View the Role Status

1. On the Security Console, click **Administration**.
2. On the Role Status tab, you can view records of jobs to copy roles. These jobs are initiated on the Roles page. Job status is updated automatically until a final status, typically Completed, is reached.
3. Click the **Delete** icon to delete the row representing a copy job.

Retrieve Latest LDAP Changes

Information about users and roles in your LDAP directory is available automatically to Oracle Cloud Applications. However, in specific circumstances you're recommended to run the Retrieve Latest LDAP Changes process. This topic describes when and how to run Retrieve Latest LDAP Changes.

You run **Retrieve Latest LDAP Changes** if you believe data-integrity or synchronization issues may have occurred between Oracle Cloud Applications and your LDAP directory server. For example, you may notice differences between roles on the Security Console and roles on the Create Role Mapping page. You're also recommended to run this process after any release update.

Run the Process

Sign in with the IT Security Manager job role and follow these steps:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.

The Schedule New Process dialog box opens.

3. In the **Name** field, search for and select the **Retrieve Latest LDAP Changes** process.
4. Click **OK** to close the Schedule New Process dialog box.
5. In the Process Details dialog box, click **Submit**.
6. Click **OK**, then **Close**.
7. On the Scheduled Processes page, click the **Refresh** icon.

   Repeat this step periodically until the process completes.

Note: Only one instance of **Retrieve Latest LDAP Changes** can run at a time.

Security Visualizations

A Security Console visualization graph consists of nodes that represent security items. These may be users, roles, privileges, or aggregate privileges. Arrows connect the nodes to define relationships among them.

You can trace paths from any item in a role hierarchy either toward users who are granted access or toward the privileges roles can grant.

You can select one of the following two views:

- Radial: Nodes form circular (or arc) patterns. The nodes in each circular pattern relate directly to a node at the center. That focal node represents the item you select to generate a visualization, or one you expand in the visualization.
- Layers: Nodes form a series of horizontal lines. The nodes in each line relate to one node in the previous line. This is the item you select to generate a visualization, or the one you expand in the visualization.

For example, a job role might consist of several duty roles. You might select the job role as the focus of a visualization (and set the Security Console to display paths leading toward privileges):

- The Radial view initially shows nodes representing the duty roles encircling a node representing the job role.
- The Layers view initially shows the duty-role nodes in a line after the job-role node.

You can then manipulate the image, for example, by expanding a node to display the items it consists of.

Alternatively, you can generate a visualization table that lists items related to an item you select. For example, a table may list the roles that descend from a role you select, or the privileges inherited by the selected role. You can export tabular data to an Excel file.

Related Topics

- Generate a Visualization
- Options for Viewing a Visualization Graph
- Visualization Table Display Options

Options for Viewing a Visualization Graph

Within a visualization graph, you can select the Radial or Layers view. In either view, you can zoom in or out of the image. You can expand or collapse nodes, magnify them, or search for them.

You can also highlight nodes that represent types of security items.

1. To select a view, click Switch Layout in the Control Panel, which is a set of buttons on the visualization.
2. Select Radial or Layers.

Node Labels

You can enlarge or reduce a visualization, either by expanding or collapsing nodes or by zooming in or out of the image. As you do, the labels identifying nodes change:

- If the image is large, each node displays the name of the item it represents.
- If the image is small, symbols replace the names: U for user, R for role, S for predefined role, P for privilege, and A for aggregate privilege.
- If the image is smaller, the nodes are unlabeled.

Regardless of labeling, you can hover over a node to display the name and description of the user, role, or privilege it represents.

Nodes for each type of item are visually depicted such that item types are easily distinguished.

Expand or Collapse Nodes

To expand a node is to reveal roles, privileges, or users to which it connects. To collapse a node is to hide those items. To expand or collapse a node, select a node and right-click or just double-click on the node.

Using Control Panel Tools

Apart from the option to select the Radial or Layers view, the Control Panel contains these tools:

- Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.
- Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.
- Zoom to Fit: Center the image and size it so that it's as large as it can be while fitting entirely in its display window. (Nodes that you have expanded remain expanded.)
- Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area covered by the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.
- Search: Enter text to locate nodes whose names contain matching text. You can search only for nodes that the image is currently expanded to reveal.
- Control Panel: Hide or expose the Control Panel.

Using the Legend

A Legend lists the types of items currently on display. You can take the following actions:

- Hover over the entry for a particular item type to locate items of that type in the image. Items of all other types are grayed out.
- Click the entry for an item type to disable items of that type in the image. If an item of that type has child nodes, it's grayed out. If not, it disappears from the image. Click the entry a second time to restore disabled items.
- Hide or expose the Legend by clicking its button.

Using the Overview

On the image, click the plus sign to open the Overview, a thumbnail sketch of the visualization. Click any area of the thumbnail to focus the actual visualization on that area.

Alternatively, you can click the background of the visualization and move the entire image in any direction.

Refocusing the Image

You can select any node in a visualization as the focal point for a new visualization: Right-click a node, then select Set as Focus.

> **Note:** You can review role hierarchies using either a tabular or a graphical view. The default view depends on the setting of the **Enable default table view** option on the Administration tab.

Related Topics

- Visualization Table Display Options

Visualization Table Display Options

A visualization table contains records of roles, privileges, or users related to a security item you select.

The table displays records for only one type of item at a time:

- If you select a privilege as the focus of your visualization, select the Expand Toward Users option. Otherwise the table shows no results. Then use the Show option to list records of either roles or users who inherit the privilege.
- If you select a user as the focus of your visualization, select the Expand Toward Privileges option. Otherwise the table shows no results. Then use the Show option to list records of either roles or privileges assigned to the user.
- If you select any type of role or an aggregate privilege as the focus of your visualization, you can expand in either direction.
    - If you expand toward privileges, use the Show option to list records of either roles lower in hierarchy, or privileges related to your focus role.
    - If you expand toward users, use the Show option to list records of either roles higher in hierarchy, or users related to your focus role.

Tables are all-inclusive:

Table Name	What it displays
Roles	Records for all roles related directly or indirectly to your focus item. For each role, inheritance columns specify the name and code of a directly related role.
Privileges	Records for all privileges related directly or indirectly to your focus item. For each privilege, inheritance columns display the name and code of a role that directly owns the privilege.
Users	Records for all user assigned roles related directly or indirectly to your focus item. For each user, Assigned columns display the name and code of a role assigned directly to the user.

The table columns are search-enabled. Enter the search text in a column field to get the records matching your search text. You can export a table to Excel.

Generate a Visualization

The Roles tab of the Security Console lets you generate a visualization. You can choose to view the details as a graph or as a table.

1. On the Security Console, click **Roles**.
2. Search for the security item on which you want to base the visualization.
    - In a Search field, select any combination of item types, for example, job role, duty role, privilege, or user.
    - In the adjacent field, enter at least three characters. The search returns the matching records.
    - Select a record.

    Alternatively, click **Search** to load all the items in a Search Results column, and then select a record.
3. Select either **Show Graph** or **View as Table** button.

    > **Note:** On the Administration page, you can determine the default view for a role.

4. In the **Expand Toward** list, select **Privileges** to trace paths from your selected item toward items lower in its role hierarchy. Or select **Users** to trace paths from your selected item toward items higher in its hierarchy.
5. If the Table view is active, select an item type in the Show list: Roles, Privileges, or Users. (The options available to you depend on your Expand Toward selection.) The table displays records of the item type you select. Note that an aggregate privilege is considered to be a role.

Simulate Navigator Menus in the Security Console

You can simulate Navigator menus available to roles or users. From a simulation, you can review the access inherent in a role or granted to a user. You can also determine how to alter that access to create roles.

Opening a Simulation

To open a simulated menu:

1. Select the Roles tab in the Security Console.
2. Create a visualization graph, or populate the Search Results column with a selection of roles or users.
3. In the visualization graph, right-click a role or user. Or, in the Search Results column, select a user or role and click its menu icon.
4. Select **Simulate Navigator**.

Working with the Simulation

In a Simulate Navigator page:

- Select **Show All** to view all the menu and task entries that may be included in a Navigator menu.
- Select **Show Access Granted** to view the menu and task entries actually assigned to the selected role or user.

In either view:

- A padlock icon indicates that a menu or task entry can be, but isn't currently, authorized for a role or user.
- An exclamation icon indicates an item that may be hidden from a user or role with the privilege for it, because it has been modified.

To plan how this authorization may be altered:

1. Click any menu item on the Simulate Navigator page.
2. Select either of the two options:
    - **View Roles That Grant Access**: Lists roles that grant access to the menu item.
    - **View Privileges Required for Menu**: Lists privileges required for access to the menu item. Lists privileges required for access to the task panel items.

Analytics for Roles

You can review statistics about the roles that exist in your Oracle Cloud instance.

On the Analytics page, click the Roles tab. Then view these analyses:

- Role Categories. Each role belongs to a category that defines some common purpose. Typically, a category contains a type of role configured for an application, for example, "Financials - Duty Roles."

  For each category, a Roles Category grid displays the number of:

    - Roles
    - Role memberships (roles belonging to other roles within the category)
    - Security policies created for those roles

  In addition, a Roles by Category pie chart compares the number of roles in each category with those in other categories.

- Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:
  - Role memberships
  - Security policies
  - Users assigned to the role
- Individual role statistics. Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.

  Click Export to export data from this page to a spreadsheet.

Analytics for Data Resources

You can review information about data security policies that grant access to a data resource, or about roles and users granted access to that resource.

1. On the Analytics page, click the Database Resources tab.
2. Select the resource that you want to review in the **Data Resource** field.
3. Click **Go**.

   Results are presented in three tables.

Data Security Policies

The Data Security Policies table documents policies that grant access to the selected data resource.

Each row documents a policy, specifying by default:

- The data privileges that it grants.
- The condition that defines how data is selected from the data resource.
- The policy name and description.
- A role that includes the policy.

For any given policy, this table might include multiple rows, one for each role in which the policy is used.

Authorized Roles

The Authorized Roles table documents roles with direct or indirect access to the selected data resource. Any given role might include the following:

- One or more data security policies that grant access to the data resource. The Authorized Roles table includes one row for each policy belonging to the role.
- Inherit access to the data resource from one or more roles in its hierarchy. The Authorized Roles table includes one row for each inheritance.

By default, each row specifies the following:

- The name of the role it documents.

- The name of a subordinate role from which access is inherited, if any. (If the row documents access provided by a data security policy assigned directly to the subject role, this cell is blank.)
- The data privileges granted to the role.
- The condition that defines how data is selected from the data resource.

Note: A role's data security policies and hierarchy might grant access to any number of data resources. However, the Authorized Roles table displays records only of access to the data resource you selected.

Authorized Users

The Authorized Users table documents users who are assigned roles with access to the selected data resource.

By default, each row specifies a user name, a role the user is assigned, the data privileges granted to the user, and the condition that defines how data is selected from the data resource. For any given user, this table might include multiple rows, one for each grant of access by a data security policy belonging to, or inherited by, a role assigned to the user.

Manipulating the Results

In any of these three tables, you can do the following actions:

- Add or remove columns. Select **View - Columns**.
- Search among the results. Select **View - Query by Example** to add a search field on each column in a table.
- Export results to a spreadsheet. Select the **Export to Excel** option available for each table.

FAQs for Security Console

What's the difference between private, personally identifiable, and sensitive information?

Private information is confidential in some contexts.

Personally identifiable information (PII) identifies or can be used to identify, contact, or locate the person to whom the information pertains.

Some PII information is sensitive.

A person's name isn't private. It's PII but not sensitive in most contexts. The names and work phone numbers of employees may be public knowledge within an enterprise, so not sensitive but PII. In some circumstances it's reasonable to protect such information.

Some data isn't PII but is sensitive, such as medical data, or information about a person's race, religion or sexual orientation. This information can't generally be used to identify a person, but is considered sensitive.

Some data isn't private or personal, but is sensitive. Salary ranges for grades or jobs may need to be protected from view by users in those ranges and only available to senior management.

Some data isn't private or sensitive except when associated with other data that is private or sensitive. For example, date or place of birth isn't a PII attribute because by itself it can't be used to uniquely identify an individual, but it's confidential and sensitive in conjunction with a person's name.

3 Implementation Users

Overview

The implementation or setup users are typically different from the Oracle Applications Cloud application users. They are usually not part of Oracle Applications Cloud organization.

So, you don't assign them any product-specific task or let them view product-specific data. But, you must assign them the required privileges to complete the application setup. You can assign these privileges through role assignment.

The initial user can do all the setup tasks and security tasks such as, resetting passwords and granting additional privileges to self and to others. After you sign in for the first time, create additional implementation users with the same setup privileges as that of the initial user. You can also restrict the privileges of these implementation users based on your setup needs.

You can assign job roles and abstract roles to users using the Security Console. Here are the roles that you can assign to the setup users:

- Application Diagnostic Administrator
- Application Implementation Consultant
- Employee
- IT Security Manager

> **Note:** The Application Implementation Consultant abstract role has unrestricted access to a large amount of data. So, assign this role to only those implementation users who do a wide range of implementation tasks and handle the setup data across environments. For users who must do specific implementation tasks, you can assign other administrator roles, such as the Financial Applications Administrator role.

If required, you can provide the same setup permissions to users that are part of your organization. You can also create administrative users with limited permissions. These users can configure product-specific settings and perform other related setup tasks.

User Accounts

The User Accounts page of the Security Console provides summaries of user accounts that you select to review.

For each account, it always provides:

- The user's login, first name, and last name, in a User column.
- Whether the account is active and whether it's locked, in a Status column.

It may also provide:

- Associated worker information, if the user account was created in conjunction with a worker record in Human Capital Management. This may include person number, manager, job title, and business unit.

- Party information, if the user account was created in conjunction with a party record created in CRM. This may include party number and party usage.

The User Accounts page also serves as a gateway to account-management actions you can complete. These include:

- Reviewing details of, editing, or deleting existing accounts.
- Adding new accounts.
- Locking accounts.
- Resetting users' passwords.

To begin working with user accounts:

1. On the Security Console, select the Users tab.
2. To perform a search, select one or more user states, select one of the user attributes (User Name, Email, First Name, or Last Name) from the drop-down list, and enter at least three characters.

   The search returns user accounts based on the selected options.

Note: On the Security Console, you can't search for users who have APPID in their user name.

User Account Details

To review full details for an existing account, search for it in the User Accounts page and click its user login in the User column. This opens a User Account Details page.

These details always include:

- User information, which consists of user category, user name, first name, last name, and an email.
- Account information, which includes the user's password-expiration date, whether the account is active, and whether it's locked.
- A table listing the roles assigned to the user, including whether they're autoprovisioned or assignable. A role is assignable if it can be delegated to another user.

The page may also include an Associated Worker Information region or an Associated Party Information region. The former appears only if the user account is related to a worker record in Human Capital Management, and the latter if the user account is related to a party record in CRM.

To edit these details, click Edit in the User Account Details page. Be aware, however:

- You can edit values only in the User Information, Account Information, and Roles regions.
- Even in those regions, you can edit some fields only if the user isn't associated with a worker or a party. If not, for example, you can modify the First Name and Last Name values in the User Information region. But if the user is associated with a worker, you would manage these values in Human Capital Management. They would be grayed out in this Edit User Details page.
- In the Roles table, Autoprovisioned check boxes are set automatically, and you can't modify the settings. The box is checked if the user obtained the role through autoprovisioning, and cleared if the role was manually assigned. You can modify the Assignable setting for existing roles.

Note: You can edit the User Name in the Edit User Account Details page. You can update the user name irrespective of whether this account is linked to a worker record in HCM or not. All the conditions that apply for creating a user name applies while updating it. The user name can be in any format and up to a maximum length of 80 characters. The user name can include multibyte characters.

Click Add Autoprovisioned Roles to add any roles for which the user is eligible. Or, to add roles manually, click Add Role. Search for roles you want to add, select them, and click Add Role Membership. You can remove all roles that are associated with a user using the corresponding button.

You can also delete roles. Click the x icon in the row for the role, and then respond to the confirmation message.

Add User Accounts

The user accounts that you add in the Security Console are used for implementation users. Usually, an implementation user sets up Oracle Fusion Cloud Human Capital Management Cloud (HCM). Then, you can use HCM to create accounts for application users.

Follow these steps to add a user account in the Security Console:

1. In the Security Console, click the **Users** tab.
2. On the User Accounts page, click the **Add User Account** button.
3. From the **Associated Person Type** list, select **Worker** to link this account to a worker record in HCM. Otherwise, leave it as **None**.
4. In the Account Information section, change the default settings if you don't want the account to be active or unlocked.
5. Fill in the User Information section.
    - Select the user category that you want to associate the user with. The user category includes a password policy and a rule that determines how the user name is automatically generated.
    - Enter the user's first name only if the rule from the selected user category makes use of the first name or the first name initial to generate user names.
    - Enter a password that conforms to the password policy from the selected user category.
6. In the Roles section, click the **Add Role** button.
7. Search for the role that you want to assign to the user and the click **Add Role Membership** button. The role is added to the list of existing roles.
8. Repeat the previous step to add more roles if required, or just click **Done**.
9. Click the **Add Auto-Provisioned Roles** button to add any roles that the user is eligible for, based on role provisioning rules. If nothing happens, that means there aren't any roles to autoprovision. You can add auto-provisioned roles only to users who have associated worker information.
10. In the Roles table, click the **Assignable** check box for any role that can be delegated to another user. The **Auto-Provisioned** column displays a tick mark if the user has roles that were assigned through autoprovisioning.
11. Click the **Delete** icon to unassign any role.
12. Click **Save and Close**.

Related Topics

- Overview of User Categories

Compare Users

You can compare users to identify their access permissions and assign the missing permissions as required. This comparison includes both direct and inherited roles. From the results, you can find out if there are any discrepancies in roles.

Users with the following privileges can compare users:

- Create User Account (ASE_CREATE_USER_ACCOUNT_PRIV)
- Edit User Account (ASE_EDIT_USER_ACCOUNT_PRIV)
- View User Account (ASE_VIEW_USER_ACCOUNT_PRIV)
- Delete User Account (ASE_DELETE_USER_ACCOUNT_PRIV)
- Lock and Unlock User Account (ASE_LOCK_UNLOCK_USER_PRIV)
- Update Password for User Account (ASE_UPDATE_PASSWORD_FOR_USER_PRIV)

On the User Accounts page, you can compare users in two different ways:

- Use the Compare Users button.
- Search for a user and then click Compare Users from the Actions menu of that user.

Follow these steps:

1. On the Security Console, click **Users**.
2. Click **Compare Users**.
3. Search for and select both users one after another.
4. Click **Compare**. All the details of both the users are displayed.

In the comparison results, you can do the following actions:

- Click one of the **Show** options to view the corresponding details in the results.
- Click the Query By Example icon to enter the name of a specific role that you want to see from the search results.

You can then use the Export to Excel option to export the filtered search results.

Copy Roles from One User to Another

If the user you're creating must have the same set of roles that an existing user has, you can consider copying the required roles instead of manually assigning them.

Adding roles manually to replicate an existing user is a time-taking task. Instead, use the Copy User option in Security Console to create the user with all the roles assigned, at one go.

There are two ways in which you can copy the roles from an existing user to another user:

- Use the Copy User option in the Actions menu of the selected user on the User Accounts page. You can copy the user category and assigned roles of the selected user. Additionally, you can copy the Enable Administration Access for Sign In-Sign Out Audit REST API setting if the Enable access to Advanced User Management Settings profile option is enabled.

- Use the Add Role button on the Add User Account page.

If you have more than 20 roles to copy, then the application runs an asynchronous process in the background. You must wait for the asynchronous process to complete before you can edit, delete, copy, or compare roles on the target user. You can view the status of up to 25 recently run asynchronous processes at any time using the User-to-User Role Membership Transfer Status tab on the Administration page.

Note: You can search for an asynchronous process based on the user name or status.

Using the Copy User Option

1. On the Security Console, click **Users**.
2. On the User Accounts page, search for the user from which you want to copy the roles.
3. From the **Action** menu of that user, click **Copy User**. On the Add User Account page, the user category and assigned roles of the selected user appear. The Enable Administration Access for Sign In-Sign Out Audit REST API setting is selected if this setting is enabled for the source user.
4. Enter the details of the user and click **Save and Close**.

Using the Add Role Button

1. On the Security Console, click **Users**.
2. On the User Accounts page, click **Add User Account**.
3. On the Add User Account page, select a user category and enter the details of the user.
4. Click **Add Role**.
5. Select **Users** from the **Search** drop-down list and search for the user from which you want to copy the roles.
6. Select the user and click **Add Role Membership from User**. A confirmation message appears.
7. Click **OK** and click **Done**.
8. Click **Save and Close**.

Related Topics

- Role Copying or Editing

Guidance for Assigning Predefined Roles

As a security administrator, you have access to the predefined roles and privileges that are readily available for assignment. However, you must assess the user's need before assigning those roles as is with the complete set of privileges.

When you assign predefined roles and privileges as is, you're entrusting users with full access to all data and functionality. Such unrestricted access without really determining the business need might pose a security concern. Also, the assigned privileges might account for subscription consumption irrespective of whether you purchased the cloud service or not. A detailed list of all the predefined roles that impact subscription is available for reference. See the spreadsheet *Predefined Roles with Subscription Impact*.

If you are aware of a requirement or recommendation to assign specific predefined roles as is, it's fine to do so. For example, only while setting up an application, you may need to assign the predefined Application Implementation Consultant role as is. Once the setup is complete, you can unassign it. Otherwise, the recommended process is to always make a copy of the predefined role, remove the privileges you don't need, and assign only the required privileges. That way, you will hit the subscription usage in a controlled way, based on your business need.

Note: Updates to Fusion Applications might also include changes to certain predefined roles. Check the release readiness documents for your product area to know if there are any updates to the predefined roles that are in use. If you find changes that are relevant, incorporate the same changes to your custom role. This will remain an ongoing maintenance activity for the custom roles.

For insights into how Oracle measures and counts Oracle Fusion licenses, see *Metrics Description for Fusion Offerings*.

Related Topics

- Compare Roles
- Role Copying or Editing
- Create Roles in the Security Console

Assign Roles to an Existing User

Use the Security Console to assign a specific role to an existing user. Or, remove roles that were already assigned to the user.

1. In the Security Console, click the **Users** tab.
2. Search for and select the user you want to assign roles to.
3. On the User Account Details page, click the **Edit** button.
4. In the Roles section, click the **Add Role** button.
5. Search for the role that you want to assign to the user and the click **Add Role Membership** button. The role is added to the list of existing roles.
6. Repeat the previous step to add more roles if required, or just click **Done**.
7. Click the **Add Auto-Provisioned Roles** button to add any roles that the user is eligible for, based on role provisioning rules. If nothing happens, that means there aren't any roles to autoprovision.
8. In the Roles table, click the **Assignable** check box for any role that can be delegated to another user. The **Auto-Provisioned** column displays a tick mark if the user has roles that were assigned through autoprovisioning.
9. Click the **Delete** icon to unassign any role.
10. Click **Save and Close**.

Reset Passwords

Use the Security Console to reset other users' passwords. The new password must conform to the password policy from the user category that's assigned to the user.

1. In the Security Console, click the **Users** tab.
2. On the User Accounts page, search for the user whose password you want to change.
3. In the **Action** drop-down list for the user, select **Reset Password**. Or, you can click the display name and then click the **Reset Password** button on the User Account Details page.
4. In the **Reset Password** dialog box, select whether to generate the password automatically or change it manually. For a manual change, enter a new password.

   Note: If you don't see the manual reset option, go to the user category assigned to the user and select the **Administrator can manually reset password** check box in the Password Policy tab of the user category.

5. Click **Reset Password**.

An email with a link to reset the password is sent to the user.

Related Topics

- Configure the Security Console
- Overview of User Categories

Delete User Accounts

An administrator may use the Security Console to delete users' accounts.

1. Open the User Accounts page and search for the user whose account you want to delete.
2. In the user's row, click the Action icon, then Delete.
3. Respond Yes to a confirmation message.

Get User Sign-in Sign-out Information

You can get the last seven days of user sign-in sign-out information using a setting available on the Add User Account page in Security Console. To view the setting, you must enable a profile option.

You can access the sign-in sign-out information through REST APIs. For more information, see the topic Sign In and Sign Out Audit REST Endpoints in *REST API for Common Features in Oracle Fusion Cloud Applications* on the Oracle Help Center.

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search the following **Profile Option Code**:
   ASE_ADVANCED_USER_MANAGEMENT_SETTING
3. In the **Profile Value** drop-down list, select **Yes**.
4. Click Save and Close.

Note: The audit data is available for seven days.

The profile option is enabled. On the Add User Account page in Security Console, the setting to get user sign-in sign-out information appears now in the Advanced Information section.

On the Security Console, click **Users**. On the User Accounts page, click **Add User Account** and select **Enable Administration Access for Sign In-Sign Out Audit REST API**. You can also enable this option on the User Account Details Edit page.

Create Notification Templates

Users may receive Email notifications of user account events, such as account creation or password expiration. These notifications are generated from a set of templates, each of which specifies an event.

A template generates a message to a user when that user is involved in the event tied to the template.

You can enable or disable templates, edit templates, or create templates to replace existing ones. There are 16 events, and a predefined template exists for each event. You can enable only one template linked to a given event at a time.

Here's how you can create a template:

1. Click the **User Categories** tab in the Security Console.
2. Select a user category and on the **User Category Information** page, click the **Notifications** tab.
3. Click the **Edit** button to make changes.

