Oracle Supply Chain Management Cloud
Securing Oracle SCM Cloud

Release 10
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, 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 Corporation 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 on 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. 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.

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 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**

**1 Introduction**

- Securing Oracle Supply Chain Management Cloud: Overview
- Roles-Based Applications Security: Explained
- Role Types: Explained
- Role Inheritance: Explained
- Duty Role Components: Explained
- Aggregate Privileges: Explained
- Security Customization in Oracle Applications Cloud: Points to Consider
- Role-based Security in Oracle SCM Cloud: Explained
- Security Setup in Oracle SCM Cloud: Explained
- Getting Started with Security Implementation in Oracle SCM Cloud

**2 Managing Implementation Users**

- Creating Implementation Users
- Assigning Roles to Implementation Users

**3 Preparing for Application Users**

- Preparing Oracle Applications Cloud for Application Users: Overview
- User and Role-Provisioning Setup: Critical Choices
- User Account Creation Option: Explained
- Default User Name Format Option: Explained
- User Account Role Provisioning Option: Explained
- User Account Maintenance Option: Explained
- Send User Name and Password Option: Explained
- Setting the User and Role Provisioning Options: Procedure
- Oracle Applications Cloud Password Policy: Explained
- Provisioning Abstract Roles to Users Automatically: Procedure
- FAQs for Preparing for Application Users
# Oracle Supply Chain Management Cloud

## Securing Oracle SCM Cloud

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Creating and Managing Application Users</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Creating Users</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Managing Users</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>FAQs for Creating and Managing Application Users</td>
<td>47</td>
</tr>
<tr>
<td>5</td>
<td>Provisioning Roles to Application Users</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Role Mappings: Explained</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Creating a Role Mapping: Procedure</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Role Provisioning and Deprovisioning: Explained</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Autoprovisioning: Explained</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>Role Provisioning Status Values: Explained</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>User and Role Access Audit Report Reference</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>FAQs for Provisioning Roles to Application Users</td>
<td>59</td>
</tr>
<tr>
<td>6</td>
<td>Customizing Security</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Customizing Security: Points to Consider</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Managing Resources and Roles</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Managing Data Roles</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>Managing Data Security Policies</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>Creating Custom Duty Roles</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>FAQs for Customizing Security</td>
<td>81</td>
</tr>
<tr>
<td>7</td>
<td>Using the Security Console</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Setting Up the Security Console: Explained</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Security Visualizations: Explained</td>
<td>86</td>
</tr>
<tr>
<td></td>
<td>Simulating Navigator Menus in the Security Console: Procedure</td>
<td>87</td>
</tr>
<tr>
<td></td>
<td>Security Console Analytics: Explained</td>
<td>88</td>
</tr>
<tr>
<td></td>
<td>FAQs for Using the Security Console</td>
<td>88</td>
</tr>
<tr>
<td>8</td>
<td>Reviewing Roles and Role Assignments</td>
<td>89</td>
</tr>
<tr>
<td></td>
<td>Reviewing Roles and Role Assignments on the Security Console: Procedure</td>
<td>89</td>
</tr>
<tr>
<td></td>
<td>Reviewing Job and Abstract Roles on the Security Console: Explained</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>Comparing Roles: Procedure</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>User and Role Access Audit Report Reference</td>
<td>91</td>
</tr>
</tbody>
</table>
9 Customizing Roles Using the Security Console

Creating Custom Roles
Role Optimization

10 Synchronizing User and Role Information with Oracle Identity Management

Synchronization of User and Role Information with Oracle Identity Management: How It’s Processed
Scheduling the LDAP Daily Processes: Procedure
Send Pending LDAP Requests: Explained
Retrieve Latest LDAP Changes: Explained

11 Managing Certificates and Keys

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

This Preface introduces information sources available to help you use Oracle Applications.

Oracle Applications Help

Use the help icon to access Oracle Applications Help in the application.

Note

If you don’t see any help icons on your page, click the Show Help button in the global area. Not all pages have help icons.

You can also access Oracle Applications Help at https://fusionhelp.oracle.com/.

