# Oracle Fusion Cloud Student Management

## Securing Student Management

23D

Oracle Fusion Cloud Student Management
Securing Student Management

23D

F85726-01



Author: Oracle Student Management Information Development Team

# Contents

# Get Help

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

## Get Help in the Applications

Use help icons to access help in the application. 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.

## 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 An Introduction to Student Management Security in the Cloud

## Overview of Securing Oracle Student Management Cloud

Oracle Student Management Cloud is secured as delivered. You need to enable user access to the Student Management functions and data by configuring the various security tasks.

This guide explains how to do so. This topic summarizes the contents of each chapter.

### Guide Structure

This table describes the contents of each chapter in this guide.

| Chapter | Contents |
|---|---|
| An Introduction to Student Management Security in the Cloud | An overview of the concepts of role-based security and an introduction to the Oracle Cloud Applications Security Console |
| Implementation Users Management | Why implementation users are needed and how you create them |
| Applications Security Setup | How you set up the enterprise options on the Security Console and maintain the Oracle Cloud Applications security tables |
| Application Users Setup | What are the enterprise-wide options that affect application users, and how you set them up |
| Application Users Management | How you create and manage the accounts for application users |
| Role Provisioning for Application Users | What are some of the standard role mappings, and how you create and manage them for application users |
| Location-Based Access | How location-based access works, and what you must do to enable or disable this access, allowlisting certain IP addresses, and making certain roles public |
| Single Sign-On | How you set up single sign-on |
| Export and Import of Security Data and Role Hierarchy | How you migrate Security Console setup data and custom role hierarchy from one environment to another |
| Reports for Application Users and Roles | What are the reports that you can look at for user accounts, inactive users, role provisioning, and password changes |

| Chapter | Contents |
|---|---|
| Security Console | How you use the Security Console to review role hierarchies and role analytics |
| Job, Abstract, and Duty Roles | How you create roles either from the beginning or by copying predefined roles, and how you edit custom roles |
| Roles for Workflow Access | What are the predefined roles that enable access to the Workflow feature |
| Role Optimization | How you use the optional Role Optimization Report to analyze the role hierarchy for redundancies and other inefficiencies |

During implementation, you do certain security-related tasks from a functional area task list or for an implementation project. After the implementation is complete, you can do most of the security-related tasks through the Security Console.

# Role-Based Application Security

In Oracle Applications Cloud, users have roles through which they gain access to functions and data.

Users can have any number of roles. Roles are grouped hierarchically to reflect lines of authority and responsibility. User access to functions and data is determined by roles, arranged in hierarchies and provisioned to that user.

Role-based security in Oracle Applications Cloud controls who can do what on which data.

| Component | Description |
|---|---|
| Who | Role assigned to a user |
| What | Function that users with that role can perform |
| Which Data | Set of data that users with the role can access when performing the function |

Here's an example. Assume that a user named **`Lynda Jones`** has these three roles.

- **`Admissions coordinator`**, by which she can access applicant functions and data.
- **`Employee`**, by which she can access employee functions and data.
- **`Part-time continuing education student`**, by which she can access student functions and data.

When **`Lynda Jones`** signs in to Oracle Student Management Cloud, she doesn't have to select a role. All of her roles, and the related access permissions, are active concurrently. The functions and data that she can access are determined by this combination of roles, which means she can access all of the functions and data relating to applicants, employees, and students.

# Predefined Student Management Roles

The security reference implementation in Oracle Student Management Cloud is delivered with several pre-defined roles.

Here are some examples:

- Academic Coordinator
- Admissions Coordinator
- Bursar
- Cashier
- Higher Education Application Administrator
- Higher Education Instructor
- Registrar
- Student
- Student Adviser
- Student Prospect
- Student Services Manager

Additionally, the security reference implementation includes roles that are common to all Oracle Cloud applications. Here are some examples:

- Application Implementation Consultant
- IT Security Manager

You can use these roles as supplied.

# Role Types

Oracle Student Management Cloud has these types of roles: job roles, abstract roles, and duty roles.

## Job Roles

Job roles are for the jobs that people in an organization do. `Bursar` and `Registrar` are examples of predefined job roles. You can create your own job roles too.

## Abstract Roles

Abstract roles represent people in the enterprise independently of the jobs they do. `Employee` and `Transactional Business Intelligence Worker` are examples of predefined abstract roles. You can also create your own abstract roles.

You can assign abstract roles directly to users. You will likely assign at least one abstract role to all users so that they have access to a set of standard functions, such as managing their own information and searching the worker directory.

## Duty Roles

Duty roles are for a logical collection of privileges that grant access to tasks. `Instruct Class` and `Fee Assessment` are examples of predefined duty roles.

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

Duty roles differ from aggregate privileges in these ways:

- You can create duty roles, and edit, and copy them. Aggregate privileges, however, are predefined, and you can't create, modify, or copy them.
- Duty roles inherit aggregate privileges and other duty roles. Aggregate roles don't.
- Duty roles include multiple function security privileges.

## Summary of differences

Here are the differences between the role types.

| Role type | Create | Predefined | Assign directly to users |
|---|---|---|---|
| Job role | Yes | Yes | Yes |
| Abstract role | Yes | Yes | Yes |
| Duty role | No | Yes | No |

# Role Inheritance

Almost every role is a hierarchy or collection of other roles. When you assign roles, this is how users inherit all of the data and function security associated with those roles:

- Job roles and abstract roles can inherit duty roles.

  You can directly grant many function security privileges and data security policies to job roles and abstract roles. Use the Security Console to explore the complete structure of a job role or abstract role.
- Duty roles can inherit other duty roles and aggregate privileges.

# Duty Role Components

A typical duty role comprises two components, namely, data security policies and functional security privileges. Duty roles can also inherit other duty roles.

## Data Security Policies

A data security policy assigned to a duty role has the components listed below. For example, the duty role Student Party View has:

- A business object that's being accessed, such as `Trading Community Party`.
- The condition, if any, that controls access to specific instances of the business object. For example, you can create a condition that allows managers to access all data pertaining to people who report to them.
- A data security privilege, which defines what can be done with the specified data, such as `View Trading Community Person (Data)`.

## Function Security Privileges

A function privilege assigned to a duty role secures user interfaces, such as `Maintain Grade Roster` and `Maintain Class Roster` pages.

> **Tip:** The predefined duty roles represent logical groupings of privileges that you might want to manage as a group. They also represent real-world groups of tasks. For example, the predefined `Higher Education Instructor`job role inherits the `Student Detail View` duty role. To create your own `Higher Education Instructor` job role with no access to personal information of students, copy the predefined job role and remove `Student Detail View` duty role from the role hierarchy.

# Options for Reviewing Predefined Roles

You need information about predefined roles so that you can identify which users need each role and whether to make any changes before provisioning roles. Use the Security Console to review this information.

## The Security Console

On the Security Console, you can do these things:

- Review the role hierarchy of any job, abstract, or duty role.
- Extract the role hierarchy to a spreadsheet.
- Identify the function security privileges and data security policies granted to a role.
- Compare roles to identify differences.

> **Tip:** Role codes of all predefined roles have the **ORA_** prefix.

## Reports

To see the the function security privileges and data security policies for a specified role, all roles, a specified user, or all users, you can run the User and Role Access Audit Report, which is in the XML format.

## The Security Reference Manuals

Two manuals describe the security reference implementation for Oracle Student Management Cloud users:

- The Security Reference for Oracle Applications Cloud includes descriptions of all predefined security data that's common to Oracle Fusion Applications.
- The Security Reference for Oracle Student Management Cloud includes descriptions of all predefined security data for Oracle Student Management Cloud.

These components are described.

- Duty roles and aggregate privileges
- Role hierarchy
- Function security privileges
- Data security policies

The security reference manuals are at **https://docs.oracle.com**.

# Overview of Security Configuration

During implementation, you evaluate the predefined roles and decide whether changes are needed. If the predefined security reference implementation doesn't fully represent your enterprise, you can change it.

For example, the predefined `Admissions Coordinator` job role includes View Student Management Rules privileges. If some of your admissions coordinators don't handle rules, you can create a admissions coordinator role without this privilege. To create a role, you can either copy an existing role and edit it, or create a new one.