   Ensure that the **Enable Notifications** check box is selected.
4. Click **Add Template**.
5. Specify a name and description for the template.
6. Select **Enabled** to use the template immediately. If selected, template that had been enabled for the event which you select, is automatically disabled.
7. Select an **Event** from the corresponding drop-down list.

   The values for **Message Subject** and **Message** are copied from an already-configured template for which the same event is selected.
8. Update the **Message Subject** and **Message** as required.

   > **Note:** The message text includes tokens which are replaced in runtime by literal values appropriate for a given user or account.

9. Click **Save and Close**.

To edit a template, select it from the templates listed in the Notification Templates table. Then follow the same process as you would to create a template. You can't modify the event selected for a template that has been saved. You cam only enable or disable an individual template when you edit it.

> **Note:** You can't edit or delete predefined templates that begin with the prefix name **ORA**. You also can't modify the message subject or the message. However, you can only enable or disable the predefined templates.

You can delete the templates you created. Select the template row in the table and click **Delete**.

Here's the table that lists the tokens that you can use in the message text for a template:

Token	Meaning	Events
`${userLoginId}`	The user name of the person whose account is being created or modified.	• Forgot user name • Password expired • Password reset confirmation • New account created
`${firstName}`	The given name of the person whose account is being created or modified.	• Administration activity location based access disabled confirmation • Administration activity requested • Administration activity single sign-on disabled confirmation • Expiring external IDP signing certificate

Token	Meaning	Events
		• Expiring service provider encryption certificate • Expiring service provider signing certificate • Forgot user name • New account created - manager • New user created • Password expired • Password expiry warning • Password generated • Password reset • Password reset - manager • Password reset confirmation • Password reset confirmation - manager
`${lastName}`	The surname of the person whose account is being created or modified.	• Administration activity location based access disabled confirmation • Administration activity requested • Administration activity single sign-on disabled confirmation • Expiring external IDP signing certificate • Expiring service provider encryption certificate • Expiring service provider signing certificate • Forgot user name • New account created - manager • New user created • Password expired • Password expiry warning • Password generated • Password reset • Password reset - manager • Password reset confirmation • Password reset confirmation - manager
`${managerFirstName}`	The given name of the person who manages the person whose account is being created or modified.	• New account created - manager • Password reset confirmation - manager • Password reset - manager
`${managerLastName}`	The surname of the person who manages the person whose account is being created or modified.	• New account created - manager • Password reset confirmation - manager

Token	Meaning	Events
		• Password reset - manager
`${loginUrl}`	The web address to sign in to Oracle Cloud. The user can sign in and use the Preferences page to change a password that's about to expire. Or, without signing in, the user can engage a forgot-password procedure to change a password that has already expired.	• Expiring external IDP signing certificate • Password expired • Password expiry warning
`${resetUrl}`	A one-time web address expressly for the purpose of resetting a password, used in the Password Generated, Password Reset, New Account, and New Account Manager templates.	• New account created - manager • New user created • Password generated • Password reset • Password reset - manager
`${CRLFX}`	Insert line break.	All events
`${SP4}`	Insert four spaces.	All events
`${adminActivityUrl}`	A URL of the page in which an administrator initiates an administration activity.	Administration activity requested
`${providerName}`	The name of an external Identity Provider.	Expiring external IDP signing certificate
`${signingCertDN}`	The signing certificate of an external Identity Provider.	Expiring external IDP signing certificate
`${signingCertExpiration}`	The expiration date of the external Identity Provider signing certificate or of the service provider signing certificate.	• Expiring external IDP signing certificate • Expiring service provider signing certificate
`${encryptionCertExpiration}`	The expiration date of the Service Provider encryption certificate.	Expiring service provider encryption certificate
`${adminFirstName}`	The given name of the person who has administrator rights.	• Administration activity location based access disabled confirmation • Administration activity single sign-on disabled confirmation
`${adminLastName}`	The surname of the person who has administrator rights.	• Administration activity location based access disabled confirmation • Administration activity single sign-on disabled confirmation

Synchronize User and Role Information

You run the process Retrieve Latest LDAP Changes once during implementation. This process copies data from the LDAP directory to the Oracle Fusion Applications Security tables. Thereafter, the data is synchronized automatically.

To run this process, perform the task **Run User and Roles Synchronization Process** as described in this topic.

Run the Retrieve Latest LDAP Changes Process

Follow these steps:

1. Sign in to your Oracle Applications Cloud service environment as the service administrator.
2. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Initial Users
    - Task: Run User and Roles Synchronization Process
3. On the process submission page for the **Retrieve Latest LDAP Changes** process:
    a. Click **Submit**.
    b. Click **OK** to close the confirmation message.

Reset the Cloud Service Administrator Sign-In Details

After setting up your implementation users, you can reset the service administrator sign-in details for your Oracle Applications Cloud service. You reset these details to avoid problems later when you're loaded to the service as an employee.

Sign in to your Oracle Applications Cloud service using the TechAdmin user name and password and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
    - Functional Area: Initial Users
    - Task: Create Implementation Users

    > **Note:** If you can't see this task, make sure you've selected All Tasks in the **Show** drop-down list.
2. On the User Accounts page of the Security Console, search for your service administrator user name, which is typically your email. Your service activation mail contains this value.
3. In the search results, click your service administrator user name to open the User Account Details page.
4. Click **Edit**.
5. Change the **User Name** value to **ServiceAdmin**.
6. Delete any value in the **First Name** field.
7. Change the value in the **Last Name** field to **ServiceAdmin**.
8. Delete the value in the **Email** field.
9. Click **Save and Close**.

10. Sign out of your Oracle Applications Cloud service.

After making these changes, you use the user name ServiceAdmin when signing in as the service administrator.

4 User Categories

Overview of User Categories

You can categorize and segregate users based on the various functional and operational requirements. A user category provides you with an option to group a set of users such that the specified settings apply to everyone in that group.

Typical scenarios in which you may want to group users are:

- Users have different preferences in receiving automated notifications from the Security Console. For example, employees of your organization using the organization's single sign-on don't require notifications from the Security Console about creating new users, password expiry, or password reset. However, the suppliers of your organization who aren't using the organization's single sign-on, must receive such notifications from the Security Console.
- You have built an external application for a group of users using the REST APIs of Oracle Fusion Applications. You intend to redirect this user group to the external application when using the Security Console to reset passwords or create new users.

On the Security Console page, click the User Category tab. You can perform the following tasks:

- Segregate users into categories
- Specify Next URL
- Set user preferences

Segregate Users into Categories

Create user categories and add existing users to them. All existing users are automatically assigned to the Default user category unless otherwise specified. You may create more categories depending upon your requirement and assign users to those categories.

Note: You can assign a user to only one category.

Specify Next URL

Specify a URL to redirect your users to a website or an application instead of going back to the Sign In page, whenever they reset their password. For example, a user places a password reset request and receives an Email for resetting the password. After the new password is authenticated, the user can be directed to a website or application. If nothing is specified, the user is directed to Oracle Applications Cloud Sign In page. You can specify only one URL per user category.

Set User Preferences

Select the format of the User Name, the value that identifies a user when signed in. It is generated automatically in the format you select. Options include first and last name delimited by a period, email address, first-name initial and full last name, and person or party number. Select the check box **Generate system user name when generation rule fails** to enable the automatic generation of User Name values if the selected generation rule can't be implemented.

Related Topics

- Add Users to a User Category
- How can I direct users to a specific application or website after password reset?

Define Password Policy

Creating a password policy lets you set up the rules or conditions for the use of password by all users in your organization.

You can define a password policy for a user category so that it applies to all the users of that user category.

1. On the User Category: Details page, click **Password Policy**.
2. Click **Edit**.
3. Set the following values:
    - **Days Before Password Expiration** – Specifies the number of days for which a password remains valid. After this period, users must reset their passwords. By default, users whose passwords expire must use the Forgot Password option.
    - **Days Before Password Expiry Warning** – Specifies when a user is notified that a password is about to expire. By default, users are prompted to sign in and change their passwords. This value must be equal to or less than the value of the **Days Before Password Expiration** option.

      > **Note:** Make sure that the value you provide for **Days Before Password Expiry Warning** is lesser than the value for **Days Before Password Expiration**. Otherwise, there wouldn't be enough time for users to respond to the expiry warning notification.

    - **Hours Before Password Reset Token Expiration** – Specifies how long a reset-password link remains active, in the notification email that's sent when users request a password reset. If the link expires before the password is reset, then reset must be requested again.

      > **Note:** The Password Expiry Report sends the password expiration warning and password expired notifications. We recommend that you schedule this report to run daily to help users know when their passwords have to be reset.

4. Select a password complexity type that defines a password format. The parameters and their values automatically change based on the selected option.

    Password Complexity Options

Complexity Type	Requirement
Simple	Must contain at least 8 characters, 1 number. This is the default complexity type.
Complex	Must contain at least 8 characters, 1 uppercase, 1 number
Very Complex	Must contain at least 8 characters, 1 uppercase, 1 number, 1 special character
Custom	Provides the flexibility to specify a combination of parameters to define a custom password. By default, the parameters are populated with predefined set of values to get you started.

Complexity Type	Requirement
	Note: For more information about defining custom password, see topic Configure a Custom Password Policy in the Related Topics section.

5. Select **Disallow last password** to ensure that the new password is different from the last password. If the user requests password reset by selecting **Settings and Actions** > **Set Preferences** > **Password**, then this option determines whether the last password can be reused. However, when a user's password expires, the user can reuse the last password. This option doesn't affect password reuse after expiry. This option doesn't take affect the first time a password is reset if a user is moved from a user category that didn't have the **Disallow last password** option checked.
6. Leave the **Administrator can manually reset password** option selected. Passwords can be either generated automatically or reset manually by the IT Security Manager. Select this option to allow user passwords to be reset manually. All passwords, whether reset manually or generated automatically, must satisfy the current complexity rule.

   Note: If you deselect this option, then the Reset Password dialog box doesn't display the option to manually change the password. The application automatically resets the password when the user requests it.
7. Click **Save and Close**.

Related Topics

- Password Expiry Report
- Configure a Custom Password Policy

Enable Notifications

Notifications are enabled by default, but you can disable them if required.

You can also enable or disable notifications separately for each user category. If users belonging to a specific category don't want to receive any notification, you can disable notifications for all life-cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events.

Notifications are sent for a set of predefined events. To trigger a notification, you must create a notification template and map it to the required event. Depending on the requirement, you can add or delete a template that's mapped to a particular event.

Note: You can't edit or delete predefined notification templates that begin with the prefix ORA. You can only enable or disable them. However, you can update or delete the user-defined templates.

User Category feature supports both SCIM protocol and HCM Data Loader for performing any bulk updates.

Note: Both pending workers and terminated workers receive emails at their personal email address.

Related Topics

- Create Notification Templates
- How can I enable or disable notifications for users?

Add Users to a User Category

Using the Security Console, you can add existing users to an existing user category or create a new category and add them. When you create new users, they're automatically assigned to the default category.

At a later point, you can edit the user account and update the user category. You can assign a user to only one category.

Note: If you're creating new users using Security Console, you can also assign a user category at the time of creation.

You can add users to a user category in three different ways:

- Create a user category and add users to it
- Add users to an existing user category
- Specify the user category for an existing user

Note: You can create and delete a user category only using the Security Console. Once the required user categories are available in the application, you can use them in SCIM REST APIs and data loaders. You can't rename a user category.

Adding Users to a New User Category

To create a user category and add users:

1. On the Security Console, click **User Categories** > **Create**.
2. Click **Edit**, specify the user category details, and click **Save and Close**.
3. Click the Users tab and click **Edit**.
4. On the Users Category: Users page, click **Add**.
5. In the Add Users dialog box, search for and select the user, and click **Add**.
6. Repeat adding users until you have added the required users and click **Done**.
7. Click **Done** on each page until you return to the User Categories page.

Adding Users to an Existing User Category

To add users to an existing user category:

1. On the Security Console, click **User Categories** and click an existing user category to open it.
2. Click the Users tab and click **Edit**.
3. On the Users Category: Users page, click **Add**.
4. On the Add Users dialog box, search for and select the user, and click **Add**.
5. Repeat adding users until you have added the required users and click **Done**.
6. Click **Done** on each page until you return to the User Categories page.

Specifying the User Category for an Existing User

To add an existing user to a user category:

1. On the Security Console, click **Users**.
2. Search for and select the user for whom you want to specify the user category.
3. On the User Account Details page, click **Edit**.
4. In the User Information section, select the **User Category**. The Default user category remains set for a user until you change it.
5. Click **Save and Close**.
6. On the User Account Details page, click **Done**.

You can delete user categories if you don't require them. However, you must ensure that no user is associated with that user category. Otherwise, you can't proceed with the delete task. On the User Categories page, click the **X** icon in the row to delete the user category.

Notifications for Users Based on Status

Security Console sends notifications to users for important events that occur in the application. However, some notifications aren't sent to users if they're inactive or have been locked out of the application.

Here's the list of notifications that are either sent or not sent to users based on their status:

Template Name	Event Name	When is the notification sent?	Sent to Inactive Users?	Sent to Locked Users?
ORA Expiring External IDP Signing Certificate	Expiring External IDP Signing Certificate	When an external identity provider certificate is about to expire	No	Yes
ORA Expiring Service Provider Encryption Certificate	Expiring service provider encryption certificate	When a service provider encryption certificate is about to expire	No	Yes
ORA Expiring Service Provider Signing Certificate	Expiring service provider signing certificate	When a service provider signing certificate is about to expire	No	Yes
ORA Forgot User Name	Forgot user name	When a forgot user name request is processed	No	Yes
ORA Password Expiration	Password expired	When a password has expired	No	No
ORA Password Expiry Warning	Password expiry warning	When a password expiry warning is sent	No	No

Template Name	Event Name	When is the notification sent?	Sent to Inactive Users?	Sent to Locked Users?
ORA Password Reset Confirmation Manager	Password reset confirmation - manager	When a password is changed and the manager must be notified	No	Yes
ORA Password Reset Confirmation	Password reset confirmation	When a password is changed	No	Yes
ORA Password Reset Manager	Password reset - manager	When a password is reset and the manager must be notified	No	Yes
ORA Password Reset	Password reset	When a password reset request is processed	No	Yes
ORA Administration Activity Request Template	Administration activity request	When an administrator initiates an administration activity	Yes	Yes
ORA Location Based Access Disabled Confirmation	Administration activity location-based access disabled confirmation	When an administrator disables location-based access through an administration activity request	Yes	Yes
ORA New Account Manager	New account created - manager	When a new account request is processed and the manager must be notified	Yes	Yes
ORA New Account	New user created	When a new account request is processed	Yes	Yes
ORA Password Generated	Password generated	When a password is issued	Yes	Yes
ORA Single Sign-On Disabled Confirmation	Administration activity single sign-on disabled confirmation	When an administrator disables single sign-on through an administration activity request	Yes	Yes

Configure a Custom Password Policy

Single Sign-On (SSO) configuration enforces users to use complex passwords. But, some users might want to use simpler passwords that don't enforce the use of minimum number of digits or characters. Using Security Console, you can create a custom password policy for such users.

Since password policies are linked with user categories, you can define a custom password policy for a specific user category. The policy automatically applies all users in that user category. However, there are a few conditions for creating a custom password policy. Users who use an SSO password can't use a custom password because their organization sets the SSO password policy. You can't create a custom password policy using the default Simple, Complex, and Very Complex password complexity options. You must use the Custom option and set values based on your security requirements.

1. On the Security Console, click **User Categories**.
2. Select a user category for which you want to create a custom password policy.
3. Click **Password Policy** > **Edit**.
4. Select **Custom** in the **Password Complexity** drop-down list.
5. Enter the values for all the password parameters as required.
6. Click **Save and Close**.

If you add existing users to the selected user category, then the custom password policy is enforced when they reset their password. If you want to create more custom passwords, then you must create user categories for each custom password.

Enable Multifactor Authentication

Multifactor Authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user's identity.

With MFA enabled in OCI IAM identity domain, when a user signs in to an application, they are prompted for their user name and password, which is the first factor – something that they know. The user is then required to provide a second type of verification. This is called 2-Step Verification. The two factors work together to add an additional layer of security by using either additional information or a second device to verify the user's identity and complete the login process.

Users are increasingly connected, accessing their accounts and applications from anywhere. As an administrator, when you add MFA on top of the traditional user name and password, that helps you to protect access to data and applications. This also reduces the likelihood of online identity theft and fraud, which secures your business applications even if an account password is compromised.

With the identity service upgrade to the Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain, you can enable MFA for signing in to Oracle Fusion Cloud Applications. Oracle Fusion Cloud Applications leverages the MFA functionality available within the OCI IAM identity domain and supports six different factors. Security administrators can choose among these six factors and make them available for users to set up MFA. Users can set up MFA with the provisioned factors when they sign-in. MFA is supported only in non-federated single sign-on (SSO) environments. Here are the six factors:

- One-Time PIN over Email
- One-Time PIN over SMS
- Passcode on Oracle Mobile Authenticator
- Push-based notification from Oracle Mobile Authenticator
- FIDO Passkey Authenticator
- Bypass code

For the One-Time PIN over SMS factor, the work mobile is used as the phone number for authentication. User details such as phone number (work mobile) and email (work email) are stored in the product-specific user settings in Oracle Fusion Cloud Applications, and not on the OCI IAM identity domain.

After the identity upgrade, you can run the Send Personal Data for Multiple Users to LDAP Process to copy the phone number (work mobile) of all existing users to the OCI IAM identity domain. To manage the MFA settings in Security Console, you must be assigned a custom role based on the IT Security Manager role.

Determine the Authentication Factors Available to Users

Security administrators can assess their authentication requirements and decide on the number of factors to be enabled.

1. On the User Categories page of Security Console, select the user category that's associated with the target users.
2. Click **Two-Factor Authentication**.
3. Click **Edit**.
4. Select all the authentication options that you want for your users

   One-Time PIN over Email, One-Time PIN over SMS, and Passcode on Oracle Mobile Authenticator are selected by default, but you can modify if required.

After you enable MFA, when users of that user category sign in to Oracle Fusion Cloud Applications, they'll be redirected to the Oracle Cloud Console page and prompted to enable secure verification for themselves. See *Set Up Multifactor Authentication Methods*.

Enable Passwordless Authentication

Passwordless authentication lets users sign in without entering their user name and password every time.

The first time the user signs in, they enter their user name and password on the standard sign-in page. The next time, and on future occasions, the user is shown two pages when they sign in. In the first page, the user provides their user name, and then clicks Sign in. OCI IAM identity domain evaluates the authentication factors (such as Email, Mobile App notification, or Mobile App passcode) that are available to use to sign in to Oracle Fusion Cloud Applications. The authentication factors appear in the second sign in page. The user uses one of the authentication factors to access Oracle Fusion Cloud Applications.

Passwordless authentication is sometimes confused with Multifactor Authentication (MFA). Both MFA and passwordless authentication use a wide variety of authentication factors, but MFA is often used as an extra layer of security on top of regular password-based authentication. Whereas passwordless authentication doesn't require a memorized secret and usually uses just one secure factor to authenticate identity, making it faster and simpler for users.

If you later choose to turn off passwordless authentication, then the user can authenticate to Oracle Fusion Cloud Applications at the sign-in page by providing their credentials (user name and password), or by using a SAML or identity provider.

To define passwordless authentication, you must be assigned the IT Security Manager role.

Prerequisite to Enable Passwordless Authentication

Before enabling passwordless authentication, make sure that every user has at least one MFA factor enabled.

> **Note:** Once passwordless authentication is enabled, it's applicable for all users.

Configure Passwordless Authentication

If passwordless authentication enabled, users can use their phone number or email as the user name on the sign-in page. Once enabled, when signing in for the first time, only the user name is displayed on the sign-in page and there's no option to enter password. On entering the user name in the sign-in page, users are prompted with the MFA options that were configured by the administrator.

1. In the Oracle Cloud console, expand the Navigation Drawer, select **Settings**, and then click **Session Settings**.
2. In the **Session Settings** page, select **Enable User Name First**.
3. Click **Save**.

User Sign-In Experience

After you have configured passwordless authentication for your users, their sign-in experience changes.

1. The sign in page has only a username field. There isn't a password field.
2. The user enters their user name, and they select **Sign In**.
3. A second page appears where they enter the verification required by the authentication factor you have chosen, for example a passcode in an email.
4. If there is more than one passwordless authentication factor, the user can select **Show alternative login methods** to choose a different one.

FAQs for User Categories

How can I direct users to a specific application or website after password reset?

Use this task if you want to direct your users to another application or a website instead of the Oracle Applications Cloud sign in page, after they reset the password.

Using the Security Console, you can specify the URL of the application or the website to which the users can be directed.

1. On the Security Console, click User Category.
2. Select the user category and on the User Category: Details page, click **Edit**.
3. Specify the URL in the Next URL field and click **Save and Close**.

When users of that user category successfully reset their password, they're automatically redirected to the specified application or the web page instead of the Oracle Applications Cloud sign in page.

Related Topics

- Reset Passwords

How can I enable or disable notifications for users?

Using the Security Console, you can determine whether to turn notifications on or off for the users.

1. On the Security Console, click User Categories and from the list, select the specific user category.

2. Click the Notifications tab and click **Edit**.
3. Select the **Enable Notifications** check box to enable notifications for all users of that user category. To disable notifications, deselect the check box.
4. Click **Save**.

To determine which notifications to send, you have to enable the notification template for each required event.

Related Topics

- Create Notification Templates

How can I enable notifications for pending workers?

You can send notifications to the personal email address of pending workers and terminated workers. To send the notification, you must enable the ORA_PER_USER_ACCOUNT_NOTIFY_HOME_EMAIL profile option.

1. In the Setup and Maintenance work area, go to the **Manage Administrator Profile Values** task.
2. On the Manage Administrator Profile Values page, search for and select the ORA_PER_USER_ACCOUNT_NOTIFY_HOME_EMAIL profile option code.
3. In the Profile Values section, enter **Y** as the profile value.
4. Click **Save and Close**.

Why don't I see my user name in the forgot password email notification?

That's because there are two user names associated with your email address. The application can include only one user name in the email notification.

Why don't I see my user name in the forgot user name email notification?

That's because there are two user names associated with your email address. The application can include only one user name in the email notification.

5 Application Users Management

Overview of Application Users

During implementation, you prepare your Oracle Applications Cloud service for application users. Decisions made during this phase determine how you manage users by default. Most of these decisions can be overridden.

However, for efficient user management, you're recommended to configure your environment to both reflect enterprise policy and support most or all users.

The following table lists some key decisions and tasks that are explained in this chapter.

Decision or Task	Topic
Whether user accounts are created automatically for application users	User Account Creation Option: Explained
How user names are formed	Default User Name Format Option: Explained
How role provisioning is managed	User Account Role Provisioning Option: Explained
Whether user accounts are maintained automatically	User Account Maintenance Option: Explained
Whether and where user sign-in details are sent	Send User Name and Password Option: Explained
Understanding user account password policy	Password Policy: Explained
Ensuring that the employee, contingent worker, and line manager abstract roles are provisioned automatically either within a Human Capital Management setup or by using the Create Users user interface.	Provisioning Abstract Roles to Users Automatically: Procedure

User and Role-Provisioning Setup Options

User and role-provisioning options control the default management of some user account features. To set these options, perform the Manage Enterprise HCM Information task in the Workforce Structures functional area for your offering. You can edit these values and specify an effective start date.

User Account Creation

The **User Account Creation** option controls:

- Whether user accounts are created automatically when you create a person, user, or party record
- The automatic provisioning of roles to users at account creation

> **Note:** User accounts without roles are suspended automatically. Therefore, roles are provisioned automatically at account creation to avoid this automatic suspension.

The **User Account Creation** option may be of interest if:

- Some workers don't need access to Oracle Applications Cloud.
- Your existing provisioning infrastructure creates user accounts, and you plan to integrate it with Oracle Applications Cloud.

User Account Role Provisioning

After a user account exists, users both acquire and lose roles as specified by current role-provisioning rules. For example, managers may provision roles to users manually, and the termination process may remove roles from users automatically. You can control role provisioning by setting the **User Account Role Provisioning** option.

> **Note:** Roles that you provision to users directly on the Security Console aren't affected by this option.

User Account Maintenance

The **User Account Maintenance** option controls whether user accounts are suspended and reactivated automatically. By default, a user's account is suspended automatically when the user is terminated and reactivated automatically if the user is rehired.

User Account Creation for Terminated Workers

The **User Account Creation for Terminated Workers** option controls whether user account requests for terminated workers are processed or suppressed. This option takes effect when you run the **Send Pending LDAP Requests** process.

Related Topics

- User Account Creation Option
- User Account Role Provisioning Option
- User Account Maintenance Option
- User Account Creation for Terminated Workers Option

User Account Creation Option

The User Account Creation option controls whether user accounts are created automatically when you create a person or party record. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **User Account Creation** option values.

Value	Description
Both person and party users	User accounts are created automatically for both person and party users. This value is the default value.
Party users only	User accounts are created automatically for party users only. User accounts aren't created automatically when you create person records. Instead, account requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.
None	User accounts aren't created automatically. All user account requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.

If user accounts are created automatically, then role provisioning also occurs automatically, as specified by current role mappings when the accounts are created. If user accounts aren't created automatically, then role requests are held in the LDAP requests table, where they're identified as suppressed. They aren't processed.

If you disable the automatic creation of user accounts for some or all users, then you can:

- Create user accounts individually on the Security Console.
- Link existing user accounts to person and party records using the **Manage User Account** or **Manage Users** task.

Alternatively, you can use an external provisioning infrastructure to create and manage user accounts. In this case, you're responsible for managing the interface with Oracle Applications Cloud, including any user account related updates.