Oracle Applications Guides

To find other guides for Oracle Applications, go to:

- Oracle Applications Help, and select Documentation Library from the Navigator menu.
- Oracle Help Center at http://docs.oracle.com/

Other Information Sources

My Oracle Support

Oracle customers 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.


Oracle Enterprise Repository for Oracle Fusion Applications

Oracle Enterprise Repository for Oracle Fusion Applications (http://fusionappsoer.oracle.com) provides details on assets (such as services, integration tables, and composites) to help you manage the lifecycle of your software.

Documentation Accessibility

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.
Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides!

- Send e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.
- Click your user name in the global area of Oracle Applications Help, and select Send Feedback to Oracle.
1 Introduction

Securing Oracle Supply Chain Management 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.

To manage roles, you may use Oracle Identity Manager, Authorization Policy Manager, and other tasks available in the Setup and Maintenance work area. Or you may use a Security Console, which is accessible in the Tools category of the Navigator. You may use either of these options to create or customize roles, or to view and work with them later; the choice is a matter of your preference. Some chapters in this guide discuss the use of Setup and Maintenance tasks, and later chapters discuss the use of the Security Console.

Guide Structure

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

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>A brief introduction to the concepts of role-based security</td>
</tr>
<tr>
<td>Managing Implementation Users</td>
<td>The purpose of implementation users and how you create them</td>
</tr>
<tr>
<td>Preparing the Cloud Service for Application Users</td>
<td>Enterprise-wide options and related decisions that affect application users</td>
</tr>
<tr>
<td>Creating and Managing Application Users</td>
<td>How to use tasks available from Setup and Maintenance to enable application users to acquire roles, with instructions for some methods</td>
</tr>
<tr>
<td>Provisioning Roles to Application Users</td>
<td>The ways that application users can acquire roles, with instructions for creating some standard role mappings</td>
</tr>
<tr>
<td>Customizing Security</td>
<td>How to use Oracle Identity Manager and Authorization Policy Manager to create, review, and modify security components, with recommended best practices</td>
</tr>
</tbody>
</table>
## Chapter 1

### Introduction

During implementation, you can perform security-related tasks:

- From an implementation project
- By opening the Setup and Maintenance work area

Select **Navigator - Tools - Setup and Maintenance** and search for the task on the All Tasks tab.

After the implementation is complete, you can perform most security-related tasks from the Setup and Maintenance work area or in the 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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who</td>
<td>Role assigned to a user</td>
</tr>
<tr>
<td>What</td>
<td>Function that users with the role can perform</td>
</tr>
<tr>
<td>Which Data</td>
<td>Set of data that users with the role can access when performing the function</td>
</tr>
</tbody>
</table>
The following topics introduce the four types of roles and how they work together through role inheritance to secure Oracle Applications Cloud.

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

Data Roles
Data roles combine a worker’s job and the specific data that users with the job can access. You must create your own data roles because data roles aren’t part of the security reference implementation. You can define them locally and assign them directly to users.

A job role such as Warehouse Manager provides access to the functions needed to perform certain duties. A data role specifies which rows of invoice data within a business unit, such as the US business unit, can be accessed. The result can be the Warehouse Manager - M1 Inventory Organization data role. This role can perform any warehouse management duties that it inherits from the Warehouse Manager job role on the data associated with the M1 Inventory Organization.

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. Typically, you include job roles in data roles and assign those data roles to users. 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:

- Data roles inherit job or abstract roles.
- Job and abstract roles inherit duty roles.
- Duty roles can inherit other duty roles.
When you assign data roles and abstract roles to users, they inherit the data and function security in the role hierarchy. In this figure, user Linda Swift has three 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.

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.
Role Types: Explained

Oracle Enterprise Resource Planning (Oracle SCM) Cloud defines five types of roles:

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

This topic introduces the five role types.

Data Roles

Data roles combine a job and the data that users with the job must access. For example, the SCM data role Warehouse Manager - M1 Inventory Organization combines a job (Warehouse Manager) with a stripe, or set, of data (M1 Inventory Organization). You define the scope of data in a data role template.

SCM data roles are not included in the security reference implementation. You must create your own data roles locally.

You assign data roles directly to users.

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.

