

Oracle

SCM Cloud

Securing Oracle SCM Cloud

Release 12

This guide also applies to on-premises implementations

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

The business names used in this documentation are fictitious, and are not intended to identify any real companies currently or previously in existence.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Contents

Preface **i**

1 Introduction **1**

Securing Oracle SCM Cloud: Overview	1
Roles-Based Applications Security: Explained	2
Role Types: Explained	4
Role Inheritance: Explained	6
Duty Role Components: Explained	6
Aggregate Privileges: Explained	7
Security Customization in Oracle Applications Cloud: Points to Consider	7
Role-based Security in Oracle SCM Cloud: Explained	8
Security Setup in Oracle SCM Cloud: Explained	10
Getting Started with Security Implementation in Oracle SCM Cloud: Procedure	11

2 Using the Security Console **13**

Security Console: Overview	13
Administering the Security Console: Explained	14
Running Retrieve Latest LDAP Changes: Procedure	15
Security Visualizations: Explained	16
Working with a Visualization Graph: Explained	16
Working with a Visualization Table: Explained	18
Generating a Visualization: Procedure	19
Simulating Navigator Menus in the Security Console: Procedure	19
Security Console Analytics: Explained	20
Bridge for Active Directory: Explained	20
FAQs for Using the Security Console	21

3 Managing Implementation Users **23**

Creating Implementation Users	23
Assigning Roles to Implementation Users	30

4	Preparing for Application Users	33
	Preparing Oracle Applications Cloud for Application Users: Overview	33
	User and Role-Provisioning Setup: Critical Choices	33
	User Account Creation Option: Explained	34
	User Account Role Provisioning Option: Explained	35
	User Account Maintenance Option: Explained	35
	Setting the User and Role Provisioning Options: Procedure	36
	Provisioning Abstract Roles to Users Automatically: Procedure	37
	FAQs for Preparing for Application Users	38
5	Creating and Managing Application Users	41
	Creating Users	41
	Managing Users	43
	FAQs for Creating and Managing Application Users	51
6	Provisioning Roles to Application Users	55
	Role Mappings: Explained	55
	Creating a Role Mapping: Procedure	56
	Role Provisioning and Deprovisioning: Explained	58
	Autoprovisioning: Explained	60
	User and Role Access Audit Report	61
	Managing Data Access for Users: Explained	63
	Assigning Data Access to Users: Worked Example	64
	FAQs for Provisioning Roles to Application Users	66
7	Customizing Security	69
	Managing Data Security Policies	69
	FAQs for Customizing Security	74
8	Reviewing Roles and Role Assignments	77
	Reviewing Role Assignments: Procedure	77
	Reviewing Role Hierarchies: Explained	77
	Comparing Roles: Procedure	78
	User and Role Access Audit Report	79

9 Customizing Roles Using the Security Console 83

Creating Custom Roles	83
Role Optimization	94
FAQs for Customizing Roles Using the Security Console	98

10 Managing Certificates and Keys 99

Managing Certificates: Explained	99
Generating Certificates: Explained	99
Generating a Signing Request: Procedure	100
Importing and Exporting X.509 Certificates: Procedure	100
Importing and Exporting PGP Certificates: Procedure	101
Deleting Certificates: Procedure	101



11 Security for SCM Analytics and Reports 103

Security for Oracle SCM Cloud Analytics: Overview	103
Security for Oracle SCM Cloud Reports: Overview	104
Business Intelligence Roles: Explained	105


Preface

This preface introduces information sources that can help you use the application.

Oracle Applications Help

Use the help icon  to access Oracle Applications Help in the application. If you don't see any help icons on your page, click the Show Help icon  in the global header. Not all pages have help icons. You can also access Oracle Applications Help at <https://fusionhelp.oracle.com>.

Using Applications Help

 **Watch:** This video tutorial shows you how to find help and use help features.

Additional Resources

- **Community:** Use [Oracle Applications Customer Connect](#) to get information from experts at Oracle, the partner community, and other users.
- **Guides and Videos:** Go to the [Oracle Help Center](#) to find guides and videos.
- **Training:** Take courses on Oracle Cloud from [Oracle University](#).

Documentation Accessibility

For information about Oracle's commitment to accessibility, see the [Oracle Accessibility Program](#).


Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.

1 Introduction

Securing Oracle SCM Cloud: Overview

Oracle SCM Cloud is secure as delivered. This guide explains how to enable user access to SCM functions and data. You perform some of the tasks in this guide either only or mainly during implementation. Most, however, can also be performed later and as requirements emerge. This topic summarizes the scope of this guide and identifies the contents of each chapter.

 **Note:** As of Release 12, data roles are no longer used in Oracle SCM Cloud. Assume that references in this guide to data roles are only applicable to Oracle HCM Cloud. For important background, details, and instructions, see the Oracle ERP Cloud and Oracle SCM Cloud Security Upgrade Guide (2211555.1) on My Oracle Support at <https://support.oracle.com>.

Guide Structure

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

Chapter	Contents
Introduction	A brief introduction to the concepts of role-based security
Using the Security Console	How to set up and manage the centralized security work area
Managing Implementation Users	The purpose of implementation users and how you create them
Preparing for Application Users	Enterprise-wide options and related decisions that affect application users
Creating and Managing Application Users	The different ways you can create application users and maintain user accounts, with instructions for some methods
Provisioning Roles to Application Users	The ways that application users can acquire roles, with instructions for creating some standard role mappings
Customizing Security	How to create, review, and modify security components, with recommended best practices.
Reviewing Roles and Role Assignments	How to review roles and identify the users assigned to them
Customizing Roles Using the Security Console	How to create, review, and modify roles using the Security Console, with recommended best practices
Managing Certificates and Keys	How to generate, import, export, and delete digital certificates
Security for SCM Analytics and Reports	How to manage security features that affect SCM analytics and reports

During implementation, you can perform security-related tasks from the Security Console if you have the IT Security Manager role. To use the Security Console, navigate to: **Tools > Security Console**.

Roles-Based Applications Security: Explained

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. In role-based access:

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

The following topics introduce different types of roles and how they work together through role inheritance to secure Oracle Applications Cloud.

- Abstract roles
- Job roles
- Duty roles
- Role inheritance

Abstract Roles

Abstract roles represent a worker's role in the enterprise independently of the job that you hire the worker to do. You can create your own abstract roles. All workers are likely to have at least one abstract role that allows them to access standard functions, such as managing their own information and searching the worker directory. You assign abstract roles directly to users. Employee is an example of an abstract role.

Job Roles

Job roles represent the job that you hire a worker to perform. You can create your own job roles. However, the IT Security Manager and Application Implementation Consultant predefined job roles are exceptions to this general rule because they're not considered Oracle Applications Cloud job roles. Warehouse Manager is an example of a job role.

Duty Roles

Duty roles represent the individual duties that users perform as part of their job. They grant access to work areas, dashboards, task flows, application pages, reports, batch programs, and so on. Job roles and abstract roles inherit duty

roles. Duty roles can also inherit other duty roles. They're part of the security reference implementation, and are the building blocks of custom job and abstract roles. You can also create custom duty roles. You don't assign duty roles directly to users.

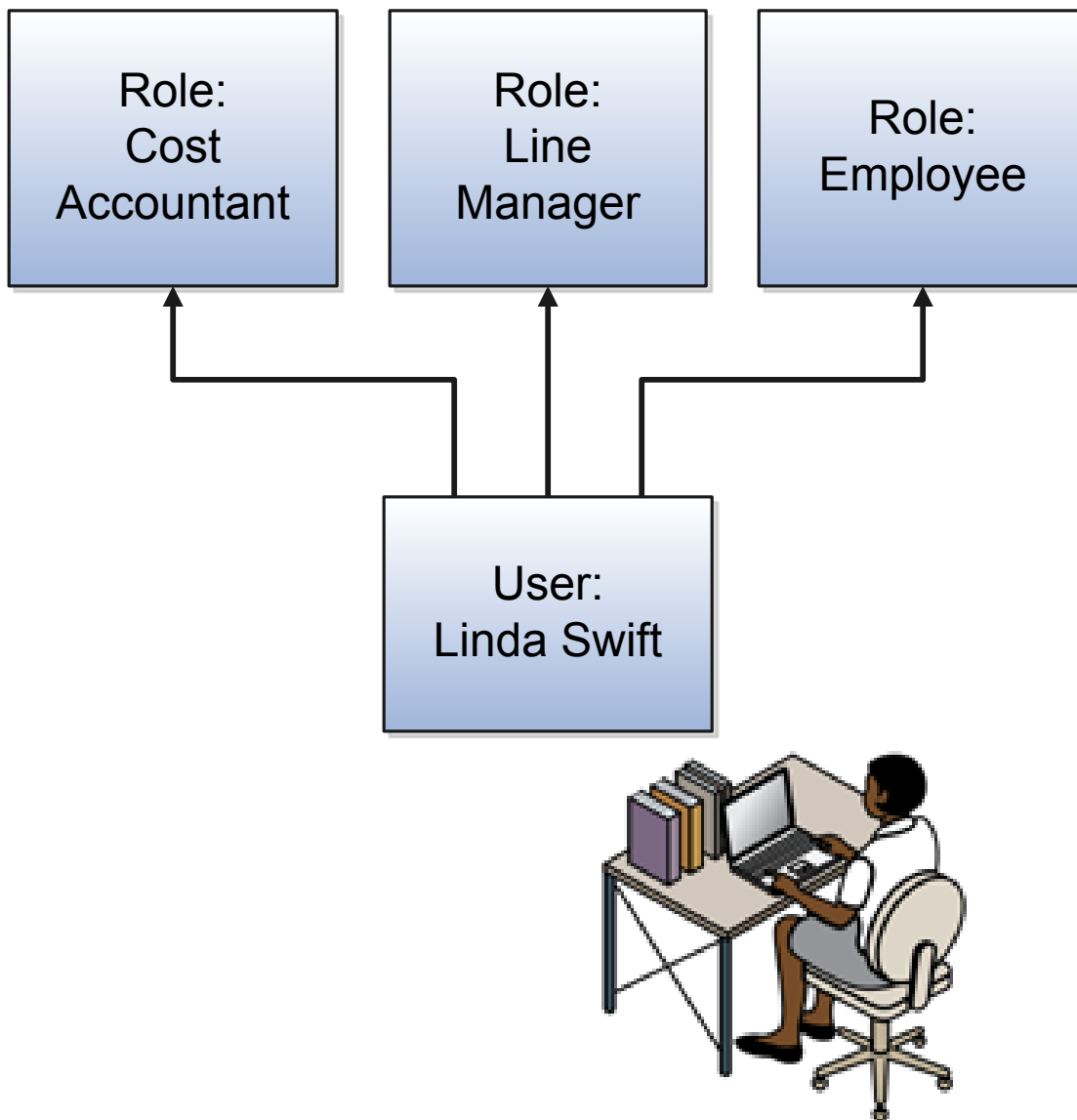
An example of a duty role is the Inventory Transaction Management Duty. Job and abstract roles inherit duty roles that determine the access to functions appropriate to the job. For example, the job role Warehouse Manager inherits the Inventory Transaction Management Duty.

Role Inheritance

Each role is a hierarchy of other roles:

- Job and abstract roles inherit duty roles.
- Duty roles can inherit other duty roles.

In this figure, user Linda Swift has three roles.



When Linda signs in to Oracle Applications Cloud, she doesn't have to select a role. All of these roles are active concurrently.

The functions and data that Linda can access are determined by this combination of roles.

- As an employee, Linda can access employee functions and data.
- As a line manager, Linda can access line-manager functions and data.
- As a cost accountant, Linda can access cost accountant related functions and data for Vision Operations.

Role Types: Explained

Oracle Supply Chain Management (Oracle SCM) Cloud defines the following types of roles:

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

This topic introduces the role types.

Job Roles

Job roles represent the jobs that users perform in an organization. Warehouse Manager and Inventory Manager are examples of predefined job roles. You can also create custom job roles.

Abstract Roles

Abstract roles represent people in the enterprise independently of the jobs they perform. Some predefined abstract roles in Oracle Applications Cloud include Employee and Transactional Business Intelligence Worker. You can also create custom abstract roles.

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

Duty Roles

Duty roles represent a logical collection of privileges that grant access to tasks that someone performs as part of a job. Inventory Transaction Management Duty and Inventory Count Management Duty are examples of predefined duty roles. You can also create custom duty roles. Other characteristics of duty roles include:

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

Job and abstract roles may inherit predefined or custom duty roles either directly or indirectly.