User Account Role Provisioning Option

Existing users both acquire and lose roles as specified by current role-provisioning rules. For example, users may request some roles for themselves and acquire others automatically. All provisioning changes are role requests that are processed by default.

You can control what happens to role requests by setting the **User Account Role Provisioning** option. Use the **Manage Enterprise HCM Information** task to set this option. This table describes the **User Account Role Provisioning** option values.

Value	Description
Both person and party users	Role provisioning and deprovisioning occur for both person and party users. This value is the default value.
Party users only	Role provisioning and deprovisioning occur for party users only. For person users, role requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.
None	For both person and party users, role requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.

Note: When a user account is created, roles may be provisioned to it automatically based on current role-provisioning rules. This provisioning occurs because user accounts without roles are suspended automatically. Automatic creation of user accounts and the associated role provisioning are controlled by the **User Account Creation** option.

User Account Maintenance Option

By default, a user's account is suspended automatically when the user has no roles. This situation occurs typically at termination. The user account is reactivated automatically if you reverse the termination or rehire the worker. The User Account Maintenance option controls these actions.

Use the **Manage Enterprise HCM Information** task to set this option. This table describes the **User Account Maintenance** option values.

Value	Description
Both person and party users	User accounts are maintained automatically for both person and party users. This value is the default value.
Party users only	User accounts are maintained automatically for party users only. For person users, account-maintenance requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed. Select this value if you manage accounts for person users in some other way.
None	For both person and party users, account-maintenance requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed. Select this value if you manage accounts for both person and party users in some other way.

Set the User and Role Provisioning Options

The user and role provisioning options control the creation and maintenance of user accounts for the enterprise. This procedure explains how to set these options. To create and maintain Oracle Applications Cloud user accounts automatically for all users, you can use the default settings.

1. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Workforce Structures
    - Task: Manage Enterprise HCM Information
2. On the Enterprise page, select **Edit** > **Update**.
3. In the Update Enterprise dialog box, enter the effective date of any changes and click **OK**. The Edit Enterprise page opens.
4. Scroll down to the User and Role Provisioning Information section.
5. Set the User Account Options, as appropriate. The User Account Options are:
    - User Account Creation
    - User Account Role Provisioning
    - User Account Maintenance
    - User Account Creation for Terminated Workers

    These options are independent of each other. For example, you can set **User Account Creation** to **None** and **User Account Role Provisioning** to **Yes**.
6. Click **Submit** to save your changes.
7. Click **OK** to close the Confirmation dialog box.

Related Topics

- User and Role-Provisioning Setup Options

Provision Abstract Roles to Users Automatically

Provisioning the Employee, Contingent Worker, and Line Manager abstract roles automatically to users is efficient, as most users have at least one of these roles. It also ensures that users have basic access to functions and data when they first sign in.

Provision the Employee Role Automatically to Employees

1. Sign in as the TechAdmin user or another user with the IT Security Manager (ORA_FND_IT_SECURITY_MANAGER_JOB) job role or privileges.
2. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Users and Security
    - Task: Manage Role Provisioning Rules

3. In the Search Results section of the **Manage Role Mappings** page, click the **Create** icon. The **Create Role Mapping** page opens.
4. In the **Mapping Name** field, enter **Employee**.
5. Complete the fields in the Conditions section of the Create Role Mapping page as shown in the following table.

Field	Value
System Person Type	Employee
HR Assignment Status	Active

6. In the Associated Roles section of the **Create Role Mapping** page, add a row.
7. In the **Role Name** field of the Associated Roles section, click **Search**.
8. In the Search and Select dialog box, enter **Employee** in the **Role Name** field and click **Search**.
9. Select **Employee** in the search results and click **OK**.
10. If **Autoprovision** isn't selected automatically, then select it. Ensure that the **Requestable** and **Self-Requestable** options aren't selected.
11. Click **Save and Close**.

Provision the Contingent Worker Role Automatically to Contingent Workers

Repeat the steps in Provisioning the Employee Role Automatically to Employees, with the following changes:

- In step 4, enter **Contingent Worker** as the mapping name.
- In step 5, set **System Person Type** to **Contingent Worker**.
- In steps 8 and 9, search for and select the Contingent Worker role.

Provision the Line Manager Role Automatically to Line Managers

1. In the Search Results section of the **Manage Role Mappings** page, click the **Create** icon. The **Create Role Mapping** page opens.
2. In the **Mapping Name** field, enter **Line Manager**.
3. Complete the fields in the Conditions section of the Create Role Mapping page as shown in the following table.

Field	Value
System Person Type	Employee
HR Assignment Status	Active
Manager with Reports	Yes

> **Tip:** Setting **Manager with Reports** to **Yes** is the same as setting **Manager Type** to **Line Manager**. You don't need both values.

4. In the Associated Roles section of the **Create Role Mapping** page, add a row.
5. In the **Role Name** field of the Associated Roles section, click **Search**.
6. In the **Search and Select** dialog box, enter Line Manager in the **Role Name** field and click **Search**.
7. Select Line Manager in the search results and click **OK**.
8. If Autoprovision isn't selected automatically, then select it. Ensure that the **Requestable** and **Self-Requestable** options aren't selected.
9. Click **Save and Close**.
10. On the **Manage Role Mappings** page, click **Done**.

To provision the line manager role automatically to contingent workers, follow these steps to create an additional role mapping. In step 2, use a unique mapping name (for example, Contingent Worker Line Manager). In step 3, set **System Person Type** to **Contingent Worker**.

Users

Create Users

During implementation, you can use the Create User task to create test application users. By default, this task creates a minimal person record and a user account. After implementation, you should use the Hire an Employee task to create application users.

The Create User task isn't recommended after implementation is complete. This topic describes how to create a test user using the Create User task.

Sign in and follow these steps:

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.
2. In the Search Results section, click the **Create** icon.
   The Create User page opens.

Completing Personal Details

1. Enter the user's name.
2. In the **Email** field, enter the user's primary work email.
3. In the **Hire Date** field, enter the hire date for a worker. For other types of users, enter a user start date. You can't edit this date after you create the user.

Completing User Details

You can enter a user name for the user. If you leave the **User Name** field blank, then the user name follows the enterprise default user-name format.

Setting User Notification Preferences

The **Send user name and password** option controls whether a notification containing the new user's sign-in details is sent when the account is created. This option is enabled only if notifications are enabled on the Security Console and an appropriate notification template exists. For example, if the predefined notification template New Account Template is enabled, then a notification is sent to the new user. If you deselect this option, then you can send the email later by running the Send User Name and Password Email Notifications process. An appropriate notification template must be enabled at that time.

Completing Employment Information

1. Select a **Person Type** value.
2. Select **Legal Employer** and **Business Unit** values.

Adding Roles

1. Click **Autoprovision Roles**. Any roles for which the user qualifies automatically, based on the information that you have entered so far, appear in the Role Requests table.
2. To provision a role manually to the user, click **Add Role**. The Add Role dialog box opens.
3. Search for and select the role. The role must appear in a role mapping for which you satisfy the role-mapping conditions and where the **Requestable** option is selected for the role.

   The role appears in the Role Requests region with the status **Add requested**. The role request is created when you click **Save and Close**.

   Repeat steps 2 and 3 for additional roles.
4. Click **Save and Close**.
5. Click **Done**.

User Data Import from Legacy Applications

You can import workers from legacy applications to Oracle Fusion Applications using the Import Worker Users task . You can access this task from the Setup and Maintenance work area.

By enabling you to bulk-load existing data, this task is an efficient way of creating and enabling users of Oracle Applications Cloud.

The Import Worker Users Process

Importing worker users is a two-stage process:

1. When you perform the Import Worker Users task, the Initiate Spreadsheet Load page opens. On the Initiate Spreadsheet Load page, you generate and complete the Create Worker spreadsheet. You must map your data to the spreadsheet columns and provide all required attributes. Once the spreadsheet is complete, you click **Upload** in the spreadsheet to import the data to the Load Batch Data stage tables.
2. As the upload process imports valid data rows to the Load Batch Data stage tables, the Load Batch Data process runs automatically. Load Batch Data is a generic utility for loading data to Oracle Fusion Human Capital Management from external sources. This process loads data from the Load Batch Data stage tables to the Oracle Fusion application tables.

User Account Creation

The application creates Oracle Fusion user accounts automatically for imported workers.

By default, user account names and passwords are sent automatically to users when their accounts are created. This default action may have been changed at enterprise level, as follows:

- You can disable notifications for all user life cycle events.
- You can disable notifications for the New User Created and New Account Create Manager events.

Role Provisioning

Once user accounts exist, roles are provisioned to users automatically in accordance with current role-provisioning rules. For example, current rules could provision the employee abstract role to every worker. Role provisioning occurs automatically and can't be disabled for the enterprise.

Related Topics

- User and Role-Provisioning Setup Options
- Import Users in Bulk Using a Spreadsheet
- How Data Is Uploaded Using HCM Spreadsheet Data Loader
- Upload Data Using HCM Spreadsheet Data Loader

Import Users in Bulk Using a Spreadsheet

This example shows how to import worker users from legacy applications to Oracle Fusion Applications.

The following table summarizes key decisions for this task.

Decisions to Consider	In This Example
What's my spreadsheet name? You can define your own naming convention. In this example, the name is selected to make identifying the spreadsheet contents easy.	WorkersMMDDYYBatchnn.xlsx For example, Workers042713Batch01.xlsx.
What's my batch name? You can define your own batch name, which must be unique.	Workers042713Batchnn

Summary of the Tasks

Import worker users by:

1. Selecting the Import Worker Users task
2. Creating the spreadsheet
3. Entering worker data in the spreadsheet
4. Importing worker data and correcting import errors
5. Reviewing and correcting load errors

Prerequisites

Before you can complete this task, you must have:

1. Installed the desktop client Oracle ADF Desktop Integration Add-in for Excel
2. Enabled the Trust Center setting **Trust access to the VBA project object model** in Microsoft Excel

Selecting the Import Worker Users Task

1. On the Overview page of the Setup and Maintenance work area, click the All Tasks tab.
2. In the Search region, complete the fields as shown in this table.

Field	Name
Search	Task
Name	Import Worker Users

3. Click **Search**.
4. In the search results, click **Go to Task** for the task Import Worker Users.

   The Initiate Spreadsheet Load page opens.

   Alternatively, you can select the Import Worker Users task from an implementation project.

Creating the Spreadsheet

1. On the Initiate Spreadsheet Load page, find the entry for Create Worker in the list of business objects.

   Create Worker appears after other business objects such as departments, locations, and jobs. You must create those business objects before worker users, regardless of how you create them.
2. Click **Create Spreadsheet** for the Create Worker entry.
3. When prompted, save the spreadsheet locally using the name Workers042713Batch01.xlsx.
4. When prompted, sign in to Oracle Fusion Applications using your Oracle Fusion user name and password.

Entering Worker Data in the Spreadsheet

1. In the **Batch Name** field of the spreadsheet Workers042713Batch01.xlsx, replace the default batch name with the batch name Workers042713Batch01.
2. If your data includes flexfields, then click **Configure Flexfield** to configure flexfield data. Otherwise, go to step 5 of this task.
3. In the **Configure Flexfield** window, select an attribute value and click **OK**.
4. See the Flexfields Reference tab for information about the configured flexfield.
5. Enter worker data in the spreadsheet.

   Ensure that you provide any required values and follow instructions in the spreadsheet for creating rows.

Importing Worker Data and Correcting Import Errors

Use the default values except where indicated.

1. In the workers spreadsheet, click **Upload**.
2. In the **Upload Options** window, click **OK**.

   As each row of data uploads to the Load Batch Data stage tables, its status updates.
3. When uploading completes, identify any spreadsheet rows with the status **Insert Failed**, which indicates that the row didn't import to the stage tables.
4. For any row that failed, double-click the status value to display a description of the error.

5. Correct any import errors and click **Upload** again to import the remaining rows to the same batch.

   As rows import successfully to the stage tables, the data loads automatically to the application tables.

Reviewing and Correcting Load Errors

1. In the spreadsheet, click **Refresh** to display latest load status.

   Any errors that occur during the load process appear in the spreadsheet.
2. Correct any load errors in the spreadsheet.
3. Repeat this process from Importing Worker Data and Correcting Import Errors until all spreadsheet rows both import and load successfully.
4. Close the spreadsheet.

   To load a second batch of worker users on the same date, increment the batch number in the spreadsheet and batch names (for example, Workers042713Batch02).

Schedule the Import User Login History Process

During implementation, you perform the Import User Login History task in the Setup and Maintenance work area. This task runs a process that imports information about user access to Oracle Fusion Applications to the Oracle Fusion Applications Security tables.

This information is required by the Inactive Users Report, which reports on users who have been inactive for a specified period. After you perform the **Import User Login History** task for the first time, you're recommended to schedule it to run daily. In this way, you can ensure that the Inactive Users Report is up to date.

Schedule the Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User Login History** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Every** to **1**.
8. Enter start and end dates and times.
9. Click **Submit**.
10. Click **OK** to close the **Confirmation** message.

Related Topics

- Inactive Users Report

Inactive Users Report

Scheduling the Import User Login History process to run daily is a prerequisite to get a valid report about inactive users.

The Import User Login History process imports information that the Inactive Users Report process uses to identify inactive users. The Inactive Users Report process helps to identify users who haven't signed in for a specified period.

Before you run the inactive users report for a certain period, make sure that the Import User Login History data exists for that period. It's important to know when the user last signed in. That's why it's recommended to always run the Import User Login History process for a longer duration to offer greater flexibility with the date range.

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the **Inactive Users Report** process.
3. In the Process Details dialog box, set parameters to identify one or more users.
4. Click **Submit**.

Inactive Users Report Parameters

All parameters except Days Since Last Activity are optional.

User Name Begins With

Enter one or more characters.

First Name Begins With

Enter one or more characters.

Last Name Begins With

Enter one or more characters.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Days Since Last Activity

Enter the number of days since the user last signed in. Use this parameter to specify the meaning of the term inactive user in your enterprise. Use other parameters to filter the results.

This value is required and is 30 by default. This value identifies users who haven't signed in during the last 30 or more days.

Last Activity Start Date

Specify the start date of a period in which the last activity must fall.

Last Activity End Date

Specify the end date of a period in which the last activity must fall.

Viewing the Report

The process produces an **Inactive_Users_List_processID.xml** file and a **Diagnostics_processID.zip** file.

The report includes the following details for each user who satisfies the report parameters:

- Number of days since the user was last active
- Date of last activity

- User name
- First and last names
- Assignment department
- Assignment location
- City and country
- Report time stamp

Note: The information in the report relating to the user's latest activity isn't based solely on actions performed by the user in the UI. Actions performed on behalf of the user, which create user sessions, also affect these values. For example, running processes, making web service requests, and running batch processes are interpreted as user activity.

Related Topics

- Schedule the Import User Login History Process

User Accounts

Manage HCM User Accounts

Human resource specialists (HR specialists) can manage user accounts for users whose records they can access. This topic describes how to update a Human Capital Management (HCM) user account.

To access the user account page for a person:

1. On the **My Client Groups** tab, find and select the **Manage User Account** quick action. You must click **Show More** if it isn't visible by default.
2. Search for and select the person whose account you're updating.

IT Security Managers can manage user accounts and user roles using the security console. For more information, see the topic *Oracle Fusion Applications Security Console* .

Manage User Roles

To add a role:

1. Click **Add Role**.
   The Add Role dialog box opens.
2. In the **Role Name** field, search for the role that you want to add. The list of available roles is decided by role provisioning rules that have been configured using the Role Mappings UI.
3. In the search results, select the role and click **OK**.
4. Click **Save**.

To remove a role:

1. Select the role and click **Remove**.
2. In the Warning dialog box, click **Yes** to continue.
3. Click **Save**.

To update a user's roles automatically, select **Actions** > **Update Role Assignments**. This action applies to roles for which the **Autoprovision** option is selected in all current role mappings. The user immediately:

- Acquires any role for which they qualify but don't currently have
- Loses any role for which they no longer qualify

You're recommended to autoprovision roles for individual users if you know that additional or updated role mappings exist that affect those users.

Synchronize Personal Data with Identity Store

By default, changes to personal data, such as person name and phone, are copied to your Identity Store periodically. To copy any changes immediately:

1. Select **Actions** > **Synchronize with Identity Store**.
2. Click **Synchronize**.

Reset Passwords

To reset a user's password:

1. Select **Actions** > **Reset Password**.
2. In the Warning dialog box, click **Yes** to continue.

   This action sends a notification containing a reset-password link to the user's work email.

   > **Note:** A notification template for the password-reset event must exist and be enabled for the user's user category. Otherwise, no notification is sent.

Edit User Names

To edit a user name:

1. Select **Actions** > **Edit User Name**.
2. In the Update User Name dialog box, enter the user name and click **OK**. The maximum length of the user name is 80 characters.
3. Click **Save**.

This action sends the updated user name to your Identity Store. Once the request is processed, the user can sign in using the updated name. As the user receives no automatic notification of the change, you're recommended to send the details to the user.

User Names

By default, user names are generated automatically in the format specified for the default user category when you create a person record. Users who have the human resource specialist (HR specialist) role can change user names for existing HCM users.

This topic describes the automatic generation of user names and explains how to change an existing user name.

User Names When Creating Users

You create an HCM user by selecting a task, such as **Hire an Employee**, in the New Person work area. The user name is generated automatically in the format specified for the default user category. This table summarizes the effects of the available formats for Oracle Fusion Cloud HCM users.

User-Name Format	Description
Email	The worker's work email is the user name. If you don't enter the work email when hiring the worker, then it can be entered later on the Security Console. This format is used by default. A different default format can be selected on the Security Console.
FirstName.LastName	The user name is the worker's first and last names separated by a single period.
FLastName	The user name is the worker's last name prefixed with the initial of the worker's first name.
Person number	If your enterprise uses manual numbering, then any number that you enter becomes the user name. Otherwise, the number is generated automatically and you can't edit it. The automatically generated number becomes the user name.

Note: If the default user-name rule fails, then a system user name can be generated. The option to generate a system user name is enabled by default but you can disable it on the Security Console.

Existing User Names

HR specialists can change an existing user name on the Manage User Account page.

To change a worker's user name:

1. On the **My Client Groups** tab, find and select the **Manage User Account** quick action. You may have to click **Show More** if it is not visible by default. Line Managers can use the quick action on the My Team tab.
2. Search for and select the worker.
3. On the Manage User Account page, select **Actions** > **Edit User Name**.
4. Select **Actions** >

The updated name, which can be in any format, is sent automatically to your Identity Store. The maximum length of the user name is 80 characters.

Tip: When you change an existing user name, the user's password and roles remain the same. However, the user receives no automatic notification of the change. Therefore, you're recommended to send details of the updated user name to the user.

Why You Send Personal Data to Identity Store

User accounts for users of Oracle Fusion Applications are maintained on your Identity Store. By default, Oracle Fusion Cloud HCM sends some personal information about users to the Identity Store.

This information includes the person number, person name, phone, and manager of the person's primary assignment. HCM Cloud shares these details to ensure that user account information matches the information about users in HCM Cloud. This topic describes how and when you can send personal information explicitly to your Identity Store.

Bulk Creation of Users

After loading person records using HCM Data Loader, for example, you run the **Send Pending LDAP Requests** process. This process sends bulk requests for user accounts to the Identity Store.

When you load person records in bulk, the order in which they're created is undefined. Therefore, a person's record may exist before the record for his or her manager. In such cases, the **Send Pending LDAP Requests** process includes no manager details for the person in the user account request. The Identity Store information therefore differs from the information that HCM Cloud holds for the person. To correct any differences between these versions of personal details, you run the **Send Personal Data for Multiple Users to LDAP** process.

The Send Personal Data for Multiple Users to LDAP Process

Send Personal Data for Multiple Users to LDAP updates the Identity Store information to match information held by HCM Cloud. You run the process for either all users or changed users only, as described in this table.

User Population	Description
All users	The process sends personal details for all users to the Identity Store, regardless of whether they have changed since personal details were last sent.
Changed users only	The process sends only personal details that have changed since details were last sent to the Identity Store (regardless of how they were sent). This option is the default setting.

Note: If **User Account Maintenance** is set to **No** for the enterprise, then the process doesn't run.

The process doesn't apply to party users.

You must have the Human Capital Management Application Administrator job role to run this process.

Synchronize Personal Data with the Identity Store

Users can synchronize their personal data with the Identity Store from the Manage User Account page. Human resource specialists and line managers can also perform this action for users whose records they can access. By default, personal data changes are copied periodically to the Identity Store directory. However, this action is available for copying changes immediately, if necessary.

Related Topics

- User and Role-Provisioning Setup Options

How You Manage an Incomplete Request for an HCM User Account

This topic describes the Process User Account Request action, which may appear on the Manage User Account page for users who have no user account.

The Process User Account Request Action

The **Process User Account Request** action is available when the status of the worker's user account is either **Requested** or **Failed**. These values indicate that the account request hasn't completed.

Selecting this action submits the request again. Once the request completes successfully, the account becomes available to the user. Depending on your enterprise setup, the user may receive an email containing the user name and password.

Role Provisioning

Any roles that the user will have appear in the Roles section of the Manage User Account page. You can add or remove roles before selecting the **Process User Account Request** action. If you make changes to roles, then you must click **Save**.

The Send Pending LDAP Requests Process

The **Process User Account Request** action has the same effect as the **Send Pending LDAP Requests** process. If **Send Pending LDAP Requests** runs automatically at intervals, then you can wait for that process to run if you prefer. Using the **Process User Account Request** action, you can submit user account requests immediately for individual workers.

How User Accounts Are Suspended

By default, user accounts are suspended automatically when a user has no roles. This automatic suspension of user accounts is controlled by the User Account Maintenance enterprise option. Human resource (HR) specialists can also suspend a user account manually, if necessary.

This topic describes how automatic account suspension and reactivation occur. It also explains how to suspend a user account manually.

Automatic Suspension of User Accounts

When you terminate a work relationship:

- The user loses any automatically provisioned roles for which he or she no longer qualifies. This deprovisioning is automatic.

- If the user has no other active work relationships, then the user also loses manually provisioned roles. These are:
  - Roles that he or she requested
  - Roles that another user, such as a line manager, provisioned to the user

  If the user has other, active work relationships, then he or she keeps any manually provisioned roles.

When terminating a work relationship, you specify whether the user is to lose roles on the termination date or on the day following termination.

A terminated worker's user account is suspended automatically at termination only if he or she has no roles. Users can acquire roles automatically at termination, if an appropriate role mapping exists. In this case, the user account remains active.

Automatic Reactivation of User Accounts

User accounts are reactivated automatically when you reverse a termination or rehire a worker. If you reverse the termination of a work relationship, then:

- The user regains any role that he or she lost automatically at termination. For example, if the user automatically lost roles that had been provisioned manually, then those roles are reinstated.

  > **Note:** If you removed any roles from the user manually at termination, then you must restore them to the user manually, if required.

- The user loses any role that he or she acquired automatically at termination.
- If the user account was suspended automatically at termination, then it's automatically reactivated.

The autoprovisioning process runs automatically when you reverse a termination. Therefore, the user's roles are updated automatically as specified by current role mappings.

When you rehire a worker, the user account is reactivated automatically and roles are provisioned automatically as specified by current role mappings. In all other cases, you must reactivate suspended user accounts manually on the Edit User page.

> **Tip:** Authorized users can also manage user account status directly on the Security Console.

Manual Suspension of User Accounts

To suspend a user account manually, HR specialists follow these steps:

1. Select **Navigator** > **My Team** > **Users and Roles**.
2. Search for and select the user to open the Edit User page.
3. In the User Details section of the Edit User page, set the **Active** value to **Inactive**. You can reactivate the account by setting the **Active** value back to **Active**.
4. Click **Save and Close**.

> **Note:** Role provisioning isn't affected by the manual suspension and reactivation of user accounts. For example, when you reactivate a user account manually, the user's autoprovisioned roles are updated only when you click **Autoprovision Roles** on the **Edit User** page. Similarly, a suspended user account isn't reactivated when you click **Autoprovision Roles**. You must explicitly reactivate the user account first.

IT security managers can lock user accounts on the Security Console. Locking a user account on the Security Console or setting it to **Inactive** on the Edit User page prevents the user from signing in.

Related Topics

- User Account Maintenance Option

User Details System Extract Report

The Oracle BI Publisher User Details System Extract Report includes details of Oracle Fusion Applications user accounts. This topic describes the report contents.

Run the report in the Reports and Analytics work area.

Report Results

The report is an XML-formatted file where user accounts are grouped by type, as follows:

- Group 1 (G_1) includes HCM user accounts.
- Group 2 (G_2) includes TCA party user accounts.
- Group 3 (G_3) includes LDAP user accounts.

The information in the extract varies with the account type.

Business Unit Name
The business unit from the primary work relationship.

Composite Last Update Date
The date when any one of a number of values, including assignment managers, location, job, and person type, was last updated.

Department
The department from the primary assignment.

Worker Type
The worker type from the user's primary work relationship.

Generation Qualifier
The user's name suffix (for example, Jr., Sr., or III).

Hire Date
The enterprise hire date.

Role Name
A list of roles currently provisioned to workers whose work relationships are all terminated. This value appears for active user accounts only.

Title
The job title from the user's primary assignment.

Organizations
A resource group.

Roles

A list of job, abstract, and data roles provisioned to the user.

Managers
The manager of a resource group.

Start Date
The account's start date.

Created By
The user name of the user who created the account.