Typically, you add job roles to data roles and you assign the data roles to users. The IT Security Manager and Application Implementation Consultant predefined job roles are exceptions to this general rule. They are not job roles associated with an offering. Also, you don’t need to define a scope of data directly against 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.

- Data roles inherit job or abstract 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 data and abstract roles to users, they inherit all of the data and function security associated with those roles.
Role Inheritance Example

This example shows how roles are inherited.

In this example, the user has two roles:

- Warehouse Manager-M1 Inventory Organization, a data role
- Employee, an abstract role

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warehouse Manager-M1 Inventory Organization, a data role</td>
<td>Inherits the job role Warehouse Manager. This role inherits the aggregate privilege and duty roles that provide access to the tasks and functions that a warehouse manager performs.</td>
</tr>
<tr>
<td>Employee, an abstract role</td>
<td>Inherits aggregate privileges and duty roles that provide access to tasks and functions that are both unrelated to a specific job and performed by every employee.</td>
</tr>
</tbody>
</table>
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. In addition to its aggregate privileges, a duty role is granted many function security privileges and data security policies.

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. If you copy a job or abstract role, then the source role’s 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.

During implementation, you evaluate the predefined roles and decide whether changes are needed.

Important

Never edit the predefined roles. (In the Security Console, you can identify predefined application roles by the ORA_prefix in the Role Code field.) During each upgrade, predefined roles are updated to the specifications for that release, so any customizations would be overwritten. Instead, use one of these options:

• Copy the predefined roles and edit the copies.

• Create custom roles from scratch.

You can perform both tasks on the Security Console.

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 the predefined role and editing the copy 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.

Note

The Functional Setups User abstract role is required for any custom role intended to perform implementation tasks.
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 aggregate privileges and 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:

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
<th>Data Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Accountant</td>
<td>Can manage cost transactions</td>
<td>To the cost organizations for which they are authorized</td>
</tr>
<tr>
<td>Warehouse Manager</td>
<td>Can manage inventory transactions</td>
<td>To the inventory organizations in which they operate</td>
</tr>
</tbody>
</table>

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 in SCM Cloud**

This example shows different types of roles.

<table>
<thead>
<tr>
<th>Data Role</th>
<th>Abstract Role</th>
<th>Job Role</th>
<th>Duty Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Warehouse Manager</td>
<td></td>
</tr>
</tbody>
</table>

Duty roles are associated with function security privileges and data security policies. For example, the Inventory Balances Management Duty is associated with function security privileges and data security policies, as follows:

- The function security privileges Manage On-Hand Quantity, Request Item Issue, Request Subinventory Transfer, Request Cycle Count, Manage Material Status, and Edit Lot Grade secure the respective pages.
- 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 in SCM Cloud**

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, data roles are automatically generated that inherit job roles based on data role templates.

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.
### Getting Started with Security Implementation in Oracle SCM Cloud

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 into Oracle Identity Manager (OIM) as the OIM Administration users 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:
   
   
   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 data 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 data 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.
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 the your Oracle Applications Cloud organization.
- You don’t create them as users in Oracle Applications Cloud. You create them in the integrated Oracle Identity Manager.
- 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 integrated Oracle Identity Manager. 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 a 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.

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task or Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create Implementation Users</td>
<td>The Application Implementation Consultant user may be your only implementation user. However, you can create the implementation users OIMAdmin, 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. 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 to replace these users or change their definitions.</td>
</tr>
<tr>
<td>2</td>
<td>Run User and Roles Synchronization Process</td>
<td>You run the process Retrieve Latest LDAP Changes to copy changes made in Oracle Identity Manager to Oracle Fusion Human Capital Management (Oracle Fusion HCM).</td>
</tr>
</tbody>
</table>
### Managing Implementation Users

<table>
<thead>
<tr>
<th>Step</th>
<th>Task or Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Assign Security Profiles to Abstract Roles</td>
<td>Enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles.</td>
</tr>
<tr>
<td>4</td>
<td>Create a Generic Role Mapping for the Data Roles</td>
<td>Enable the data roles created in step 3 to be provisioned to implementation users.</td>
</tr>
<tr>
<td>5</td>
<td>Assign Abstract and Data Roles to the Implementation User</td>
<td>Assign the implementation user with the roles that enable functional implementation to proceed.</td>
</tr>
<tr>
<td>6</td>
<td>Verify Implementation User Access</td>
<td>Confirm that the implementation user can access the functions enabled by the assigned roles.</td>
</tr>
</tbody>
</table>