All predefined roles have many function security privileges and data security policies. They also inherit duty roles.

You can identify predefined application roles easily by their role codes, which all have the prefix *ORA_*. For example, the role code of the `Admissions Coordinator` application job role *is ORA_HEQ_ADMISSIONS_COORDINATOR_JOB*.

If you need only minor changes to a predefined job or abstract role, copy the role and edit the copy to add or remove duty roles, function security privileges, and data security policies, as appropriate.

Consider creating a role if it has very few privileges and you can identify them easily.

# Overview of Security Console

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.

# 2 Implementation Users Management

## About Implementation Users in Student Management

Implementation users are those who configure and implement the Oracle Student Management Cloud service for other users.

They do these tasks:

- Implement Oracle Student Management Cloud.
- Administer application users and security, both during and after implementation.
- Set up basic enterprise structures.

To set up the Oracle Student Management Cloud service, you must create at least one implementation user. Implementation users have the access permissions for both implementation as well as maintenance of the service.

### How are Implementation Users Different From Other Users?

As an implementation user, you will most probably use the job role called **`Application Implementation Consultant`**. Such a job role gives you unrestricted access to large amounts of data. However, you don't need this level of access after you're done with the implementation. After implementation, both application users and administrators can do their tasks with job roles that don't have as much access to data.

The other difference is that as an implementation user, no record of you as a person exists in Oracle Student Management Cloud; you exist only as a user account. Person records exist, however, for application users and administrators.

### Who Creates Implementation Users?

The administrator of the Oracle Student Management Cloud service creates the initial implementation users.

### Do You Have Any Recommendations For Creating Implementation Users?

To ensure segregation of critical duties, consider creating at least these two implementation users.

| Implementation User | Description |
|---|---|
| TechAdmin | As a technical super-user, this user will do the technical and security setup for the cloud service. |
| SMUser | As the person who implements Oracle Student Management Cloud, this user will do the functional setup for the cloud service. |

You might need to create other implementation users also, for example:

- An application implementation manager, who can assign implementation tasks to other implementation users. This implementation user has the **`Application Implementation Manager`** job role.

- A product family application administrator, who can do the implementation tasks for a specific product. You might find this useful if you're implementing multiple Oracle Cloud products and want a separate implementor for each product.

**Tip:** The `Application Implementation Consultant` job role can access all setup tasks for Oracle Cloud Applications.

# About Creating Implementation Users for Student Management

If you're the service administrator for the Oracle Student Management Cloud service, you will receive your sign-in details when your environments are provisioned.

Thereafter, you can access the service for the first time and set up the user accounts for implementation users. Unless you do so, your implementation team won't be able to do their job.

Create implementation users in the test environment first. Only after you have validated the implementation should you move it to the production environment. If you follow this approach, your implementation team learns how to implement security before they set up accounts for application users in the production environment.

## Access the Oracle Student Management Cloud Service

The welcome or service-activation email from Oracle contains the service URLs, user name, and temporary password for the test or production environment. The Identity Domain value is the environment name. For example, STUDENT could be the production environment and STUDENT-TEST could be the test environment.

1. Use the service home URL and the password in the welcome or service-activation email to sign in to the Oracle Student Management Cloud service.
2. Change the password, and make a note of it. This password is the service administrator password for subsequent access to the service.
3. Don't share your sign-in details with other users.

You're now ready to synchronize user and role information, import the user roles into application security, and create the implementation users.

# 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.

# 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.

# Import Users and Roles into Applications Security

To implement security, you must use the Security Console. Before you can use the Security Console, you must initialize the Oracle Fusion Applications Security tables with existing user and role information.

To initialize these tables, you perform the **Import Users and Roles into Application Security** task. This topic describes how to perform this task.

## Run the Import User and Role Application Security Data Process

Sign in as the Oracle HCM Cloud service administrator and follow these steps:

1. In the Setup and Maintenance work area, go to the following for your offering:
    - Functional Area: Initial Users
    - Task: Import Users and Roles into Application Security
2. On the Import Users and Roles into Application Security page, click **Submit**.

The **Import User and Role Application Security Data** process starts. When the process completes, you can use the Security Console.

**Note:** You're recommended to schedule this process to run daily after your implementation users exist.

*Related Topics*

- Schedule the Import User and Role Application Security Data Process

# Create the Technical Implementation User

You need a technical implementation user to do the technical and security setup for the Oracle Student Management Cloud service. You first create the user and then assign job roles to that user.

## Creating the Technical Implementation User

Sign in as the Oracle Student Management Cloud service administrator and follow these steps:

1. Click **Setup and Maintenance**. In the Functional area, click **Initial Users**. In the Task area, click **Create Implementation Users**.
2. On the User Accounts page of the Security Console, click **Add User Account**.
3. Enter these values on the Add User Account page.

| Field | Value |
|---|---|
| **Associated Person Type** | None |
| **Last Name** | TechAdmin |
| **Email** | A valid email for the user |
| **User Name** | TechAdmin |
| **Password** | Any value that complies with the password policy |

| Field | Value |
| --- | --- |
| | |

To view the password policy, click the **Help** icon next to the **Password** field.

4. Make a note of the password and give it to the user who first signs in as TechAdmin. This user must change the password.

## Assigning Roles to TechAdmin

To assign job roles to the TechAdmin implementation user, follow these steps:

1. In the Roles section of the Add User Account page, click **Add Role**.
2. In the **Add Role Membership** dialog box, search for the IT Security Manager job role.
3. In the search results, select the role and click **Add Role Membership**.
4. Click **OK** to close the **Confirmation** dialog box.
5. Repeat from step 2 to add each of these job roles to the TechAdmin user:
    - Application Implementation Consultant
    - Application Diagnostics Administrator
    - Application Diagnostics Advanced User

    When you're done, four job roles are displayed in the Roles section of the Add User Account page.
6. Click **Save and Close**.

**CAUTION:** `Application Implementation Consultant` is a powerful role that has unrestricted access to a large amount of data. After the implementation is complete, remember to revoke this role from all users. To do so, use **Implementation Users** > **Revoke Data Role**. For ongoing maintenance of Oracle Student Management Cloud setup data, use a less powerful role.

# Create the Functional Implementation User

You need a functional implementation user to do the functional setup for the Oracle Student Management Cloud service. You first create the user and then assign job roles to that user.

## Create the Functional Implementation User

A functional user won't have access to the technical setup tasks, including setting up the security for other users.

1. Sign in as the Oracle Student Management Cloud service administrator.
2. Click **Setup and Maintenance**. In the Functional area, click **Initial Users**. In the Task area, click **Create Implementation Users**.
3. On the User Accounts page of the Security Console, click **Add User Account**.

4. Enter these values on the Add User Account page.

| Field | Value |
|---|---|
| **Associated Person Type** | None |
| **Last Name** | SMUser |
| **Email** | A valid email for the user |
| **User Name** | SMUser |
| **Password** | Any value that complies with the password policy |

5. Make a note of the password. You must give the user name and password to the person who first signs in as SMUser. This person must change the password after the first sign-in.

## Assign Roles to the Functional Implementation user

To assign job roles to the functional implementation user, follow these steps:

1. In the Roles section of the Add User Account page, click **Add Role**.
2. In the **Add Role Membership** dialog box, search for the Application Administrator job role.
3. In the search results, select the role and click **Add Role Membership**.
4. Click **OK** to close the **Confirmation** dialog box.
5. Repeat steps 2 through 4 to add each of these job roles to the functional implementation user:
    - Application Implementation Consultant
    - Application Diagnostics Regular User
    - Application Diagnostics Viewer

    When you're done, you see four job roles in the Roles section of the Add User Account page.
6. Click **Save and Close**.

**CAUTION:** `Application Implementation Consultant` is a powerful role that has unrestricted access to a large amount of data. After the implementation is complete, remember to revoke this role from all users. To do so, use **Implementation Users** > **Revoke Data Role**. For ongoing maintenance of the Oracle Student Management Cloud setup data, use a less powerful role, such as Application Administrator.

# 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.

*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**.

# 3 Applications Security Setup

## 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.

# Default User-Name Formats

People who use your implementation of the Oracle Student Management Cloud service need user names to sign in to the application. During implementation, you specify the default format that these user names will use.