Related Topics

- Run the User Details System Extract Report
- User Details System Extract Report Parameters

User Details System Extract Report Parameters

The Oracle BI Publisher User Details System Extract Report includes details of Oracle Fusion Applications user accounts. This topic describes the report parameters. Run the report in the Reports and Analytics work area.

Parameters

User Population

Enter one of the values shown in this table to identify user accounts to include in the report.

Value	Description
HCM	User accounts with an associated HCM person record.
TCA	User accounts with an associated party record.
LDAP	Accounts for users in the PER_USERS table who have no person number or party ID. Implementation users are in this category.
ALL	HCM, TCA, and LDAP user accounts.

From Date

Accounts for HCM and LDAP users that exist on or after this date appear in the report. If you specify no **From Date** value, then the report includes accounts with any creation date, subject only to any **To Date** value.

From and to dates don't apply to the TCA user population. The report includes all TCA users if you include them in the report's user population.

To Date

Accounts for HCM and LDAP users that exist on or before this date appear in the report. If you specify no **To Date** value, then the report includes accounts with any creation date, subject only to any **From Date** value.

From and to dates don't apply to the TCA user population. The report includes all TCA users if you include them in the report's user population.

User Active Status

Enter one of the values shown in this table to identify the user account status.

Value	Description
A	Include users with active accounts.
I	Include users with inactive accounts.
All	Include both active and inactive user accounts.

Related Topics

- Run the User Details System Extract Report
- User Details System Extract Report

User Password Changes Audit Report

This report identifies users whose passwords were changed in a specified period. You must have the ASE_USER_PASSWORD_CHANGES_AUDIT_REPORT_PRIV function security privilege to run this report. The predefined IT Security Manager job role has this privilege by default.

To run the User Password Changes Audit Report:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the **User Password Changes Audit Report** process.
4. In the Process Details dialog box, set parameters and click **Submit**.
5. Click **OK** to close the confirmation message.

User Password Changes Audit Report Parameters

Search Type

Specify whether the report is for all users, a single, named user, or a subset of users identified by a name pattern that you specify.

User Name

Search for and select the user on whom you want to report. This field is enabled only when **Search Type** is set to **Single user**.

User Name Pattern

Enter one or more characters that appear in the user names on which you want to report. For example, you could report on all users whose user names begin with the characters **SAL** by entering **SAL%**. This field is enabled only when **Search Type** is set to **User name** pattern.

Start Date

Select the start date of the period during which password changes occurred. Changes made before this date don't appear in the report.

To Date

Select the end date of the period during which password changes occurred. Changes made after this date don't appear in the report.

Sort By

Specify how the report output is sorted. The report can be organized by either user name or the date when the password was changed.

Viewing the Report Results

The report produces these files:

- **UserPasswordUpdateReport.csv**
- **UserPasswordUpdateReport.xml**
- **Diagnostics_[process ID].log**

For each user whose password changed in the specified period, the report includes:

- The user name.
- The first and last names of the user.
- The user name of the person who changed the password.
- How the password was changed:
    - ADMIN means that the change was made for the user by a line manager or the IT Security manager, for example.
    - SELF_SERVICE means that the user made the change by setting preferences or requesting a password reset, for example.
    - FORGOT_PASSWORD means that the user clicked the **Forgot Password** link when signing in.
    - REST_API means that the change was made for the user by SCIM REST APIs.
- The date and time of the change. The format of date and time of the change is "dd/MM/yyyy HH:mm:ss".

View Locked Users and Unlock Users

A user gets locked in the application on entering incorrect password for multiple times. The locked users report provides the list of locked users for both these scenarios.

You can get a list of locked users using the Locked Users scheduled process. You can then manually unlock the users using the Security Console. Only an administration user with the IT Security Manager job role can run the locked users report.

View Locked Users

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search and select the **Locked Users** process and click **OK**.
3. In the Process Details dialog box, click **Submit**.
4. Click **OK** in the confirmation message dialog box.
5. Click **Succeeded** for the selected Locked Users report.
6. In the **Log and Output** section, click **Attachment** to download the report spreadsheet.

   The spreadsheet shows the list of users who are locked.

The Locked Users spreadsheet contains the following two tabs:

- LOCKED_USERS_<Request ID> - This tab contains the list of locked and active users who can't sign in to the application because of locked status.
- LOCKED_AND_INACTIVE_USERS_<Request ID> - This tab contains list of locked and inactive users who can't sign in to the application because of locked and inactive status.

Unlock Users

1. On the Security Console, click **Users**.
2. From the **Search** drop-down list, select **Locked Users** and click the search icon.

   All the locked users are displayed.
3. Click the display name of a user to view the details.
4. Click **Edit**.
5. In the Account Information section, deselect **Locked**.
6. Click **Save and Close**.
7. Click **Done**.

   The user is unlocked and can sign in to the application.

Reset Passwords

Use the Security Console to reset other users' passwords. The new password must conform to the password policy from the user category that's assigned to the user.

1. In the Security Console, click the **Users** tab.
2. On the User Accounts page, search for the user whose password you want to change.
3. In the **Action** drop-down list for the user, select **Reset Password**. Or, you can click the display name and then click the **Reset Password** button on the User Account Details page.
4. In the **Reset Password** dialog box, select whether to generate the password automatically or change it manually. For a manual change, enter a new password.

   > **Note:** If you don't see the manual reset option, go to the user category assigned to the user and select the **Administrator can manually reset password** check box in the Password Policy tab of the user category.

5. Click **Reset Password**.

An email with a link to reset the password is sent to the user.

Related Topics

- Configure the Security Console
- Overview of User Categories

Password Expiry Report

The Password Expiry Report sends the password expiration warning and password expired notifications. You must schedule this report to run daily to help users know when their passwords have to be reset.

If the password expiration date set for users is in the past and if the users haven't reset the password, then this report automatically resets the password and notifies them about the change. Similarly, if the password expiration warning date set for users is in the future, then this report sends a warning notification to the users that their password is about to expire.

Here are the steps to schedule a password expiry report:

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. In the Schedule Process dialog box, search for and select the **Password Expiry Report** process.
3. Click **OK**.
4. In the Process Details dialog box, click **Advanced**.
5. On the Schedule tab, set **Run** to **Using a schedule**.
6. Select a **Frequency** value. For example, select **Daily**.
7. Select a start date and time.
8. Click **Submit**.

FAQs for Application Users Management

Where do default user names come from?

User names are generated automatically in the format specified on the Security Console for the user category. The default format is the worker's primary work email, but you can override this value for each user category.

For example, your enterprise may use person number as the default user name for the default user category.

Why did some roles appear automatically?

In a role mapping:

- The conditions specified for the role match the user's assignment attributes, such as job.
- The role has the **Autoprovision** option selected.

How can I create a user?

If you want to create application users, access the Manage Users task. When the Search Person page appears, click the New icon in Search Results grid. The Create User page appears for you to fill in and save.

If you use the HCM pages to upload workers, hire employees, or add contingent workers, you also automatically create application users and identities.

When you create a new user, it automatically triggers role provisioning requests based on role provisioning rules.

Related Topics

- Create Users

What happens when I autoprovision roles for a user?

The role-provisioning process reviews the user's assignments against all current role mappings.

The user immediately:

- Acquires any role for which he or she qualifies but doesn't have
- Loses any role for which he or she no longer qualifies

You're recommended to autoprovision roles to individual users on the Manage User Account page when new or changed role mappings exist. Otherwise, no automatic updating of roles occurs until you next update the user's assignments.

Why is the user losing roles automatically?

The user acquired these roles automatically based on his or her assignment information. Changes to the user's assignments mean that the user is no longer eligible for these roles. Therefore, the roles no longer appear.

If a deprovisioned role is one that you can provision manually to users, then you can reassign the role to the user, if appropriate.

Why can't I see the roles that I want to assign to a user?

You can see the roles that you want to assign, if the role satisfies all of the following conditions:

- A role mapping exists for the role. For more information on creating a role mapping, see the topic *Create a Role Mapping*.
- The Requestable option is selected for the role in the role mapping. For more information, see the topic *How do I provision HCM data roles to users?*.
- At least one of your assignments satisfies the role-mapping conditions.

What happens if I deprovision a role from a user?

The user loses the access to functions and data that the removed role was providing exclusively. The user becomes aware of the change when he or she next signs in.

If the user acquired the role automatically, then future updates to the user's assignments may mean that the user acquires the role again.

What happens if I edit a user name?

The updated user name is sent to your LDAP directory for processing when you click Save on the Manage User Account or Edit User page. The account status remains Active, and the user's roles and password are unaffected.

As the user isn't notified automatically of the change, you're recommended to notify the user. Only human resource specialists can edit user names.

What happens if I send the user name and password?

The user name and password go to the work email of the user or user's line manager, if any. Notification templates for this event must exist and be enabled.

You can send these details once only for any user. If you deselect this option on the Manage User Account or Create User page, then you can send the details later. To do this, run the **Send User Name and Password Email Notifications** process.

What happens if I reset a user's password?

A notification containing a reset-password link is sent to the user's work email. If the user has no work email, then the notification is sent to the user's line manager. Notification templates for this event must exist and be enabled.

How can I notify users of their user names and passwords?

You can run the Send User Name and Password Email Notifications process in the Scheduled Processes work area. For users for whom you haven't so far requested an email, this process sends out user names and reset-password links.

The email goes to the work email of the user or the user's line manager. You can send the user name and password once only to any user. A notification template for this event must exist and be enabled.

6 Data Security Policies

Data Security

By default, users are denied access to all data.

Data security makes data available to users by the following means.

- Policies that define grants available through provisioned roles
- Policies defined in application code

You secure data by provisioning roles that provide the necessary access.

Data roles also can be generated based on HCM security profiles. Data roles and HCM security profiles enable defining the instance sets specified in data security policies.

When you provision a job role to a user, the job role limits data access based on the data security policies of the inherited duty roles. When you provision a data role to a user, the data role limits the data access of the inherited job role to a dimension of data.

Data security consists of privileges conditionally granted to a role and used to control access to the data. A privilege is a single, real world action on a single business object. A data security policy is a grant of a set of privileges to a principal on an object or attribute group for a given condition. A grant authorizes a role, the grantee, to actions on a set of data resources. A data resource is an object, object instance, or object instance set. An entitlement is one or more allowable actions applied to a set of data resources.

The following table describes the ways through which data is secured.

Data security feature	Does what?
Data security policy	Defines the conditions in which access to data is granted to a role.
Role	Applies data security policies with conditions to users through role provisioning.
HCM security profile	Defines data security conditions on instances of object types such as person records, positions, and document types without requiring users to enter SQL code

The sets of data that a user can access are defined by creating and provisioning data roles. Oracle data security integrates with Oracle Platform Security Services (OPSS) to entitle users or roles (which are stored externally) with access to data. Users are granted access through the privilege assigned to the roles or role hierarchy with which the user is provisioned. Conditions are WHERE clauses that specify access within a particular dimension, such as by business unit to which the user is authorized.

Data Security Policies

Data security policies articulate the security requirement "Who can do what on which set of data."

The following table provides an example, accounts payable managers can view AP disbursements for their business unit.

Who	can do	what	on which set of data
Accounts payable managers	view	AP disbursements	for their business unit

A data security policy is a statement in a natural language, such as English, that typically defines the grant by which a role secures business objects. The grant records the following.

- Table or view
- Entitlement (actions expressed by privileges)
- Instance set (data identified by the condition)

For example, disbursement is a business object that an accounts payable manager can manage by payment function for any employee expenses in the payment process.

Note: Some data security policies aren't defined as grants but directly in applications code. The security reference manuals for Oracle Fusion Applications offerings differentiate between data security policies that define a grant and data security policies defined in Oracle Fusion applications code.

A data security policy identifies the entitlement (the actions that can be made on logical business objects or dashboards), the roles that can perform those actions, and the conditions that limit access. Conditions are readable WHERE clauses. The WHERE clause is defined in the data as an instance set and this is then referenced on a grant that also records the table name and required entitlement.

HCM Security Profiles

HCM security profiles are used to secure HCM data, such as people and departments. Data authorization for some roles, such as the Manager role, is managed in HCM, even in ERP and SCM applications. You can use HCM security profiles to generate grants for a job role such as Manager. The resulting data role with its role hierarchy and grants operates in the same way as any other data role.

For example, an HCM security profile identifies all employees in the Finance division.

Applications outside of HCM can use the HCM Data Roles UI pages to give roles access to HR people.

Advanced Data Security

Advanced Data Security offers two types of added data protection. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest.

Oracle Database Vault

Database Vault reduces the risk of highly privileged users such as database and application administrators accessing and viewing your application data. This feature restricts access to specific database objects, such as the application tables and SOA objects.

Administrators can perform regular database maintenance activities, but can't select from the application tables. If a DBA requires access to the application tables, request temporary access to the Oracle Fusion schema at which point keystroke auditing is enabled.

Transparent Data Encryption

Transparent Data Encryption (TDE) protects Oracle Fusion Applications data, which is at rest on the file system from being read or used. Data in the database files (DBF) is protected because DBF files are encrypted. Data in backups and in temporary files is protected. All data from an encrypted tablespace is automatically encrypted when written to the undo tablespace, to the redo logs, and to any temporary tablespace.

Advanced security enables encryption at the tablespace level on all tablespaces, which contain applications data. This includes SOA tablespaces which might contain dehydrated payloads with applications data.

Encryption keys are stored in the Oracle Wallet. The Oracle Wallet is an encrypted container outside the database that stores authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by secure sockets layer (SSL). Tablespace keys are stored in the header of the tablespace and in the header of each operating system (OS) file that makes up the tablespace. These keys are encrypted with the master key, which is stored in the Oracle Wallet. Tablespace keys are AES128-bit encryption while the TDE master key is always an AES256-bit encryption.

How Data Resources and Data Security Policies Work Together

A data security policy applies a condition and allowable actions to a data resource for a role. When that role is provisioned to a user, the user has access to data defined by the policy.

In the case of the predefined security reference implementation, this role is always a duty role.

The data resource defines an instance of a data object. The data object is a table, view, or flexfield.

Data Resources

A data resource specifies access to a table, view, or flexfield that's secured by a data security policy.

- Name providing a means of identifying the data resource
- Data object to which the data resource points

Data Security Policies

Data security policies consist of actions and conditions for accessing all, some, or a single row of a data resource.

- Condition identifying the instance set of values in the data object
- Action specifying the type of access allowed on the available values

> **Note:** If the data security policy needs to be less restrictive than any available data resource for a data object, define a new data security policy.

Actions

Actions correspond to privileges that entitle kinds of access to objects, such as view, edit, or delete. The actions allowed by a data security policy include all or a subset of the actions that exist for the data resource.

Conditions

A condition is either a SQL predicate or an XML filter. A condition expresses the values in the data object by a search operator or a relationship in a tree hierarchy. A SQL predicate, unlike an XML filter, is entered in a text field in the data security user interface pages and supports more complex filtering than an XML filter, such as nesting of conditions or sub queries. An XML filter, unlike a SQL predicate, is assembled from choices in the UI pages as an AND statement.

> **Note:** An XML filter can be effective in downstream processes such as business intelligence metrics. A SQL predicate can't be used in downstream metrics.

FAQs for Data Security Policies

What's the difference between function security and data security?

Function security is a statement of what actions you can perform in which user interface pages.

Data security is a statement of what action can be taken against which data.

Function security controls access to user interfaces and actions needed to perform the tasks of a job. For example, an accounts payable manager can view invoices. The Accounts Payable Manager role provisioned to the accounts payable manager authorizes access the functions required to view invoices.

Data security controls access to data. In this example, the accounts payable manager for the North American Commercial Operation can view invoices in the North American Business Unit. Since invoices are secured objects, and a data role template exists for limiting the Accounts Payable Manager role to the business unit for which the provisioned user is authorized, a data role inherits the job role to limit access to those invoices that are in the North American Business Unit. Objects not secured explicitly with a data role are secured implicitly by the data security policies of the job role.

Both function and data are secured through role-based access control.

Related Topics

- Data Security

How can I mask data in an environment?

To have an environment created with the data masked, create a service request using the Production to Test (P2T) template. Before you submit the request, be sure you select the Data Mask check box.

*How can I mask data in an environment?*To have the data in an existing nonproduction environment masked, create a standard service request. Enter the following as the service request title: Data Mask for Environment: **`Name_of_The_Environment_To_Mask`**

7 Role Provisioning, Role Assignments, and Role Configuration

Role Mappings

Roles give users access to data and functions. To provision a role to users, you define a relationship, called a role mapping, between the role and some conditions. This topic describes how to provision roles to users both automatically and manually.

Use the **Manage Role Provisioning Rules** task in the Setup and Maintenance work area to provision roles.

> **Note:** Role provisioning generates requests to provision roles. Only when those requests are processed successfully is role provisioning complete.

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

- At least one of the user's assignments matches all role-mapping conditions.
- You select the **Autoprovision** option for the role in the role mapping.

For example, for the data role Sales Manager Finance Department, you could select the **Autoprovision** option and specify the conditions shown in this table.

Attribute	Value
Department	Finance Department
Job	Sales Manager
HR Assignment Status	Active

Users with at least one assignment that matches these conditions acquire the role automatically when you either create or update the assignment. The provisioning process also removes automatically provisioned roles from users who no longer satisfy the role-mapping conditions.

Manual Provisioning of Roles to Users

Users such as line managers can provision roles manually to other users if:

- At least one of the assignments of the user who's provisioning the role, for example, the line manager, matches all role-mapping conditions.
- You select the **Requestable** option for the role in the role mapping.

For example, for the data role Training Team Leader, you could select the **Requestable** option and specify the conditions shown in this table.

Attribute	Value
Manager with Reports	Yes
HR Assignment Status	Active

Any user with at least one assignment that matches both conditions can provision the role Training Team Leader manually to other users.

Users keep manually provisioned roles until either all of their work relationships are terminated or you deprovision the roles manually.

Role Requests from Users

Users can request a role when managing their own accounts if:

- At least one of their assignments matches all role-mapping conditions.
- You select the **Self-requestable** option for the role in the role mapping.

For example, for the data role Expenses Reporter you could select the **Self-requestable** option and specify the conditions shown in this table.

Attribute	Value
Department	Finance Department
System Person Type	Employee
HR Assignment Status	Active

Any user with at least one assignment that matches these conditions can request the role. Self-requested roles are defined as manually provisioned.

Users keep manually provisioned roles until either all of their work relationships are terminated or you deprovision the roles manually.

Role-Mapping Names

Role-mapping names must be unique in the enterprise. Devise a naming scheme that shows the scope of each role mapping. For example, the role mapping Autoprovisioned Roles Sales could include all roles provisioned automatically to workers in the sales department.

Related Topics

- Autoprovisioning
- Examples of Role Mappings

Create a Role Mapping

To provision roles to users, you create role mappings. This topic explains how to create a role mapping.

Sign in as IT Security Manager and follow these steps:

1. In the Setup and Maintenance work area, go to the following:
    - Functional Area: Users and Security
    - Task: Manage Role Provisioning Rules
2. In the Search Results section of the Manage Role Mappings page, click **Create**.

    The Create Role Mapping page opens.

Defining the Role-Mapping Conditions

Set values in the Conditions section to specify when the role mapping applies. For example, use the values given in the following table to limit the role mapping to current employees of the Finance Department in Redwood Shores whose job is Accounts Payable Supervisor.

Field	Value
Department	Finance Department
Job	Accounts Payable Supervisor
Location	Redwood Shores
System Person Type	Employee
HR Assignment Status	Active

Users must have at least one assignment that meets all these conditions.

Identifying the Roles

1. In the Associated Roles section, click **Add Row**.
2. In the **Role Name** field, search for and select the role that you're provisioning.

3. Select one or more of the role-provisioning options as listed in the following table:

Role-Provisioning Option	Description
Requestable	Qualifying users can provision the role to other users.
Self-requestable	Qualifying users can request the role for themselves.
Autoprovision	Qualifying users acquire the role automatically.

Qualifying users have at least one assignment that matches the role-mapping conditions.

> **Note:** **Autoprovision** is selected by default. Remember to deselect it if you don't want autoprovisioning.

The **Delegation Allowed** option indicates whether users who have the role or can provision it to others can also delegate it. You can't change this value, which is part of the role definition. When adding roles to a role mapping, you can search for roles that allow delegation.

4. If appropriate, add more rows to the Associated Roles section and select provisioning options. The role-mapping conditions apply to all roles in this section.
5. Click **Save and Close**.

Applying Autoprovisioning

You're recommended to run the process Autoprovision Roles for All Users after creating or editing role mappings and after loading person records in bulk. This process compares all current user assignments with all current role mappings and creates appropriate autoprovisioning requests.

Role Provisioning and Deprovisioning

You must provision roles to users. Otherwise, they have no access to data or functions and can't perform application tasks. This topic explains how role mappings control role provisioning and deprovisioning.

Use the **Manage Role Provisioning Rules** or **Manage HCM Role Provisioning Rules** task to create role mappings.

Role Provisioning Methods

You can provision roles to users:

- Automatically
- Manually
  - Users such as line managers can provision roles manually to other users.
  - Users can request roles for themselves.

For both automatic and manual role provisioning, you create a role mapping to specify when a user becomes eligible for a role.

Role Types

You can provision data roles, abstract roles, and job roles to users. However, for Oracle Fusion Cloud HCM users, you typically include job roles in HCM data roles and provision those data roles.

Automatic Role Provisioning

Users acquire a role automatically when at least one of their assignments satisfies the conditions in the relevant role mapping. Provisioning occurs when you create or update worker assignments. For example, when you promote a worker to a management position, the worker acquires the line manager role automatically if an appropriate role mapping exists. All changes to assignments cause review and update of a worker's automatically provisioned roles.

Role Deprovisioning

Users lose automatically provisioned roles when they no longer satisfy the role-mapping conditions. For example, a line manager loses an automatically provisioned line manager role when he or she stops being a line manager. You can also manually deprovision automatically provisioned roles at any time.

Users lose manually provisioned roles automatically only when all of their work relationships are terminated. Otherwise, users keep manually provisioned roles until you deprovision them manually.

Roles at Termination

When you terminate a work relationship, the user automatically loses all automatically provisioned roles for which he or she no longer qualifies. The user loses manually provisioned roles only if he or she has no other work relationships. Otherwise, the user keeps manually provisioned roles until you remove them manually.

The user who's terminating a work relationship specifies when the user loses roles. Deprovisioning can occur:

- On the termination date
- On the day after the termination date

If you enter a future termination date, then role deprovisioning doesn't occur until that date or the day after. The Role Requests in the Last 30 Days section on the Manage User Account page is updated only when the deprovisioning request is created. Entries remain in that section until they're processed.

Role mappings can provision roles to users automatically at termination. For example, a terminated worker could acquire the custom role Retiree at termination based on assignment status and person type values.

Reversal of Termination

Reversing a termination removes any roles that the user acquired automatically at termination. It also provisions roles to the user as follows:

- Any manually provisioned roles that were lost automatically at termination are reinstated.
- As the autoprovisioning process runs automatically when a termination is reversed, roles are provisioned automatically as specified by current role-provisioning rules.

You must reinstate manually any roles that you removed manually, if appropriate.

Date-Effective Changes to Assignments

Automatic role provisioning and deprovisioning are based on current data. For a future-dated transaction, such as a future promotion, role provisioning occurs on the day the changes take effect. The **Send Pending LDAP Requests** process identifies future-dated transactions and manages role provisioning and deprovisioning at the appropriate time. These role-provisioning changes take effect on the system date. Therefore, a delay of up to 24 hours may occur before users in other time zones acquire their roles.

Autoprovisioning

Autoprovisioning is the automatic allocation or removal of user roles. It occurs for individual users when you create or update assignments. You can also apply autoprovisioning explicitly for the enterprise using the Autoprovision Roles for All Users process.

Roles That Autoprovisioning Affects

Autoprovisioning applies only to roles that have the **Autoprovision** option enabled in a role mapping.

It doesn't apply to roles without the **Autoprovision** option enabled.

The Autoprovision Roles for All Users Process

The **Autoprovision Roles for All Users** process compares all current user assignments with all current role mappings.

- Users with at least one assignment that matches the conditions in a role mapping and who don't currently have the associated roles acquire those roles.
- Users who currently have the roles but no longer satisfy the associated role-mapping conditions lose those roles.

When a user has no roles, his or her user account is also suspended automatically by default.

The process creates requests immediately to add or remove roles. These requests are processed by the **Send Pending LDAP Requests** process. When running **Autoprovision Roles for All Users**, you can specify when role requests are to be processed. You can either process them immediately or defer them as a batch to the next run of the **Send Pending LDAP Requests** process. Deferring the processing is better for performance, especially when thousands of role requests may be generated. Set the **Process Generated Role Requests** parameter to **No** to defer the processing. If you process the requests immediately, then **Autoprovision Roles for All Users** produces a report identifying the LDAP request ranges that were generated. Requests are processed on their effective dates.

When to Run the Process

You're recommended to run **Autoprovision Roles for All Users** after creating or editing role mappings. You may also have to run it after loading person records in bulk if you request user accounts for those records. If an appropriate role mapping exists before the load, then this process isn't necessary. Otherwise, you must run it to provision roles to new users loaded in bulk. Avoid running the process more than once in any day. Otherwise, the number of role requests that the process generates may slow the provisioning process. Only one instance of the process can run at a time.

Options for the Process

When processing a large number of requests, you can enable bulk mode for this process to improve performance. In the bulk mode, the process groups all users for the same role into one request, and assigns multiple users to single role at once. In the default non-bulk mode, one user is assigned to a role at a time.