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

### Related Topics

- Creating the OIMAdmin Implementation User: Procedure
- Creating the TechAdmin Implementation User: Procedure

### Synchronizing User and Role Information: Procedure

You run the process Retrieve Latest LDAP Changes during implementation whenever you make changes directly in Oracle Identity Manager. This process copies your changes to Oracle Fusion Applications. 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

1. Sign in to your Oracle Applications Cloud service environment as the TechAdmin user.

   If this is the first use of this user name, then you’re prompted to change the password. You also select some challenge questions and enter the answers. Make a note of the password, the challenge questions, and their answers. You use the updated password whenever you sign in as this user subsequently.

2. Select **Navigator - Setup and Maintenance** to open the Setup and Maintenance work area.

3. On the All Tasks tab of the Overview page, 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.

### Important

During implementation, whenever you make changes to user and role information directly in Oracle Identity Manager, you must run the Retrieve Latest LDAP Changes process as described here. Otherwise, the changes you make in Oracle Identity Manager don’t appear in Oracle Fusion Applications.

---

## 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. On the All Tasks tab of the Overview page, 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

Values in the Conditions section determine 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Procurement Department</td>
</tr>
<tr>
<td>Job</td>
<td>Chief Buyer</td>
</tr>
<tr>
<td>Location</td>
<td>Denver</td>
</tr>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>
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 data role Procurement Analyst Denver.

3. Select one or more of the role-provisioning options:

<table>
<thead>
<tr>
<th>Role-Provisioning Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestable</td>
<td>Qualifying users can provision the role to other users.</td>
</tr>
<tr>
<td>Self-Requestable</td>
<td>Qualifying users can request the role for themselves.</td>
</tr>
<tr>
<td>Autoprovision</td>
<td>Qualifying users acquire the role automatically.</td>
</tr>
</tbody>
</table>

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

**Important**
Autoproduction is selected by default. Remember to deselect it if you don’t want autoproductioning.

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 Autoproduction

You’re recommended to run the process Autoproduction 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 autoproduction requests. Therefore, no further action is necessary to put new role mappings that include autoproductioned roles into effect.

Related Topics

- Autoproduction: Explained
Assigning Abstract and Data Roles to Users in Oracle Identity Manager: Procedure

An implementation user can have some job roles that were assigned when the user was created. This topic explains how to assign abstract and data roles to enable users to complete a functional implementation.

**Note**

Only assign abstract and data roles to the user for the business requirements they are responsible for implementing. Refer to the appropriate Security Reference Manual to identify the roles that match your business requirements.

Accessing Oracle Identity Manager Delegated Administration

You assign additional roles to implementation users on the Oracle Identity Manager - Delegated Administration page. Follow these steps to open the page:

1. Sign in to the service environment using the IT Security Manager user name and password.

   If this is the first use of this user name, then you're prompted to change the password. You also select some challenge questions and enter the answers. Make a note of the password, the challenge questions, and their answers. You use the updated password whenever you sign in as this user subsequently.

2. On the home page, click **Setup and Maintenance** to open the Setup and Maintenance work area.

3. On the All Tasks tab of the Overview page, search for and select the Create Implementation Users task.

   The Oracle Identity Manager - Self Service page opens.

4. On the Oracle Identity Manager - Self Service page, click **Administration** in the top-right corner.

   The Oracle Identity Manager - Delegated Administration page opens.

Assigning Roles to Implementation Users

1. In the Users section of the Oracle Identity Manager - Delegated Administration page, select **Advanced Search - Users**.

   The Advanced Search - Users page opens.

2. In the **User Login** field in the Advanced Search section, enter the implementation user name and click **Search**.

3. In the search results, click the name of the implementation user in the **Display Name** column. The user page for the user opens.