## What Are The Default User-Name Formats?

To select a format, use the Manage Applications Security Preferences task. Go to **Security Console Administration** > **General** > **User Preferences**. Select a user-name format, and click **Save**.

You can change the enterprise formats at any time. Select a different format and click **Save**. The change takes effect immediately.

Here are the available user-name formats.

| User-Name Format | Description |
|---|---|
| **Email** | The work email (or party email, for party users) is the user name. For example, the user name for john.smith@example.com is john.smith@example.com. To make duplicate names unique, a number is added. For example, if john.smith@example.com and john.smith1@example.com already exist, john.smith2@example.com is used. |

| User-Name Format | Description |
|---|---|
| | **Email** is the default format. |
| **FirstName.LastName** | The user name is the worker's first and last names separated by a period. For example, the user name for John Frank Smith is john.smith. To make duplicate names unique, either the user's middle name or a random character is used. For example, John Smith's user name could be john.frank.smith or john.x.smith. |
| **FLastName** | The user name is the worker's last name prefixed with the initial of the worker's first name. For example, the user name for John Smith is jsmith. |
| **Person or party number** | The party number or person number is the user name. If your enterprise uses manual person numbering, the number that's entered during the hiring process becomes the user name. Otherwise, the number is generated automatically and can't be edited. The automatically generated number becomes the user name. For example, if John Smith's person number is 987654, the user name is 987654. |

## What Are System User Names?

Sometimes, the rule that you specified for user names could fail. For example, a person's party number, person number, or email might not be available when the user account is requested. In such cases, a system user name is generated by applying these options, in the order they're listed, until a unique user name is obtained.

1. Email
2. FirstName.LastName
3. If only the last name is available, a random character is prefixed to the last name.

The Security Console option **Generate system user name when generation rule fails** controls whether a system user name is generated. You can disable this option. If you do so, an error is raised if the user name can't be generated in the selected format.

**Tip:** You can always edit a system-generated user name.

## Can I Override the Default Format?

When hiring workers, human resource (HR) specialists and line managers can enter user names in any format by overriding the default user names. HR specialists can also edit user names for individual users through the Edit User and Manage User Account pages. A user name can contain up to 80 characters.

## Can I Add a Work Email Later?

During the hiring process of employees, the line manager or HR specialist might not enter the work email. In such cases, the employee details can't be edited later to include the work email . However, you can use the Security Console to edit the user details and enter the work email there. To use work email as the user name after a different user name has been generated, edit the existing user name.

# Password Policy

During implementation, you set the password policy for the default user category. This topic describes the available options. To set the password policy, you perform the Manage Applications Security Preferences task, which opens the Administration page of the Security Console.

Click the **User Categories** tab and click the name of the default category to open it. Click **Edit** on the **Password Policy** subtab to edit the policy. You can change the password policy for any user category at any time.

## Password Policy Options

This table describes the available options for setting password policy.

| Password-Policy Option | Description | Default Value |
|---|---|---|
| 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 follow the Forgot Password process. | 90 |
| 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. | 80<br><br>**Note:** This value is 10 for new installations from Update 18B. |
| Hours Before Password Reset Token Expiration | When users request a password reset, they're sent a password-reset link. This option specifies how long a reset-password link remains active. If the link expires before the password is reset, then reset must be requested again. You can enter any value between 1 and 9999. | 4 |
| Password Complexity | Specifies whether passwords must be simple, complex, or very complex. Password validation rules identify passwords that fail the selected complexity test.<br><br>The following password complexity types are available:<br>• Simple: Must contain at least 8 characters, 1 number. This is the default complexity type.<br>• Complex: Must contain at least 8 characters, 1 uppercase, 1 number.<br>• Very Complex: Must contain at least 8 characters, 1 uppercase, 1 number, 1 special character.<br>• Custom: Provides the flexibility to specify a combination of parameters to define | Simple |

| Password-Policy Option | Description | Default Value |
|---|---|---|
| | a custom password. By default, the parameters are populated with predefined set of values to get you started.<br><br>**Note:**<br>For more information about defining custom password, see topic Configure a Custom Password Policy in the Related Topics section | |
| Disallow last password | Select to ensure that the new password is different from the last password.<br><br>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.<br><br>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. | No |
| Administrator can manually reset password | 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. | Yes |

**Note:** Users are notified of password events only if appropriate notification templates are enabled for their user categories. The predefined notification templates for these events are Password Expiry Warning Template, Password Expiration Template, and Password Reset Template.

*Related Topics*

- Configure a Custom Password Policy

# 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.

# Role Preferences

During implementation, you set default role preferences for the enterprise.

To set role preferences, you perform the Manage Applications Security Preferences task, which opens the General tab of the Security Console Administration tab. From there, click the Roles tab. You can also set role preferences at any time on the Security Console.

## Copied-Role Names

To create roles, copy predefined roles and edit the copied roles. Here's what happens when you copy a predefined role:

- The **ORA_** prefix, which identifies predefined roles, is removed automatically from the role code of the copied role.
- The enterprise prefix and suffix values are added automatically to the role name and code of the copied role.

You specify enterprise prefix and suffix values on the Roles tab of the Security Console Administration tab. These are the default values:

- Prefix values are blank.
- The role-name suffix is **Custom**.
- The role-code suffix is **_CUSTOM**.

You can supply prefix values and change the suffix values, as required. If you change these values, click **Save**. The changes take effect immediately.

## Graph Nodes and Default Views

Use the Roles tab of the Security Console to view role hierarchies. By default, these hierarchies are displayed in tabular format. To use graphical format by default, clear the **Enable default table view** option on the Roles tab of the Security Console Administration tab.

When role hierarchies are displayed on the Roles tab, the number of nodes can be very high. To limit the number of nodes in the graphical view, set the **Graph Node Limit** option on the Roles tab of the Security Console Administration tab. When you display a role hierarchy with more nodes than the specified limit, switch to the tabular format.

# 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<br>• Password expired |

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

| Token | Meaning | Events |
|---|---|---|
| | | • Password reset confirmation - manager |
| `${managerFirstName}` | The given name of the person who manages the person whose account is being created or modified. | • New account created - manager<br>• Password reset confirmation - manager<br>• Password reset - manager |
| `${managerLastName}` | The surname of the person who manages the person whose account is being created or modified. | • New account created - manager<br>• Password reset confirmation - manager<br>• Password reset - manager |
| `${loginUrl}` | The web address to sign in to Oracle Cloud. The user can sign in and use the Preferences page to change a password that's about to expire. Or, without signing in, the user can engage a forgot-password procedure to change a password that has already expired. | • Expiring external IDP signing certificate<br>• Password expired<br>• Password expiry warning |
| `${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<br>• New user created<br>• Password generated<br>• Password reset<br>• 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<br>• 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<br>• Administration activity single sign-on disabled confirmation |

| Token | Meaning | Events |
|---|---|---|
| `${adminLastName}` | The surname of the person who has administrator rights. | • Administration activity location based access disabled confirmation<br>• Administration activity single sign-on disabled confirmation |

# Schedule the Import User and Role Application Security Data Process

You must run the Import User and Role Application Security Data process to set up and maintain the Security Console. During implementation, you perform the Import Users and Roles into Application Security task to run this process.

The process copies users, roles, privileges, and data security policies from the LDAP directory, policy store, and Applications Core Grants schema to Oracle Fusion Applications Security tables. Having this information in the Oracle Fusion Applications Security tables makes the assisted search feature of the Security Console fast and reliable. After the process runs to completion for the first time, you're recommended to schedule the **Import User and Role Application Security Data** process to run daily. This topic describes how to schedule the process.

**Note:** Whenever you run the process, it copies only those changes that were made since it last ran.

## Schedule the Process

Follow these steps to schedule 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.

## Review Synchronization Process Preferences

On the **General** subtab of the Security Console Administration tab, you can set the **Synchronization Process Preferences** option. This option controls how frequently you're reminded to run the **Import User and Role Application Security Data** process. By default, the warning appears if the process hasn't run successfully in the last 6 hours. If you schedule the process to run daily, then you may want to increment this option to a value greater than 24.