To enable bulk mode, follow these steps:

1. In the Setup and Maintenance work area, search and open the task **Manage Profile Options**.
2. In the **Search Results** section, click the + (New) icon.
3. On the **Create Profile Option** page, enter the following values:
    - Profile Option Code = PER_AUTO_PROVISION_ROLES_ENABLE_BULK
    - Profile Display Name = PER_AUTO_PROVISION_ROLES_ENABLE_BULK
    - Application = Global Human Resources
    - Module = Users
    - Start Date = <Today's date>

    Click **Save and Close**.
4. On the **Manage Profile Options** page, select the **Enabled** and **Updateable** check boxes for Site Level. Click Save and Close.
5. In the Setup and Maintenance work area, search and open the **Manage Administrator Profile Values** task.
6. Search for the profile option code PER_AUTO_PROVISION_ROLES_ENABLE_BULK. In the Profile Value text box, enter 'Y'. Note that this value is for one-time use, and you need to reset the value again for the next run of the process. Click **Save and Close**.

You can enable multithreading for the process by setting the profile option ORA_PER_AUTO_PROVISION_ROLES_ENABLE_MULTITHREADING to 'Y'. This creates child jobs, which help in improving the performance.

For more information, see the topic Best Practices for User and Role Provisioning in HCM.

Autoprovisioning for Individual Users

You can apply autoprovisioning for individual users on the Manage User Account page.

Related Topics

- What happens when I autoprovision roles for a user?
- Schedule the Send Pending LDAP Requests Process
- Best Practices for User and Role Provisioning in HCM

User and Role Access Audit Report

The User and Role Access Audit Report provides details of the function and data security privileges granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console.

This report is based on data in the Applications Security tables, which you populate by running the **Import User and Role Application Security Data** process. To run the User and Role Access Audit Report:

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the **User and Role Access Audit Report** process.
3. In the Process Details dialog box, set parameters and click **Submit**.
4. Click **OK** to close the confirmation message.

Note: Only the roles at the top of a role hierarchy are included in the Role Name column of the All roles report. If you want to review a role that is lower down the role hierarchy, then apply a filter for the role in which you're interested, to the Inherited Role Hierarchy column.

User and Role Access Audit Report Parameters

Population Type

Set this parameter to one of these values to run the report for one user, one role, multiple users, or all roles.

- All roles
- Multiple users
- Role name
- User name

User Name

Search for and select the user name of a single user.

This field is enabled only when **Population Type** is **User name**.

Role Name

Search for and select the name of a single aggregate privilege or data, job, abstract, or duty role.

This field is enabled only when **Population Type** is **Role name**.

From User Name Starting With

Enter one or more characters from the start of the first user name in a range of user names.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of all users.

To User Name Starting With

Enter one or more characters from the start of the last user name in a range of user names.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of all users.

User Role Name Starts With

Enter one or more characters from the start of a role name.

This field is enabled only when **Population Type** is **Multiple users**. It enables you to report on a subset of all users and roles.

Data Security Policies

Select **Data Security Policies** to view the data security report for any population. If you leave the option deselected, then only the function security report is generated.

> **Note:** If you don't need the data security report, then leave the option deselected to reduce the report processing time.

Debug

Select **Debug** to include the role GUID in the report. The role GUID is used to troubleshoot. Select this option only when requested to do so by Oracle Support.

Viewing the Report Results

The report produces either one or two .zip files, depending on the parameters you select. When you select **Data Security Policies**, two .zip files are generated, one for data security policies and one for functional security policies in a hierarchical format.

The file names are in the following format: **[FILE_PREFIX]_[PROCESS_ID]_[DATE]_[TIME]_[FILE_SUFFIX]**. The file prefix depends on the specified **Population Type** value.

This table shows the file prefix values for each report type.

Report Type	File Prefix
User name	USER_NAME
Role name	ROLE_NAME
Multiple users	MULTIPLE_USERS
All roles	ALL_ROLES

This table shows the file suffix, file format, and file contents for each report type.

Report Type	File Suffix	File Format	File Contents
Any	DataSec	CSV	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when **Data Security Policies** is selected. **Note:** Extract the data security policies only when necessary, as generating this report is time consuming.
Any	Hierarchical	CSV	Functional security policies in a hierarchical format. The .zip file

Report Type	File Suffix	File Format	File Contents
			contains one file for each user or role.
• **Multiple users** • **All roles**	CSV	CSV	Functional security policies in a comma-separated, tabular format.

The process also produces a .zip file containing a diagnostic log.

For example, if you report on a job role at 13.30 on 17 December 2015 with process ID 201547 and the **Data Security Policies** option selected, then the report files are:

- **ROLE_NAME_201547_12-17-2015_13-30-00_DataSec.zip**
- **ROLE_NAME_201547_12-17-2015_13-30-00_Hierarchical.zip**
- **Diagnostic.zip**

Data Access

You can assign users access to appropriate data based on their job roles. The Oracle Fusion security model requires a three-way link between users, role, and data. It's summarized as: who can do what on which data.

Who refers to the users, what are the job roles the user is assigned, and which refers to the data that's specific to a particular security context, typically an element of the enterprise structure, such as a business unit, asset book, or ledger.

For example, consider a user, Mary Johnson, who manages accounts payable functions, such as processing supplier invoices for the US Operations business unit. In this scenario, Mary Johnson must be assigned a job role such as the predefined Accounts Payable Manager, and given access to the US Operations business unit.

The following table lists the elements of the enterprise structure to which users can be assigned access based on their job roles.

Product	Security Context
Oracle Fusion Cloud Financials	Business Unit Data Access Set Ledger Asset Book Control Budget Intercompany Organization Reference Data Set Legal Entity

Product	Security Context
Oracle Fusion Cloud Supply Chain Management	Inventory Organization Reference Data Set Cost Organization Inventory Organization Manufacturing Plant
Oracle Fusion Cloud Procurement	Business Unit
Oracle Fusion Cloud Project Portfolio Management	Project Organization Classification
Oracle Fusion Cloud Incentive Compensation	Business Unit

Assigning Data Access

Assigning data access to users is a three step process:

1. Create users using one of the following:
    - Manage Users task in Oracle Fusion Cloud Functional Setup Manager

      Specify user attributes such as user name, assigned business unit, legal employer, department, job, position, grade, and location.
    - Security Console
2. Assign at least one job role to users. Use Oracle Fusion Cloud Human Capital Management or the Security Console to assign job roles. Alternatively, define Role Provisioning Rules to auto-provision roles to users based on the users' work assignments.
3. Assign data access to users for each applicable job role. Use the Manage Data Access for Users task in the Functional Setup Manager. For General Ledger users, you can also use the Manage Data Access Set Data Access for Users task to assign data access. Alternatively, define Data Provisioning Rules to auto-provision data access to users based on the users' work assignments.

Related Topics

- Assign Data Access to Users

Assign Data Access to Users

Use the Manage Data Access for Users page to assign data access to users based on their job roles. You can assign data access to only one user at a time.

The following table lists the questions you can consider before assigning data access to users.

Decision to Consider	In This Example
Which user role is being given data access?	Accounts Payable Manager
What is the security context to which access is being given?	Business Unit

Prerequisites

Before you can complete this task, you must:

1. Create users and specify the user attributes such as a user name, assigned business unit, legal employer, department, job, position, grade and location, and so on. To create users, use the Manage Users task in the Functional Setup Manager or the Create User page. If you're implementing Oracle Fusion Cloud HCM, you can also use the Hire an Employee page. You can also use the Security Console to create the implementation users who create the setups, such as legal entities, business units, and so on, that are required to create the users in the Manage Users or Hire an Employee page.
2. Assign users their job roles. You can either use Oracle Fusion Cloud Human Capital Management or the Security Console to assign job roles.
3. Run the Retrieve Latest LDAP Changes process.

Assigning Data Access to Users Using a Spreadsheet

1. Sign in to the Functional Setup Manager as an IT Security Manager or Application Implementation Consultant and navigate to the Setup and Maintenance page.
2. Search for and select the Manage Data Access for Users task. Alternatively, you can perform this task through the product-specific task list.
3. Click **Users without Data Access** to view users who don't have data access. Alternatively, to assign additional data access to users, use the **Users with Data Access** option.
4. Select the **Security Context**, for our example, select **Business Unit**.
5. Search for users with no data access. For our example, enter **Accounts Payable Specialist** in the **Role** field.

   > **Note:** The search fields are related to the user attributes.

6. Click **Search**. The Search Results region displays users who don't have any data access.
7. Click the **Authorize Data Access** button to export the search results to a Microsoft Excel spreadsheet. You can provide data access to a group of users through the spreadsheet.
8. Click **OK** to open the spreadsheet using Microsoft Excel.
9. Select the **Security Context** from the list for each user.
10. Enter the **Security Context Value**.
    - To provide additional data access to the user, add a new row and enter the user name, role, security context, and security context value.
    - You can click the **View Data Access** button to see what other data access the user already has even if this is outside the parameters of the search. This may help to identify users you want to grant access to because of existing access.
11. Click the **Upload** button on the spreadsheet when you have assigned data access.
12. Select the upload options on the Upload Options window and click **OK**.
13. Note the status of your upload in the **Upload** column.

- If the status of the upload is **Successful** and there are no validation errors in the log file, you can view the data access assignment to the users using the search criteria on the Manage Data Access for Users page.
- If the upload status is **Failed**, check the details in your upload file, correct any errors, and upload the file again.

Related Topics

- Data Access

Revoke Data Access from Users

Use the Manage Data Access for Users page to revoke data access from users.

1. Sign-in to the Functional Setup Manager as an IT Security Manager or Application Implementation Consultant and navigate to the Setup and Maintenance page.
2. Search for and select the Manage Data Access for Users task. Alternatively, you can perform this task through the product-specific task list.
3. Click the **Users with Data Access** option.
4. Search for existing data access assignments you want to revoke by entering either a user name or a role name.
5. Click **Search**. The Search Results region displays data access assignments that match the search criteria.
6. Select the data access assignment you wish to revoke.
7. On the **Actions** menu, click **Revoke Data Access Assignments**.

   The selected data access assignment is revoked.

Revoking Data Access from Users Using a Spreadsheet

On the Manage Data Access for Users page, you can revoke access of multiple users using a spreadsheet

1. Sign-in to the Functional Setup Manager as an IT Security Manager or Application Implementation Consultant and navigate to the Setup and Maintenance page.
2. Search for and select the Manage Data Access for Users task. Alternatively, you can perform this task through the product-specific task list.
3. Click the **Authorize Data Access** button which would generate the security data access template spreadsheet. Save the spreadsheet and open it with Microsoft Excel.
4. To revoke a data access assignment, specify the assignment by providing the **Security Context**, **Security Context Value**, **User Name**, and **Role** in the spreadsheet, then select the value **No** in the **Active** column. Create a new row for each data access assignment you wish to revoke.
5. Click the **Upload** button when you have entered all the assignments you need to revoke in the spreadsheet.
   - If the status of the upload is Successful, it means the data access assignment is successfully revoked.
   - If the upload status is Failed, check the details in your upload file, correct any errors, and upload the file again.
   - If you see the following message, then the assignment for the entered combination of Security Context, Security Context Value, User Name, and Role can't be found or is no longer active:

     “This assignment doesn't exist. Enter an active assignment.”

View Role Information Using Security Dashboard

As an IT Security Manager, you can use the Security Dashboard to get a snapshot of the security roles and how those roles are provisioned in the Oracle Cloud Applications.

The information is sorted by role category and you can view details such as data security policy, function security policy, and users associated with a role. You can also perform a reverse search on a data security policy or a function security policy and view the associated roles.

You can search for roles using the Role Overview page. You can view the count of the roles which includes the inherited roles, data security policies, and function security policies on this page. Clicking the number in a tile on this page takes you to the corresponding page in the Role Dashboard. You can view role details either on the Role Overview page of the Security Dashboard or the Role Dashboard.

You can view role information such as the directly assigned function security policies and data security policies, roles assigned to users, directly assigned roles, and inherited roles list using the Role Dashboard. Clicking any role-related link on a page of the Security Dashboard takes you to the relevant page in the Role Dashboard. You can export the role information to a spreadsheet. The information on each tab is exported to a sheet in the spreadsheet. This dashboard supports a print-friendly view for a single role.

Here are the steps to view the Security Dashboard:

1. In the Reports and Analytics work area, click **Browse Catalog**.
2. On the Oracle BI page, open **Shared Folders** > **Security** > **Transaction Analysis Samples** > **Security Dashboard**.

   All pages of the dashboard are listed.
3. To view the Role Category Overview page, click **Open**.

   The page displays the number of roles in each role category in both tabular and graphical formats.
4. In the **Number of Roles** column, click the numeral value to view the role-related details.
5. Click **Role Overview** to view the role-specific information in the Role Dashboard.

Review Role Assignments

You can use the Security Console to either view the roles assigned to a user, or to identify the users who have a specific role.

You must have the IT Security Manager job role to perform these tasks.

View the Roles Assigned to a User

Follow these steps:

1. Open the Security Console.

2. On the Roles tab, search for and select the user.

   Depending on the enterprise setting, either a table or a graphical representation of the user's role hierarchy appears. Switch to the graphical representation if necessary to see the user and any roles that the user inherits directly. User and role names appear on hover. To expand an inherited role:

   a. Select the role and right-click.
   b. Select **Expand**. Repeat these steps as required to move down the hierarchy.

> **Tip:** Switch to the table to see the complete role hierarchy at once. You can export the details to Microsoft Excel from this view.

Identify Users Who Have a Specific Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select the role.
2. Depending on the enterprise setting, either a table or a graphical representation of the role hierarchy appears. Switch to the graphical representation if it doesn't appear by default.
3. Set **Expand Toward** to **Users**.

   > **Tip:** Set the **Expand Toward** option to control the direction of the graph. You can move either up the hierarchy from the selected role (toward users) or down the hierarchy from the selected role (toward privileges).

   In the refreshed graph, user names appear on hover. Users may inherit roles either directly or indirectly from other roles. Expand a role to view its hierarchy.
4. In the Legend, click the **Tabular View** icon for the **User** icon. The table lists all users who have the role. You can export this information to Microsoft Excel.

Review Role Hierarchies

On the Security Console you can review the role hierarchy of a job role, an abstract role, a duty role, or an HCM data role. You must have the IT Security Manager job role to perform this task.

> **Note:** Although you can review HCM data roles on the Security Console, you must manage them on the Manage HCM Data Role and Security Profiles page. Don't attempt to edit them on the Security Console.

Follow these steps:

1. On the Roles tab of the Security Console, ensure that **Expand Toward** is set to **Privileges**.
2. Search for and select the role. Depending on the enterprise setting, either a table or a graphical representation of the role appears.
3. If the table doesn't appear by default, click the **View as Table** icon. The table lists every role inherited either directly or indirectly by the selected role. Set **Show** to **Privileges** to switch from roles to privileges.

   > **Tip:** Enter text in a column search field and press **Enter** to show only those roles or privileges that contain the specified text.

Click **Export to Excel** to export the current table data to Microsoft Excel.

Compare Roles

You can compare any two roles to see the structural differences between them. As you compare roles, you can also add function and data security policies existing in the first role to the second role, providing that the second role isn't a predefined role.

For example, assume you have copied a role and edited the copy. You then upgrade to a new release. You can compare your edited role from the earlier release with the role as shipped in the later release. You may then decide whether to incorporate upgrade changes into your edited role. If the changes consist of new function or data security policies, you can upgrade your edited role by adding the new policies to it.

Selecting Roles for Comparison

1. Select the Roles tab in the Security Console.
2. Do any of the following:
    - Click the **Compare Roles** button.
    - Create a visualization graph, right-click one of its roles, and select the **Compare Roles** option.
    - Generate a list of roles in the Search Results column of the Roles page. Select one of them, and click its menu icon. In the menu, select **Compare Roles**.
3. Select roles for comparison:
    - If you began by clicking the **Compare Roles** button, select roles in both **First Role** and **Second Role** fields.
    - If you began by selecting a role in a visualization graph or the Search Results column, the **First Role** field displays the name of the role you selected. Select another role in the **Second Role** field.

    For either field, click the search icon, enter text, and select from a list of roles whose names contain that text.

Comparing Roles

1. Select two roles for comparison.
2. Use the **Filter Criteria** field to filter for any combination of these artifacts in the two roles:
    - Function security policies
    - Data security policies
    - Inherited roles
3. Use the **Show** field to determine whether the comparison returns:
    - All artifacts existing in each role
    - Those that exist only in one role, or only in the other role
    - Those that exist only in both roles
4. Click the **Compare** button.

You can export the results of a comparison to a spreadsheet. Select the **Export to Excel** option.

After you create the initial comparison, you can change the filter and show options. When you do, a new comparison is generated automatically.

Adding Policies to a Role

1. Select two roles for comparison.
    - As the **First Role**, select a role in which policies already exist.
    - As the **Second Role**, select the role to which you're adding the policies. This must be a custom role. You can't modify a predefined role.
2. Ensure that your selection in the Filter Criteria field excludes the **Inherited roles** option. You may select **Data security policies**, **Function security policies**, or both.
3. As a Show value, select **Only in first role**.
4. Click the **Compare** button.
5. Among the artifacts returned by the comparison, select those you want to copy.
6. An **Add to Second Role** option becomes active. Select it.

Create Roles in the Security Console

You can create a duty role, job role, or an abstract role using the Security Console.

In many cases, an efficient method of creating a role is to copy an existing role, then edit the copy to meet your requirements. Typically, you would create a role from scratch if no existing role is similar to the role you want to create.

To create a role from scratch, select the Roles tab in the Security Console, then click the Create Role button. Enter values in a series of role-creation pages, selecting Next or Back to navigate among them.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see topic *Guidance for Assigning Predefined Roles*.

Providing Basic Information

On a Basic Information page:

1. In the Role Name field, create a display name, for example North America Accounts Receivable Specialist.
2. In the Role Code field, create an internal name for the role, such as AR_NA_ACCOUNTS_RECEIVABLE_SPECIALIST_JOB.

    > **Note:** Do not use "ORA_" as the beginning of a role code. This prefix is reserved for roles predefined by Oracle. You can't edit a role with the ORA_ prefix.

3. In the Role Category field, select a tag that identifies a purpose the role serves in common with other roles. Typically, a tag specifies a role type and an application to which the role applies, such as Financials - Job Roles.

    If you select a duty-role category, you can't assign the role you're creating directly to users. To assign it, you would include it in the hierarchy of a job or abstract role, then assign that role to users.

> **Note:** You can't change the role category for existing roles.

4. Optionally, describe the role in the Description field.

Adding Function Security Policies

A function security policy selects a set of functional privileges, each of which permits use of a field or other user-interface feature. On a Function Security Policies page, you may define a policy for:

- A duty role. In this case, the policy selects functional privileges that may be inherited by duty, job, or abstract roles to which the duty is to belong.
- A job or abstract role. In this case, the policy selects functional privileges specific to that role.

As you define a policy, you can either add an individual privilege or copy all the privileges that belong to an existing role:

1. Select Add Function Security Policy.
2. In the Search field, select the value Privileges or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select a privilege or role. If you select a privilege, click Add Privilege to Role. If you select a role, click Add Selected Privileges.

> **Note:** The search results display all roles, whether they contain privileges or not. If a role doesn't contain privileges, there's nothing to add here. To add roles that don't contain privileges, go to the Role Hierarchy page.

The Function Security Policies page lists all selected privileges. When appropriate, it also lists the role from which a privilege is inherited. You can:

- Click a privilege to view details of the code resource it secures.
- Delete a privilege. You may, for example, have added the privileges associated with a role. If you want to use only some of them, you must delete the rest. To delete a privilege, click its x icon.

Adding Data Security Policies

A data security policy may be explicit or implicit.

- An explicit policy grants access to a particular set of data, such as that pertaining to a particular business unit. This type of policy isn't used in predefined roles in Oracle Fusion Cloud ERP.
- An implicit policy applies a data privilege (such as read) to a set of data from a specified data resource. Create this type of policy for a duty, job, or abstract role. For each implicit policy, you must grant at least the read and view privileges.

You can use a Data Security Policies page to manage implicit policies.

To create a data security policy, click the Create Data Security Policy button, then enter values that define the policy. A start date is required; a name, an end date, and a description are optional. Values that define the data access include:

- Data Resource: A database table.

- Data Set: A definition that selects a subset of the data made available by the data resource.
    - Select by key. Choose a primary key value, to limit the data set to a record in the data resource whose primary key matches the value you select.
    - Select by instance set. Choose a condition that defines a subset of the data in the data resource. Conditions vary by resource.
    - All values: Include all data from the data resource in your data set.
- Actions: Select one or more data privileges to apply to the data set you have defined.

The Data Security Polices page lists all policies defined for the role. You can edit or delete a policy: click the Actions button, and select the Edit or Remove option.

Configuring the Role Hierarchy

A Role Hierarchy page displays either a visualization graph, with the role you're creating as its focus, or a visualization table. Select the Show Graph button or View as Table button to select between them. In either case, link the role you're creating to other roles from which it's to inherit function and data security privileges.

- If you're creating a duty role, you can add duty roles or aggregate privileges to it. In effect, you're creating an expanded set of duties for incorporation into a job or abstract role.
- If you're creating a job or abstract role, you can add aggregate privileges, duty roles, or other job or abstract roles to it.

To add a role:

1. Select Add Role.
2. In a Search field, select a combination of role types and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select the role you want, and click Add Role Membership. You add not only the role you have selected, but also its entire hierarchy.

In the graph view, you can use the visualization Control Panel, Legend, and Overview tools to manipulate the nodes that define your role hierarchy.

Adding Users

On a Users page, you can select users to whom you want to assign a job or abstract role you're creating. (You can't assign a duty role directly to users.)

To add a user:

1. Select Add User.
2. In a Search field, select the value Users or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select a user or role. If you select a user, click Add User to Role. If you select a role, click Add Selected Users; this adds all its assigned users to the role you're creating.

The Users page lists all selected users. You can delete a user. You may, for example, have added all the users associated with a role. If you want to assign your new role only to some of them, you must delete the rest. To delete a user, click its x icon.

Completing the Role

On a Summary and Impact Report page, review the selections you have made. Summary listings show the numbers of function security policies, data security policies, roles, and users you have added and removed. An Impact listing shows the number of roles and users affected by your changes. Expand any of these listings to see names of policies, roles, or users included in its counts.

If you determine you must make changes, navigate back to the appropriate page and do so. If you're satisfied with the role, select Save and Close.

Related Topics

- Options for Viewing a Visualization Graph

Role Copying or Editing

Rather than create a role from scratch, you can copy a role, then edit the copy to create a new role. Or you can edit existing roles.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see topic *Guidance for Assigning Predefined Roles*.

Initiate a copy or an edit from the Roles tab in the Security Console. Do either of the following:

- Create a visualization graph and select any role in it. Right-click and select **Copy Role** or **Edit Role**.
- Generate a list of roles in the Search Results column of the Roles page. Select one of them and click its menu icon. In the menu, select **Copy Role** or **Edit Role**.

If you're copying a role, select one of two options in a Copy Option dialog:

- **Copy top role**: You copy only the role you have selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. If you select this option, subsequent changes to the inherited roles affect not only the source highest role, but also your copy.
- **Copy top role and inherited roles**: You copy not only the role you have selected, but also all of the roles in its hierarchy. Your copy of the highest role is connected to the new copies of subordinate roles. If you select this option, you insulate the copied role from changes to the original versions of the inherited roles.

Next, an editing train opens. Essentially, you follow the same process in editing a role as you would follow to create one. However, note the following:

- In the Basic Information page, a **Predefined role** box is checked if you selected the Edit Role option for a role shipped by Oracle. In that case, you can:
    - Add custom data security policies. Modify or remove those custom data security policies.
    - Add or remove users if the role is a job, abstract, or discretionary role.

  You can't:
    - Modify, add, or remove function security policies.
    - Modify or remove data security policies provided by Oracle.

- Modify the role hierarchy.

The **Predefined role** check box is cleared if you're editing a custom role or if you have copied a role. In that case, you can make any changes to role components.

- By default, the name and code of a copied role match the source role's, except a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.
- A copied role can't inherit users from a source job or abstract role. You must select users for the copied role. (They may include users who belong to the source role.)
- When you copy a role, the Role Hierarchy page displays all roles subordinate to it. However, you can add roles only to, or remove them from, the highest role you copied.

To monitor the status of a role-copy job, select the Administration tab, and then the Role Status tab of the Administration page.

Related Topics

- Generate a Visualization
- Create Roles in the Security Console

Security Console Role-Copy Options

When you copy a role on the Security Console, you have the option to either copy top role, or copy top role and inherited roles. This topic explains the effects of each of these options.