4. On the user page, click the Roles tab.

   Some roles might already appear in the list of roles assigned:

5. Click **Assign**.
The **Add Role** dialog box opens.

6. In the **Add Role** dialog box, search for and select abstract or data roles. Click **Add** to add a selected roles to the implementation user.

   **Tip**

   If you add a role by mistake, you can select it and click **Revoke**.

7. Click **Close Single Tab** to close the user tab for the implementation user.

8. Close the Oracle Identity Manager Delegated Administration Console.

9. Run the Retrieve Latest LDAP Changes process to make these changes available in Oracle Applications Cloud.

### Verifying User Access: Procedure

This topic explains how to verify that the product-specific implementation user can access the functions enabled by the assigned roles.

1. Sign in to the Oracle Applications Cloud service using the product-specific user name and password.

   As this is the first use of this user name, you’re prompted to change the password. You also select some challenge questions and enter the answers. Make a note of the new password, the challenge questions, and their answers. You use the new password whenever you sign in as this user subsequently.

2. Click **Submit** on the Password Management page.

3. Open the Oracle Applications Navigator. In the Navigator, verify that the specific menu appears that corresponds to the product under implementation.

4. Sign out of the Oracle Applications Cloud service.

### 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 OIMAdmin 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 Oracle Identity Manager Self Service page opens.

3. Click **Administration** in the top-right of the page.

The Identity Manager - Delegated Administration page opens.

4. In the Users section, select **Advanced Search - Users**. The Advanced Search - Users page opens.

5. In the **User Login** field, enter your service administrator user name, which is typically your e-mail. Your service activation mail contains this value.

6. Click **Search**. In the search results, select your service administrator user name in the **Display Name** column. The page for managing your user details opens.

7. Delete the value in the **First Name** field.

8. Change the value in the **Last Name** field to ServiceAdmin.

9. Delete the value in the **Email** field.

10. Change the **User Login** value to ServiceAdmin.

11. Click **Apply**.

12. Sign out of Identity Manager - Delegated Administration and close the tab.

13. 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.
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 such 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:

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

User and Role-Provisioning Setup: Critical Choices

This topic introduces the user and role-provisioning options, which control the default management of user accounts. 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 in Oracle Identity Management 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 Fusion Applications.

• 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 in Oracle Identity Management aren’t affected by this option.

User Account Maintenance

The User Account Maintenance option controls whether user accounts are maintained, suspended, and reactivated automatically. By default, user accounts are suspended automatically when the user has no roles. In some circumstances, user accounts are reactivated automatically when the user acquires roles. In addition, some person information is sent automatically to Oracle Identity Management when you update a person record.

Alternate Contact E-Mail Address

The alternate contact e-mail is an enterprise-wide e-mail that can receive user names and passwords for all Oracle Identity Management user accounts.

Send User Name and Password

Send User Name and Password controls whether an e-mail containing the user name and password is sent automatically when a user account is created. The e-mail may be sent to the alternate contact e-mail, the user, or the user’s line manager.

Default User Name Format

You can set the default format of user names for the enterprise to one of these values:

• Defined by Oracle Identity Management

• Party number

• Person number

• Primary work e-mail
User Account Creation Option: Explained

The User Account Creation option controls whether user accounts are created automatically in Oracle Identity Management when you create a person or party record. It applies whether you create person and party records individually or in bulk. Use the Manage Enterprise HCM Information task to set this option.

This table describes the User Account Creation option values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both person and party users</td>
<td>User accounts are created automatically for both person and party users. This value is the default value.</td>
</tr>
<tr>
<td>Party users only</td>
<td>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 passed to Oracle Identity Management.</td>
</tr>
<tr>
<td>None</td>
<td>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 passed to Oracle Identity Management.</td>
</tr>
</tbody>
</table>

If user accounts:

- Are created automatically, then role provisioning occurs automatically, as specified by current role mappings when the accounts are created.
- Aren’t created automatically, then role requests are held in the LDAP requests table, where they’re identified as Suppressed. They’re not passed to Oracle Identity Management.

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

- Create user accounts individually in Oracle Identity Manager.
- Link existing Oracle Identity Management user accounts to person and party records using the Manage User Account or Manage Users task.