You don't assign duty roles directly to users.

Aggregate Privileges

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

Aggregate privileges differ from duty roles in these ways:

- You can't create aggregate privileges. They are all predefined.
- You can't modify aggregate privileges.

- You can't copy aggregate privileges.
- They don't inherit any type of roles.

You can include the predefined aggregate privileges in your custom job and abstract roles. You assign aggregate privileges to these roles directly.

You don't assign aggregate privileges directly to users.

Role Inheritance: Explained

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

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

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

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

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

Duty Role Components: Explained

This topic describes the components of a typical duty role. Function security privileges and data security policies are granted to duty roles. Duty roles may also inherit aggregate privileges and other duty roles.

Data Security Policies

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


Each data security policy combines:

- A duty role, for example Inventory Transaction Management Duty.
- A business object that's being accessed, for example Inventory Transaction.
- The condition, if any, that controls access to specific instances of the business object. For example, a condition may allow access to data for the inventory organizations in which the user can operate.
- A data security privilege, which defines what may be done with the specified data, for example Manage Inventory Transaction Data.

Function Security Privileges

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

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

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

Aggregate Privileges: Explained

Aggregate privileges are a type of role. Each aggregate privilege combines a single function security privilege with related data security policies. All aggregate privileges are predefined.

Aggregate Privilege Names

An aggregate privilege takes its name from the function security privilege that it includes. For example, the Manage Accounts Payable Accounting Period Status aggregate privilege includes the Manage Accounting Period Status function security privilege.

Aggregate Privileges in the Role Hierarchy

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

Use of Aggregate Privileges in Custom Roles

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

Customization of Aggregate Privileges

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

If you copy a job or abstract role, then the source roles' aggregate privileges aren't copied, even if you select the **Copy top role and inherited roles** option. Instead, role membership is added automatically to the aggregate privilege for the copied role.

The Security Console enforces the recommended approach to aggregate privileges, which is that you use them as supplied.

Security Customization in Oracle Applications Cloud: Points to Consider

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

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

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

Missing Enterprise Jobs

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

Predefined Roles with Different Privileges

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

Predefined Roles with Missing Privileges

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

Related Topics

- [Reviewing Predefined Roles: Explained](#)

Role-based Security in Oracle SCM Cloud: Explained

Role-based security in Oracle SCM Cloud is defined for users as shown here:

Role Name	Description	Data Access
Cost Accountant	Can manage cost transactions	To the cost organizations for which they are authorized

Role Name	Description	Data Access
Warehouse Manager	Can manage inventory transactions	To the inventory organizations in which they operate

Many job and abstract roles are predefined in Oracle SCM Cloud.

- Product Manager
- Cost Accountant
- Warehouse Manager
- Supply Chain Controller
- Receiving Agent
- Shipping Manager
- Inventory Manager
- Order Manager
- Product Design Manager
- Product Portfolio Manager

These predefined roles are part of the Oracle Applications Cloud Security Reference Implementation. The Security Reference Implementation is a predefined set of security definitions that you can use as supplied. Also included in the Security Reference Implementation are roles that are common to all Oracle Applications Cloud, such as:

- Application Implementation Consultant
- IT Security Manager

Examples of Role Types

This example shows different types of roles.

Abstract Role	Job Roles	Duty Role
Procurement Requester	Cost Accountant (with data scope of US Operations)	Inventory Balances Management Duty
	Warehouse Manager	

Duty roles are associated with function security privileges and data security policies. For example, the Inventory Balances Management Duty is associated with six function security privileges and two data security policies, as illustrated in the following list.

- These function security privileges secure the respective pages:
 - Manage On-Hand Quantity
 - Request Item Issue
 - Request Subinventory Transfer
 - Request Cycle Count
 - Manage Material Status

- Edit Lot Grade
- The data security policy On-Hand Quantity Data determines the inventory organizations in which the users with this duty role can manage On Hand Quantity.

The data security policy Expected Supply Data determines the inventory organizations in which the users with this duty role can manage the expected Supply.

For example, an Inventory Manager who is assigned the Inventory Balances Management Duty role for On Hand Quantity and has the data security privilege Manage On-Hand Quantity Data is able to manage on-hand quantity for the inventory organization in which the set of users operate.

Example of Role Inheritance

One of the duties that a Product Manager performs is managing items. So, the Product Manager job role inherits the Item Management Duty, which is granted the Manage Item privilege. In reality, the Product Manager job role inherits many duty roles, each of which is typically granted multiple security privileges.

Security Setup in Oracle SCM Cloud: Explained

After the initial security setup at the enterprise level, you can set up security for Oracle SCM Cloud. When setting up the enterprise with structures such as business units, you create roles with new data security policies..

A Supply Chain Application Administrator or an Application Implementation Consultant sets up enterprise structures, such as business units and ledgers, using Define Common Application Configuration activities. Basic enterprise structures may already be set up by Oracle in some Oracle Cloud Application Services implementations. After the enterprise has been set up, you can proceed with the following security setup tasks.

The following table shows the tasks in a likely order, as well as the conditions and purposes of the tasks and in which user interface pages these tasks are performed.

Task	Condition	Purpose	Performed In
Manage Job Roles	None	Manage job and abstract (enterprise) roles.	Roles tab of Security Console
Manage Duties	None	Manage duty (application) roles and provision to job roles.	Roles tab of Security Console
Manage Data Security Policies	None	Manage data security grants to roles.	Roles tab of Security Console
Manage Data Access For Users	None	Explicitly assign users to the appropriate data set, such as a business unit or a ledger, for a particular role.	Setup and Maintenance work area
Manage Supplier User Roles	Supplier Portal in Procurement is provisioned and requires trading partner security.	Manage roles that can be provisioned to supplier users.	Supplier Portal or Sourcing

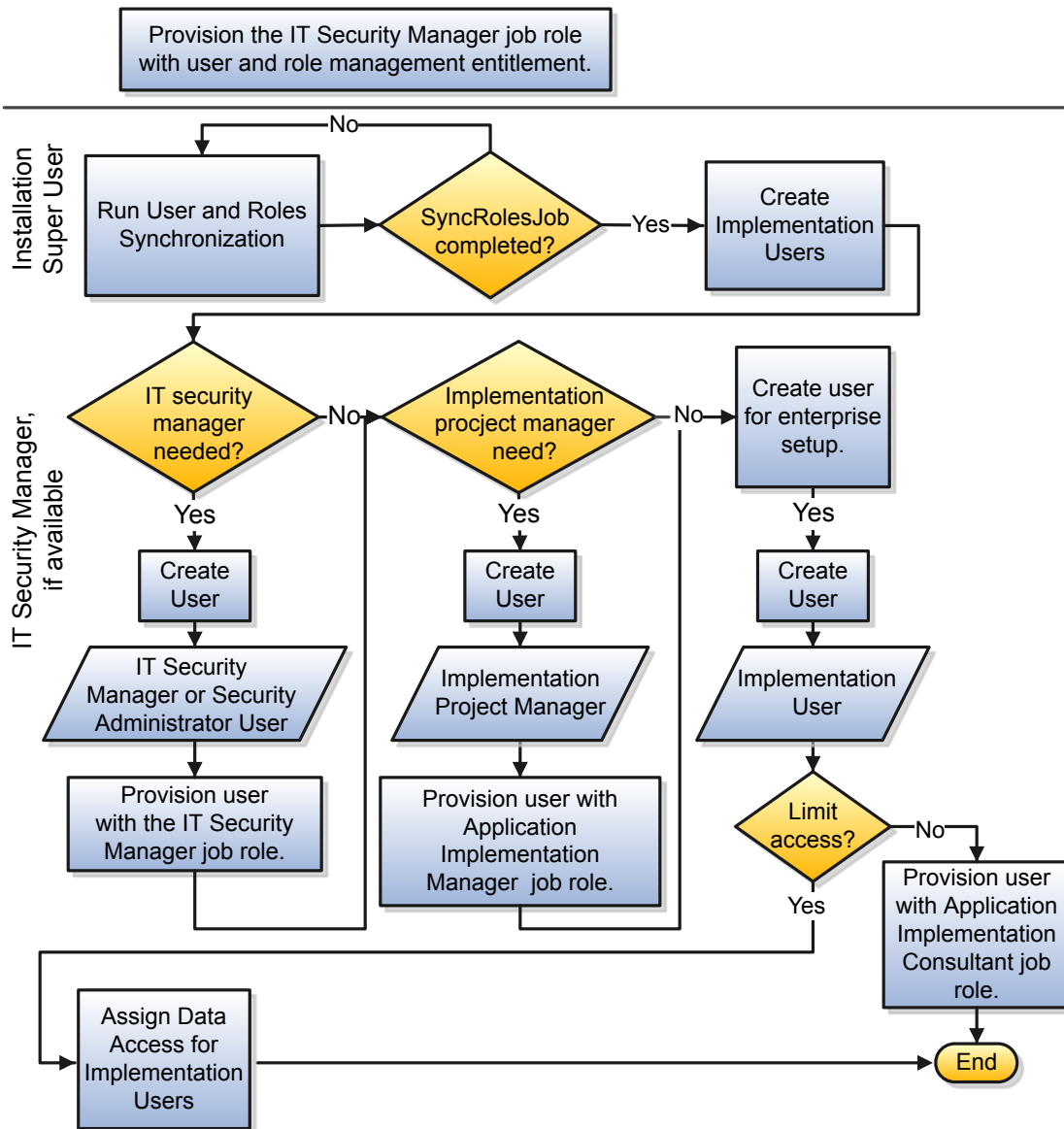
Task	Condition	Purpose	Performed In
Manage Supplier User Role Usages	Supplier Portal in Procurement is provisioned and requires trading partner security.	Manage the supplier roles that can be provisioned by supplier users, and set default roles for Supplier Portal or Sourcing, based on the set of supplier roles that are defined by performing the Manage Supplier User Roles task.	Supplier Portal or Sourcing

Getting Started with Security Implementation in Oracle SCM Cloud: Procedure

To start an Oracle SCM Cloud implementation, you must set up one or more initial users using the super user that was created during installation and provisioning of the Oracle Applications Cloud environment, or using the initial administrator user provided by Oracle for Oracle Cloud implementations. Because Oracle SCM Cloud is secure as delivered, the process of enabling the necessary setup access for initial users requires the following steps when getting started with an implementation.

1. If you are not starting an Oracle Cloud implementation, sign in as the super user of the security console and provision the IT Security Manager job role with roles for user and role management. This enables the super user account, which is provisioned with the IT Security Manager job role, to create implementation users.
2. For starting all implementations, sign in as the user with initial access: either the Oracle SCM Cloud installation super user or the initial Oracle Cloud administrator user.
3. Select an offering to implement, and generate the setup tasks needed to implement the offering.
4. Perform the following security tasks:
 - a. Synchronize users and roles in the Lightweight Directory Access Protocol (LDAP) store with HCM user management by using the Run User and Roles Synchronization Process task.
 - b. Create an IT security manager user by using the Create Implementation Users task.
 - c. Provision the IT security manager with the IT Security Manager role by using the Provision Roles to Implementation Users task.
5. As the newly created IT security manager user, sign in to Oracle SCM Cloud and set up at least one implementation user for setting up enterprise structures.
 - a. Create an implementation user by using the Create Implementation Users task.
 - b. Provision the implementation user with the Application Implementation Manager job role or the Application Implementation Consultant job role. The Application Implementation Consultant job role inherits from all product-specific application administrators and entitles the necessary View All access to all secured objects.
 - c. Optionally, create a custom role for an implementation user who needs only the limited access of a product-specific Application Administrator by using the Supply Chain Application Administrator role. Then assign the resulting custom role to the implementation user by using the Provision Roles to Implementation Users task.

The following figure shows the task flow from provisioning the IT Security Manager job role with the user and role management entitlement to creating and provisioning implementation users for enterprise setup.



2 Using the Security Console

Security Console: Overview

Use the Security Console to manage application security in your Oracle Applications Cloud service. Use the IT Security Manager role to perform security-related tasks pertinent to role management, role analysis, user-account management, and certificate management.

Security Console Tasks

You can perform these tasks in the Security Console:

- Roles
 - Create custom job, abstract, and duty roles.
 - Edit custom roles.
 - Copy roles.
 - Compare roles.
 - Visualize role hierarchies and assignments to users.
 - Review Navigator menus available to roles or users, identifying roles that grant access to Navigator 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 concerning role categories, the roles belonging to each category, and the components of each role.
- 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.