# 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

# Why You Run the Send Pending LDAP Requests Process

Run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to your LDAP directory server. Schedule the process in the Scheduled Processes work area.

The `Send Pending LDAP Requests` process sends these items to the LDAP directory:

- Requests to create, suspend, and reactivate user accounts.
    - When you create a person record for a worker, a user-account request is generated automatically.
    - When a person has no roles and no current work relationships, a request to suspend the user account is generated automatically.
    - A request to reactivate a suspended user account is generated automatically if you rehire a terminated worker.

  The process sends these requests to the LDAP directory unless the automatic creation and management of user accounts are disabled for the enterprise.

- Work emails.

  If you include work emails when you create person records, the process sends those emails to the LDAP directory.
- Role provisioning and deprovisioning requests.

  The process sends these requests to the LDAP directory unless automatic role provisioning is disabled for the enterprise.
- Changes to person attributes for individual users.

  The process sends this information to the LDAP directory unless the automatic management of user accounts is disabled for the enterprise.

**Note:** All of these items are sent to the LDAP directory automatically unless they're either future-dated or generated by bulk data upload. You run the `Send Pending LDAP Requests` process to send future-dated and bulk requests to the LDAP directory.

Only one instance of the `Send Pending LDAP Requests` process can run at a time.

# 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.

# Schedule the Send Pending LDAP Requests Process

The Send Pending LDAP Requests process sends bulk requests and future-dated requests that are now active to your LDAP directory. You're recommended to schedule the Send Pending LDAP Requests process to run daily. This procedure explains how to schedule the process.

> **Note:** Schedule the process only when your implementation is complete. After you schedule the process you can't run it on an as-needed basis, which may be necessary during implementation.

## Schedule the Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.
3. In the Schedule New Process dialog box, search for and select the **Send Pending LDAP Requests** process.
4. In the Process Details dialog box, set **User Type** to identify the types of users to be processed. Values are **Person**, **Party**, and **All**. You're recommended to leave **User Type** set to **All**.
5. The **Batch Size** field specifies the number of requests in a single batch. For example, if 400 requests exist and you set **Batch Size** to **25**, then the process creates 16 batches of requests to process in parallel.

   The value **A**, which means that the batch size is calculated automatically, is recommended.
6. Click **Advanced**.
7. On the Schedule tab, set **Run** to **Using a schedule**.
8. In the **Frequency** field, select **Daily**.
9. Enter the start and end dates and times.
10. Click **Submit**.

*Related Topics*

- Why You Should Run the Send Pending LDAP Requests Process

# 4 Application Users Setup

## 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.<br><br>This value is the default value. |
| Party users only | User accounts are created automatically for party users only.<br><br>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.<br><br>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.<br><br>This value is the default value. |
| Party users only | Role provisioning and deprovisioning occur for party users only.<br><br>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.<br><br>This value is the default value. |
| Party users only | User accounts are maintained automatically for party users only.<br><br>For person users, account-maintenance requests are held in the LDAP requests table, where they're identified as suppressed. They're not processed.<br><br>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.<br><br>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**.

# Redirect Self-service Users to the Home Page Automatically

Redirect users automatically to the self-service home page after they sign up and set their password.

To enable this redirection, use the User Category Name field on the Manage User Role Mapping page. The User Category Name field contains the URL of the home page, and is set up through the Security Console.

To enable the automatic redirection of users to the home page after they sign up:

1. Sign in as IT Security Manager.
2. Make sure you have a user category that contains the URL of the home page.

   If you don't have such a user category, open the Security Console, and create a user category where the **Next URL** field contains the URL of the home page.
3. Click **Setup and Maintenance**, and go to the Application Access functional area. Ensure that the Show field specifies All Tasks. Click the **Manage User Role Mappings** task.
4. In the role mapping row, select the user category that contains the URL of the home page, and click **Save and Close**.

# 5 Application Users Management

## Create Users

### Options for Creating Application Users

Application users can be created in several ways. The User and Role Provisioning options control whether user accounts are created and maintained automatically. You set these options for the institution during implementation.

These are some of the ways that application users can be created:

- When prospects register to apply to your institution, they create their own security account.

  Students and prospects can use your institution's web page to register as new users. Security accounts are created as part of that process, and roles are provisioned depending on how the role mapping was set up.

  Users can create their own managed student groups, and add either an existing user to it or create a user and add them. When they create a managed student group, they themselves get added to the group.
- In Student Management, to create users with specific person record accounts, use the Person Profiles work area. After creating a user, you can add them to managed student groups.
- If you're using Student Management with HCM Cloud, new employees are provisioned security accounts in the hire process.

  Use the Hire an Employee task to create a user account and assign roles to new employees.

You can create a user with an employee role who can be later assigned a student role. To assign a student role, go to person profiles work area and click **Activate User** for that particular user. You can also create a user with student role using person profiles work area and then, later on, assign employee role using security console or using hire employee process in HCM Cloud.

*Related Topics*

- Create Person Profiles
- Manage Persons

### 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 **E-Mail** field, enter the user's primary work e-mail.
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 e-mail later by running the Send User Name and Password E-Mail 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**.

# Create Managed Student Groups

A signed-in user can become a group manager by creating a managed student group and adding students to the group.

Doing so also makes the group manager the group owner. Only a group owner can edit group information, add or remove members, assign relationships to various group members, and view relationships for all group members in the group. If a student or group manager doesn't exist, they will have an option to create a new user who then can be added to the group.

The parent or guardian of the fully managed or jointly managed student gets consent communication whenever the student is added to a group.

Group owners must first capture the relationship of a student with themselves before the student can be added to the group. Additionally, they can capture the relationships of all the students with all the other group managers in the group.

A group manager who's not a group owner can't add or remove other students or group manager members.

A group manager or group owner can act on behalf of students in the group they own or in a group they're a member of. For example, a group manager or group owner can make payments on behalf of a student.

To create a user account, a group owner must specify four bits of information: name, user name, email ID, and date of birth. Before creating a user account, Student Management Cloud runs a search to see if the account exists and create a user account if one doesn't already exist.

Here's how you create a managed student group:

1. Depending on your permissions, access the appropriate task:
    - If you're signed in as an administrator, from Student Central, click **Search**, search for **Application Access**, and then click **Managed Student Groups** > **Create Group**.
    - If you're signed in as a user, from Student Central, click **Search** and search for **Create Managed Student Group**.
2. Enter a group name and description, and click **Add**.
3. Add other group manager members that you want to, and student members.
4. Click **Save**.

## Group Owner Approval

Approval is always required to add a student or additional group manager user to a group. You can set the age limits by defining the age range of a fully, jointly, or self-managed user. From Student Central, click **Search** and search for **Age Settings**. Move the self-managed age slider to set the age limit for self-service users to own a group and add other group managers and students to their group, with their approval.

You need to set up a confirmation email request for the parent or guardian of the fully managed or jointly managed students or group managers to accept or deny an invitation to join a group. The recipient can respond to the invitation either by email or by viewing the information in the Message Center. You can also send a reminder using date-based communication to the members of a group to accept or deny the invitation. A group owner within a group can act as group owner for only students in that group who have accepted the group owner approval request. The student's status is **Pending** until the parent or guardian of the fully managed or jointly managed student responds to the email or through their Message Center. That status then changes to **Accepted** or **Denied**.

*Related Topics*

- Create Person Profiles
- Overview of Communications
- Manage Persons
- Create a Communication

# Enable Group Owner Change Notification

Whenever you change a managed student group owner to a different group manager in the group, Student Management Cloud sends a notification to all group managers in the group including the old and new managed student group owners.

To enable the managed student group owner change notification:

1. From Student Central, click **Search** and search for **Communications**.
2. Create an event-based communication.
3. From the **Select Event** drop-down list, select **Group Owner Changed**.
4. Define the communication details for this event.

*Related Topics*

- Overview of Communications

# 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

# FAQs for Creating Users

## 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

## 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.

# Manage Users

## Implementation Users

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.

# Overview of ERP Implementation Users

As the service administrator for the Oracle ERP Cloud service, you're sent sign-in details when your environments are provisioned. This topic summarizes how to access the service for the first time and set up implementation users to perform the implementation. You must complete these

> **Tip:** Create implementation users in the test environment first. Migrate your implementation to the production environment only after you have validated it. With this approach, the implementation team can learn how to implement security before setting up application users in the production environment.