Alternatively, you can use a provisioning infrastructure other than Oracle Identity Management 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.
Default User Name Format Option: Explained

The **Default User Name Format** option controls the default format of user names for the enterprise. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **Default User Name Format** option values.

<table>
<thead>
<tr>
<th>Format Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Defined by Oracle Identity Management</strong></td>
<td>The user name follows the Oracle Identity Management user-name policy. By default, Oracle Identity Management uses the person’s first and last names. To make duplicate user names unique, Oracle Identity Management includes either the person’s middle name or a random alphabetic character. To change the Oracle Identity Management user-name policy, Oracle Applications Cloud customers submit a service request. The Oracle Identity Management user-name format is used automatically unless you select a different value for the <strong>Default User Name Format</strong> option.</td>
</tr>
<tr>
<td><strong>Party number</strong></td>
<td>The party number is the user name.</td>
</tr>
<tr>
<td><strong>Person number</strong></td>
<td>The HCM person number is the user name. For party users who have no person number, the party e-mail is used instead when person number is the default user name.</td>
</tr>
<tr>
<td><strong>Primary work e-mail</strong></td>
<td>The primary work e-mail (or party e-mail, for party users) is the user name.</td>
</tr>
</tbody>
</table>

A person’s party number, person number, or e-mail may not be available when the user account is requested. In this case, the account status is **Failed** until the value becomes available and you resubmit the request. If you run the Send Pending LDAP Requests process daily, then the request is likely to be resubmitted when the value becomes available. Alternatively, for individual requests, you can perform the **Process User Account Request** action on the Manage User Account page.

Human resource specialists (HR specialists) and line managers can enter user names, and thereby override default user names, when hiring workers. HR specialists can edit user names for individual users on the Edit User and Manage User Account pages.

User Account Role Provisioning Option: Explained

Existing users both acquire and lose roles as specified by current role-provisioning rules. For example, a user may request some roles and acquire others automatically. All provisioning changes are role requests that are sent to Oracle Identity Management 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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both person and party users</td>
<td>Role provisioning and deprovisioning occur for both person and party users.</td>
</tr>
<tr>
<td></td>
<td>This value is the default value.</td>
</tr>
<tr>
<td>Party users only</td>
<td>Role provisioning and deprovisioning occur for party users only.</td>
</tr>
<tr>
<td></td>
<td>For person users, role requests are held in the LDAP requests table, where they're identified as Suppressed. They're not passed to Oracle Identity Management.</td>
</tr>
<tr>
<td>None</td>
<td>For both person and party users, role requests are held in the LDAP requests table, where they’re identified as Suppressed. They’re not passed to Oracle Identity Management.</td>
</tr>
</tbody>
</table>

**User Account Maintenance Option: Explained**

By default, user accounts are suspended automatically when the user has no roles. In some circumstances (for example, following a rehire) user accounts are reactivated automatically when the user acquires roles again. In addition, some person information is sent to Oracle Identity Management automatically when you update a person record. 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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both person and party users</td>
<td>User accounts are maintained automatically for both person and party users.</td>
</tr>
<tr>
<td></td>
<td>This value is the default value.</td>
</tr>
<tr>
<td>Party users only</td>
<td>User accounts are maintained automatically for party users only.</td>
</tr>
<tr>
<td></td>
<td>For person users, account-maintenance requests are held in the LDAP requests table, where they're identified as Suppressed and not passed to Oracle Identity Management.</td>
</tr>
<tr>
<td></td>
<td>Select this value if you maintain accounts for person users in some other way.</td>
</tr>
</tbody>
</table>
For both person and party users, account-maintenance requests are held in the LDAP requests table, where they’re identified as Suppressed and not passed to Oracle Identity Management.

Select this value if you maintain accounts for both person and party users in some other way.

You can maintain any Oracle Identity Management user account automatically, even if you created it outside Oracle Fusion Applications.