Security Console Access

You must have the IT Security Manager role to use the Security Console. This role inherits the following duty roles:

- Role Management Duty
- Certificate Management Duty
- Security Reporting duty

Administering the Security Console: Explained

To prepare the Security Console for use, arrange to run background processes that replenish security data. Also use Security Console Administration pages to select general and role-oriented options, track the status of role-copy jobs, and select, edit, or add notification templates. These generate messages to notify users of events that concern them, such as password-expiration warnings.

Background Processes

Run two background processes:

- The Retrieve Latest LDAP Changes process copies data from the LDAP directory to Oracle Cloud Applications Security tables. Run it once, during implementation. Select Setup and Maintenance from the Navigator. In the Setup and Maintenance work area, search for and select the Run User and Roles Synchronization Process task.
- The Import User and Role Application Security Data process copies users, roles, privileges, and data security policies from the identity store, policy store, and ApplCore grants schema to Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables: Select Scheduled Processes in the Tools work area, and then select the process from the Schedule New Process option.

General Administration Options

Select the Security Console Administration tab, and then the General tab on the Administration page, to set these options:

- User Preferences
 - Select the format of the User Name, the value that identifies a user as he signs in. It is generated automatically in the format you select. Options include first and last name delimited by a period, e-mail address, first-name initial and full last name, and person or party number.
 - Select the check box labeled "Generate system user name when generation rule fails" to enable the automatic generation of User Name values if the selected generation rule cannot be implemented.
- Password Policy
 - Establish the number of days a password remains valid. Set the number of days before expiration that a user receives a warning to reset the password. And define the period in which a user must respond to a notification to reset his password ("Hours Before Password Reset Token Expiration").
 - Select a password format.

- Determine whether a previous password may be reused.
- Determine whether an administrator can manually modify passwords in the Reset Password dialog, available from a given user's record in the Users tab. This option applies only to the manual-reset capability. An administrator can always use the Reset Password dialog to initiate the automatic reset of a user's password.
- Certificate Preferences: 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.)
- Synchronization Process Preferences: Specify a number of hours since the last run of the Import User and Role Application Security Data process. When a user selects the Security Console Roles tab, a warning message appears if the process has not been run in this period.

Role Administration Options

Select the Security Console Administration tab, and then the Roles tab on the Administration page, to set these options:

- Role prefixes and suffixes: Create the prefix and suffix added 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 adopts 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."
- Graph node limit: Set the maximum number of nodes a visualization graph can display. When a visualization graph would contain a greater number of nodes, the visualizer displays a message advising the user to select the table view.
- Enable edit of data security policies: Determine whether users can enter data in the Data Security Policies page of the role-creation and role-edit trains available from the Roles tab.
- Enable edit of user role membership: Determine whether users can enter data in the Users page of the role-creation and role-edit trains available from the Roles tab.
- Enable default table view: Determine whether visualizations generated from the Roles tab default to the table view or, if this option is cleared, the radial graph view.

Role Copy Status

Select the Security Console Administration tab, and then the Role Copy Status tab on the Administration page, to view records of jobs to copy roles. These jobs are initiated in the Roles page. Job status is updated automatically until a final status, typically Completed, is reached. You can delete the row representing a copy job; click its x icon.

Running Retrieve Latest LDAP Changes: Procedure

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. On-premises customers should also run this process after applying monthly updates.

Running Retrieve Latest LDAP Changes

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

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
The **Schedule New Process** dialog box opens.
3. In the **Name** field, search for and select the Retrieve Latest LDAP Changes process.
4. Click **OK** to close the **Schedule New Process** dialog box.
5. In the **Process Details** dialog box, click **Submit**.
6. Click **OK**, then **Close**.
7. On the Scheduled Processes page, click the **Refresh** icon.

Repeat this step periodically until the process completes.

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

Security Visualizations: Explained

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 either of two views:

- **Radial:** Nodes form circular (or arc) patterns. The nodes in each circle relate directly to a node at the center of the circle. 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 line above. This is the item you select to generate a visualization, or 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 would initially show nodes representing the duty roles encircling a node representing the job role.
- The Layers view would initially show the duty-role nodes in a line beneath the job-role node.

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

As an alternative, 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.

Working with a Visualization Graph: Explained

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.

To select one of the views, click Switch Layout in the Control Panel, which is a set of buttons at the upper left of the visualization. Then 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 enough, each node displays the name of the item it represents.
- If the image is smaller, 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 still, 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 depicted in a distinct color, so that item types are easily distinguished. For example nodes representing predefined roles are coral, while nodes representing custom roles are light green.

Expanding or Collapsing 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 perform these actions:

1. Select a node and right-click.
2. Select one of these options:
 - Expand reveals nodes to which the selected node connects directly, and Collapse hides those nodes.
 - Expand All reveals all generations of connecting nodes, and Collapse All hides those nodes.

Alternatively, double-click a collapsed node to expand it, or an expanded node to collapse it.

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 is 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 beneath 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

At the upper right of the image, a Legend lists the types of items currently on display. You can:

- 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 is 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

At the lower right of the image, click a plus sign to open the Overview, a thumbnail sketch of the visualization. In it, click any area of the thumbnail to focus the actual visualization on that area.

As an alternative, click the background of the visualization, then drag 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.

Working with a Visualization Table: Explained

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 beneath, or privileges related to, your focus role.
 - If you expand toward users, use the Show option to list records of either roles above, or users related to, your focus role.

Tables are all-inclusive:

- A Roles table displays 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.

- A Privileges table displays 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.
- A Users table displays records for all users 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.


Use a field above any column to enter search text, then press Enter. The table displays records whose column values contain text matching your search text.

You can export a table to Excel. Click the Export to Excel button. You may either open the Excel file directly or save it. If you opt to save the file, you're prompted to define a path.

Generating a Visualization: Procedure

To generate a visualization:

1. Select the Roles tab in the Security Console.
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 a field immediately to the right, enter at least three characters. The search returns items of the types you selected, whose names contain the characters you entered.
 - Select one of those items. Or, click the Search button to load all the items in a Search Results column, and select an item there.
3. Select either a Show Graph button or a View as Table button.

 **Note:** In a page for role administration, you can determine which of these is the default view.

4. In the Expand Toward list box, 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 box: 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.

Simulating Navigator Menus in the Security Console: Procedure

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 is not 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 blue menu entry.
2. 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.

Security Console Analytics: Explained

Use the Analytics page in the Security Console functional area to review statistics about:

- 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 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.

Bridge for Active Directory: Explained

The bridge for Microsoft Active Directory synchronizes user account information between Oracle Applications Cloud and Microsoft Active Directory.

Using the Bridge for Microsoft Active Directory

To use the bridge for Active Directory and synchronize information between Oracle Applications Cloud and Active Directory, perform the following steps:

1. Configure the bridge for Active Directory. Set the configuration options on the Administration tab in the Security Console.
2. Map attributes between source and target applications for synchronization.
3. Download and install the bridge for Active Directory.
4. Perform initial synchronization of users.
5. Perform manual or automatic synchronization regularly to maintain consistency of data on the source and target applications.

Prerequisites

Before setting up the bridge between Active Directory and Oracle Applications Cloud, you must:

- Install Java Runtime environment (JRE). The bridge is compatible with JRE versions 6, 7, and 8.
- Install the bridge on a computer that can connect to your Active Directory server.
- Enable Single Sign-On (SSO) between Oracle Applications Cloud and your Active Directory instance.

Source and Target

The bridge synchronizes information between the source and target:

- Source: Is the application that contains the user and role information that is copied to the target.
- Target: Is the application that is updated to contain the same user and role information as the source.

You can select either Oracle Applications Cloud or Active Directory as the source.

Related Topics

- [Getting Started with Oracle Applications Cloud Bridge for Active Directory](#)

FAQs for Using the Security Console

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

Private information is confidential in some contexts.

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

Some PII information is sensitive.

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

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

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

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

3 Managing Implementation Users

Creating Implementation Users

Implementation Users: Explained

The initial user can perform all the necessary setup tasks. She can also perform security tasks, including resetting passwords and the granting of additional privileges to herself and to others. After you sign in the first time, you can create additional implementation users with the same broad setup privileges that Oracle provides to the initial user. If you prefer, you can restrict the privileges of these implementation users based on your own setup needs.


The setup or implementation users are typically different from the Oracle Applications Cloud application users. For example:

- Setup users are usually not part of your Oracle Applications Cloud organization.
- You don't assign them product-specific work or make it possible for them to view product-specific data.

You do, however, have to give them the necessary privileges they require to complete application setup. You provide these privileges through role assignment.

Your application includes several types of roles. A job role, such as the IT Security Manager role, corresponds to a specific job that a person does in the organization. An abstract role, such as the Employee role, corresponds to general categories of people in an organization. You assign both types of roles to users in the security console. For the setup users, these roles are:

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

 **Note:** The Application Implementation Consultant role has unrestricted access to large amounts of data. Limit assignment of the Application Implementation Consultant abstract role to implementation users who perform a wide range of implementation tasks and move the setup data across environments. Use other administrator roles such as the Financials Applications Administrator for users required to perform specific implementation tasks.

There is nothing to stop you from providing the same setup permissions to users that are part of the organization, if you need to. Highly privileged implementation users are not the only users who can do setup. You can create administrative users who don't have such broad permissions, yet can configure product-specific structures and perform other related setup tasks.

Define Implementation Users: Overview

Implementation users perform the setup tasks in Oracle Enterprise Resource Planning (ERP) Cloud and Oracle Supply Chain Management (SCM) Cloud implementation projects. This topic introduces the tasks in the Define Implementation Users task list. You can find more information about implementation users and tasks they perform in the product specific implementation and security guides for your offering.


Create Implementation Users

You must have at least one implementation user. To ensure segregation of critical duties, multiple implementation users are recommended. For example, one implementation user typically performs functional setup tasks and another performs security setup tasks. When you create implementation users, you also assign predefined job roles to them directly. The job roles vary with the tasks that the implementation users perform.

The cloud service administrator creates implementation users.

Creating SCM Implementation Users: Overview

As the service administrator for the Oracle SCM 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 steps before you release the environment to your implementation team.

 **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.

Signing In to the Oracle SCM 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, SCMA could be the production environment and SCMA-TEST could be the test environment.

Sign in to the test or production Oracle SCM 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	<p>The Application Implementation Consultant user may be your only implementation user. However, you can create the implementation users TechAdmin and SCMUser and assign the required job roles to them if you need these implementation users and they don't already exist in your environment.</p> <p>You don't associate named workers with these users at this time because your service isn't yet configured to onboard users in the integrated HCM core. As your implementation progresses, you may decide</p>

Step	Task or Activity	Description
		to replace these users or change their definitions.
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 Fusion Human Capital Management (Oracle Fusion HCM).
3	Assign Security Profiles to Abstract Roles	Enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles.
4	Create a Generic Role Mapping for the Roles	Enable the roles created in step 3 to be provisioned to implementation users.
5	Assign Abstract 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.

Related Topics

- [Creating the TechAdmin Implementation User: Procedure](#)

Managing User Accounts: Explained

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, whether it is locked, and the user's password-expiration date, 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. Select the Users tab in the Security Console.
2. In a Search field, select any combination of user states, which may include active, inactive, locked, or unlocked.
3. In a field immediately to the right, enter at least three characters. The search returns user accounts at the states you selected, whose login, first name, or last name begins with the characters you entered.

Reviewing and Editing User Accounts: Explained

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, first, and last name values, and an e-mail address. It also includes an external identifier if one has been created. This is an external-system identifier, such as a single sign-on account ID if single sign-on is enabled.
- Account information, which comprises the user's password-expiration date, whether the account is active, and whether it is locked.
- A table listing the roles assigned to the user, including whether they are 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 is not 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 cannot 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.

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

Adding User Accounts: Procedure

The ability to add user accounts in the Security Console is intended for the creation of implementation users. The expectation is that an implementation user would set up Oracle Human Capital Management (HCM). You would then use HCM to create accounts for application users.