## Accessing the Oracle ERP Cloud Service

The service activation mail from Oracle provides the service URLs, user name, and temporary password for the test or production environment. Refer to the e-mail for the environment that you're setting up. The Identity Domain value is the environment name. For example, ERPA could be the production environment and ERPA-TEST could be the test environment.

Sign in to the test or production Oracle ERP Cloud service using the service home URL from the service activation mail. The URL ends with either **AtkHomePageWelcome** or **FuseWelcome**.

When you first sign in, use the password in the service activation mail. You're prompted to change the password and answer some challenge questions. Make a note of the new password. You must use it for subsequent access to the service.

Don't share your sign-in details with other users.

## Creating Implementation Users

This table summarizes the process of creating implementation users and assigning roles to them.

| Step | Task or Activity | Description |
|---|---|---|
| 1 | Create Implementation Users | You can create the implementation users like TechAdmin and ERPUser, and assign the required job roles to them if you need these implementation users and they don't already exist in your environment. |
| 2 | Run User and Roles Synchronization Process | Run the process Retrieve Latest LDAP Changes to copy changes to users and their assigned roles to Oracle HCM Cloud. |
| 3 | Assign Security Profiles to Abstract Roles | Enable basic data access for the predefined Employee abstract roles. |
| 4 | Create a Generic Role Mapping for the Roles | Enable the roles created in step 3 to be provisioned to implementation users. |

| Step | Task or Activity | Description |
|---|---|---|
| 5 | Assign Abstract Role and Data Access to the Implementation User | Assign the implementation user with the roles that enable functional implementation to proceed. |
| 6 | Verify Implementation User Access | Confirm that the implementation user can access the functions enabled by the assigned roles. |

Once these steps are complete, you're recommended to reset the service administrator sign-in details.

# 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.

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

# 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**.

# 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_<RequestID> - 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_<RequestID> - 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.

# 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.

# 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.

# FAQs for Application Users Management

## 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 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.

## 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 Role Provisioning for Application Users

## 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

# Map a Party Usage Name to a Role

Roles give users access to data and functions. To automatically provision student and instructor roles, you map the roles with party usage names.

Party usages describe how a party is implemented in Student Management. Prospects signing up to apply to the institution are implemented as `constituent` party usages. If your institution defined a custom role to be assigned to

prospects, you define the role mapping between this custom role and the constituent party usage. This will enable the application to provision the custom role to all prospects who sign up with the institution.

To enable this provisioning, sign in as IT Security Manager and follow these steps:

1. Click **Setup and Maintenance**. In the Functional area, click **Application Access**. In the Task area, click **Manage User Role Mappings**.
2. Click the **New** icon.
3. In the **Party Usage Name** column, select a value from the list. For example, select the `constituent` party usage if the role mapping is for signing up a prospect user.
4. In the **Role Code** column, select the role that's to be mapped automatically to the party usage. For example, when a visitor signs up as a user, you can specify that the `student` role be automatically assigned to this visitor.
5. *Optional:* In the **User Category Name** column, select a user category.

# When do Edits to Role Mappings Take Effect

You use the Edit Role Mapping page to update a role mapping. To edit a role mapping, perform the Manage Role Provisioning Rules task in the Setup and Maintenance work area.

Changes that you make to start and end dates, role-mapping conditions, and the associated roles can affect current role provisioning. Let's look at how the changes take effect.

## Automatically Provisioned Roles

Changes to roles that were provisioned automatically take effect as soon as one of these things happen:

- The Autoprovision Roles for All Users process runs.

  This process compares all current user assignments with all current role mappings and updates role provisioning as appropriate. Run this process after creating or editing role mappings and after loading person records in bulk.
- An administrator clicks **Apply Autoprovisioning** on the Manage User Account or Edit User page for individual users affected by the role mapping.

  This action compares the user's current assignments with all current role mappings and updates the user's roles as appropriate.
- An administrator creates or updates assignments of users affected by the role mapping.

  These actions cause a user's roles to be re-evaluated.

## Requestable Roles

Changes to requestable roles take effect immediately. If you remove a requestable role from the role mapping or change the role-mapping conditions, these things happen:

- Users who currently have the role keep it.

  Users such as line managers provision requestable roles manually to other users. Users lose manually provisioned roles automatically only when all of their work relationships are terminated. Otherwise, users keep manually provisioned roles until you manually deprovision them.

- Users who could provision the role to other users can no longer do so, unless they satisfy the revised role-mapping conditions.

### Self-Requestable Roles

Changes to self-requestable roles take effect immediately. If you remove a self-requestable role from the role mapping or change the role-mapping conditions, these things happen:

- Users who currently have the role keep it.

  Users lose manually provisioned roles automatically only when all of their work relationships are terminated. Otherwise, users keep manually provisioned roles until you manually deprovision them.
- Users who could request the role can no longer do so, unless they satisfy the revised role-mapping conditions.

# FAQs for Role Provisioning for Application Users

## 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

# 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.

# 7 Role-Based Access for Student Management

## Overview of Role-Based Access to Data and Pages

Configure the access to application and data through role groups, page groups, and data profiles.

Create groups of roles or pages, and use these groups to assign access permissions to application pages. By doing so, you ensure these things:

- You restrict the access of every user to only those pages that are appropriate for their role.
- You minimize the effort in assigning default page permissions for pages because you use groups to do bulk assignments.

You can create role groups and page groups. At any time, you can add or remove roles or pages to and from groups. You can also delete these groups. Deleting the groups doesn't affect the page access permissions for users. Page-level data access is governed by user profiles, which are mapped to individual roles, and, in turn, mapped to pages.

## Control Page Access by Role

Show or hide pages or parts of a page to a user by specifying the page elements that their role has access to.

You can specify access levels to an application page and also to the elements of the page such as sections, fields, and action buttons.

Here's how to set up page access:

1. Sign in as IT Security Manager.
2. From Student Central, click **Search** and search for **Application Access**.
3. Click **Pages**.
4. Locate the page you want to specify the access permissions for, click the ellipses in that row, and click **Assign Page Access to Roles**.
5. In the **Role Name** column, select the role you're specifying the permissions for.
6. If it's a custom role, click the **Page Access by Role** option to automatically assign default access for all delivered page elements to that role. You can further modify permissions for the page elements if needed.
7. Expand the **Page Elements** list, and for each page element, click inside the **Permissions** field, and select the permissions. If the page elements aren't displayed, ensure that the **Page Access** toggle is set to show the elements. You can specify permissions for as many roles as you need to.
8. When you're done, click **Save**.

### Global Data Profiles

When the security administrator assigns page access to a role, they will also see default data access for the page assigned to the role. Define default data access by assigning global data profiles, associated with the business objects on the page, to the role.

Here's how to review global data profile assignments to a predefined role:

1. Sign in as IT Security Manager.

2. From Student Central, click **Search** and search for **Application Access**.
3. Click the **Roles** tab.
4. Click **Yes** in the **Predefined** filter to list only predefined roles.
5. Select a predefined role **Name**.
6. On the Assigned Data Profiles tab, you can see the global data profiles seeded for the role.

## Bulk Assignment

Security administrators can assign default page and data access for multiple pages to multiple roles.

Here's how to assign pages access to roles in bulk:

1. Sign in as IT Security Manager.
2. From Student Central, click **Search** and search for **Application Access**.
3. Click **Pages**.
4. Click the **Assign Bulk Access to Roles** button.
5. Search for, add, and remove roles, role groups, pages, and page groups on the Assign Bulk Access to Roles page: Assign Access tab.
6. When you're done, click **Assign** to create a bulk assignment request.
7. Monitor its progress on the Active Assignment Requests tab, or download a log to review the assignments that were made.

*Related Topics*

- Create and Manage Role Groups
- Create and Manage Page Groups

# Control Data Access by Role

To control what data is visible to users, create a mapping between a data profile and a role.

When users sign in, they see only those parts of data from the business object that their role has access to, through the data profile.

> **Note:** If you created a custom role by copying a delivered role, remove all data security policies that were copied from the delivered role. You can assign and manage all data access through data profiles by using the Manage Application Access task.