**Attributes Sent to Oracle Identity Management**

By default, the values of the following attributes are sent to Oracle Identity Management automatically whenever you update them:

- Person number
- System person type from the person's primary assignment
- The Globally Unique Identifier (GUID) of the manager of the person's primary assignment
- Work phone
- Work fax
- Both local and global versions of the person's display name
- Global versions of the following name components:
  - First name
  - Middle name
  - Last name
  - Name suffix
- Both the formatted work-location address and the following components of the work-location address from the person's primary assignment:
  - Address line 1
  - City
  - State
  - Postal code
The application sends equivalent information for party users to Oracle Identity Management.

**Send User Name and Password Option: Explained**

When Oracle Identity Management creates a user account, it may send an e-mail containing the user name and password to a specified recipient. The **Send User Name and Password** option controls whether Oracle Identity Management sends this e-mail. Use the Manage Enterprise HCM Information task to set this option for the enterprise.

This table describes where Oracle Identity Management sends the user-credentials e-mail when you set **Send User Name and Password** to **Yes**.

<table>
<thead>
<tr>
<th>E-Mail Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternate contact e-mail</td>
<td>Oracle Identity Management sends e-mails for all new accounts in the enterprise to this single address. You can specify an alternate contact e-mail when you perform the Manage Enterprise HCM Information task.</td>
</tr>
<tr>
<td>User’s primary work e-mail</td>
<td>Used if:</td>
</tr>
<tr>
<td></td>
<td>• You specify no alternate contact e-mail.</td>
</tr>
<tr>
<td></td>
<td>• The user’s primary work e-mail exists.</td>
</tr>
<tr>
<td>Primary work e-mail of the user’s line manager</td>
<td>Used if:</td>
</tr>
<tr>
<td></td>
<td>• You specify no alternate contact e-mail.</td>
</tr>
<tr>
<td></td>
<td>• The user’s primary work e-mail doesn’t exist.</td>
</tr>
<tr>
<td></td>
<td>• The primary work e-mail of the user’s line manager exists.</td>
</tr>
<tr>
<td>None</td>
<td>Oracle Identity Management sends no e-mail if:</td>
</tr>
<tr>
<td></td>
<td>• You specify no alternate contact e-mail.</td>
</tr>
<tr>
<td></td>
<td>• The user’s primary work e-mail doesn’t exist.</td>
</tr>
<tr>
<td></td>
<td>• The primary work e-mail of the user’s line manager doesn’t exist.</td>
</tr>
</tbody>
</table>
Note

Send User Name and Password is set to Yes by default. Set this option to No if you don’t want user credentials to be sent as users are created.

When Send User Name and Password Is No

If you set Send User Name and Password to No, then Oracle Identity Management sends no e-mails.

In this case, you can:

- Request e-mails for individual users on the Create User or Manage User Account page. If the user has no primary work e-mail, then Oracle Identity Management sends the e-mail to the user's line manager, if available. Oracle Identity Management doesn’t send it to the alternate contact e-mail.

- Run the process Send User Name and Password E-Mail Notifications. This process sends e-mails for all users for whom e-mails haven’t yet been sent. The process sends e-mails to users or their line managers. It doesn’t send them to the alternate contact e-mail.

Note

E-mails containing user names and passwords are sent once only for any user.

Setting the User and Role Provisioning Options: Procedure

The user and role provisioning options control the creation and management of user accounts for the enterprise. This procedure explains how to set these options. For the typical case, where accounts are created and maintained automatically for all users, you can use the default settings.

Accessing the User and Role Provisioning Options

1. Select Navigator - Setup and Maintenance to open the Setup and Maintenance work area.
2. On the All Tasks tab, 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.

Setting the User Account Options

The User Account Options are:

- User Account Creation
- User Account Role Provisioning
• User Account Maintenance
• Default User Name Format

These options are independent of each other. For example, you can set User Account Creation to None and User Account Role Provisioning to Yes. The Default User Name Format value applies only to user accounts that are created automatically.

Setting E-Mail Options

The e-mail options are Send User Name and Password and Alternate Contact E-Mail Address.

1. Select a Send User Name and Password value.
2. Enter an e-mail in the Alternate Contact E-Mail Address field if:
   - Send User Name and Password is Yes.
   - All user names and passwords must be sent to this single e-mail.
   - If Send User Name and Password is No or the users themselves must receive the e-mails, then leave this field blank.
3. Click Submit.