To add a user account in the Security Console:

1. Select the Users tab in the Security Console to open the User Accounts page.
2. Click the Add User Account button.

3. Select a value for Associated Person Type: Worker if this account is to be linked to a worker record in HCM, or None if not.
4. By default, the account is set to be active and unlocked in the Account Information area. Typically these values are appropriate, but you may modify them.
5. Enter name, e-mail, and password values in the User Information region.
 - You need not enter a User Name value. It is generated automatically according to the user-name-generation rule selected in the General Administration page.
 - The First Name value is not required. However, you are expected to enter one if the selected user-name-generation rule makes use of the first name or the first-name initial.
 - The Password value must conform to the password policy established in the General Administration page. The Confirm Password value must match the Password value.
 - An external identifier is the user's ID in another system, such as a single sign-on account ID if single sign-on is enabled.
6. Click Add Autoprovisioned Roles, to assign roles for which role-provisioning rules make the user eligible.
7. Click Add Roles to assign other roles. Search for roles you want to assign, select them, then click Add Role Membership. Select Done when you are finished.
8. In the Roles table, select Assignable for any role that can be delegated to another user.
9. Click Save and Close.

Resetting Passwords: Procedure

An administrator may use the Security Console to reset other users' passwords. That action triggers an e-mail notification to each user, informing him or her of the new password.


A new password must conform to your password policy. You establish this policy in the General Administration page. The page in which you reset the password displays the policy.

To reset a password:

1. In the User Accounts page, search for the user whose password you want to change.
2. In that user's row, click the Action icon, then Reset Password.

As an alternative, open the user's account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page. In that page, select Reset Password.

3. In a Reset Password dialog, select whether to generate the password automatically or change it manually. For a manual change, also enter a new password value and a confirmation value, which must match the new value.

 **Note:** The option to reset a password to an automatically generated value is always available. For the manual-reset option to be available, an "Administrator can manually reset password" option must be selected on the General Administration page.

4. Click the Reset Password button.

Related Topics

- [Administering the Security Console: Explained](#)

Locking and Unlocking User Accounts: Procedure

An administrator may use the Security Console to lock users' accounts. When an account is locked, its user cannot sign in. He or she must either use the "forgot password" flow to reset the password or contact the help desk to have the account unlocked.

You can lock a user account in either of two ways. In either case, open the User Accounts page and search for the user whose account you want to lock.

To complete the first procedure:

1. In the user's row, click the Action icon, then Lock Account.
2. Respond Yes to a confirmation message.

To complete the second procedure:

1. Open the user's account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page.
2. In the Edit User Account page, select the Locked check box in the Account Information region.
3. Select Save and Close.

You can unlock the account only from the Edit User Account page, by clearing the Locked check box.

Deleting User Accounts: Procedure

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.

Defining Notification Templates: Explained

Users may receive e-mail 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.

To work with templates, select the Administration tab in the Security Console, and then the Notifications tab in the Administration page.

There are eight events, and a predefined template exists for each event. Only one template linked to a given event can be enabled at a time. So to use notification templates, you need do nothing more than ensure that notifications are enabled. To do that, see that the Enable Notifications check box is selected in the Notification Preferences region of the Notifications Administration page.

Even so, you can enable or disable templates, edit them, or create templates to replace existing ones. To create a template:

1. Click the Add Template button in the Notifications Administration page.
2. Enter a name for the template and, optionally, a description.
3. Select an event. When you do, values for Message Subject and Message are copied from an already-configured template for which the same event is selected.

4. Edit the message subject, message text, or both. Note that message text may include tokens, which are replaced in run time by literal values appropriate for a given user or account.
5. Select the Enabled check box if you want to use the template immediately. If you do, the application automatically disables the template that had been enabled for that event. Or, leave the check box cleared to hold the template in reserve.
6. Click Save and Close.

To edit a template, click its name in the Notifications Administration page. Then follow essentially the same process as you would to create a template. Note, however, that you cannot modify the event selected for a template that has been saved. You may enable or disable an individual template by selecting or clearing its Enabled check box as you edit it.

You can disable, but cannot delete, predefined templates. You can delete custom templates. To do so, click the x icon in the row for a template in the Notifications Administration page. Then respond to a confirmation message. If you delete a template that had been enabled, no other template is enabled automatically.

You can use the following tokens in the message text for a template:

Token	Meaning
\${userId}	The user name of the person whose account is being created or modified.
\${firstName}	The given name of the person whose account is being created or modified.
\${lastName}	The surname of the person whose account is being created or modified.
\${managerFirstName}	The given name of the person who manages the person whose account is being created or modified.
\${managerLastName}	The surname of the person who manages the person whose account is being created or modified.
\${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 is about to expire. Or, without signing in, the user can engage a forgot-password procedure to change a password that has already expired.
\${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.
\${CRLF}	Insert line break.
\${SP4}	Insert four spaces.

Synchronizing User and Role Information: Procedure

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.

Running the Retrieve Latest LDAP Changes Process

Follow these steps:

1. Sign in to your Oracle Applications Cloud service environment as the service administrator.
2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
3. Search for and select the Run User and Roles Synchronization Process task.

The process submission page for the Retrieve Latest LDAP Changes process opens.

4. Click **Submit**.
5. Click **OK** to close the confirmation message.

Assigning Roles to Implementation Users

Creating a Role Mapping: Procedure

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. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules task.

The Manage Role Mappings page opens.

3. In the Search Results section of the 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, these values limit the role mapping to current employees of the Procurement Department in Denver whose job is Chief Buyer.

Field	Value
Department	Procurement Department
Job	Chief Buyer
Location	Denver
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. For example, search for the HCM data role **Procurement Analyst Denver**.
3. Select one or more of the role-provisioning options:

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 autoprovioning requests.

Related Topics

- [Autoprovisioning: Explained](#)

Resetting the Cloud Service Administrator Sign-In Details: Procedure

Once you have set up your implementation users, you can reset the service administrator sign-in details for your Oracle Applications Cloud service. You reset these details to avoid problems later when you're loaded to the service as an employee. This topic describes how to reset the service administrator sign-in details.

Resetting the Service Administrator Sign-In Details

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

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Create Implementation Users task.
The User Accounts page of the Security Console opens.
3. Search for your service administrator user name, which is typically your e-mail. Your service activation mail contains this value.

4. In the search results, click your service administrator user name to open the User Account Details page.
5. Click **Edit**.
6. Change the **User Name** value to **ServiceAdmin**.
7. Delete any value in the **First Name** field.
8. Change the value in the **Last Name** field to **ServiceAdmin**.
9. Delete the value in the **E-Mail** field.
10. Click **Save and Close**.
11. Sign out of your Oracle Applications Cloud service.

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

4 Preparing for Application Users

Preparing Oracle Applications Cloud for Application Users: Overview

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.

Some key decisions and tasks are explained in this chapter. They include:

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: Critical Choices

This topic introduces the user and role-provisioning options, which control the default management of some user-account features. To set these options, perform the Manage Enterprise HCM Information task in the Setup and Maintenance work area. You can edit these values as necessary and specify an effective start date for changed values.

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

This 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

Once 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 for Terminated Workers Option: Explained](#)

User Account Creation Option: Explained

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

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

Value	Description
Both person and party users	User accounts are created automatically for both person and party users. This value is the default value.

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

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

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

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

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

User Account Role Provisioning Option: Explained

Existing users both acquire and lose roles as specified by current role-provisioning rules. For example, users may request some roles for themselves and acquire others automatically. All provisioning changes are role requests that are processed by default. You can control what happens to role requests by setting the **User Account Role Provisioning** option. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **User Account Role Provisioning** option values.

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

User Account Maintenance Option: Explained

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

Setting the User and Role Provisioning Options: Procedure

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.

Setting the User and Role Provisioning Options

Follow these steps:

1. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Manage Enterprise HCM Information task.
3. On the Enterprise page, select **Edit - Update**.
4. In the **Update Enterprise** dialog box, enter the effective date of any changes and click **OK**. The Edit Enterprise page opens.
5. Scroll down to the User and Role Provisioning Information section.
6. 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**.

7. Click **Submit** to save your changes.
8. Click **OK** to close the **Confirmation** dialog box.

Provisioning Abstract Roles to Users Automatically: Procedure

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. This topic explains how to set up automatic role provisioning during implementation using the Manage Role Provisioning Rules task.

Provisioning the Employee Role Automatically to Employees

Follow these steps:

1. Sign in as IT Security Manager or as the TechAdmin user.
2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
3. Search for and select the Manage Role Provisioning Rules task. The Manage Role Mappings page opens.
4. In the Search Results section of the Manage Role Mappings page, click the **Create** icon. The Create Role Mapping page opens.
5. In the **Mapping Name** field enter Employee.
6. 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

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

Provisioning 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 5, enter Contingent Worker as the mapping name.


- In step 6, set **System Person Type** to Contingent Worker.
- In steps 9 and 10, search for and select the Contingent Worker role.

Provisioning the Line Manager Role Automatically to Line Managers

Follow these steps:

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.

FAQs for Preparing for Application Users

Can I implement single sign-on in the cloud?

Yes. Single sign-on enables users to sign in once but access multiple applications, including Oracle Human Capital Management Cloud.

Submit a service request for implementation of single sign-on. For more information, see Oracle Applications Cloud Service Entitlements (2004494.1) on My Oracle Support at <https://support.oracle.com>.

Related Topics

- [Oracle Applications Cloud Service Entitlements \(2004494.1\)](#)

5 Creating and Managing Application Users

Creating Users

Creating Users: Procedure

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 - - Manage Users** to open the Manage Users page.
2. In the Search Results section, click **Create**.

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**.

The role appears in the Role Requests region with the status **Add requested**.

Repeat steps 2 and 3 for additional roles.


4. Click **Save and Close**.
5. Click **Done**.

Inactive Users Report

Run the Inactive Users Report to identify users who haven't signed in for a specified period.

To run the report:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the Import User Login History process.

 **Note:** Whenever you run the Inactive Users Report process, you must first run the Import User Login History process. This process imports information that the Inactive Users Report process uses to identify inactive users. You're recommended to schedule Import User Login History to run daily.

4. When the Import User Login History process completes, search for and select the Inactive Users Report process.
5. In the **Process Details** dialog box, set parameters to identify one or more users.
6. 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

Related Topics

- [Importing User Login History: Explained](#)

Managing Users

Managing User Accounts: Procedure

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

To access the user account page for a person:

1. On the home page, select **My Workforce - Person Management** to open the Search Person page.
2. Search for the person whose account you're updating.
3. In the search results, select the person and select **Actions - Personal and Employment - Manage User Account**. The Manage User Account page opens.

Managing User Roles

To add a role:

1. Click **Add Role**.

The **Add Role** dialog box opens.

2. In the **Role Name** field, search for the role that you want to add.
3. In the search results, select the role and click **OK**.

The role appears in the Role Requests region with the status **Add Requested**.

4. Click **Save**.

To remove a role from any section of this page:

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

Clicking **Save** sends requests to add or remove roles to your LDAP directory server. Requests appear in the Role Requests in the Last 30 Days section. Once provisioned, roles appear in the Current Roles section.

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

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

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

Copying Personal Data to LDAP

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


1. Select **Actions - Copy Personal Data to LDAP**.
2. In the **Copy Personal Data to LDAP** dialog box, click **Overwrite LDAP**.

Resetting Passwords

To reset a user's password:

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

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

 **Note:** A notification template for the password reset event must exist and be enabled. Otherwise, no notification is sent.


Editing User Names

To edit a user name:

1. Select **Actions - Edit User Name**.

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

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

 **Tip:** Users can add roles, autoprovision roles, and copy their personal data to LDAP by selecting **About Me - My Account** from the home page. Line managers can add, remove, and autoprovision roles and copy personal data to LDAP for their reports from the Directory or by selecting **My Team** in the Navigator.


Changing User Names: Explained

By default, user names are generated automatically in the enterprise default format when you create a person record. Users who have the human resource specialist (HR specialist) role can change user names for existing HCM users whose records they can access. 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 enterprise default format. This table summarizes the effects of the available formats for Oracle HCM Cloud users.

User-Name Format	Description
E-Mail	The worker's work e-mail is the user name. If you don't enter the work e-mail 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 Administration tab of 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 can be disabled 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. Search for and select the worker in the Person Management work area.
2. For the selected worker, select **Actions - Personal and Employment - Manage User Account**.

3. On the Manage User Account page, select **Actions - Edit User Name**.

The updated name, which can be in any format, is sent automatically to your LDAP directory server. 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.

Sending Personal Data to LDAP: Explained

User accounts for users of Oracle Fusion Applications are maintained on your LDAP directory server. By default, Oracle HCM Cloud sends some personal information about users to the LDAP directory. This information includes the person number, person name, phone, and manager of the person's primary assignment. HCM Cloud shares these details to ensure that user-account information matches the information about users in HCM Cloud.