To set up data access:

1. Sign in as IT Security Manager.
2. From Student Central, click **Search** and search for **Application Access**.
3. Click **Data Profiles**.
4. Click **New Data Profile**.
5. Specify a name and description for the profile.
6. Select a business object. To see the fields associated with that business object, click inside the **Fields** field.
7. Select the fields whose values will define the data access to this profile. You can add as many fields as you need to.

8. When you're done, click **Save**. The data profile you created is displayed on the list.
9. Click the ellipses on the row for the data profile you just created, and click **Assign to Roles**. If you don't see the ellipses, scroll to the right.
10. On the Assign Data Access to Roles page, click **Add Role**, select a role to add to the data profile, and click **Add**.
11. For each of the fields that you enabled for the data profile, select the values to define the security filter conditions on the data set for the business object.

    The list of values for dependent security condition fields are filtered based on the values selected on previous fields. That is, a driving field or column is ordered to the left of a dependent field or column, so that the values in the dependent field are filtered based on the values from the driving column.
12. When done, click **Add**.
13. Use the **Add Row** option to add more security filter conditions on the data set for the business object. All of the security conditions rows are aggregated to define the data set from the business object that this role has access to.
14. When done, click **Save**.

# Create and Manage Role Groups

Create a group of roles, and use these groups to assign page-level permissions to users. By using role groups, you minimize the time taken to define the access permissions that users have to application pages.

To create a role group:

1. Sign in as IT Security Manager.
2. From Student Central, click **Search** and search for **Application Access**.
3. Click **Role Groups**.
4. Click **Create Role Group**.
5. On the **Details** tab, enter the basic details for the new role group, and click **Next**.
6. On the **Assign Roles** tab, select the roles to add to the role group, click **Add**, and then click **Save**. The role group is displayed on the appropriate list.

You can use these role groups to specify the access permissions that users have to application pages.

At any time, you can add or remove roles from the group, or delete the entire role group. Deleting a role group doesn't affect the page access permissions to users. Their access is governed by their user profiles, which are mapped to individual roles and, in turn, mapped to pages.

# Create and Manage Page Groups

Create a group of pages, and use these groups to assign page-level permissions to users. By using page groups, you minimize the time taken to define the access permissions that users have to application pages.

To create a page group:

1. Sign in as IT Security Manager.
2. From Student Central, click **Search** and search for **Application Access**.
3. Click **Page Groups**.
4. Click **Create Page Group**.

5. On the Create Page Group page, enter a name and an optional description for the page group.
6. Select the pages to add to the group, click **Add**, and then click **Save**. The page group is displayed on the appropriate list.

You can use these page groups to specify the access permissions that users have to application pages.

At any time, you can add or remove pages from the group, or delete the entire page group. Deleting a page group doesn't affect the page access permissions to users. Their access is governed by their user profiles, which are mapped to individual roles and, in turn, mapped to pages.

# Assign Data Privileges

As an IT security Manager, you can assign data access on a secured business object by assigning data profiles to custom roles.

Data is visible to the end user based on the data security conditions defined in these data profiles. You can assign only intended data privileges that correspond to the permitted actions (for example, view, add, or delete) on this data. Or, you can choose to assign full data access on all secured business objects to custom roles by assigning global data profiles and default data privileges to custom roles.

If you created a custom role by copying a delivered role, remove all data security policies that were copied from the delivered role. Thereafter, assign and manage data access through data profiles by using the Manage Application Access task.

Here's how you assign full data access on all security business objects to custom roles:

1. Sign in as IT Security Manager.
2. Click **Tools** > **Scheduled Processes**.
3. Click **Schedule New Process**.
4. Specify the type as **Job**.
5. Select **Synchronize Default Data Privileges for Custom Job Roles** and click **OK**.
6. Click **Submit** and return to the Scheduled Processes page.
7. Click **Search**. The process you just submitted is listed at the top of all scheduled processes.

When the status of the process changes to `Completed`, all custom roles are assigned with the global data profiles and default data privileges if a more restrictive data profile isn't already assigned to the role.

Here's how you assign restricted privileges for data access:

1. Sign in as IT Security Manager.
2. From Student Central, click **Search** and search for **Application Access**.
3. Click **Data Profiles** and, in the row for the data profile that contains the roles to assign the privileges to, click **Assign to Roles**.
4. In the Security Conditions section, select a role. The users in that role are displayed. For each user, in the Privileges column, click **Choose Value**, and assign the appropriate privileges.
5. When you're done assigning privileges, click **Assign**.
6. Click **Save**.

Now, when the users with the data profile log in, they can do only those actions on the application pages that their data profiles have privileges for.

# 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.<br>• 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.<br>• 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.<br>**CAUTION:**<br>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 (both Oracle and non-Oracle) 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

# 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.

### 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
- 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 **Manage SSO** 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.

# 10 Export and Import of Security Data and Role Hierarchy

## 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<br>• Role preferences<br>• Location-based access settings<br>• 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<br>• Password policy information |
| Security Console User Category Notifications | Notification preferences.<br><br>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

- 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:<br>• Manually using the Manage Database Resources page in the security console.<br>• Manually using the Edit role/Copy role flow in the security console<br>• Automatically when you copy a role using the Role Copy in the security profile<br>• Automatically when you create profile content types<br>• Automatically when you map HCM spreadsheet business objects to roles<br>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.<br><br>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.<br><br>**Note:**<br>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.<br><br>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.<br><br>This profile option is no longer used and no values are exported for this business object. |

| Business Object | Information Included in Export and Import |
|---|---|
| Functional Security Custom Roles | The custom role includes the following details:<br>• Role Code<br>• Role Name<br>• Role Description<br>• Role Category<br>• 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.<br>**Note:**<br>The scope is limited to User Assignable roles only. |
| Functional Security Custom Role Hierarchy | The role hierarchy includes the following details:<br>• Parent Role<br>• Member Role<br>• Add or Remove Role Membership |
| Functional Security Custom Role Privilege Membership | The role privilege membership includes the following details:<br>• Parent Role<br>• Member Privilege<br>• Add or Remove Privilege Membership |
| HCM Data Role | The HCM data role includes the following details:<br>• Data Role Code<br>• Data Role Name<br>• Data Role Description<br>• Inherited Job Role Code<br>• Delegation Allowed Check Box |
| HCM Data Role Security Profile | The HCM data role security profile includes the following details:<br>• Data Role Code<br>• Securing Object<br>• Security Profile Name |
| HCM Exclusion Rule | HCM exclusion rule and HCM exclusion rule detail includes HCM exclusion rule definitions.<br>• HCM Exclusion Rule<br>• HCM Exclusion Rule Detail |
| Legislative Data Group Security Profile List | Legislative data group security profile list includes the following details:<br>• Legislative data group security profile name |

| Business Object | Information Included in Export and Import |
|---|---|
| | • Legislative data groups that are included in the legislative data group security profile |
| Organization Security Profile | Organization security profile includes the following details:<br>• Organization Security Profile Name<br>• Enabled Check Box<br>• View All Check Box<br>• Include Future Organizations Check Box<br>• Code indicating Department Hierarchy or Generic Organization Hierarchy<br>• Hierarchy Name (if securing by organization hierarchy)<br>• Top Organization Name (if securing by organization hierarchy)<br>• Include Top Organization Check Box<br>• Secure by Organization Hierarchy Check Box<br>• Secure by Organization Classification Check Box<br>• Secure by Organization List Check Box |
| Organization Security Profile Classification List | Organization security profile classification list includes the following details:<br>• Organization Security Profile Name<br>• Organization Classification Name |
| Organization Security Profile Organization List | Organization security profile organization list includes the following details:<br>• Organization Security Profile Name<br>• Organization name<br>• Organization Classification<br>• Include/Exclude Check Box |
| Country Security Profile | Country security profile includes the following details:<br>• Country Security Profile Name<br>• Enabled Check Box |
| Country Security Profile List | Country security profile list includes the following details:<br>• Country Security Profile Name<br>• Country code |
| Position Security Profile | Position security profile includes the following details:<br>• Position Security Profile Name<br>• Description<br>• Enabled Check Box<br>• View All Check Box<br>• Include Future Positions Check Box<br>• Hierarchy Name (if securing by position hierarchy) |