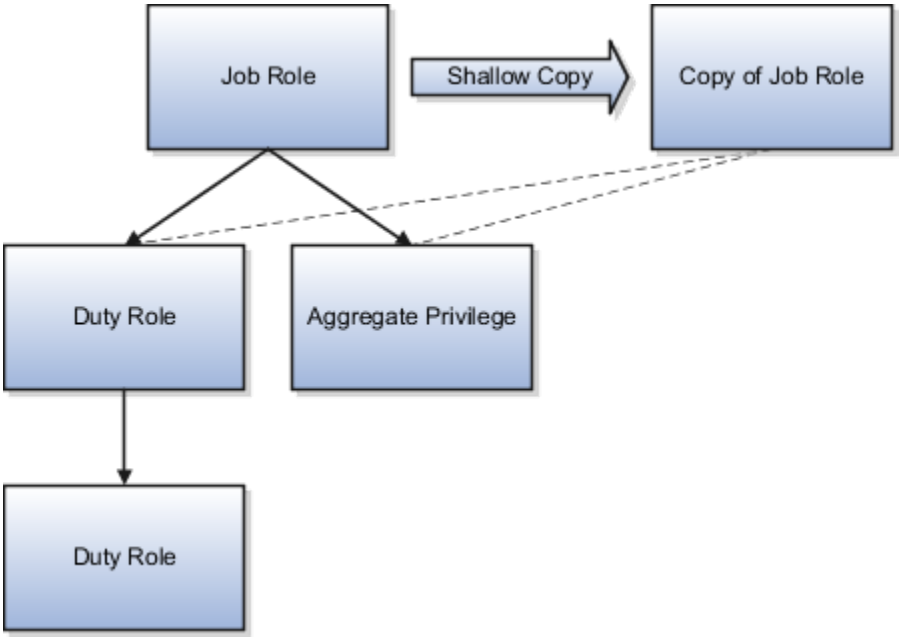
Copy Top Role

If you select the **Copy top role** option, then only the top role from the selected role hierarchy is copied. Memberships are created for the copy in the roles of which the original is a member. That is, the copy of the top role references the inherited role hierarchy of the source role. Any changes made to those inherited roles appear in both the source role and the copy. Therefore, you must take care when you edit the role hierarchy of the copy. You can:

- Add roles directly to the copy without affecting the source role.
- Remove any role from the copy that it inherits directly without affecting the source role. However, if you remove any role that's inherited indirectly by the copy, then any role that inherits the removed role's parent role is affected.
- Add or remove function and data security privileges that are granted directly to the copy of the top role.

If you copy a custom role and edit any inherited role, then the changes affect any role that inherits the edited role.

The option of copying the top role is referred to as a shallow copy. This figure summarizes the effects of a shallow copy. It shows that the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.



You're recommended to create a shallow copy unless you must make changes that could affect other roles or that you couldn't make to predefined roles. To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. To copy the inherited roles, select the **Copy top role and inherited roles** option.

> **Tip:** The Copy Role: Summary and Impact Report page provides a useful summary of your changes. Review this information to ensure that you haven't accidentally made a change that affects other roles.

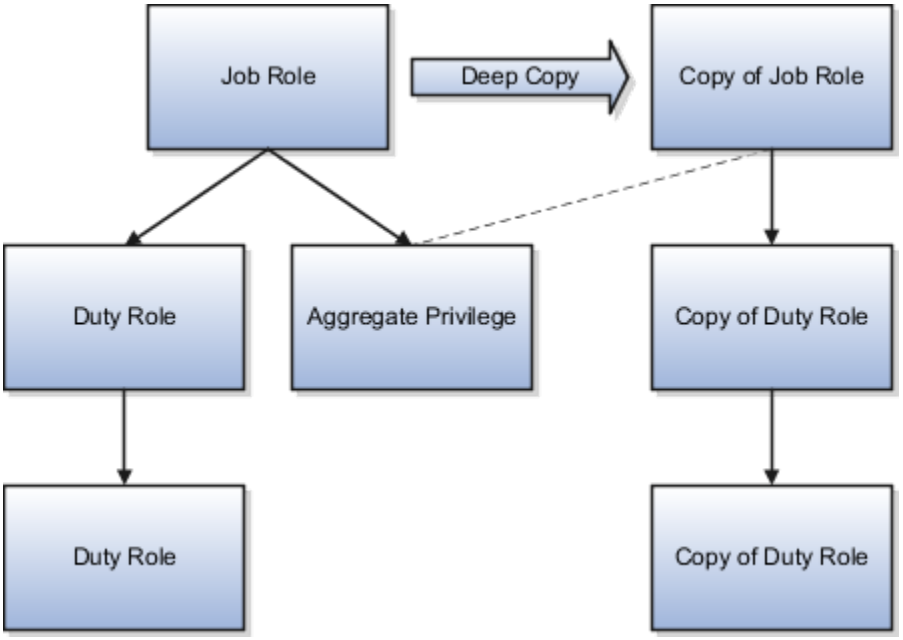
Copy Top Role and Inherited Roles

Selecting **Copy top role and inherited roles** is a request to copy the entire role hierarchy. These rules apply:

- Inherited aggregate privileges and middleware roles are never copied. Instead, membership is added to each aggregate privilege, or middleware role, for the copy of the source role.
- Inherited duty roles are copied if a copy with the same name doesn't already exist. Otherwise, membership is added to the existing **copies** of the duty roles for the new role.

When inherited duty roles are copied, custom duty roles are created. Therefore, you can edit them without affecting other roles. Equally, changes made subsequently to the source duty roles don't appear in the copies of those roles. For example, if those duty roles are predefined and are updated during upgrade, then you may have to update your copies manually after upgrade. This option is referred to as a deep copy.

This figure shows the effects of a deep copy. In this example, copies of the inherited duty roles with the same name don't already exist. Therefore, the inherited duty roles are copied when you copy the top role. Aggregate privileges are referenced from the new role.



Related Topics

- Guidelines for Copying HCM Roles
- Copy Job Role and Abstract Role

Copy Job Role and Abstract Role

You can copy any job role or abstract role and use it as the basis for a custom role. Copying roles is more efficient than creating them from scratch. You must have the IT Security Manager job role or privileges for this task.

Copy a Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

   > **Tip:** If you prefer, click the **Show Graph** icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the Copy Options dialog box, select a copy option.
5. Click **Copy Role**.

6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, **Description**, and **Enable Role for Access from All IP Addresses** values, as appropriate. **Enable Role for Access from All IP Addresses** appears only if location-based access is enabled.

   > **Tip:** The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make on the Copy Role: Basic Information page.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Status subtab of the Security Console Administration tab. When the status is **Complete**, you can edit the copied role.

   If you prefer, you can visit the intermediate train stops after the Copy Role: Basic Information page and edit your copy of the role before you save it.

Related Topics

- Security Console Role-Copy Options
- Edit Job Role and Abstract Role
- Guidelines for Copying HCM Roles

Edit Job Role and Abstract Role

You can create a role by copying a predefined job role or abstract role and editing the copy. You must have the IT Security Manager job role or privileges to perform this task.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see the topic *Guidance for Assigning Predefined Roles*.

Edit the Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code. If location-based access is enabled, then you can also manage the **Enable Role for Access from All IP Addresses** option.
4. Click **Next**.

Manage Functional Security Privileges

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. Select a privilege to view details of the code resources that it secures in the Details section of the page.

To remove a privilege from the role, select the privilege and click the **Delete** icon. To add a privilege to the role:

1. Click **Add Function Security Policy**.
2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from the selected role to your custom role.

   > **Tip:** If the role has no function security privileges, then you see an error message. You can add the role to the role hierarchy on the Edit Role: Role Hierarchy page, if appropriate.

   If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the Add Function Security Policy dialog box.
7. Click **Next**.

> **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Manage Data Security Policies

Make no changes on the Copy Role: Data Security Policies page.

Add and Remove Inherited Roles

The Edit Role: Role Hierarchy page shows the copied role and its inherited aggregate privileges and duty roles. The hierarchy is in tabular format by default. You can add or remove roles.

To remove a role:

1. Select the role in the table.
2. Click the **Delete** icon.
3. Click **OK** to close the confirmation message.

> **Note:** The role that you're removing must be inherited directly by the role that you're editing. If the role is inherited indirectly, then you must edit its parent role.

To add a role:

1. Click the **Add Role** icon.
2. In the Add Role Membership dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the Add Role Membership dialog box.

   The Edit Role: Role Hierarchy page shows the updated role hierarchy.

7. Click **Next**.

Provision the Role to Users

To provision the role to users, you must create a role mapping. Don't provision the role to users on the Security Console.

Review the Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

The role is available immediately.

Related Topics

- Copy Job Role and Abstract Role

Create Job Role and Abstract Role from Scratch

If the predefined roles aren't suitable or you need a role with few privileges, then you can create a role from scratch. To perform this task, you must have the IT Security Manager job role or privileges.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see the topic *Guidelines for Configuring Security*.

Enter Basic Information

Follow these steps:

1. On the Roles tab of the Security Console, click **Create Role**.
2. On the **Create Role: Basic Information** page, enter the role's display name in the **Role Name** field. For example, enter **XYZ HR Business Partner**.
3. Complete the **Role Code** field. For example, enter **XYZ_HR_BUSINESS_PARTNER_JOB**.

   Abstract roles have the suffix **_ABSTRACT**, and job roles have the suffix **_JOB**. Default prefixes for role codes and role names can be specified on the Roles subtab of the Security Console's Administration tab. These are used when copying roles. It's a good practice to use the same prefixes when defining job and abstract roles from scratch as when copying roles. This ensures that your custom roles follow the same naming pattern, whether they have been copied from other roles or created from scratch.
4. In the **Role Category** field, select either **HCM - Abstract Roles** or **HCM - Job Roles**, as appropriate.

   > **Note:** Be sure to select the **HCM - Job Roles** category when creating job roles. Otherwise, your job roles don't appear in the list of available job roles when you create an HCM data role.

5. If you're using location-based access, then you see the **Enable Role for Access from All IP Addresses** option. If you select this option, then users who have the role can access the tasks that the role secures from any IP address.

6. Click **Next**.

Add Functional Security Policies

When you create a role from scratch, you're most likely to add one or more aggregate privileges or duty roles to your role. You're less likely to grant function security privileges directly to the role.

If you aren't granting function security privileges, then click **Next**. Otherwise, to grant function security privileges to the role:

1. On the Privileges tab of the **Create Role: Functional Security Policies** page, click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from a selected role to your custom role.

   > **Tip:** If the role has no function security privileges, then you see an error message. You can add the role to the role hierarchy on the **Create Role: Role Hierarchy** page, if appropriate.

   If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the Add Function Security Policy dialog box.
7. Click **Next**.

You're recommended to include the following function security privileges in all HCM custom job and abstract roles:

- Approve Transactions - PER_APPROVE_TRANSACTIONS_PRIV
- View Notification Details - PER_VIEW_NOTIFICATION_DETAILS_PRIV
- Access HCM Common Components - HRC_ACCESS_HCM_COMMON_COMPONENTS_PRIV

If your custom job and abstract role are granted access to any of the responsive user experience pages, you might need to also add function security privileges that grant access to Lists of Values. For more information, see the topic *Privileges Roles Securing Lists of Values in Responsive User Experience Pages*.

> **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

Create Data Security Policies

Make no entries on the **Create Role: Data Security Policies** page.

Build the Role Hierarchy

The **Create Role: Role Hierarchy** page shows the hierarchy of your custom role in tabular format by default. You can add one or more aggregate privileges, job roles, abstract roles, and duty roles to the role. Typically, when creating a job or abstract role you add aggregate privileges. Roles are always added directly to the role that you're creating.

To add a role:

1. Click the **Add Role** icon.
2. In the Add Role Membership dialog box, search for and select the role to add.

3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. When you finish adding roles, close the Add Role Membership dialog box.
7. Click **Next**.

If your custom job and abstract role are granted access to any of the responsive user experience pages, you might need to also add aggregate privileges that grant access to Lists of Values. For more information, see the topic *Privileges and Roles Securing Lists of Values in Responsive User Experience Pages*.

Provision the Role

To provision the role to users, you must create a role mapping when the role exists. Don't provision the role to users on the Security Console.

Review the Role

On the Create Role: Summary and Impact Report page, review the summary of the changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

Your custom role is available immediately.

Copy and Edit Duty Roles

You can copy a duty role and edit the copy to create a duty role. Copying duty roles is the recommended way of creating duty roles. You must have the IT Security Manager job role or privileges to perform these tasks.

Copy a Duty Role

Follow these steps:

1. On the Roles tab of the Security Console, search for the duty role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

   > **Tip:** If you prefer, click the **Show Graph** icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the Copy Options dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

   > **Tip:** The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make on the Copy Role: Basic Information page.

7. Click the **Summary and Impact Report** train stop.

8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Edit the Copied Duty Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select your copy of the duty role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.

Manage Functional Security Policies

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. Select a privilege to view details of the code resources that it secures.

To remove a privilege from the role, select the privilege and click the **Delete** icon. To add a privilege to the role:

1. Click **Add Function Security Policy**.
2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to grant all function security privileges from the selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.

   > **Tip:** If the role has no function security privileges, then you see an error message. You can add the role to the role hierarchy on the Edit Role: Role Hierarchy page, if appropriate.

4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the Add Functional Security Policies dialog box.
7. Click **Next**.

> **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Manage Data Security Policies

Make no changes on the Edit Role: Data Security Policies page.

Add and Remove Inherited Roles

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles and aggregate privileges that it inherits. The hierarchy is in tabular format by default. You can add or remove roles.

To remove a role:

1. Select the role in the table.
2. Click the **Delete** icon.

3. Click **OK** to close the information message.

To add a role:

1. Click **Add Role**.
2. In the Add Role Membership dialog box, search for and select the role to add.
3. Click **Add Role Membership**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the Add Role Membership dialog box.
   The Edit Role: Role Hierarchy page shows the updated role hierarchy.
7. Click **Next**.

Review the Role

On the Edit Role: Summary and Impact Report page, review the summary of changes. Click **Back** to make corrections. Otherwise:

1. Click **Save and Close** to save the role.
2. Click **OK** to close the confirmation message.

The role is available immediately.

Related Topics

- Security Console Role-Copy Options
- Guidelines for Copying HCM Roles

Assign Roles for Access to Manage Scheduled Processes

Users can view and manage the scheduled processes that they submit, for example, to cancel the process or see the output. But, if they need to do that for processes other people submitted, they need certain roles.

Here are the roles and what they let users do with scheduled processes that anyone submitted.

Role Name	Role Code	View	Update	Cancel	See Output	Republish Output
ESS Operator Role	ESSOperator	Yes	No	No	No	No
ESS Monitor Role	ESSMonitor	Yes	No	No	No	No
ESS Administrator Role	ESSAdmin	Yes	Yes	Yes	No	No
BI Administrator Role	BIAdministrator	No	No	No	Yes	Yes

You can use the Security Console to create a custom role that has the needed roles, and assign the custom role to the user. Usually it's best to give access just by giving users the needed roles.

- But, sometimes you might need to give more access to specific tasks. For example, someone with ESS Monitor Role can see scheduled processes from others, but they also need to put processes on hold. And you don't want to give them the ESS Administrator Role because that would be too much access.
- Another case is that a user should not have access to all processes, but they still need to do certain tasks for some processes.

In these cases, the custom role you assign to users should have a data security policy, which gives users access to certain tasks. Here are the actions you should choose from for the policy, for the specific tasks you want to give users access to.

Action	Description
ESS_REQUEST_CANCEL	Cancel processes.
ESS_REQUEST_HOLD	Put processes on hold.
ESS_REQUEST_OUTPUT_READ	See the output from processes.
ESS_REQUEST_OUTPUT_UPDATE	Update the output from processes, for example to change what output you want if the process hasn't started running yet.
ESS_REQUEST_READ	Access processes and view details.
ESS_REQUEST_RELEASE	Release processes that were put on hold.

Access for All Scheduled Processes

Here's how you give someone access to manage all processes:

1. On the Roles page in the Security Console, click **Create Role**.
2. On the Create Role: Data Security Policies page, create a data security policy only if you need to give access to specific tasks.
    a. For the **Data Resource** field, select **ESS_REQUEST_HISTORY**.
    b. For the **Data Set** list, select **All Values**.
    c. For the **Actions** list, select any of the tasks that you want to give access to.
3. On the Create Role: Role Hierarchy page, add any of the needed roles.
4. On the Create Role: Users page, enter the users you want to assign this custom role to.

Access to Do Certain Tasks for Specific Processes

Say you don't want to give users access to all scheduled processes. When you create the custom role, instead of selecting a role like ESS Monitor Role, you enter a condition that controls what processes are included. You first create the condition in a data resource:

1. On the Administration page in the Security Console, click **Manage Database Resources** on the General tab.

2. On the Manage Database Resources and Policies page, search with **ESS_REQUEST_HISTORY** in the **Object Name** field.
3. In the Search Results table, select the ESS_REQUEST_HISTORY database resource and click **Edit**.
4. On the Edit Data Security page, click the Condition tab.
5. On the Condition tab, click the **Create** icon.
6. In the Create Database Resource Condition dialog box, select **SQL predicate** for the **Condition Type** option.
7. In the **SQL Predicate** field, enter SQL that identify what processes to give access to, for example:

```
EXISTS
(select 1 from dual)
and DEFINITION in (
'JobDefinition://oracle/apps/ess/hcm/users/SyncRolesJob'
)
```

8. Save your work.

Now you're ready to create your custom role and assign it to users:

1. On the Roles page in the Security Console, click **Create Role**.
2. On the Create Role: Data Security Policies page, create a data security policy.
    a. For the **Data Resource** field, select **ESS_REQUEST_HISTORY**.
    b. For the **Data Set** list, select **Select by instance set**.
    c. For the **Condition Name** list, select the condition you created.
    d. For the **Actions** list, select **ESS_REQUEST_READ** so users can access the process in the first place. Include any other action that you want to give access to. For example, if the user needs to see output, select **ESS_REQUEST_OUTPUT_READ** too.
3. On the Create Role: Users page, enter the users you want to assign this custom role to.

Related Topics

- Create Roles in the Security Console

Roles That Give Workflow Administrators Access

Workflow administrators for a specific product family need a predefined, family-specific workflow role to access tasks and manage submitted tasks for that family. To configure workflow tasks, they also need BPM Workflow System Admin Role (BPMWorkflowAdmin).

For example, administrators with the family-specific roles can do things like reassign submitted tasks, but they also need BPM Workflow System Admin Role to define approval rules. Other than the family-specific workflow roles, there's also BPM Workflow All Domains Administrator Role (BPMWorkflowAllDomainsAdmin). This gives administrators access to all product families. Assign to the administrators a role that contains the workflow roles appropriate for their needs.

Workflow Roles

Here are the roles that give access to workflow administration.

Product Family	Role Name	Role Code
All	BPM Workflow All Domains Administrator Role	BPMWorkflowAllDomainsAdmin

Product Family	Role Name	Role Code
All	BPM Workflow System Admin Role	BPMWorkflowAdmin
Financials	BPM Workflow Financials Administrator	BPMWorkflowFINAdmin
Higher Education	BPM Workflow Higher Education Administrator	BPMWorkflowHEDAdmin
Human Capital Management	BPM Workflow Human Capital Management	BPMWorkflowHCMAdmin
Incentive Compensation	BPM Workflow Incentive Compensation Administrator	BPMWorkflowOICAdmin
Procurement	BPM Workflow Procurement Administrator	BPMWorkflowPRCAdmin
Project Management	BPM Workflow Project Administrator	BPMWorkflowPRJAdmin
Sales	BPM Workflow Customer Relationship Management Administrator	BPMWorkflowCRMAdmin
Supply Chain Management	BPM Workflow Supply Chain Administrator	BPMWorkflowSCMAdmin

Things to Know About the Roles

Here are some things to know about how these workflow roles should be used and what the roles let administrators do.

- If your administrators manage workflow for multiple product families, you should give those users a custom role with the appropriate family-specific workflow roles added.
- If your administrators manage workflow for all product families, give them a custom role with BPM Workflow All Domains Administrator Role.

  > **CAUTION:** Assign BPM Workflow All Domains Administrator Role only if your administrators really do need access to workflow tasks from all product families. For access in multiple product families, but not all, use the workflow roles for the corresponding families instead.

- All administrators can see to-do tasks, no matter which role they have for workflow administration.
- Only administrators with either BPM Workflow All Domains Administrator Role or BPM Workflow System Admin Role would have Skip Current Assignment as an action to take on workflow tasks.

Related Topics

- Assign Roles to an Existing User
- Edit Job Role and Abstract Role
- Role Copying or Editing
- Create Roles in the Security Console
- Actions and Statuses for Workflow Tasks

User Role Membership Report

The User Role Membership Report lists role memberships for specified users.

To run the report process:

1. Open the Scheduled Processes work area.
2. Search for and select the **User Role Membership Report** process.

User Role Membership Report Parameters

You can specify any combination of the following parameters to identify the users whose role memberships are to appear in the report.

> **Note:** The report might take a while to complete if you run it for all users, depending on the number of users and their roles.

User Name Begins With

Enter one or more characters of the user name.

First Name Begins With

Enter one or more characters from the user's first name.

Last Name Begins With

Enter one or more characters from the user's last name.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Viewing the Report

The process produces a **UserRoleMemberships_processID_CSV.zip** file and a **Diagnostics_processID.zip** file. The **UserRoleMemberships_processID_CSV.zip** file contains the report output in CSV format. The report shows the parameters that you specified, followed by the user details for each user in the specified population. The user details include the user name, first and last names, user status, department, location, and role memberships.

The following table lists a brief description of these columns:

Column Name	Description
User Name	User ID assigned to the user.
First Name	First name of the user.
Last Name	Last name of the user.
LDAP User	Indicates whether the user exists in the Identity Store.
Department	Department of the user.
Location	Location of the user.
Policy Stripe	The policy store's application stripe where the user to role membership exists.
Assigned Role Name	Role code of the role assigned to the user.
Assigned Role Display Name	Role display name of the role assigned to the user.
Assigned Role Description	Description of the role assigned to the user.

Tip: First Name, Last Name, Department, and Location column values are applicable only to users that are linked to a person/worker.

Create a Custom Role with Limited Access

To delegate some of the IT security management tasks to a help desk member within your company without assigning the IT Security Manager role, create a custom role with specific privileges.

These privileges are exclusively meant for controlling user management access. You can assign these privileges directly to a custom role.

Users without the IT Security Manager role who are assigned custom roles with these privileges have limited access to the Security Console. These users can only lock or unlock other users, reset their password, or view user details. They can't create users or edit user details.

The following table lists the privileges and the associated access controls. It also includes details of pages where the user does the task:

Table with Privileges, Access Control Details, and Pages Where User Does the Task

Privilege Name and Code	Access Control Details	Page Where You Do this Task
Lock and Unlock User Account (ASE_LOCK_UNLOCK_USER_PRIV)	Lock or unlock a user account	User Accounts

Privilege Name and Code	Access Control Details	Page Where You Do this Task
Update Password for User Account (ASE_UPDATE_PASSWORD_FOR_USER_PRIV)	Reset the password for a user account	User Accounts and User Account Details
View User Account (ASE_VIEW_USER_ACCOUNT_PRIV)	View the details of a user account	User Account Details

Related Topics

- View Locked Users and Unlock Users
- Reset Passwords

Manage Roles in Custom OAuth Client Applications Using Application Extensions Page

You can manage user assignments and role assignments for platform applications and custom applications respectively from the Security Console.

In environments provisioned with an Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain, the Security Console displays the Application Extensions page. On this page, you can view all the available Platform Applications and Custom OAuth Client Applications.

- Platform Applications are provisioned by default in an OCI IAM identity domain environment. The roles assigned to these applications are the ones created in Oracle Fusion Cloud Applications. You can add or remove users to roles that are associated with a platform application.
- Custom OAuth Client Applications are those that the users create in an OCI IAM identity domain. The roles assigned to these applications have permission groups enabled. You can add or remove roles to a custom application.

Add User to Role Associated with Platform Application

1. On the **Application Extensions** page, in the Platform Applications section, click an application.
2. Click **Roles** (These roles are application-specific service roles available in the OCI IAM identity domain).
3. From the roles that are listed, click a role to which you want to add users to.
4. Click **Add** to search for and add users to the role.
5. Click **Done**.

Add Role to Custom OAuth Client Application

1. On the **Application Extensions** page, in the Custom OAuth Client Applications section, click an application.
2. Click **Roles** (These roles are permission groups enabled roles).
3. On the Roles page, click **Add** to search for and add roles to the application.
4. Click **Done**.

FAQs for Role Provisioning, Role Assignments, and Role Configuration

What's a role-mapping condition?

Most are assignment attributes, such as job or department. At least one of a user's assignments must match all assignment values in the role mapping for the user to qualify for the associated roles.

What's an associated role in a role mapping?

Any role that you want to provision to users. You can provision data roles, abstract roles, and job roles to users. The roles can be either predefined or custom.

What's the provisioning method?

The provisioning method identifies how the user acquired the role. This table describes its values.

Provisioning Method	Meaning
Automatic	The user qualifies for the role automatically based on his or her assignment attribute values.
Manual	Either another user assigned the role to the user, or the user requested the role.
External	The user acquired the role outside Oracle Applications Cloud.

How do I provision roles to users?

Use the following tasks to provision roles to users.

- Manage Users
- Provision Roles to Implementation Users

The Manage Users task is available in Oracle Fusion Cloud HCM, Oracle CX Sales, Oracle ERP Cloud, Oracle SCM Cloud, and Oracle Fusion Suppliers.

Human Resources (HR) transaction flows such as Hire and Promote also provision roles.

Related Topics

- Role Provisioning and Deprovisioning

How do I view the privileges or policies for a job role?

The most efficient way is to use the Security Console to search for and select the job role. When it appears in the visualizer, you can see all inherited roles, aggregate privileges, and privileges.

If you edit the role from the visualizer, you can see the policies on the function policies and data policies pages.

How can I tell which roles are provisioned to a user?

Use the Security Console to search for the user. When you select the user, the user and any roles assigned to the user appear in the visualizer. Navigate the nodes to see the role hierarchies and privileges.

You must be assigned the IT Security Manager role to access the Security Console.

Why can't a user access a task?

If a task doesn't appear in a user's task list, you may need to provision roles to the user.

A position or job and its included duties determine the tasks that users can perform. Provisioned roles provide access to tasks through the inherited duty roles.