This topic describes how and when you can send personal information explicitly to your LDAP directory.

Bulk Creation of Users

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

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

The Send Personal Data for Multiple Users to LDAP Process

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

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

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

The process doesn't apply to party users.

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

The Copy Personal Data to LDAP Action

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

Related Topics

- [User and Role-Provisioning Setup: Critical Choices](#)

Processing a User Account Request: Explained

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

The Process User Account Request Action

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

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

Role Provisioning

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

The Send Pending LDAP Requests Process

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

Suspending User Accounts: Explained

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

Automatic Suspension of User Accounts

When you terminate a work relationship:

- The user loses any automatically provisioned roles for which he or she no longer qualifies. This deprovisioning is automatic.
- If the user has no other active work relationships, then the user also loses manually provisioned roles. These are:
 - Roles that he or she requested

- Roles that another user, such as a line manager, provisioned to the user

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


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

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

Automatic Reactivation of User Accounts

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

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

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

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

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


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

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

Manual Suspension of User Accounts

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

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

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

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

Related Topics

- [User Account Maintenance Option: Explained](#)

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. Select **Tools - Reports and Analytics** on the home page.

Parameters

User Population

Enter one of these values 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 these values to identify the user-account status.

Value	Description
A	Include active accounts, which belong to users with current roles.
I	Include inactive accounts, which belong to users with no current roles.

Value	Description
All	Include both active and inactive user accounts.

Related Topics

- [Running the User Details System Extract Report: Procedure](#)

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. Select **Tools - Reports and Analytics** on the home page.

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.

HCM User Accounts

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.

TCA User Accounts

Organizations

A resource group.

Roles

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

Managers

The manager of a resource group.

LDAP User Accounts

Start Date

The account's start date.

Created By

The user name of the user who created the account.

Related Topics

- [Running the User Details System Extract Report: Procedure](#)

FAQs for Creating and Managing Application Users

Where do default user names come from?

User names are generated automatically in the format specified on the Security Console. The default format is the worker's primary work e-mail, but this value can be overridden for the enterprise. For example, your enterprise may use person number as the default user name.

Why did some roles appear automatically?

In a role mapping:

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

How can I create a user?

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

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

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

Related Topics

- [Creating Partner User Accounts: Explained](#)

What happens when I autoprovision roles for a user?

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

The user immediately:

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

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

Why is the user losing roles automatically?

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

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

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

You can provision a role if a role mapping exists for the role, the **Requestable** option is selected for the role in the role mapping, and at least one of your assignments satisfies the role-mapping conditions. Otherwise, you can't provision the role to other users.

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 e-mail 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 process Send User Name and Password E-Mail Notifications.

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

You can run the process Send User Name and Password E-Mail Notifications in the Scheduled Processes work area. For users for whom you haven't so far requested an e-mail, this process sends out user names and reset-password links. The e-mail goes to the work e-mail 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 Provisioning Roles to Application Users

Role Mappings: Explained

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 or Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area.

Automatic Provisioning of Roles to Users for SCM

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 job role Cost Accountant Finance Department, you could select the **Autoprovision** option and specify the following conditions.

Attribute	Value
Department	Finance Department
Job	Cost Accountant
HR Assignment Status	Active

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

 **Note:** The examples in the following sections pertain to HCM roles.

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 following conditions.

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 following conditions.

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.

Creating a Role Mapping: Procedure

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. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and select the Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules task.
The Manage Role Mappings page opens.
3. In the Search Results section of the page, click **Create**.
The Create Role Mapping page opens.

Defining the Role-Mapping Conditions for SCM

Values in the Conditions section determine when the role mapping applies. For example, these values limit the role mapping to current employees of the Materials Management Department at the Seattle Distribution Center whose Job is Warehouse Manager.

Field	Value
Department	Materials Management Department
Job	Warehouse Manager
Location	Seattle Distribution Center
System Person Type	Employee
HR Assignment Status	Active

Users must have at least one assignment that meets all of 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. For example, search for the HCM data role **Procurement Analyst Denver**.
3. Select one or more of the role-provisioning options:

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

Role-Provisioning Option	Description
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: Explained

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 HCM Cloud 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: Explained

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. This topic explains the effects of applying autoprovisioning for the enterprise.

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. When running the process, 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 Autoprovision Roles for All Users can run at a time.

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?](#)

- [Scheduling the Send Pending LDAP Requests Process: Procedure](#)

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.
3. In the **Process Details** dialog box, set parameters and click **Submit**.
4. Click **OK** to close the confirmation message.

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 multiple 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 multiple 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 the **Data Security Policies** check box, when you want to view the data security report for any population. When you leave the option unchecked, only the function report is generated.

 **Note:** If you don't need the data security policy document, leave the option unchecked. This reduces the processing time to run the report.

Debug

Select the **Debug** check box to include role GUID in the report. The role GUID is used to troubleshoot. Use this option only when requested by the Oracle Support team.

Viewing the Report Results

The report produces one or two **.zip** files depending on the parameters you select. When you select the Data Security Policies check box, two **.zip** files are generated: one with information on the data security policies and the other on 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, as shown in this table.

Population 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 population type.

Population Type	File Suffix	File Format	File Contents
Any	DataSec	CVS	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when the Data Security Policies check box is selected.

Population Type	File Suffix	File Format	File Contents
Any	Hierarchical	CVS	Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.
Multiple users	CSV	CSV	Functional security policies in a comma-separated, tabular format.
All roles			

 **Note:** Extract the data security policies only when needed as it takes a long time to generate the file.

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

Managing Data Access for Users: Explained

You can assign users access to appropriate data based on their job roles. The Oracle Fusion security model requires a three-way link between users, role, and data. It is summarized as: who can do what on which data. Who refers to the users, what are the job roles the user is assigned, and which refers to the data that is specific to a particular security context, typically an element of the enterprise structure, such as a business unit, asset book, or ledger.

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

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

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

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

Assigning Data Access

Assigning data access to users is a three step process:

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

Specify user attributes such as user name, assigned business unit, legal employer, department, job, position, grade, and location.
 - o Security Console
2. Assign at least one job role to users. Use Oracle Fusion Human Capital Management or the Security Console to assign job roles.
3. Assign data access using the Manage Data Access for Users task in the Functional Setup Manager. For General Ledger users, you can also use the Manage Data Access Set Data Access for Users task to assign data access.

Assigning Data Access to Users: Worked Example

Use the Manage Data Access for Users page to assign data access to users based on their job roles. You can assign data access to:

- One user at a time
- Group of users with similar job roles

This example demonstrates how you can assign access to a business unit to a group of users with similar job roles. The following table summarizes the key decisions for this scenario:

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

Prerequisites

Before you can complete this task, you must:

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

Assigning Data Access to Users Using a Spreadsheet

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

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

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

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

FAQs for Provisioning Roles to 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 Human Capital Management (HCM) Cloud, Oracle Fusion Sales Cloud, Oracle Fusion ERP Cloud, and Oracle Fusion Suppliers.

Human Resources (HR) transaction flows such as Hire and Promote also provision roles.

How do I view the privileges or policies carried by a job role?

The most efficient way is to use the Security Console to search for and select the job role. When it appears in the visualizer, you can see all inherited roles, aggregate privileges, and privileges. If you edit the role from the visualizer, you can see the policies on the function policies and data policies pages.

How can I tell which roles are provisioned to a user?

Use the Security Console to search for the user. When you select the user, the user and any roles assigned to the user appear in the visualizer. Navigate the nodes to see the role hierarchies and privileges. You must be assigned the IT Security Manager role to access the Security Console.

Why can't a user access a task?

If a task doesn't appear in a user's task list, you may need to provision roles to the user.

A position or job and its included duties determine the tasks that users can perform. Provisioned roles provide access to tasks through the inherited duty roles.

The duty roles in a role hierarchy carry privileges to access functions and data. You don't assign duty roles directly to users. Instead, duty roles are assigned to job or abstract roles in a role hierarchy. If the duties assigned to a predefined job role don't match the corresponding job in your enterprise, you can create copies of job roles and add duties to or remove duties from the copy.

! Important: You cannot 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 and are displayed in red color in the role graph. 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 Customizing Security

Managing Data Security Policies

Data Security: Explained

By default, users are denied access to all data.
Data security makes data available to users by the following means.

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

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

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

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

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

Data is secured by the following means.

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

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

Data Security Policies

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


For example, warehouse managers can manage inventory transaction data for the inventory organizations in which they can operate.

Who	can do	what	on which set of data
warehouse managers	manage	inventory transactions	for the inventory organizations in which they can operate

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

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

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

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

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

HCM Security Profiles

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

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

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

Data Security Considerations for Oracle Fusion Product Hub

Some products within SCM support data security on a combination of dimensions. Oracle Fusion Product Hub enables customers to build flexible, scalable, security solutions for complex access control requirements for managing product information.

Product Hub Data Security is built on a combination of the criteria listed in the following table with examples of the values for those criteria.


Criteria	Example
who	user Eric Boyer

Criteria	Example
or which job role	or Product Data Steward
for which item organization	for Seattle branch
can perform what actions	is allowed to perform View Item Structure
on which set of Product Hub business objects	for Printer Item Class

Before creating or viewing items, you define data security for each item class and organization. Data security for an item is set up in the corresponding item class, for each person or group and for each inventory or item organization. All items that you create using an item class inherit the item data security that is defined for the item class. You can also define item-specific data security at the item level.

For each user or user group, you can grant view or maintain data level rights to user-defined attributes. To define data security for user-defined attribute groups, you use extensible attribute group security to secure the data of attribute groups by allowing only certain groups or users to have access. After creating data grants for users or roles, you assign the data grants to an attribute group, then assign data grants to specific groups or users.

You can also provide data security for product data uploaded through Oracle Fusion Product Hub Portal, by assigning appropriate item data privileges to supplier users for the specific item classes that the suppliers will upload product data for.

 **Note:** For more details about data security for Oracle Fusion Product Hub and Product Hub Portal, see the user assistance and implementation course for that product.

Data Security Considerations for Oracle Fusion Planning Central

Oracle Fusion Planning Central is another product within SCM that supports data security on a combination of dimensions. Planning Central has a flexible model of filters and rules for configuring data access for different users based on their role in the organization.

You enable data security for Planning Central when you administer planning security, as part of plan inputs. You can then select whether to allow full access, or no access, for any entity for which no data access condition is defined.


Users can be granted access based on one of the following:

- Organizational structure, such as organization or business unit
- Product structure, such as product line or category
- Access to specific trading partners, such as customers or suppliers

You can define data access sets, which define the visibility for any job role, using the one of the following criteria:

- Products
- Inventory organizations
- Customers
- Suppliers

In each of the criteria, you can set up filters at the lowest level (such as Item) or at a higher level (such as Category) by selecting the appropriate hierarchy. Data access sets are then assigned to different users to provide access.

 **Note:** For more details about data security for Oracle Fusion Planning Central, see the user assistance and implementation course for that product.

Advanced Data Security: Explained

Advanced Data Security offers two types of extended data protections. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest. Advanced Data Security is available for Oracle Applications Cloud by subscription to Break-Glass service.