| Business Object | Information Included in Export and Import |
|---|---|
| | • Top Position Name (if securing by position hierarchy)<br>• Include Top Position Check Box<br>• Top Position Name (if securing by organization hierarchy)<br>• Secure by Position Hierarchy Check Box<br>• Secure by Department Check Box<br>• Department Organization Security Profile Name (if securing by department)<br>• Secure by Business Unit Check Box<br>• Business Unit Organization Security Profile Name (if securing by business unit)<br>• Secure by Position List Check Box<br>• Secure by Area of Responsibility Check Box |
| Position Security Profile Position List | Position security profile position list includes the following details:<br>• Position Security Profile Name<br>• Position Code<br>• Include/Exclude Check Box |
| Position Security Profile Area of Responsibility Scope | Position security profile area of responsibility scope includes the following details:<br>• Position Security Profile Name<br>• Responsibility Type<br>• Scope of Responsibility |
| HR Document Type Security Profile | HR document type security profile includes the following details:<br>• HR Document Type Security Profile Name<br>• Enabled Check Box<br>• View All Check Box<br>• Include/Exclude Check Box |
| HR Document Type Security Profile List | HR document type security profile list includes the following details:<br>• HR Document Type Security Profile Name<br>• Document Type Name |
| Payroll Security Profile | Payroll security profile includes the following details:<br>• Payroll Security Profile Name<br>• Enabled Check Box<br>• View All Check Box |
| Payroll Security Profile Pay | Payroll security profile pay includes the following details:<br>• Payroll Security Profile Name<br>• Payroll Name |

| Business Object | Information Included in Export and Import |
|---|---|
| | • Legislative Data Group Name |
| Payroll Flow Security Profile | Payroll flow security profile includes the following details:<br>• Payroll Flow Security Profile Name<br>• Enabled Check Box<br>• View All Check Box |
| Payroll Flow Security Profile Pay | Payroll flow security profile pay includes the following details:<br>• Payroll Flow Security Profile Name<br>• Flow Name |
| Person Security Profile | Person security profile includes the following details:<br>• Person Security Profile Name<br>• Description<br>• Enabled Check Box<br>• Access to Own Record Check Box<br>• Include Future People Check Box<br>• Include Shared People Information Check Box<br>• Access to Candidates with Offers Check Box<br>• Secure by Area of Responsibility<br>• Secure by Manager Hierarchy Check Box<br>• Person or Assignment Check Box<br>• Maximum Levels in Hierarchy<br>• Manager Hierarchy Type<br>• Hierarchy Content Code<br>• Secure by Person Type Check Box<br>• Secure by Department Check Box<br>• Department Security Profile Name (if securing by department)<br>• Secure by Business Unit Check Box<br>• Business Unit Profile Name (if securing by business unit)<br>• Secure by Legal Employer Check Box<br>• Legal Employer Security Profile Name (if securing by legal employer)<br>• Secure by Position Check Box<br>• Position Security Profile Name (if securing by position)<br>• Secure by Legislative Data Group Check Box<br>• Legislative Data Group Security Profile Name (if securing by legislative group)<br>• Secure by Payroll Check Box<br>• Payroll Security Profile Name (if securing by payroll)<br>• Secure by Global Name Range Check Box |

| Business Object | Information Included in Export and Import |
|---|---|
| | • Global Name Range Start Value (if securing by global name range)<br>• Global Name Range End Value (if securing by global name range)<br>• Apply Exclusion Rules Check Box<br>• Secure by Custom Criteria Check Box<br>• Custom Restriction Text (if securing by custom criteria)<br>• |
| Person Security Profile Manager Type | Person security profile manager type includes the following details:<br>• Person Security Profile Name<br>• 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:<br>• Person Security Profile Name<br>• Responsibility Type<br>• Scope of Responsibility<br>• Employee Check Box<br>• Contingent Worker Check Box<br>• Pending Worker Check Box<br>• Nonworker Check Box<br>• Candidate with Offer Check Box |
| Person Security Profile Exclusion | Person security profile exclusion includes the following details:<br>• Person Security Profile Name<br>• Exclusion Rule Name |
| Talent Pools Security Profile | Talent pools security profile includes the following details:<br>• Talent Pool Security Profile Name<br>• Enabled Check Box<br>• View by Ownership Check Box<br>• View All Check Box<br>• View All Public Talent Pools Check Box<br>• Secure by Business Unit Check Box<br>• Secure by Department Check Box<br>• Secure by Job Family Check Box |
| Talent Pools Security Profile Job Family | Talent pools security profile job family includes the following details:<br>• Talent Pool Security Profile Name<br>• Job Family Name |
| Talent Pools Security Profile Department | Talent pools security profile department includes the following details: |

| Business Object | Information Included in Export and Import |
|---|---|
| | • Talent Pool Security Profile Name<br>• Department Name |
| Talent Pools Security Profile Business Unit | Talent pools security profile business unit includes the following details:<br>• Talent Pool Security Profile Name<br>• Business Unit Name |
| Transaction Security Profile | Transaction security profile includes the following details:<br>• Transaction Security Profile Name<br>• Description<br>• Enabled Check Box<br>• View All Check Box |
| Transaction Security Profile Entries | Transaction security profile entries include the following details:<br>• Transaction Security Profile Name<br>• Product Family<br>• Category Code<br>• All Sub-Categories Check Box<br>• Exclude Sub-Category Check Box |
| Transaction Security Profile Sub-Categories | Transaction security profile sub-categories include the following details:<br>• Transaction Security Profile Name<br>• Product Family<br>• Category Code<br>• Sub-Category Code |
| Role Provisioning Rule | Role provisioning rule includes the following details:<br>• Mapping Rule Name<br>• Legal Employer Name<br>• Business Unit Name<br>• Department Name<br>• Job Set Code<br>• Job Code<br>• Position Business Unit Name<br>• Position Code<br>• Grade Set Code<br>• Grade Code<br>• Location Set Code<br>• Location Code |

| Business Object | Information Included in Export and Import |
|---|---|
| | • User Person Type<br>• System Person Type<br>• Assignment Type<br>• HR Assignment Status Code<br>• Resource Role<br>• Party Type Usage Code<br>• Contact Role<br>• Manager with Reports Check Box<br>• Manager Type<br>• Responsibility Type |
| Role Provisioning Associated Role List | Role provisioning associated role list includes the following details:<br>• Mapping Rule Name<br>• Role Code<br>• Requestable Check Box<br>• Self-Requestable Check Box<br>• 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:<br>• Job Requisition Security Profile Name<br>• Enabled Check Box<br>• View All Check Box<br>• Secure by Job Family Check Box<br>• Secure by Job Function Check Box<br>• Secure by Location Check Box<br>• Secure by Organization Check Box<br>• Secure by Recruiting Type Check Box |
| Spreadsheet Business Object Security Mapping | HCM spreadsheet business object access mapping includes the following details:<br>• Role Code<br>• Business Object |

| Business Object | Information Included in Export and Import |
|---|---|
| | • Product Area<br>• Enabled Check Box<br>• 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

# Export and Import of Page and Data Access Configuration

You can export page and data access configuration from one environment and import into another environment to complete page and data access configuration more efficiently.

## Before You Begin

Before migrating your page and data access setup data, you must export and import all other product setup data.

Learn how to export and import the setup data. For more information, see the *Setup Data Export and Import Using an Offering or a Functional Area* and *Setup Data Export and Import Using Implementation Project* chapters of the Using Functional Set up Manager Guide.

## What Gets Exported and Imported

Move your page and data access setup data from one environment to another using an implementation project in the Functional Setup Manager. Create the implementation project by selecting the **Student Management Security** task list, and then create a configuration package file from the implementation project to export and import the setup data.

Alternatively, use the Application Access functional area to export and import only the page and data access setup data. Define page and data access using the **Manage Application Access** task, which is mapped to the FSM business objects that store those page and data access definitions. Then, using the **Application Access** functional area inside the Student Management offering, create a configuration package file to easily export and import the setup data.