The duty roles in a role hierarchy carry privileges to access functions and data. You don't assign duty roles directly to users. Instead, duty roles are assigned to job or abstract roles in a role hierarchy. If the duties assigned to a predefined job role don't match the corresponding job in your enterprise, you can create copies of job roles and add duties to or remove duties from the copy.

> **Note:** You can't change predefined roles to add or remove duties. In the Security Console, you can identify predefined roles by the ORA_ prefix in the Role Code field. Create copies and update the copies instead.

Users are generally provisioned with roles based on role provisioning rules. If a user requests a role to access a task, always review the security reference implementation to determine the most appropriate role.

How can I design roles?

You can simulate menus that existing roles present to users to determine how the access they provide may be expanded. Create a visualization, or populate the Search Results column with a selection of roles or users.

Select the user or role and click the Actions menu. A menu appears, click Simulate Navigator.

A simulated Navigator menu appears, listing menu and task entries. If the menu item appears without a lock, the menu isn't authorized for the role or user. If the menu item appears with a lock, the menu is authorized for the role or user.

Click any menu item and select either of two options. One lists roles that grant access to the menu item. The other lists privileges required for access to the menu item.

How do I create a role hierarchy?

The most efficient way to create role hierarchies is to use the Security Console. You use the Edit Role action to navigate through the steps and add roles and privileges in the visualizer or table view.

Why would I need to remove duty roles from a role hierarchy?

If your custom duty roles enable actions and user interface features that your enterprise doesn't want users to perform in your application.

> **Note:** Don't remove duty roles from predefined job or abstract roles in the reference implementation. In the Security Console, you can identify predefined application roles by the ORA_ prefix in the **Role Code** field. You must copy any role that doesn't match your needs, and then edit the copy.

How do I create a new job role?

Click the Create Role button in the Security Console to create job roles. Enter a job role category in the Create Roles page and then navigate to each subsequent page that you see in the page header.

You can add functional and data security policies, roles, and privileges to create the job role.

8 Location-Based Access

Overview of Location-Based Access

You can use location-based access to control user access to tasks and data based on their roles and computer IP addresses.

To enable location-based access and make a role public, you must have the IT Security Manager role. You can make a role public only when location-based access is enabled. To enable location-based access, you must register the IP addresses of computers from which the users usually sign in to the application.

Let's take an example to understand how location-based access is useful. You want your users to have complete access to tasks or features when they're signed in to the application from your office network. But you want to restrict the access if the users are signing in from a home computer or an internet kiosk. To control the user access, you must enable location-based access and register the IP addresses of your office computers on the Security Console. Users have complete access to the tasks or features if they sign in from office computers. If they sign in to the application from an unregistered computer, they can view and access only the generic tasks that aren't tied to any particular role. From an unregistered computer, they can't access the role-based tasks, which they could access from office.

What Happens When You Enable Location-Based Access

When you enable location-based access, users who sign in to the application from registered IP addresses have complete access to all tasks. On the other hand, users signing in from unregistered IP addresses have no access to their role-based tasks and data. However, you can grant complete access to these users too, when required. You can also grant public access (access from all IP addresses) to certain roles. The users associated with those roles can access all tasks, no matter which IP address they sign in from.

Prerequisite

To make sure that an administrator can regain access to Oracle Applications Cloud if an accidental account lock out occurs, the administrator must have the following settings configured:

- A valid email
- The IT Security Manager role
- Email notifications are enabled

Related Topics

- How Location-Based Access Works
- Enable and Disable Location-Based Access

How Location-Based Access Works

Location-based access combines the registered IP addresses of the computers and public roles to control access to the application.

Scenarios

To understand how location-based access works, consider the following scenarios and their effect on user access.

To avoid any access-related issue, carefully examine the given scenarios and plan well before you enable location-based access.

Scenario	Impact on User Access
You disable location-based access.	All users signing into the application from their respective computers continue to have the same level of access as they had earlier.
You enable location-based access and register few IP addresses, but don't grant public access to any role.	• Users who sign into the application from the registered IP addresses have access to their tasks as usual. • Users signing in from unregistered IP addresses can access only the generic tasks that aren't tied to any particular role.
You enable location-based access, register a few IP addresses, and grant public access to certain roles.	• Users signing in from the registered IP addresses have complete access. • Users signing in from unregistered IP addresses can't access any role-based tasks unless you grant public access to those roles. If you have made a role public, users can access all the tasks tied to that role.
You enable location-based access, but don't register any valid IP address, and don't grant public access to any role.	Users can sign in with valid credentials but can access only the generic tasks that aren't assigned to a specific role. **CAUTION:** Try and avoid this scenario. Register at least one valid IP address and grant public access (access from all IP addresses) to IT Security Manager role when you enable location-based access.

Related Topics

- How can I make a role public?
- How can I ensure that I always have access to the Security Console?

Enable and Disable Location-Based Access

You can enable location-based access so that you can allow users to access tasks and data based on their roles and registered IP addresses. By default, location-based access is disabled.

Before You Start

Configure location-based access in a test environment and try it out before you configure it in a production environment. You must have the IT Security Manager role to enable location-based access. Additionally, you must:

- Set up a valid email address. When required, the location-based access control reset or recovery notification is sent to that email address.

- Add yourself to the user category for which the notification template **ORA Administration Activity Request Template** is enabled.
- Keep the list of valid IP addresses ready.

Enable Location-Based Access

1. Click **Navigator** > **Tools** > **Security Console**.
2. On the Administration page, click the Location Based Access tab.
3. Select **Enable Location Based Access**.
4. In the **IP Address Allowlist** text box, enter one or more IP addresses separated by commas. For example, 192.168.10.12, 192.168.10.0. To indicate a range of IP addresses, you may follow the Classless Inter-Domain Routing (CIDR) notation, such as 192.168.10.0/24.

   > **Note:** You can enter the IP address (IPv4 only) range suffix only up to 32 in the **IP Address Allowlist** text box. For example, 168.1.192.0/32 to 168.1.192.32/32.

   > **Tip:** Your computer's IP address appears on the page. Add that IP address to the list so that your access to the application remains unaffected when you sign in from that computer.

5. Click **Save**.
6. Review the confirmation message and click **OK**.

After you enable location-based access, make the IT Security Manager's role public to access Security Console even from an unregistered IP address.

Disable Location-Based Access

To disable location-based access, deselect the **Enable Location Based Access** check box. The existing IP addresses remain in a read-only state so that you can reuse the same information when you enable the functionality again. At that point, you can add or remove IP addresses based on your need.

Related Topics

- What is allowlisting?
- Why can't I see the Location Based Access tab on the Administration page?

FAQs for Location-Based Access

What is allowlisting?

Allowlisting is the process of granting trusted entities access to data or applications. When you enable location-based access and register the IP addresses of computers, you're storing those IP addresses as trusted points of access.

You can include IP Addresses of all computers hosting cloud applications that require access to Oracle Applications Cloud. In other words, you're allowlisting those IP addresses. Users signing in from those computers are considered as trusted users and have unrestricted access to the application.

Why can't I see the Location Based Access tab on the Administration page?

To prevent any incorrect configuration, the profile option Enable Access to Location Based Access Control associated with the Location Based Access tab is perhaps disabled. As a result, the tab isn't visible.

Contact your Application Implementation Consultant or Administrator to enable the profile option so that the Location Based Access tab appears on the Administration page.

How can I make a role public?

On the Security Console, identify the role that you want to make public. Except duty roles, you can make all roles public. On the Edit Role page, select the option Enable Role for Access from All IP Addresses and save the changes.

Note: You can make a role public only if location based access is enabled.

How can I ensure that I always have access to the Security Console?

If location-based access is enabled, you must add your computer's IP address to the allowlist. Also ensure that the IT Security Manager role is granted public access.

Even if you have to sign in from an unregistered computer, you can still access the Security Console and other tasks associated with the IT Security Manager role.

How can I disable Location-based Access when I am not signed in to the application?

You want to disable location-based access but you're locked out of the application and can't sign in to the Security Console. You must request access to the Administration Activity page using the URL provided to the administrators.

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Click the URL and you're directed to a secure Administrator Activity page. Select the **Disable Location Based Access** option and click **Submit**. You receive a confirmation that location-based access is disabled. Immediately, you're redirected to the Oracle Applications Cloud page where you can sign in using your registered user name and password, and gain access to tasks and data as earlier.

How can I disable Location-based Access when I am locked out of the application?

If you're locked out of the application for some reason, use the following Administration Activity URL to disable location-based access. Only an administration user with the IT Security Manager job role can perform this unlock operation.

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Location Based Access Disabled Confirmation Template

How many IP Addresses can I enter in the IP Address Allowlist text box?

Ensure that the number of characters of the IP Address list that you enter in the IP Addresses Allowlist text box doesn't exceed 10000 characters.

If you want to include more IP addresses beyond the 10000 characters limit, then you must enable the profile option ASE_EXTEND_LOCATION_BASED_ACCESS_CONTROL_IP_STORAGE.

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search the following **Profile Option Code**:

   ASE_EXTEND_LOCATION_BASED_ACCESS_CONTROL_IP_STORAGE
3. In the **Profile Value** drop-down list, select **Yes**.
4. Click **Save and Close**.

If your organization has a huge network of computers, then you can import a .csv file containing the list of IP addresses. If the number of characters in the file doesn't exceed 10000 characters, the import is successful. If the number of characters exceed the limit, the import completes with a warning.

Do these steps:

1. In the Setup and Maintenance work area, select **All Tasks** from the **Show** drop-down list in the Initial Users section.
2. Click **Actions** for the task **Manage Applications Security Preferences**.
3. Click **Import from CSV File**, **Create New**.
4. Click **Browse** to select the file.

5. Click **Submit**.

   If the number of characters doesn't exceed 10000, the file is imported successfully. Else, the import completes with a warning.

9 Single Sign-On

Oracle Applications Cloud as the Single Sign-On (SSO) Service Provider

Your users are likely to access different internal and external applications to perform their tasks. They might require access to different applications hosted by partners, vendors, and suppliers.

Certainly, users won't like authenticating themselves each time they access a different application. This is where you as the IT Manager can make a difference. You can provide your users with a seamless single sign-on experience, when you set up Oracle Applications Cloud as a single sign-on service provider.

Your users are registered with identity providers who store and manage their identity and credentials. In Security Console, you can add those identity providers so that you can verify those users without having to store that information.

> **Note:** The identity service associated with your Oracle Fusion Cloud Applications is getting upgraded to the Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain.If your environment is yet to be upgraded, you can continue to use the Security Console to configure the Single Sign-On settings with the information provided in this section. After your environment is upgraded, see *Federating with Identity Providers* to federate an Oracle Fusion Cloud Applications environment identity domain. See also *How do I find the identity domain for a Fusion Applications environment?*

Initial Sign-in

On a typical working day, when users sign in for the first time, they request access to an application or a web page. Oracle Applications Cloud, which is set up as a service provider, sends a verification request to the user's identity provider who's already added to the Security Console. The identity provider verifies the user credentials and sends the authorization and authentication response back to the service provider. After successful authentication, users are granted access to the required application or web page. Because the authentication is valid across your enterprise network, users don't have to sign in again when accessing different applications available on the same network. This entire trust chain between the service provider and the various identity providers is established using the Security Assertion Markup Language (SAML) 2.0 standards.

Final Sign-out

Single sign-on also applies to signing out of the enterprise network. When users sign out from one application, they're automatically signed out from all applications on the network. This is to prevent unauthorized access and to ensure that data remains secure all the time.

Prerequisite

To make sure that an administrator can regain access to Oracle Applications Cloud if an accidental account lock out occurs, the administrator must have the following settings configured:

- A valid email

- The IT Security Manager role
- Email notifications are enabled

Configure Single Sign-On

To enable single sign-on in your environment, complete the settings in the Single Sign-on Configuration section on the Security Console. This configuration lets you enable a login page and a page to which users must be redirected to after logging out of the application.

Do these steps:

1. On the Security Console, click the **Single Sign-On** tab.
2. In the Single Sign-On Configuration section, click **Edit**.
3. Enter the **Sign Out URL**. Users are redirected to this page once they sign out from the application.

   Note: The Sign Out URL is the same for all the identity providers that you configure.

4. If **Enable Chooser Login Page** isn't enabled already, select it to display the service provider's single sign-on page along with your company's login page.
5. Click **Save**.

To configure Oracle Applications Cloud as the service provider, you must do the following:

- Review the service provider details
- Add an identity provider
- Test the identity provider
- Enable the identity provider

On the Security Console, go to the Single Sign-On tab and click **Create Identity Provider**.

Note: Oracle Cloud Applications support all SAML 2.0 compatible federation servers.

Review Service Provider Details

- Service provider metadata. The URL references to an XML file that you can download and view.
- Service provider signing certificate.
- Service provider encryption certificate.

You must share these details with the identity providers so that they can use them to configure your application as the associated service provider.

Add an Identity Provider

You can add as many identity providers as required to facilitate single sign-on for all your users. However, one of them must be the default identity provider.

Before you begin:

One of the important steps in adding an identity provider is to import the metadata content of the identity provider. The metadata file contains the authentication information and also the signed and encrypted certificates of the identity

provider. Make sure you have the metadata XML file or the URL readily available. Without the file, the setup isn't complete.

Note: Including encryption certificate in the metadata file is optional.

1. On the Security Console, click **Single Sign-On** > **Create Identity Provider**.
2. On the Identity Provider Details page, click **Edit** and enter the identity provider details:
    - Provide a **Name** and **Description** for the identity provider. Ensure that the identity provider name is unique for the partnership.
    - Select the relevant Name ID Format. If you have an email as the name of the identity provider, select **Email**. Otherwise, leave it as **Unspecified**.
    - Enter the **Relay State URL**. Users are directed to this URL to sign and authenticate irrespective of which application they want to access.
    - Select the **Default Identity Provider** check box to make this identity provider the default one.
3. Import the identity provider metadata:
    - If it's an XML file, click **Browse** and select it.
    - If it's available on a web page, select the **External URL** check box and enter the URL. External URL isn't stored in this configuration and is used only for importing the identity provider metadata during identity provider creation or modification.

    Note: The metadata XML file must be Base64 encoded.
4. Click **Save and Close**.

    Note: Oracle Applications Cloud can't be used as an identity provider.

Test the Identity Provider

Click the Diagnostics and Activation tab to verify if the identity provider that you added works as expected.

1. Click the **Test** button to run the diagnostics. The Initiate Federation SSO page appears.
2. Click the **Start SSO** button. You're prompted to enter the user credentials of any user registered with the identity provider. The test validates whether the federation single sign-on is successful or not. The result summary includes the following details:
    - Status of authentication: success or failure
    - The attributes passed in the assertion
    - The assertion message in XML

You can review the log messages that appear in the Federation Logs section to identify if there are any configuration issues with the identity provider.

Note: You must run the test whenever there's a change in the identity provider configuration.

Enable the Identity Provider

If everything looks fine, you can go ahead and enable the identity provider. While you're on the Diagnostics and Activation page, click **Edit** and select the **Enable Identity Provider** check box. The identity provider is now active.

Note: You can enable an identity provider only after you import service provider metadata into the identity provider.

FAQs for Single Sign-On

Does the service provider store user passwords?

No. Passwords are stored with the identity providers. When a user signs in, the identity provider authenticates the password, authorizes the request to access an application, and sends that confirmation back to the service provider.

The service provider then allows users to access the application or web page.

Can I set up an identity provider without enabling it?

Yes, you can set up an identity provider and test it thoroughly before enabling it. By default, an identity provider remains disabled. You can disable an identity provider at any time.

How can I allow my users to sign in using their company's credentials?

On the Security Console, go to Single Sign-On Identity Provider Details page and make sure that the Enable Chooser Login Page check box is selected.

When your users access the main portal page, they can sign in using one of the following options:

- The single sign-on credentials registered with the identity provider
- The single sign-on credentials registered with their company

What should I do to extend the validity of certificates provided by the identity provider?

Pay attention to the notifications you receive about certificate expiry. Request your identity provider to share with you the updated metadata file containing renewed certificate validity details.

Once you upload the metadata file, the validity of the certificate is automatically renewed. You will have to monitor this information at intervals to ensure that the certificates remain valid at all times.

How can the identity provider obtain renewed certificates from the service provider?

The identity provider can submit a service request to the service provider asking for the renewed signing and encryption certificates.

How can I disable Single Sign-On when I am not signed in to the application?

You must request access to the Administration Activity page using the URL provided to the administrators.

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Click the URL and you're directed to a secure Administrator Activity page. Select the **Disable Single Sign On** option and click **Submit**. You receive a confirmation that single sign-on is disabled. Immediately, you're redirected to the Oracle Applications Cloud page where you can sign in using your registered user name and password.

How can I disable Single Sign-On when I am locked out of the application?

If you're locked out of the application for some reason, use the following Administration Activity URL to disable single sign-on. Only an administrator user with the IT Security Manager job role can perform this unlock operation.

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Single Sign-On Disabled Confirmation Template

What are the different events and notifications associated with the Single Sign-On functionality?

Automatic notifications are sent for the following events associated with single sign-on.

- When an administrator requests access to the Administration Activity page to disable single sign-on
- When the single sign-on functionality is disabled using the Administration Activity page, notification is sent to that user who disabled SSO.
- When the external identity provider's signing certificate is about to expire
- When the service provider's signing certificate is about to expire
- When the service provider's encryption certificate is about to expire

Note: Notifications are sent to users who are assigned the **Administer SSO** (ASE_ADMINISTER_SSO_PRIV) privilege,according to the following schedule:

- First notification - 60 days before the expiry date
- Second notification - 30 days before the expiry date
- Last notification - 10 days before the expiry date.

How do I reimport Identity Provider metadata?

Whenever you get an updated metadata file from the Identity Provider you must reimport the file into the application to continue using SSO configuration.

1. On the Identity Provider Details page, click **Edit**.
2. Import the identity provider metadata:
    - If it's an XML file, click **Browse** and select it.
    - If it's available on a web page, select the **External URL** check box and enter the URL.

      Note: The metadata XML file must be Base64 encoded.
3. Click **Save and Close**.

Note: Remember to test the Identity Provider after reimport.

Why does the company login page not appear even after enabling identity provider?

If an existing identity provider that wasn't created through Security Console was enabled before enabling single sign-on, then single sign-on isn't enabled.

Do these steps:

1. On the Security Console, click the **Single Sign-On** tab.
2. From the list of existing identity providers, click the identity provider that you want to update.
3. Click the **Diagnostics and Activation** tab and click **Edit**.
4. Clear the **Enable Identity Provider** option to disable the identity provider and click **Save and Close**.
5. On the Diagnostics and Activation page, click **Edit** again.
6. Click **Test** to test the identity provider. Click **Yes** in the warning message that appears to open the Initiate Federation SSO page.
7. Select the identity provider from the **Partner** drop-down list.
8. Click **Start SSO**. You are prompted to authenticate the identity provider. On successful authentication, a test result page appears.
9. On the Diagnostics and Activation details page, select **Enable Identity Provider**.
10. Click **Save and Close** to return to the Diagnostics and Activation page.
11. Click **Done** to return to the Single Sign-On page. In the Single Sign-On Configuration section, **Single Sign-On Enabled** has a tick mark to indicate that single sign-on has been enabled.

After enabling single sign-on, you can now see the company login page.

Is an identity provider using the SHA1 signing algorithm supported for federation?

No, an identity provider using the SHA1 signing algorithm isn't supported for federation. Delete the identity provider using the SHA1 signing algorithm.

To use the same identity provider that you deleted, create the identity provider again using the SHA2 signing algorithm to configure federation partnership.

How to access SSO Federation logs for identity providers?

1. On the Security Console, click the **Single Sign-On** tab.
2. Among the list of added identity providers, click the one for which you want to view the logs.
3. On the Identity Provider Details page, click the **Diagnostics and Activation** tab.
4. In the Federation Logs section, select the period for which you want to view the logs and click **Refresh**.
5. From the list of logs, select an entry, and in the section right after the list, expand the node to view the details.

10 API Authentication

Configure Outbound API Authentication Using JWT Custom Claims

A system account is an account used for integrating Oracle Applications Cloud with third-party applications. This account isn't associated with a user but it must have roles with access to REST APIs.

System account uses basic authentication to authenticate users even if single sign-on is enabled. Security Console's password policy applies to a system account and so the password of this account expires based on the password policy.

Critical tasks such as batch operations or data synchronizations must continue without any interruption or the need to re-authenticate at intervals. To support such tasks, you need to define custom parameters for authentication. Using Security Console, you can define a JSON Web Token (JWT) that can be used by REST APIs to automate system authentication without you having to authenticate manually.

JWT is an access token that contains custom claim name and claim values. Custom claims are name and value pairs that you can define in a JWT. To uniquely identify a user, you can add the user's email address to the token along with the standard user name and password.

Example, suppose you want to integrate Oracle Applications Cloud with a third-party application. This integration uses the JWT Custom Claims to authenticate the users who sign into Oracle Applications Cloud to access the third-party application.

Do these steps to define a JWT that will be used for integration with third-party application:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**, **Edit**.
3. Enter a name and description for the external client application that you want to create.
4. In the **Select Client Type** drop-down list, select **JWT Custom Claims** and click **Save and Close**.
5. Click the JWT Custom Claims Details tab and click **Edit**.
6. In the Token Settings section, if required, update the **Token Expiration Time** and **Signing Algorithm**. Default values are 30 minutes and RS256 respectively.
7. Click **Save**.
8. In the JWT Custom Claims section, click **Add**. You can either select a name from the predefined values in the drop-down list or select **Other** and enter a name of your choice.
9. Select a value for the custom claim. If you select **Free-form**, enter the value in the following text box. You can add more JWT custom claims using the **Add** button.
10. Click **Save**. You can add more parameters as required.
11. Click **Done** to return to the JWT Custom Claims Details page.

    You can view the token created for authentication using the **View JWT** button on the JWT Custom Claims Details page. The View JWT window displays the header and payload of the JWT.
12. Click **Done** again to return to the API Authentication page. You can view the newly created JWT Custom Claim in this page.

You can delete a JWT custom claim on the API Authentication page.

Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol

OAuth is an open industry standard protocol that allows applications access information from other third-party applications, on behalf of the users. The OAuth authorization protocol manages access securely without revealing any passwords to the client application, such as Oracle Applications Cloud.

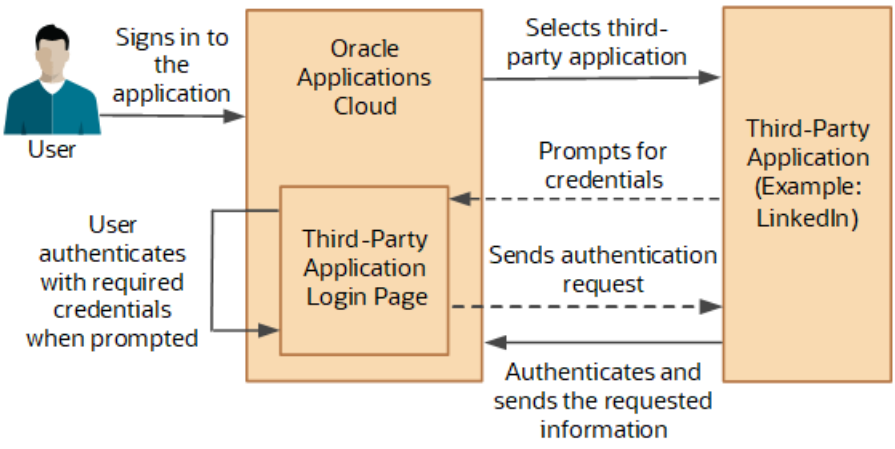
To understand the OAuth authorization protocol, let's take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required permissions to Oracle Applications Cloud to access the information from LinkedIn.

As you notice, there are three parties involved in the entire authentication process: Oracle Applications Cloud, the user who owns information on LinkedIn, and LinkedIn's authorization server. This authorization protocol always requires three such parties for the authentication to complete. Therefore, this protocol is called three-legged OAuth authorization protocol.

Here's the sequential representation of the end-to-end authorization process between Oracle Applications Cloud and the LinkedIn server:

1. Oracle Applications Cloud registers the Client ID and Client Secret and other settings required for authorization.
2. When an Oracle Applications Cloud user wants to access profile information, the LinkedIn login page appears, where the user authenticates using the required credentials.
3. On successful authentication, LinkedIn's authorization server sends an authorization code to Oracle Applications Cloud.
4. Oracle Applications Cloud receives the authorization code and sends an access token request to LinkedIn. LinkedIn processes the access token request and returns an access token.
5. Oracle Applications Cloud uses the access token to call LinkedIn APIs on behalf of the user to access the required information. At runtime, Oracle Web Services Manager manages the entire authorization process.

The following graphic shows the entire authorization process between Oracle Applications Cloud and the LinkedIn server:



Using the Security Console, you configure the three-legged OAuth authorization settings for Oracle Applications Cloud. Once configured, users can access their information from a third-party application, within Oracle Applications Cloud.

Before you proceed, you must enable a profile option to get the OAuth Three-Legged option on the External Client Applications Details page. See the Related Information section for more information.