Oracle Database Vault

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

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

Transparent Data Encryption

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

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

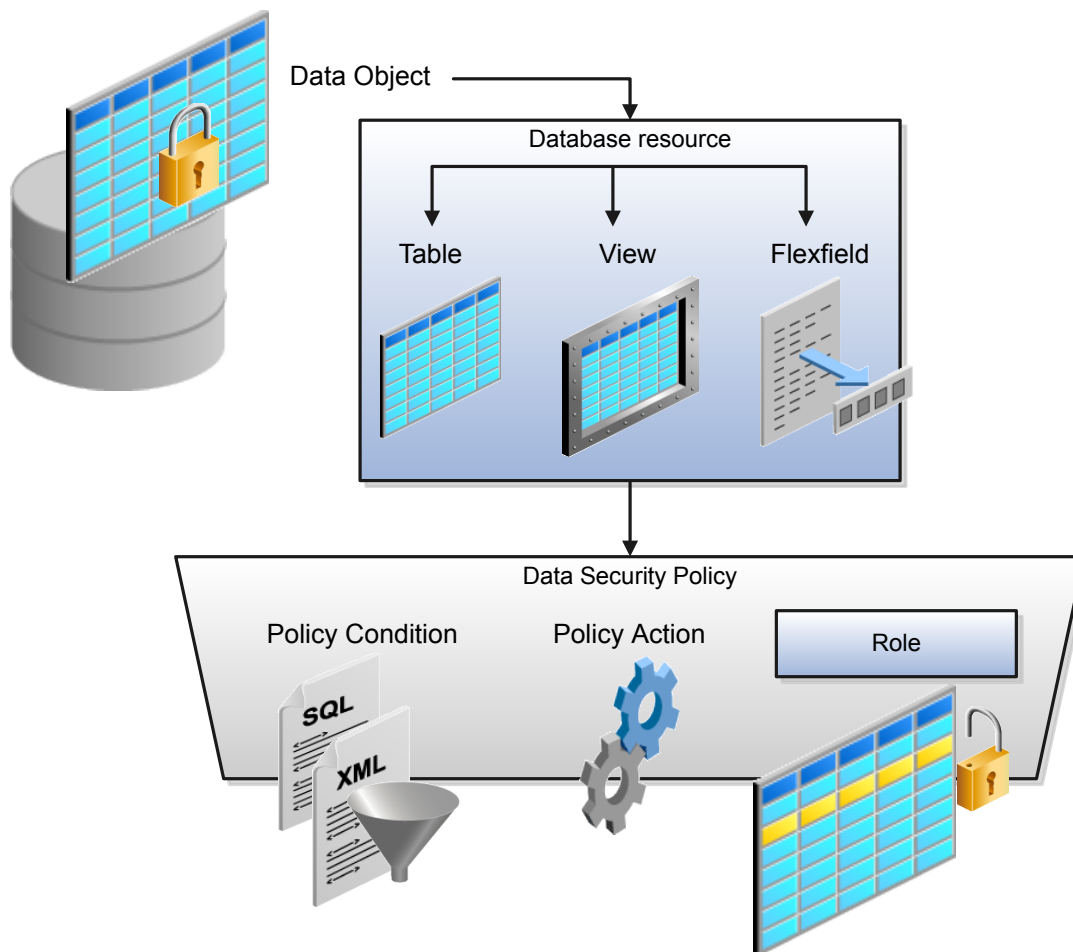
Encryption keys are stored in the Oracle Wallet. The Oracle Wallet is an encrypted container outside the database that stores authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by secure sockets layer (SSL).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

Database Resources and Data Security Policies: How They Work Together

A data security policy applies a condition and allowable actions to a database resource for a role. When that role is provisioned to a user, the user has access to data defined by the policy. In the case of the predefined security reference implementation, this role is always a duty role.

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

The following figure shows the database resource definition as the means by which a data security policy secures a data object. The database resource names the data object. The data security policy grants to a role access to that database resource based on the policy's action and condition.



Database Resources


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

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

Data Security Policies

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

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


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

Actions

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

Conditions

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

 **Tip:** An XML filter can be effective in downstream processes such as business intelligence metrics. A SQL predicate cannot be used in downstream metrics.

Related Topics

- [Securing Data Access: Points to Consider](#)

FAQs for Customizing Security

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

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

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

Function security controls access to user interfaces and actions needed to perform the tasks of a job. For example, a warehouse manager can manage inventory transactions. The Warehouse Manager role provisioned to the warehouse manager authorizes access to the functions required to manage inventory transactions.

Data security controls access to data. In this example, the warehouse manager for M1 Inventory Organization can manage inventory transactions in the M1 Inventory Organization. Objects are secured by the data security policies of the job role.

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

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. Either in the visualization or the Search Results column, right-click on a role or user. A menu appears; select Preview Navigator Simulation.

A simulated Navigator menu appears, listing menu and task entries. If the menu item appears without a lock to the right of it, the menu is not authorized for the role or user. If the menu item appears with a lock to the right of it, 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 can I have data masking applied to my non production environments in Oracle Applications Cloud services?

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


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

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 does not want users to perform in your application.

 **Warning:** 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 customize the copy.

How do I create a new job role?

Click the **Create Role** button in the Security Console to create job roles. Enter a job role category in the Create Roles page and then navigate to each subsequent page that you see in the page header. You can add functional and data security policies, roles, and privileges to create the job role.

8 Reviewing Roles and Role Assignments

Reviewing Role Assignments: Procedure

You can use the Security Console to:

- View the roles assigned to a user.
- Identify users who have a specific role.

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


Viewing the Roles Assigned to a User

Follow these steps:

1. Select **Navigator - Tools - Security Console**.
2. On the Security Console, 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:


1. Select the role and right-click.
2. 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 here.

Identifying Users Who Have a Specific Role

Follow these steps:

1. On 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, blue diamond shapes identify users. User names appear on hover. Users may inherit roles either directly or indirectly from other roles, which appear as green circles. 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.


Reviewing Role Hierarchies: Explained

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. Select **Navigator - Tools - Security Console**.
2. On the Security Console, ensure that **Expand Toward** is set to **Privileges**.
3. Search for and select the role. Depending on the enterprise setting, either a table or a graphical representation of the role appears.
4. 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 the field above a column 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.

Comparing Roles: Procedure

Compare any two roles to see the structural differences between them.

For example, assume you have copied a role and customized the copy. You then upgrade to a new release. You can compare your customized 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 custom role.

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.

4. Filter for any combination of these artifacts in the two roles:
 - Function security policies
 - Data security policies
 - Inherited roles
5. For the combination you select, choose whether to show:
 - All artifacts
 - Those that exist only in one role, or only in the other role
 - Those that exist only in both roles
6. Click the **Compare** button.

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

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.
3. In the **Process Details** dialog box, set parameters and click **Submit**.
4. Click **OK** to close the confirmation message.

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 multiple 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 multiple 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 the **Data Security Policies** check box, when you want to view the data security report for any population. When you leave the option unchecked, only the function report is generated.

 **Note:** If you don't need the data security policy document, leave the option unchecked. This reduces the processing time to run the report.

Debug

Select the **Debug** check box to include role GUID in the report. The role GUID is used to troubleshoot. Use this option only when requested by the Oracle Support team.

Viewing the Report Results


The report produces one or two **.zip** files depending on the parameters you select. When you select the Data Security Policies check box, two **.zip** files are generated: one with information on the data security policies and the other on 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, as shown in this table.

Population Type	File Prefix
User name	USER_NAME
Role name	ROLE_NAME
Multiple users	MULTIPLE_USERS

Population Type	File Prefix
All roles	ALL_ROLES

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

Population Type	File Suffix	File Format	File Contents
Any	DataSec	CVS	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when the Data Security Policies check box is selected.
 Note: Extract the data security policies only when needed as it takes a long time to generate the file.			
Any	Hierarchical	CVS	Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.
Multiple users	CSV	CSV	Functional security policies in a comma-separated, tabular format.
All roles			

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

9 Customizing Roles Using the Security Console

Creating Custom Roles

Creating Roles in the Security Console: Procedure

You can use the Security Console to create duty, job, or abstract roles.


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.

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 cannot 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 cannot assign the role you are 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 a Search field, select the value Privileges or types of role in any combination. In a field immediately to the right, 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.

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 is not used in predefined roles in Oracle ERP Cloud.
- 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 is not 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:

- Database Resource: A database table.
- Data Set: A definition that selects a subset of the data made available by the database 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 Policies page lists all policies defined for the role. You can edit or delete a policy: Click the button to the right of its row, and select the Edit or Remove option.

Configuring the Role Hierarchy

A Role Hierarchy page displays either a visualization graph, with the role you are 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 are creating to other roles from which it is to inherit function and data security privileges.

- If you are creating a duty role, you can add duty roles or aggregate privileges to it. In effect, you are creating an expanded set of duties for incorporation into a job or abstract role.
- If you are 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. In a field immediately to the right, 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 are creating. (You cannot 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 is not 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. In a field immediately to the right, 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 are 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 are satisfied with the role, select Save and Close.

Related Topics

- [Working with a Visualization Graph: Explained](#)

Copying or Editing Roles in the Security Console: Explained

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.

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 are 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 top 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 top 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 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 cannot:

- 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 are 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 cannot 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 top role you copied.

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

Related Topics

- [Generating a Visualization: Procedure](#)

Security Console Role-Copy Options: Explained

When you copy a role on the Security Console, you select one of the following options:

- Copy top role

- Copy top role and inherited roles

This topic explains the effect of each of these options on the copied role.

Copy Top Role

If you select the **Copy top role** option, then memberships are created for the copy in the roles of which the original is a member. Subsequent changes to those roles appear in your copy of the role. Therefore, you can


- Add roles directly to the copied role without affecting the source role.
- Remove any role that's inherited directly by the copied role without affecting the source role.

However, if you:

- Remove any role that's inherited indirectly by the copied role, then the removal affects any role that inherits the removed role's parent role, including the source role
- Edit any inherited role, then the changes affect any role that inherits the edited role

These types of changes aren't limited to the copied role. This option is referred to as a shallow copy.

To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. To copy the inherited roles, select the **Copy top role and inherited roles** option. Alternatively, copy individual inherited roles separately, edit the copies, and use them to replace the existing versions.

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

Copy Top Role and Inherited Roles

Selecting **Copy top role and inherited roles** is a request to copy the entire role hierarchy. If you're copying a job or abstract role, then:

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

When inherited duty roles are copied, you can edit them without affecting other roles. Equally, changes made subsequently to the source duty roles don't appear in the copied roles. This option is referred to as a deep copy.


Copying Job or Abstract Roles: Procedure

You can copy any job role or abstract role and use it as the basis for a custom role. Copying roles is more efficient than creating them from scratch, especially if your changes are minor. This topic explains how to copy a role to create a custom role. You must have the IT Security Manager job role to perform this task.


Copying a Role

Follow these steps:

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

 **Tip:** Click the **Show Graph** icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

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

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

Editing Custom Job or Abstract Roles: Procedure

You can create a custom role by copying a predefined job role or abstract role and editing the copy. This topic describes how to edit a custom role on the Security Console. You must have the IT Security Manager job role to perform this task.

Editing the Role

Follow these steps:


1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.

Managing Functional Security Privileges

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

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

1. Click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from the selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.
7. Click **Next**.

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

Managing Data Security Policies

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

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of data security policies** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Adding and Removing Inherited Roles

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

To remove a role:

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

To add a role:


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

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

7. Click **Next**.

Provisioning the Role to Users

To provision the role to users, you must create a role mapping in the usual way. Don't provision the role to users here.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of user role membership** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Reviewing the Role

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

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

The role is available immediately.


Copying HCM Roles: Points to Consider

Copying predefined roles and editing the copies is the recommended approach to creating custom roles. This topic describes what to consider when you're copying a role.

Reviewing the Role Hierarchy

When you copy a predefined job, abstract, or duty role, you're recommended first to review the role hierarchy. This review is to identify the inherited roles that you want to refer to, copy, or delete in your custom role. For example, the Payroll Manager job role inherits the Payroll Administrator job role, among others. When copying the Payroll Manager role, you must decide whether to copy the Payroll Administrator role, refer to it, or remove it from your copy. You can review the role hierarchy on the Roles tab of the Security Console in either graphical or tabular format. You can also:

- Export the role hierarchy to a spreadsheet from the Roles tab.
- Review the role hierarchy and export it to a spreadsheet from the Analytics tab.
- Run the User and Role Access Audit Report.


 **Tip:** Aggregate privileges are never copied. When you copy a job or abstract role, its inherited aggregate privileges are referred to from your copy.

Reviewing Privileges

Job and abstract roles inherit function security privileges and data security policies from the roles that they inherit. Function security privileges and data security policies may also be granted directly to a job or abstract role. You can review these directly granted privileges on the Roles tab of the Security Console, as follows:

- In the graphical view of a role, its inherited roles and function security privileges are visible at the same time.
- In the tabular view, you set the **Show** value to switch between roles and function security privileges. You can export either view to a spreadsheet.

Once your custom role exists, edit it to add or remove directly granted function security privileges.


 **Note:** Data security policies are visible only when you edit your custom role. You're recommended to leave data security policies unchanged.

Transaction Analysis Duty Roles

Some roles, such as the Human Resource Analyst job role, inherit Transaction Analysis Duty roles, which are used in Oracle Transactional Business Intelligence report permissions. If you copy the Human Resource Analyst job role, or any other role that inherits Transaction Analysis Duty roles, then don't copy the Transaction Analysis Duty roles. If you copy the roles, then you must update the permissions for the relevant reports to secure them using your copies of the roles. Instead, add the predefined Transaction Analysis Duty roles to your copy of the relevant job role, such as Human Resource Analyst.