These business objects help in the packaging of page and data access definitions:

- Security Role Group
- Security Role Group Member
- Application Page Group
- Application Page Group Member
- Page Access Role Assignment
- Role Page Permission
- Page Access Role Group Assignment
- Role Group Page Permission
- Data Security Profile
- Data Security Profile Field
- Data Profile Role assignment
- Role Data Condition
- Role Data Condition Value
- Role Data Privilege Grant
- Data Profile Role Group Assignment
- Role Group Data Condition
- Role Group Data Condition Value

- Role Group Data Privilege Grant

Let's closely examine each business object to know what it contains.

| Business Object | Information Included in Export and Import |
|---|---|
| Security Role Group | Role groups |
| Security Role Group Member | Roles within a role group |
| Application Page Group | Page groups |
| Application Page Group Member | Pages within a page group |
| Page Access Role Assignment | Page to role assignments |
| Role Page Permission | Page permission to role assignments |
| Page Access Role Group Assignment | Page to role group assignments |
| Role Group Page Permission | Page permission to role group assignments |
| Data Security Profile | Data security profiles |
| Data Security Profile Field | Fields in a data security profile |
| Data Profile Role assignment | Data security profile to role assignments |
| Role Data Condition | Data conditions in a data security profile to role assignment |
| Role Data Condition Value | Data condition values in a data security profile to role assignment |
| Role Data Privilege Grant | Privilege grants on a data condition to a role |
| Data Profile Role Group Assignment | Data security profile to role group assignments |
| Role Group Data Condition | Data conditions in a data security profile to role group assignment |
| Role Group Data Condition Value | Data condition values in a data security profile to role group assignment |
| Role Group Data Privilege Grant | Privilege grants on a data condition to a role group |

*Related Topics*

- Setup Data Export and Import Using an Offering or a Functional Area
- Setup Data Export and Import Using Implementation Project

# 11 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.

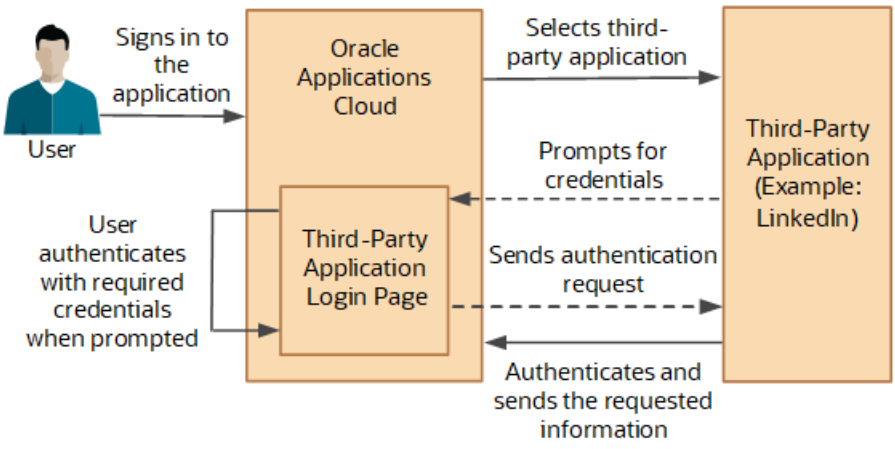
To understand the OAuth authorization protocol, let's take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required 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.

# 12 Reports for Application Users and Roles

## Run the User Details System Extract Report

The Oracle BI Publisher User Details System Extract Report includes details of selected Oracle Fusion Applications user accounts. To run this report, you must have a data role providing view-all access to person records for the Human Capital Management Application Administrator job role.

To run the report:

1. In the Contents pane of the Reports and Analytics work area, select **Shared Folders** > **Human Capital Management** > **Workforce Management** > **Human Resources Dashboard**.
2. Select the User Details System Extract report.
3. In the report window, click **More**.
4. On the Oracle Business Intelligence page for the report, select either **Open** to run the report immediately or **More** > **Schedule** to schedule the report.

*Related Topics*

- User Details System Extract Report Parameters
- User Details System Extract Report

## 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 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

# LDAP Request Information Reports

This topic describes the LDAP Request Dashboard and LDAP Request Information reports. Use these reports to extract information about the status of LDAP requests. To run the reports, you must have the IT Security Manager job role.

To run the reports:

1. Open the Reports and Analytics work area.
2. In the Contents pane, select **Shared Folders** > **Human Capital Management** > **Workforce Management** > **Human Resources Dashboard**.

Both reports appear in the Human Resources Dashboard folder.

## Running the LDAP Request Information Reports

Use the LDAP Request Dashboard report to display summaries of requests in specified categories. Follow these steps:

1. In the Human Resources Dashboard folder, click **LDAP Request Dashboard** > **More**. The Oracle Business Intelligence Catalog page opens.
2. Find the LDAP Request Dashboard entry on the Business Intelligence Catalog page and click **Open** to open the report.
3. On the LDAP Request Dashboard page, complete the parameters shown in this table to filter the report and click **Apply**.

| Parameter | Description |
|---|---|
| Within the Last N Days | Enter a number of days. The report includes LDAP requests updated within the specified period. |
| Request Type | Select an LDAP request type. The value can be one of Create, Update, Suspend, Activate, UserRoles, Terminate, and All. |
| Request Status | Select an LDAP request status. The value can be one of Complete, Faulted, In Progress, Request, Part Complete, Suppressed, Rejected, Consolidated, and All. |

The report output includes:

- A summary of the enterprise settings for user-account creation and maintenance.
- Numbers of LDAP requests by status and type in both tabular and graphical formats.
- A summary table showing, for each request type, its status, equivalent user status, any error codes and descriptions, and the number of requests. All values are for the specified period.

You can refresh the report to update it as requests are processed.

Use the LDAP Request Information report to review details of the LDAP requests in the LDAP requests table in Oracle Fusion Cloud HCM. Follow these steps:

1. In the Human Resources Dashboard folder, click **LDAP Request Information** > **More**. The Oracle Business Intelligence Catalog page opens.
2. Find the LDAP Request Information entry on the Business Intelligence Catalog page and click **Open** to open the report.

3. On the LDAP Request Information page, complete the parameters shown in this table to filter the report and click **Apply**.

| Parameter | Description |
|---|---|
| Within the Last N Days | Enter a number of days. The report includes LDAP requests updated within the specified period. |
| Request Type | Select an LDAP request type. The value can be one of Create, Update, Suspend, Activate, UserRoles, Terminate, and All. |
| Request Status | Select an LDAP request status. The value can be one of Complete, Faulted, In Progress, Request, Part Complete, Suppressed, Rejected, Consolidated, and All. |

The report includes a table showing for each request:

- The request date and type
- Whether the request is active
- The request status and its equivalent user status
- Error codes and descriptions, if appropriate
- Requested user names, if any
- The person to whom the request relates
- When the request was created and last updated

To save either of the reports to a spreadsheet, select **Actions** > **Export** > **Excel**.

# 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 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 may 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.

# 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. |

| Report Type | File Suffix | File Format | File Contents |
|---|---|---|---|
| | | | **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 contains one file for each user or role. |
| • **Multiple users**<br>• **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**

# 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_<RequestID> - 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_<RequestID> - 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.

# 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.

# FAQs for Reports for Application Users and Roles

## 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.

# 13 Security Console

## 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.

# 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.

# 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.

# 14 Job, Abstract, and Duty Roles

## 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.
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.

> **Note:** For the Data Security Policies page to be active, you must select an "Enable edit of data security policies" option. To locate it, select the Administration tab, and then the Roles tab on the Administration page. If this option isn't selected, the Data Security Policies page is read-only.

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.)

> **Note:** For the Users page to be active, you must select an "Enable edit of user role membership" option. To locate it, select the Administration tab, and then the Roles tab on the Administration page. If this option isn't selected, the Users page is read-only.

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

# Create a Custom Role with Limited Access

To delegate some of the IT security management tasks to a helpdesk 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 |
| 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

# FAQs for Job, Abstract, and Duty Roles

## 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.

# 15 Roles for Workflow Access

## 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 |
| 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
- Role Copying or Editing
- Create Roles in the Security Console
- Edit Job Role and Abstract Role
- Actions and Statuses for Workflow Tasks

# 16 Certificate Management

## Overview of Certificates

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 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.