Here's how you configure three-legged OAuth authorization:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**.
3. On the External Client Application Details page, click **Edit**.
4. Enter a name and description for the external client application that you want to create.
5. In the **Select Client Type** drop-down list, select **OAuth Three-Legged**.
6. Click **Save and Close** to return to the External Client Application Details page.
7. Click the OAuth Details tab.
8. On the Three-Legged OAuth Details page, click **Edit**.
9. Enter the appropriate values in the following required fields:
    - Authorization URL - The authorization code link that the authorization server sends to the application.
    - Redirect URL - The page to which the user is redirected to after successful authorization of application.
    - Access Token URL - The access token that's sent from the authorization server to the application.
    - Servlet Application URL - The access token that's sent from the authorization server to the application.
    - Client ID - The access token that's sent from the authorization server to the application.
    - Client Secret - The access token that's sent from the authorization server to the application.
    - Client Scope - The access token that's sent from the authorization server to the application.
10. Enter the appropriate values in the following optional fields, if required:
    - Server Scope - The access token that's sent from the authorization server to the application.
    - Federated Client Token - The access token that's sent from the authorization server to the application.
    - Include Client Credential - The access token that's sent from the authorization server to the application.
    - Client Credential Type - The access token that's sent from the authorization server to the application.
11. Click **Save and Close**.
12. Click **Done** to return to the Three-Legged OAuth Details page.
13. Click **Done** again to return to the API Authentication page. You can view the newly created three-legged OAuth configuration here.

Related Topics

- Enable OAuth Three-Legged Authentication for Creating External Client Application

Enable OAuth Three-Legged Authentication for Creating External Client Application

While creating an external client application using the Security Console, only the JWT custom claims authentication type is available in the Select Client Type list on the External Client Application Details page.

To display the OAuth three-legged authentication type for selection, you must enable it using a profile option.

Here are the steps:

1. In the Setup and Maintenance work area, go to the **Manage Administrator Profile Values** task.

2. Search for the **ORA_ASE_ENABLE_OAUTH_THREE_LEGGED_SETUP** profile option code
3. In the Profile Values section, click the **Profile Values** list for the Site profile level and select Yes.
4. Click **Save and Close**.

The OAuth three-legged authentication type is enabled now. Enabling the profile option displays the OAuth three-legged authentication type in the Select Client Type list on the External Client Application Details page.

Configure Inbound Authentication

Third-party application users can access a service of Oracle Applications Cloud if inbound authentication is configured for them. You can use an Oracle API Authentication Provider to configure inbound authentication for such users.

To configure inbound authentication, you need a public certificate and a trusted issuer which contains the tokens.

Oracle Applications Cloud supports the JSON Web Token (JWT), Security Assertion Markup Language (SAML), and Security Token Service (STS) tokens. Use the Security Console to configure the trusted issuer and public certificate details. The default trusted issuer is Oracle (www.oracle.com) and you can't delete it.

We recommend that you use JWT for inbound authentication for a system account that's created for a specific application. For authentication, JWT uses a combination of a public certificate and trusted issuer whereas a system account's password expires soon based on the security policy. In addition, you must ensure that the system account's credentials are valid.

> **Note:** For more information about how to configure a JWT for inbound authentication, see Configure JWT Authentication Provider in the Related Topics section.

How Inbound Authentication Works

When a third-party application user sends an authentication request to access a service of Oracle Applications Cloud, these actions occur in the background:

1. The third-party application generates a JWT that includes trusted issuer and public certificate information.
2. Oracle Web Services Manager authenticates the generated JWT by verifying whether the trusted issuer and public certificate are valid.
3. On successful authentication, the third-party application gets access to the Oracle Applications Cloud service.

Here's how you configure an Oracle API Authentication Provider for inbound authentication:

1. On the Security Console, click **API Authentication**.
2. Click **Create Oracle API Authentication Provider**.
3. On the Oracle API Authentication Provider Details page, click **Edit**.
4. On the API Authentication Configuration Details page, enter a name for the **Trusted Issuer**. Ensure that the name of Trusted Issuer matches the value of ISS in the JWT token.
5. Select one or more token types that you want to include in the trusted issuer.
6. Click **Save and Close**.
7. On the Oracle API Authentication Provider Details page, click the Inbound API Authentication Public Certificates tab and click **Edit**. You can use the default Oracle public certificate or add a new one.
8. On the Inbound API Authentication Public Certificates page, click **Add New Certificate** to add a different public certificate.
9. Enter the **Certificate Alias** name

10. Click **Browse** and select the public certificate that you want to import.

    Note: If the public certificate includes a certificate chain then import the complete chain.

11. Click **Save**. The newly added certificate alias is displayed on the Inbound API Authentication Public Certificates page.
12. Click **Done** to return to the API Authentication page.

Related Topics

- Configure JWT Authentication Provider
- Reset User Password
- Use JSON Web Token for Authorization

Is there a recommended format for the public certificate?

Yes. Oracle recommends that the public certificate you upload must contain only line feed (denoted by the code \n) to indicate separation of lines. Because carriage return isn't supported, make sure that the certificate doesn't contain carriage return along with the line feeds.

11 Export and Import of Security Setup Data

Export and Import of Security Console Data

You can move the Security Console setup data from one environment to another using the CSV export and import functionality.

Let's assume you have spent lot of time and effort in configuring and setting up the Security Console in your primary environment. You test the setup and find that everything's working as intended. Now, you want to replicate the same setup in another environment. And you want that to happen with the least effort and as quickly as possible. Well, it certainly can be done in a simple and less time-consuming way.

In the Setup and Maintenance work area, use the **Manage Application Security Preferences** task in the Initial Users functional area.

Before You Begin

Learn how to export business object data to a CSV file and to import business data from a CSV file. Detailed instructions are available in the *Export and Import CSV File Packages* topic of the Using Functional Setup Manager guide.

What Gets Exported and Imported

The Security Console setup data comprises information that you see on the Administration and User Categories tabs of the Security Console. The following business objects help in packaging those details into CSV files so that the data can be easily exported and imported.

- Security Console Administration Settings
- Security Console User Category
- Security Console User Category Notifications

Note:

- Lists of users or information about any specific user is never a part of the CSV file.
- After exporting the setup data to a CSV file, if you want to remove any memberships in the target environment, you must make those changes in the exported CSV file before beginning the import process. Only then, you can apply those changes to the target environment. If you make changes to the source environment alone, you can't expect the CSV file to be automatically updated with memberships that were removed. This is because there's no automatic synchronization between the source environment and the exported CSV file. So, if you don't manually update the CSV file, the changes won't reflect in the target environment.

In this table, you will find information about the contents of each business object.

Business Object	Information Included in Export and Import
Security Console Administration Settings	• General administration details • Role preferences • Location-based access settings • If location-based access isn't enabled (if the tab doesn't appear on Security Console), nothing gets included in the export or import.
Security Console User Category	• User category details • Password policy information
Security Console User Category Notifications	Notification preferences. For notifications, only the custom template information is exported from the default user category. The predefined notifications are excluded because they're available in the target environment.

Note: When you export Security Console setup data, user categories with a password policy configured with custom password complexity setting are exported with the simple password complexity setting. You must manually configure a custom password policy in the new environment with the values used earlier to create it.

When the export process successfully completes, you get the following CSV files:

- Administration Settings CSV
- User Category CSV
- User Category Notifications CSV

If there are language packs installed on your application, additional CSV files may be generated containing the translated data.

To import data into another environment, bundle these files into a .zip file to create the CSV file package and follow the process for importing setup data.

Related Topics

- Export and Import CSV File Packages
- Key Information About Setup Data Export and Import Processes

Export and Import of HCM Custom Roles and Security Profiles

You're looking at migrating your HCM custom roles, data roles, and security profiles from one environment to another. To accomplish most of your HCM security migration needs, export the business objects in the Users and Security functional area within the Workforce Deployment offering.

Other offerings have a Users and Security functional area, but only the Workforce Deployment offering has the business objects that support migration of HCM custom roles within its Users and Security functional area.

Before You Begin

Learn how to export and import business object data. Detailed instructions are available in the Overview of Setup Data Export and Import topic of the Using Functional Setup Manager guide. Refer to the Related Topics section for the link to this topic.

What Gets Exported and Imported

When you migrate HCM roles and security profiles, the following business objects are exported in the configuration package generated from the Users and Security functional area within the Workforce Deployment offering.

- Application Data Security
- Application Profile Value
- Functional Security Custom Roles
    - Functional Security Custom Role Hierarchy
    - Functional Security Custom Role Privilege Membership
- HCM Data Role
    - HCM Data Role Security Profile
- HCM Exclusion Role
    - HCM Exclusion Rule Detail
- Legislative Data Group Security Profile
    - Legislative Data Group Security Profile List
- Organization Security Profile
    - Organization Security Profile Classification List
    - Organization Security Profile Organization List
- Country Security Profile
    - Country Security Profile Country List
- Position Security Profile
    - Position Security Profile Position List
    - Position Security Profile Area of Responsibility Scope
- HR Document Type Security Profile List
    - HR Document Type Security Profile List
- Payroll Security Profile
    - Payroll Security Profile Pay
- Payroll Flow Security Profile
    - Payroll Flow Security Profile Pay

- Payroll Element Security Profile
  - Payroll Element Security Profile Details
- Person Security Profile
  - Person Security Profile Manager Type
  - Person Security Profile Area of Responsibility Scope
  - Person Security Profile Exclusion
- Talent Pools Security Profile
  - Talent Pools Security Profile Job Family
  - Talent Pools Security Profile Department
  - Talent Pools Security Profile Business Unit
- Transaction Security Profile
  - Transaction Security Profile Entries
  - Transaction Security Profile Sub Categories
- Role Provisioning Rule
  - Role Provisioning Associated Role List

Let's closely examine each business object to know what it contains.

Business Object	Information Included in Export and Import
Application Data Security	Application data security includes data security policies that are created in the following ways: • Manually using the Manage Database Resources page in the security console. • Manually using the Edit role/Copy role flow in the security console • Automatically when you copy a role using the Role Copy in the security profile • Automatically when you create profile content types • Automatically when you map HCM spreadsheet business objects to roles Data security policies that are generated by the HCM Data Roles UI aren't exported as part of the application data security business object. They're automatically created on the target environment when you import the HCM Data Role business object. Data security conditions that are generated from HCM security profiles aren't exported as part of the Application Data security business object. They're automatically created on the target environment when the HCM security profile business objects are imported. **Note:** There's no scope support for application data security policies. When you export application data security policies all data security policies are exported, even if you provided a scope value for other security business objects in your configuration package. There's no Export to CSV option for this business object.
Application Profile Value	Application profile value includes the profile values for the PER_MASTER_WORK_EMAIL profile.

Business Object	Information Included in Export and Import
	This profile option is no longer used and no values are exported for this business object.
Functional Security Custom Roles	The custom role includes the following details: • Role Code • Role Name • Role Description • Role Category • All IP Address Access - indicates that a role is granted access to the Security Control irrespective of the IP address from where it's signed in. **Note:** The scope is limited to User Assignable roles only.
Functional Security Custom Role Hierarchy	The role hierarchy includes the following details: • Parent Role • Member Role • Add or Remove Role Membership
Functional Security Custom Role Privilege Membership	The role privilege membership includes the following details: • Parent Role • Member Privilege • Add or Remove Privilege Membership
HCM Data Role	The HCM data role includes the following details: • Data Role Code • Data Role Name • Data Role Description • Inherited Job Role Code • Delegation Allowed Check Box
HCM Data Role Security Profile	The HCM data role security profile includes the following details: • Data Role Code • Securing Object • Security Profile Name
HCM Exclusion Rule	HCM exclusion rule and HCM exclusion rule detail includes HCM exclusion rule definitions. • HCM Exclusion Rule • HCM Exclusion Rule Detail
Legislative Data Group Security Profile List	Legislative data group security profile list includes the following details:

Business Object	Information Included in Export and Import
	• Legislative data group security profile name • Legislative data groups that are included in the legislative data group security profile
Organization Security Profile	Organization security profile includes the following details: • Organization Security Profile Name • Enabled Check Box • View All Check Box • Include Future Organizations Check Box • Code indicating Department Hierarchy or Generic Organization Hierarchy • Hierarchy Name (if securing by organization hierarchy) • Top Organization Name (if securing by organization hierarchy) • Include Top Organization Check Box • Secure by Organization Hierarchy Check Box • Secure by Organization Classification Check Box • Secure by Organization List Check Box
Organization Security Profile Classification List	Organization security profile classification list includes the following details: • Organization Security Profile Name • Organization Classification Name
Organization Security Profile Organization List	Organization security profile organization list includes the following details: • Organization Security Profile Name • Organization name • Organization Classification • Include/Exclude Check Box
Country Security Profile	Country security profile includes the following details: • Country Security Profile Name • Enabled Check Box
Country Security Profile List	Country security profile list includes the following details: • Country Security Profile Name • Country code
Position Security Profile	Position security profile includes the following details: • Position Security Profile Name • Description • Enabled Check Box • View All Check Box

Business Object	Information Included in Export and Import
	• Include Future Positions Check Box • Hierarchy Name (if securing by position hierarchy) • Top Position Name (if securing by position hierarchy) • Include Top Position Check Box • Top Position Name (if securing by organization hierarchy) • Secure by Position Hierarchy Check Box • Secure by Department Check Box • Department Organization Security Profile Name (if securing by department) • Secure by Business Unit Check Box • Business Unit Organization Security Profile Name (if securing by business unit) • Secure by Position List Check Box • Secure by Area of Responsibility Check Box
Position Security Profile Position List	Position security profile position list includes the following details: • Position Security Profile Name • Position Code • Include/Exclude Check Box
Position Security Profile Area of Responsibility Scope	Position security profile area of responsibility scope includes the following details: • Position Security Profile Name • Responsibility Type • Scope of Responsibility
HR Document Type Security Profile	HR document type security profile includes the following details: • HR Document Type Security Profile Name • Enabled Check Box • View All Check Box • Include/Exclude Check Box
HR Document Type Security Profile List	HR document type security profile list includes the following details: • HR Document Type Security Profile Name • Document Type Name
Payroll Security Profile	Payroll security profile includes the following details: • Payroll Security Profile Name • Enabled Check Box • View All Check Box
Payroll Security Profile Pay	Payroll security profile pay includes the following details: • Payroll Security Profile Name

Business Object	Information Included in Export and Import
	• Payroll Name • Legislative Data Group Name
Payroll Flow Security Profile	Payroll flow security profile includes the following details: • Payroll Flow Security Profile Name • Enabled Check Box • View All Check Box
Payroll Flow Security Profile Pay	Payroll flow security profile pay includes the following details: • Payroll Flow Security Profile Name • Flow Name
Payroll Element Security Profile	Payroll element security profile includes the following details: • Element Security Profile • Name
Payroll Element Security Profile Details	Payroll element security profile details includes the following details: • Name • Element Security Profile Details • Legislative Data Group Name • Classification Name • Element Name
Person Security Profile	Person security profile includes the following details: • Person Security Profile Name • Description • Enabled Check Box • Access to Own Record Check Box • Include Future People Check Box • Include Shared People Information Check Box • Access to Candidates with Offers Check Box • Secure by Area of Responsibility • Secure by Manager Hierarchy Check Box • Person or Assignment Check Box • Maximum Levels in Hierarchy • Manager Hierarchy Type • Hierarchy Content Code • Secure by Person Type Check Box • Secure by Department Check Box

Business Object	Information Included in Export and Import
	• Department Security Profile Name (if securing by department) • Secure by Business Unit Check Box • Business Unit Profile Name (if securing by business unit) • Secure by Legal Employer Check Box • Legal Employer Security Profile Name (if securing by legal employer) • Secure by Position Check Box • Position Security Profile Name (if securing by position) • Secure by Legislative Data Group Check Box • Legislative Data Group Security Profile Name (if securing by legislative group) • Secure by Payroll Check Box • Payroll Security Profile Name (if securing by payroll) • Secure by Global Name Range Check Box • Global Name Range Start Value (if securing by global name range) • Global Name Range End Value (if securing by global name range) • Apply Exclusion Rules Check Box • Secure by Custom Criteria Check Box • Custom Restriction Text (if securing by custom criteria) •
Person Security Profile Manager Type	Person security profile manager type includes the following details: • Person Security Profile Name • Manager Hierarchy Type (if something other than All or Line Manager has been selected on the security profile)
Person Security Profile Area of Responsibility Scope	Person security profile area of responsibility scope includes the following details: • Person Security Profile Name • Responsibility Type • Scope of Responsibility • Employee Check Box • Contingent Worker Check Box • Pending Worker Check Box • Nonworker Check Box • Candidate with Offer Check Box
Person Security Profile Exclusion	Person security profile exclusion includes the following details: • Person Security Profile Name • Exclusion Rule Name
Talent Pools Security Profile	Talent pools security profile includes the following details: • Talent Pool Security Profile Name

Business Object	Information Included in Export and Import
	• Enabled Check Box • View by Ownership Check Box • View All Check Box • View All Public Talent Pools Check Box • Secure by Business Unit Check Box • Secure by Department Check Box • Secure by Job Family Check Box
Talent Pools Security Profile Job Family	Talent pools security profile job family includes the following details: • Talent Pool Security Profile Name • Job Family Name
Talent Pools Security Profile Department	Talent pools security profile department includes the following details: • Talent Pool Security Profile Name • Department Name
Talent Pools Security Profile Business Unit	Talent pools security profile business unit includes the following details: • Talent Pool Security Profile Name • Business Unit Name
Transaction Security Profile	Transaction security profile includes the following details: • Transaction Security Profile Name • Description • Enabled Check Box • View All Check Box
Transaction Security Profile Entries	Transaction security profile entries include the following details: • Transaction Security Profile Name • Product Family • Category Code • All Sub Categories Check Box • Exclude Sub Category Check Box
Transaction Security Profile Sub Categories	Transaction security profile sub categories include the following details: • Transaction Security Profile Name • Product Family • Category Code • Sub Category Code
Role Provisioning Rule	Role provisioning rule includes the following details:

Business Object	Information Included in Export and Import
	• Mapping Rule Name • Legal Employer Name • Business Unit Name • Department Name • Job Set Code • Job Code • Position Business Unit Name • Position Code • Grade Set Code • Grade Code • Location Set Code • Location Code • User Person Type • System Person Type • Assignment Type • HR Assignment Status Code • Resource Role • Party Type Usage Code • Contact Role • Manager with Reports Check Box • Manager Type • Responsibility Type
Role Provisioning Associated Role List	Role provisioning associated role list includes the following details: • Mapping Rule Name • Role Code • Requestable Check Box • Self-Requestable Check Box • Autoprovision Check Box

Other business objects that you might like to export when migrating HCM custom roles are:

- Job Requisition Security Profile
- Spreadsheet Business Object Security Mapping

Let's closely examine each of these business objects to know what they contain.

Business Object	Information Included in Export and Import
Job Requisition Security Profile	Job requisition security profile includes the following details:

Business Object	Information Included in Export and Import
	• Job Requisition Security Profile Name • Enabled Check Box • View All Check Box • Secure by Job Family Check Box • Secure by Job Function Check Box • Secure by Location Check Box • Secure by Organization Check Box • Secure by Recruiting Type Check Box
Spreadsheet Business Object Security Mapping	HCM spreadsheet business object access mapping includes the following details: • Role Code • Business Object • Product Area • Enabled Check Box • All Business Objects Check Box

You can migrate job requisition security profiles by exporting the business objects in the Users and Security functional area within the Recruiting and Candidate Experience offering. You should do this before migrating the business objects in the Users and Security functional area within the Workforce Deployment offering. You must have the Recruiting Administrator role to export and import job requisition security profiles.

You can migrate HCM spreadsheet business object access mappings by exporting the business objects in the HCM Data Loader functional area within the Workforce Deployment offering. You should do this after migrating the business objects in the Users and Security functional area. You must have the Human Capital Management Integration Specialist role to export and import HCM spreadsheet business object access mappings.

After the Import Completes

You might need to wait for a period of time before all of the migrated data security policies are visible in the security console after completing the import of the configuration package that's generated from the Users and Security functional area within the Workforce Deployment.

When application data security policies are imported, a process runs in the background to synchronize the imported data security policies with the roles on the target environment. The imported data security policies aren't active until this process has completed, at which point the data security policies will be visible in the security console. This affects data security policies for custom roles that have been copied from other roles in the source environment. It also affects custom roles that have data security policies that were added manually using the security console.

> **Note:** No manual regeneration processes are needed on the target environment; the import process triggers the role regeneration process. This only applies if you're importing the HCM Data Role business object.

What's Not Included

Data security policies that have been manually created from the security console, and which reference conditions that have been generated from an HCM security profile, must be manually recreated on the target environment. You must

import the condition by importing the appropriate HCM security profile business object before creating these data security policies in the target environment.

Related Topics

- Overview of Setup Data Export and Import

12 Security Certificates

Overview

Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications. Use the Certificates page in the Security Console functional area to work with certificates in either of two formats, PGP and X.509.

For each format, a certificate consists of a public key and a private key. The Certificates page displays one record for each certificate. Each record reports these values:

- Type: For a PGP certificate, "Public Key" is the only type. For an X.509 certificate, the type is either "Self-Signed Certificate" or "Trusted Certificate" (one signed by a certificate authority).
- Private Key: A check mark indicates that the certificate's private key is present. For either certificate format, the private key is present for your own certificates (those you generate in the Security Console). The private key is absent when a certificate belongs to an external source and you import it through the Security Console.
- Status: For a PGP certificate, the only value is "Not Applicable." (A PGP certificate has no status.) For an X.509 certificate, the status is derived from the certificate.

Click the Actions menu to take an appropriate action for a certificate. Actions include:

- Generate PGP or X.509 certificates.
- Generate signing requests to transform X.509 certificates from self-signed to trusted.
- Export or import PGP or X.509 certificates.
- Delete certificates.

Types of Certificates

For a PGP or X.509 certificate, one operation creates both the public and private keys. From the Certificates page, select the Generate option. In a Generate page, select the certificate format, then enter values appropriate for the format.

For a PGP certificate, these values include:

- An alias (name) and passphrase to identify the certificate uniquely.
- The type of generated key: DSA or RSA.
- Key length: 512, 1024, or 2048.
- Encryption algorithm option for key generation: AES128, AES256

For an X.509 certificate, these values include:

- An alias (name) and private key password to identify the certificate uniquely.
- A common name, which is an element of the "distinguished name" for the certificate. The common name identifies the entity for which the certificate is being created, in its communications with other web entities. It must match the name of the entity presenting the certificate. The maximum length is 64 characters.

- Optionally, other identifying values: Organization, Organization Unit, Locality, State/Province, and Country. These are also elements of the distinguished name for the certificate, although the Security Console doesn't perform any validation on these values.
- An algorithm by which keys are generated, MD5 or SHA1.
- A key length.
- A validity period, in days. This period is preset to a value established on the General Administration page. You can enter a new value to override the preset value.

Sign a X.509 Certificate

You can generate a request for a certificate authority (CA) to sign a self-signed X.509 certificate, to make it a trusted certificate. (This process doesn't apply to PGP certificates.)

1. Select **Generate Certificate Signing Request**. This option is available in either of two menus:
    - One menu opens in the Certificates page, from the row for a self-signed X.509 certificate.
    - The other menu is the Actions menu in the details page for that certificate.
2. Provide the private key password for the certificate, then select a file location.
3. Save the request file. Its default name is [alias]_CSR.csr.

You are expected to follow a process established by your organization to forward the file to a CA. You would import the trusted certificate returned in response.

Import and Export X.509 Certificates

For an X.509 certificate, you import or export a complete certificate in a single operation.

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Certificate.
3. Select a location for the export file. By default, this file is called [alias].cer.

To import, use either of two procedures. Select the one appropriate for what you want to do:

- The first procedure replaces a self-signed certificate with a trusted version (one signed by a CA) of the same certificate. (A prerequisite is that you have received a response to a signing request.)
    a. In the Certificates page, locate the row for the self-signed certificate, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
    b. Enter the private key password for the certificate.
    c. Browse for and select the file returned by a CA in response to a signing request, and click the Import button.

    In the Certificates page, the type value for the certificate changes from self-signed to trusted.
- The second procedure imports a new X.509 certificate. You can import a .cer file, or you can import a keystore that contains one or more certificates.

a. In the Certificates page, click the Import button. An Import page opens.
b. Select X.509, then choose whether you're importing a certificate or a keystore.
c. Enter identifying values, which depend on what you have chosen to import. In either case, enter an alias (which, if you're importing a .cer file, need not match its alias). For a keystore, you must also provide a keystore password and a private key password.
d. Browse for and select the import file.
e. Select Import and Close.

Related Topics

- Sign a X.509 Certificate

Import and Export PGP Certificates

For a PGP certificate, you export the public and private keys for a certificate in separate operations. You can import only public keys. (The assumption is that you will import keys from external sources, who wouldn't provide their private keys to you.)

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Public Key or Private Key.
3. If you selected Private Key, provide its passphrase. (The public key doesn't require one.)
4. Select a location for the export file. By default, this file is called [alias]_pub.asc or [alias]_priv.asc.

To import a new PGP public key:

1. On the Certificates page, select the Import button.
2. In the Import page, select PGP and specify an alias (which need not match the alias of the file you're importing).
3. Browse for the public-key file, then select Import and Close.

The following PGP certificate formats aren't supported:

- GnuPG v2.0.22 (GNU/Linux)
- Keybase OpenPGP v1.0.0
- OpenPGP.js v4.10.10

The Certificates page displays a record for the imported certificate, with the Private Key cell unchecked.

Use a distinct import procedure if you need to replace the public key for a certificate you have already imported, and don't want to change the name of the certificate:

1. In the Certificates page, locate the row for the certificate whose public key you have imported, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
2. Browse for the public-key file, then select Import.

Delete Certificates

You can delete both PGP and X.509 certificates. On the Certificates page, select the menu available in the row for the certificate you want to delete. Or, in the details page for that certificate, select the Actions menu.

In either menu, select Delete. Respond to a warning message. If the certificate's private key is present, you must enter the passphrase (for a PGP certificate) or private key password (for an X.509 certificate) as you respond to the warning. Either value would have been created as your organization generated the certificate.