Naming Copied Roles

By default, a copied role has the same name as its source role with the suffix **Custom**. The role codes of copied roles have the suffix **_CUSTOM**. Copied roles lose the prefix **ORA_** automatically from their role codes. You can define a local naming convention for custom roles, with a prefix, suffix, or both, on the Administration tab of the Security Console.

 **Note:** Copied roles take their naming pattern from the default values specified on the Administration tab of the Security Console. You can override this pattern on the Copy Role: Basic Information page for the role that you're copying. However, the names of roles inherited by the copied role are unaffected. For example, if you perform a deep copy of the Employee role, then inherited duty roles take their naming pattern from the default values.

Duplicate Roles

If any role in the hierarchy already exists when you copy a role, then no copy of that role is made. For example, if you make a second copy of the Employee role, then copies of the inherited duty roles may already exist. In this case, membership is added to the existing **copies** of the roles. To create unique copies of inherited roles, you must enter unique values on the Administration tab of the Security Console before performing a deep copy.

To retain membership of the predefined job or abstract role hierarchy, perform a shallow copy of the predefined role.

Related Topics

- [Setting Role Preferences: Explained](#)
- [User and Role Access Audit Report](#)

Creating Job or Abstract Roles from Scratch: Procedure

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

Entering Basic Information

Follow these steps:


1. On the Roles tab of the Security Console, click **Create Role**.
2. On the Create Role: Basic Information page, enter the role's display name in the **Role Name** field. For example, enter Sales Department Administration Job Role.
3. Complete the **Role Code** field. For example, enter SALES_DEPT_ADMIN_JOB.
Abstract roles have the suffix **_ABSTRACT**, and job roles have the suffix **_JOB**.
4. In the **Role Category** field, select either **HCM - Abstract Roles** or **HCM - Job Roles**, as appropriate.
5. Click **Next**.

Adding Functional Security Policies

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

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

1. On the Create Role: Functional Security Policies page, click **Add Function Security Policy**.
2. In the **Add Function Security Policy** dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from a selected role to your custom role. If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Function Security Policy** dialog box.
7. Click **Next**.

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

Creating Data Security Policies

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

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of data security policies** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Building the Role Hierarchy


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

To add a role:

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

Provisioning the Role

To provision the role to users, you must create a role mapping in the usual way once the role exists. Don't provision the role to users here.

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of user role membership** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Reviewing the Role

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

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

Your custom role is available immediately.


Copying and Editing Duty Roles: Procedure

You can copy a duty role and edit the copy to create a custom duty role. Copying duty roles is the recommended way of creating custom duty roles. This topic explains how to copy a duty role and edit the copy. You must have the IT Security Manager job role to perform these tasks.


Copying a Duty Role

Follow these steps:

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

 **Tip:** Click the **Show Graph** icon to show the hierarchy in graphical format.

3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

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

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

Editing the Copied Duty Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select your copy of the duty role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.


Managing Functional Security Policies

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

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

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

4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the **Add Functional Security Policies** dialog box.
7. Click **Next**.

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

Managing Data Security Policies

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

 **Note:** Whether this page is enabled for edit depends on the current setting of the **Enable edit of data security policies** option. Set this option on the Roles subtab of the Security Console Administration tab.

Click **Next**.

Adding and Removing Inherited Roles

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

To remove a role:

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

To add a role:

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

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

7. Click **Next**.

Reviewing the Role

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

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

The role is available immediately.

Role Optimization

Role Optimizer: Explained

Role optimization is the process used to analyze the existing role hierarchy for redundancies or other inefficiencies. Role optimization enables you to create a role hierarchy that minimizes the number of roles necessary to authorize every job role to its currently authorized privileges. The role optimizer feature automates the analysis process and generates a report you can use to optimize your job hierarchies.

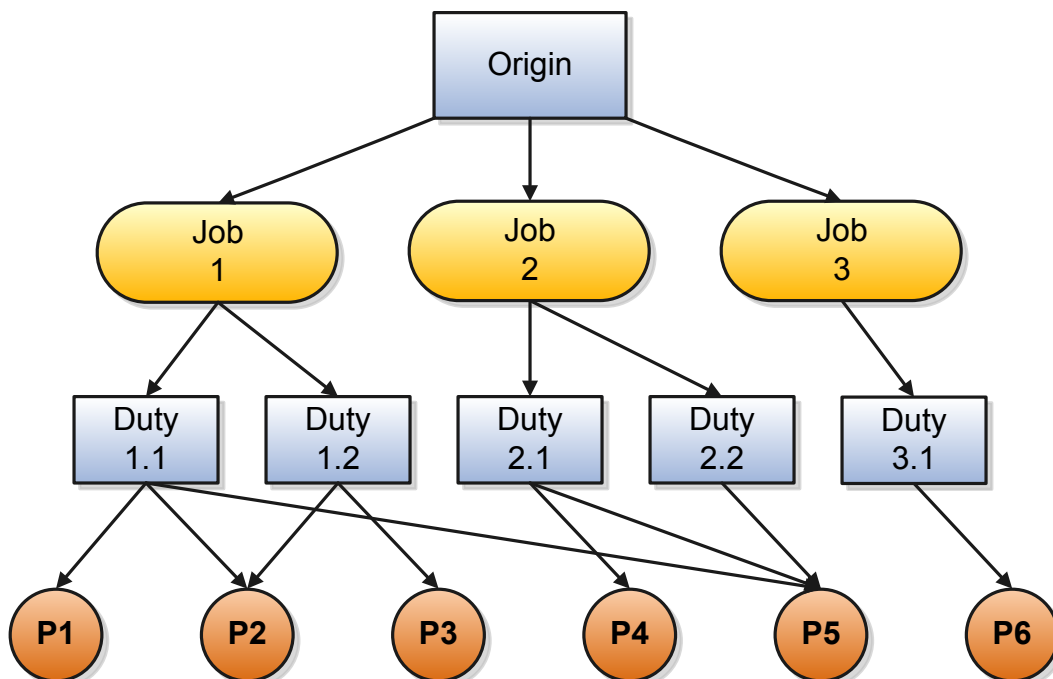
! Important: The use of the Role Optimization Report is not included in the cost of your service subscription or application license and incurs charges in addition to your subscription or licensing fee.

Reasons to Optimize

Changes to the predefined role hierarchies can put the privacy of your application data at risk. You can unintentionally make your data less secure if you:

- Create duty roles with small groups of privileges in an attempt to minimize:
 - Dependencies
 - The impact of making incremental changes
- Grant privileges that already exist in the role hierarchy

Roles can proliferate or have duplicate privileges over time to make your role hierarchy less efficient, as you see in the following figure.

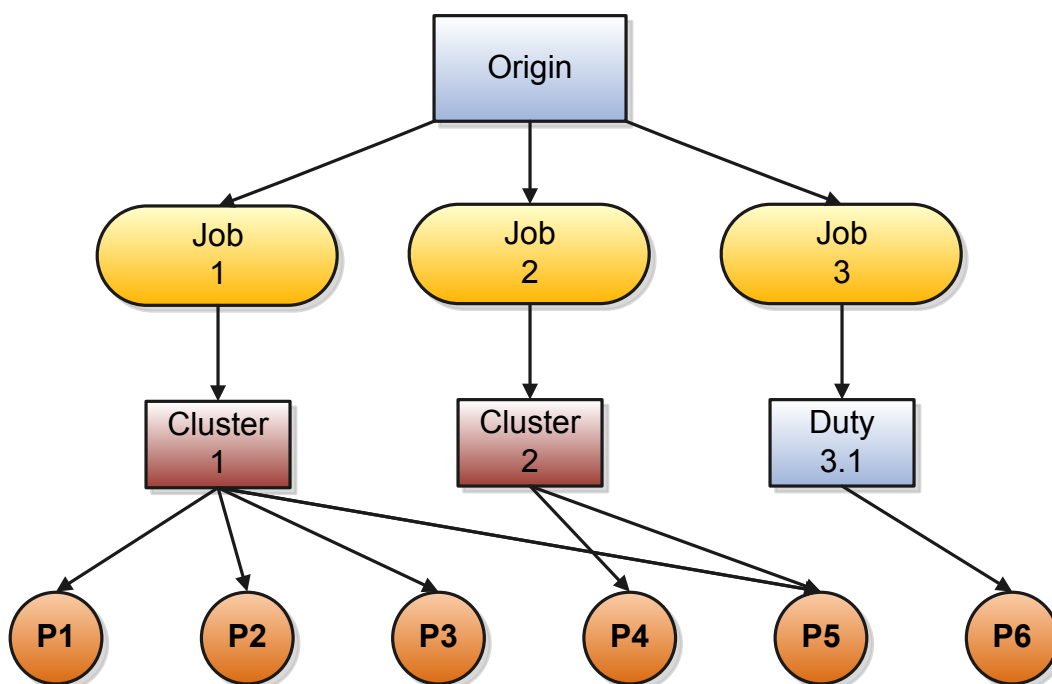


Benefits of Optimization

By using the role optimizer, you can:

- Increase user productivity.
You save time that you can perform other tasks.
- Lower administrative costs.
You reduce the number of security objects and the amount of time you spend maintaining that you must administer them.
- Decrease access risk associated with undocumented role hierarchy changes.
You identify and can eliminate redundant and inappropriate grants of privilege.

The role optimizer can suggest more efficient role hierarchies, such as the one you see in this figure.



Role Optimizer Access

The role optimizer feature is available as a predefined report. Schedule and submit the Role Optimization Report on the Overview page of the Scheduled Processes work area. The process:

1. Analyzes your existing job role hierarchies.
2. Generates the optimized job role hierarchy and stores the data for each job role in a separate CSV file.
3. Archives and attaches the CSV files as the process output.
4. Generates a log and archives it as a ZIP file. The log file includes technical details of the analysis for troubleshooting.

❗ Important: The role optimization process makes no changes to your security structures. You use the report to map privileges to roles and update the role hierarchies.

Role Optimization Report

Use the Role Optimization Report to create the most efficient role hierarchy for your organization. Use the report results to evaluate and, if necessary, update your role hierarchy. The report results enable you to create a role hierarchy with the minimum number of roles necessary to authorize every job role to every privilege it is currently authorized to.

Important: The use of the Role Optimization Report is not included in the cost of your service subscription or application license and incurs charges in addition to your subscription or licensing fee.

Users with the IT Security Manager role can run the Role Optimization Report, which is available from the security console.

You should run this report if you:

- Make changes to the predefined role hierarchy.
- Implement your own role hierarchy instead of the predefined role hierarchy.

Important: The process makes no changes to your role hierarchies.

Note: The predefined role hierarchy in the security reference implementation is optimized as delivered.

Report Files

Monitor the process status on the Overview page. When the status value is Succeeded, two files appear in the **Log and Output** section of the report details. The following table describes the two files:

File Name	Description
ClusterAnalysis-Job-CSVs. zip	<p>Contains one CSV file for every job role. Each CSV file contains the duty roles and privileges that make up the optimized job role hierarchy. The name of a CSV file, identifies the job role hierarchy data that the file contains.</p> <p>For example, the ClustersforJob-AR_ REVENUE_ MANAGER_ JOB_ 14240.csv file contains all of the role hierarchy data for the Accounts Receivables Revenue Manager job role.</p>
Diagnostics. zip	Contains a log file that provides technical details about the analysis process. You can use this file for troubleshooting purposes.

Import the raw data from the CSV file into your preferred application to read the results. Report data appears in these two sections:

- Privilege Clusters
- Cluster Details

Role Optimization Report Results

Privilege Clusters

The Privilege Clusters section lists each privilege and the name of a recommended privilege cluster. Specific cluster recommendations are described in the cluster details section.

Cluster Details

A Cluster Details section appears for each privilege cluster referenced in the Privilege Clusters section. Each detail section includes:

- Cluster name.
- Names of recommended candidate roles that map to the privilege cluster.
- Names and descriptions of the jobs and privileges associated with the cluster.

This table provides descriptions of the fields that appear the Cluster Details section:

Field Name	Description
Cluster Name	The name of the optimized cluster, usually in this format: Cluster ###
Primary, Secondary, Tertiary Candidate Role	Recommended role mappings for the privileges in the cluster. Up to three recommended duty roles map to the listed privileges. Select a role. Then assign the privileges in the cluster to that role.
Jobs in Cluster	The number of job roles that inherit the privilege cluster. A list of job names and descriptions is also included.
Privileges in Cluster	The number of privileges that make up the cluster. A list of privilege names and descriptions is also included.

FAQs for Customizing Roles Using the Security Console

Why didn't the role optimization process update my roles?

The role optimization process doesn't change any security structures. It analyzes your role hierarchy and provides data in a report you can use to optimize the role hierarchy.

10 Managing Certificates and Keys

Managing Certificates: Explained

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.

To the right in the row for each certificate, click a button to display a menu of actions appropriate for the certificate. Or, to view details for a certificate, select its name ("alias"). 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.

Generating Certificates: Explained

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 algorithm by which keys are generated, DSA or RSA.
- A key length.

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 does not 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.

Generating a Signing Request: Procedure

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 does not 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.

Importing and Exporting X.509 Certificates: Procedure

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 are 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 are 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.

Importing and Exporting PGP Certificates: Procedure

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 will not 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 does not 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 are 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 do not 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.

Deleting Certificates: Procedure

You can delete both PGP and X.509 certificates:

1. In 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.
2. In either menu, select Delete.
3. 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.

11 Security for SCM Analytics and Reports

Security for Oracle SCM Cloud Analytics: Overview

Security for viewing, creating, and editing Oracle SCM Cloud analytics includes three levels:

- Access to the folders where the analyses and dashboards are stored
- Access to the data that you want the analysis or dashboard to return
- Access to business intelligence functionality

This topic provides an overview of how analyses and dashboards are secured so that you understand what security roles or access you may need to request from your security administrator to create and edit analyses and dashboards.

Access to Subject Areas

Subject areas are functionally secured using duty roles. The names of duty roles that grant access to subject areas include the words Transaction Analysis Duty (for example, Product Transaction Analysis Duty). These duty roles belong to the OBI application.

Access to Analyses and Dashboards in the BI Catalog

To access delivered analyses and dashboards, you access the Business Intelligence Catalog (BI Catalog). The folders in the BI Catalog are functionally secured using the same duty roles that secure access to the subject areas. Therefore, a user who inherits the Workforce Transaction Analysis Duty can access both the Workforce Management folder in the Business Intelligence Catalog and the Workforce Management subject areas. Analyses and dashboards are secured based on the folders in which they're stored. You can set permissions against folders and reports for Application Roles, Catalog Groups, or Users.

Reporting Data

The data that's returned in Oracle Transactional Business Intelligence reports is secured in a similar way to the data that's returned in Oracle SCM Cloud pages. Data access is granted by roles that are linked to security profiles. Each of the Transaction Analysis Duty roles that grants access to subject areas and Business Intelligence Catalog (BI Catalog) folders inherits one or more Reporting Data Duty roles. These duty roles grant access to the data. The Reporting Data Duty roles belong to the SCM application.

Business Intelligence Roles

Business Intelligence roles apply to both Oracle Business Intelligence Publisher (Oracle BI Publisher) and Oracle Transactional Business Intelligence. They grant access to Business Intelligence functionality, such as the ability to run or author reports.

Users need one or more of these roles in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and Oracle SCM Cloud data.

Security for Oracle SCM Cloud Reports: Overview

Security for viewing, creating, and editing Oracle Business Intelligence Publisher reports for SCM includes the following concepts:

- Access to the folders where the reports are stored
- Access to the data that you want the report to return
- Access to business intelligence functionality
- Secured list views
- Personally identifiable information (PII)

This topic provides an overview of how Business Intelligence Publisher reports are secured so that you understand what security roles or access you must request from your security administrator to create and edit reports.

Access to Reports in the BI Catalog

You can access the delivered reports in the Business Intelligence Catalog (BI Catalog). The folders in the BI Catalog are functionally secured using the same duty roles that secure access to the subject areas. Therefore, a user who inherits the Cost Transaction Analysis Duty can access both the Cost Management folder in the Business Intelligence Catalog and the Cost Management subject areas. Reports are secured based on the folders in which they're stored. You can set permissions against folders and reports for Application Roles, Catalog Groups, or Users.

Functional Area Folder	Default Job Role	OTBI Transactional Analysis Duty Role
Cost Management	Cost Accountant	Cost Transactional Analysis Duty
Innovation Management	Product Management VP	Product Management VP Real Time Transaction Analysis Duty Role
Order Orchestration and Order Management	Order Administrator	Order Transaction Analysis Duty
	Order Manager	Order Transaction Analysis Duty
Product Management	Product Data Steward	Product Catalog Transaction Analysis Duty
	Product Manage	Product Catalog Transaction Analysis Duty
Warehouse Operations	Inventory Manager	Inventory Transaction Analysis Duty
	Shipping Manager	Order Pick Transaction Analysis Duty
	Warehouse Manager	<ul style="list-style-type: none"> • Inventory Transaction Analysis Duty

Functional Area Folder	Default Job Role	OTBI Transactional Analysis Duty Role
		<ul style="list-style-type: none"> Order Pick Transaction Analysis Duty Receiving Transaction Analysis Duty

Reporting Data

The data that's returned in reports is secured in a similar way to the data that's returned in Oracle SCM Cloud pages. Data access is granted by roles that are linked to security profiles. Each of the Transaction Analysis Duty roles that grants access to subject areas and Business Intelligence Catalog (BI Catalog) folders inherits one or more Reporting Data Duty roles. These duty roles grant access to the data. The Reporting Data Duty roles belong to the SCM application.

Business Intelligence Roles

Business Intelligence roles apply to both Oracle Business Intelligence Publisher (Oracle BI Publisher) and Oracle Transactional Business Intelligence. They grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and Oracle SCM Cloud data.

Secured List Views

When you access data using a BI Publisher data model that uses an SQL Query as the data source, you have two options:

- Select data directly from a database table, in which case the data you return isn't subject to data-security restrictions. Because you can create data models on unsecured data using BI Publisher, you're recommended to minimize the number of users who can create data models.
- Join to a secured list view in your select statements. The data returned is determined by the security profiles that are assigned to the roles of the user who's running the report.

PII Data

Personally identifiable information (PII) tables are secured at the database level using virtual private database (VPD) policies. Only authorized users can report on data in PII tables. This restriction also applies to Business Intelligence Publisher (BI Publisher) reports. The data in PII tables is protected using data security privileges that are granted by means of duty roles in the usual way.

Business Intelligence Roles: Explained

Business Intelligence roles apply to both Oracle Business Intelligence Publisher (Oracle BI Publisher) and Oracle Transactional Business Intelligence (OTBI). They grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and your data. This topic describes the Business Intelligence roles.

Business Intelligence roles are defined as application roles. This table identifies those roles.

Business Intelligence Role	Description
BI Consumer Role	Runs Business Intelligence reports.
BI Author Role	Creates and edits reports.
BI Administrator Role	Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on.
BI Publisher Data Model Developer Role	Creates and edits Oracle Business Intelligence Publisher data models.

BI Consumer Role

The predefined OTBI Transaction Analysis Duty roles inherit the BI Consumer Role. You can configure custom roles to inherit BI Consumer Role so that they can run reports but not author them.

BI Author Role

The BI Author Role inherits the BI Consumer Role. Users with BI Author Role can create, edit, and run OTBI reports.

BI Administrator Role

BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role.

The predefined Sales Cloud job roles do not have BI Administrator Role access.

BI Publisher Data Model Developer Role

BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Therefore, users with either of these predefined job roles can manage BI Publisher data models.

Glossary

abstract role

A description of a person's function in the enterprise that is unrelated to the person's job (position), such as employee, contingent worker, or line manager.

action

The kind of access, such as view or edit, named in a security policy.

aggregate privilege

A predefined role that combines one function security privilege with related data security policies.

assignment

A set of information, including job, position, pay, compensation, managers, working hours, and work location, that defines a worker's or nonworker's role in a legal employer.

business object

A resource in an enterprise database, such as an invoice or purchase order.

business unit

A unit of an enterprise that performs one or many business functions that can be rolled up in a management hierarchy.

condition

The part of a data security policy that specifies what portions of a database resource are secured.

contingent worker

A self-employed or agency-supplied worker. Contingent worker work relationships with legal employers are typically of a specified duration. Any person who has a contingent worker work relationship with a legal employer is a contingent worker.

dashboard

A collection of analyses and other content, presented on one or more pages to help users achieve specific business goals. Each page is a separate tab within the dashboard.

data dimension

A stripe of data accessible by a user. Sometimes referred to as data security context.

data instance set

The set of HCM data, such as one or more persons, organizations, or payrolls, identified by an HCM security profile.

data role

A role for a defined set of data describing the job a user does within that defined set of data. A data role inherits job or abstract roles and grants entitlement to access data within a specific dimension of data based on data security policies. A type of enterprise role.

data security

The control of access and action a user can take against which data.

data security policy

A grant of entitlement to a role on an object or attribute group for a given condition.

database resource

An applications data object at the instance, instance set, or global level, which is secured by data security policies.

department

A division of a business enterprise dealing with a particular area of activity.

duty role

A group of function and data privileges representing one duty of a job. Duty roles are specific to applications, stored in the policy store, and shared within an application instance.

effective start date

For a date-effective object, the start date of a physical record in the object's history. A physical record is available to transactions between its effective start and end dates.

enterprise

An organization with one or more legal entities under common control.

entitlement

Grant of access to functions and data. Oracle Fusion Middleware term for privilege.

flexfield

A flexible data field that you can customize to contain one or more segments or store additional information. Each segment has a value and a meaning.

flexfield segment

An extensible data field that represents an attribute and captures a value corresponding to a predefined, single extension column in the database. A segment appears globally or based on a context of other captured information.

function security

The control of access to a page or a specific use of a page. Function security controls what a user can do.

HCM data role

A job role, such as benefits administrator, associated with instances of HCM data, such as all employees in a department.

identity

A person representing a worker, supplier, or customer.

job

A generic role that is independent of any single department or location. For example, the jobs Manager and Consultant can occur in many departments.

job role

A role, such as an accounts payable manager or application implementation consultant, that usually identifies and aggregates the duties or responsibilities that make up the job.

LDAP

Abbreviation for Lightweight Directory Access Protocol.

party

A physical entity, such as a person, organization or group, that the deploying company has an interest in tracking.

person number

A person ID that is unique in the enterprise, allocated automatically or manually, and valid throughout the enterprise for all of a person's work and person-to-person relationships.

person type

A subcategory of a system person type, which the enterprise can define. Person type is specified for a person at the assignment level.

personally identifiable information

Any piece of information that can be used to uniquely identify, contact, or locate a single person. Within the context of an enterprise, some PII data, such as a person's name, can be considered public, while other PII data, such as national identifier or passport number is confidential.

privilege

A grant of access to functions and data; a single, real world action on a single business object.

privilege cluster

In the output of the Role Optimization Report, a group of privileges that you can map to a duty role.

resource

People designated as able to be assigned to work objects, for example, service agents, sales managers, or partner contacts. A sales manager and partner contact can be assigned to work on a lead or opportunity. A service agent can be assigned to a service request.

role

Controls access to application functions and data.

role hierarchy

Structure of roles to reflect an organization's lines of authority and responsibility. In a role hierarchy, a parent role inherits all the entitlement of one or more child roles.

role mapping

A relationship between one or more roles and one or more assignment conditions. Users with at least one assignment that matches the conditions qualify for the associated roles.

role provisioning

The automatic or manual allocation of a role to a user.

security profile

A set of criteria that identifies HCM objects of a single type for the purposes of securing access to those objects. The relevant HCM objects are persons, organizations, positions, countries, LDGs, document types, payrolls, and payroll flows.

security reference implementation

Predefined function and data security that includes role based access control, and policies that protect functions, and data. The reference implementation supports identity management, access provisioning, and security enforcement across the tools, data transformations, access methods, and the information life cycle of an enterprise.

SQL predicate

A type of condition using SQL to constrain the data secured by a data security policy.

transaction

A logical unit of work such as a promotion or an assignment change. A transaction may consist of several components, such as changes to salary, locations, and grade, but all the components are handled as a unit to be either approved or rejected.

URL

Abbreviation for uniform resource locator.

work area

A set of pages containing the tasks, searches, and other content you need to accomplish a business goal.

work relationship

An association between a person and a legal employer, where the worker type determines whether the relationship is a nonworker, contingent worker, or employee work relationship.

worker type

A classification selected on a person's work relationship, which can be employee, contingent worker, pending worker, or nonworker.

XML filter

A type of condition using XML to constrain the data secured by a data security policy.