Oracle Applications Cloud Password Policy: Explained

Oracle Identity Management defines the validation rules for user sign-in passwords.

By default, user sign-in passwords must be at least 6 characters long, start with an alphabetic character, and contain at least:

• 2 alphabetic characters
• 1 numeric character
• 1 uppercase letter
• 1 lowercase letter

In addition, passwords must not be the same as or contain the user's:

• First name
• Last name
• User name

Password Policy Update

To change the default Oracle Identity Management password policy in Oracle Applications Cloud, submit a service request.
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 to Oracle Fusion Applications. This topic explains how to set up automatic role provisioning during implementation using the Manage Role Provisioning Rules task. (You can also use the Manage HCM Role Provisioning Rules task.)

Provisioning the Employee Role Automatically to Employees

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. On the All Tasks tab, 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 Create. 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>
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, search for and select the Employee role.
9. If Autoprovision isn’t selected automatically, then select it.
10. Ensure that the Requestable and Self-Requestable options aren’t selected. 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, use Contingent Worker as the mapping name.
- In step 6, set System Person Type to Contingent Worker.
• In step 8, search for and select the Contingent Worker role.

Provisioning the Line Manager Role Automatically to Line Managers

1. In the Search Results section of the Manage Role Mappings page, click Create. 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
<tr>
<td>Manager with Reports</td>
<td>Yes</td>
</tr>
<tr>
<td>Manager Type</td>
<td>Line Manager</td>
</tr>
</tbody>
</table>

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, search for and select the Line Manager role.
6. If Autoprovision isn’t selected automatically, then select it.
7. Ensure that the Requestable and Self-Requestable options aren’t selected.
   Click Save and Close.
8. On the Manage Role Mappings page, click Done.

Note
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, within and across product families. Submit a service request for implementation of single sign-on.
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.

To perform Create User, you must have the Human Resource Specialist job role. Sign in and follow these steps:

1. Select **Navigator - Manager Resources - 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 an e-mail containing the user name and a temporary password is sent when the account is created. This option is selected by default if these e-mails are enabled for the enterprise.

When the **Send user name and password** option is selected, the e-mail is sent to:

1. The enterprise e-mail address, if it exists and sending of e-mails is enabled for the enterprise.
2. The user, if no enterprise e-mail address exists.
3. The user’s line manager, if the user’s e-mail address doesn’t exist.

If none of these addresses exists, then no e-mail is sent.

If you deselect this option, then you can send the e-mail later by running the process Send User Name and Password E-Mail Notifications.

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 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.

   **Tip**
   Roles that you can provision to others 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 sent to Oracle Identity Management when you click **Save and Close**.

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

**Importing Users: Explained**

You can import workers from legacy applications to Oracle Fusion Applications using the Import Worker Users task. You can access this task from the Setup and Maintenance work area. By enabling you to bulk-load existing data, this task is an efficient way of creating and enabling users of Oracle Fusion Applications.

The Import Worker Users Process

Importing worker users is a two-stage process:

1. When you perform the Import Worker Users task, the Initiate Spreadsheet Load page opens. On the Initiate Spreadsheet Load page, you generate and complete the Create Worker spreadsheet. You must map your data to the spreadsheet columns and provide all required attributes. Once the spreadsheet is complete, you click **Upload** in the spreadsheet to import the data to the Load Batch Data stage tables.

2. As the upload process imports valid data rows to the Load Batch Data stage tables, the Load Batch Data process runs automatically. Load Batch Data is a generic utility for loading data to Oracle Fusion Human Capital Management from external sources. This process loads data from the Load Batch Data stage tables to the Oracle Fusion application tables.

User-Account Creation

The application creates Oracle Fusion user accounts automatically for imported workers in Oracle Identity Management (OIM), unless automatic account creation is disabled.

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

- User account names and passwords may be sent to an enterprise-wide e-mail rather than to users themselves.
- Automatic sending of user account names and passwords may be disabled for the enterprise. In this case, you can notify users at an appropriate time.
Role Provisioning
Once user accounts exist, roles are provisioned to users automatically in accordance with current role-provisioning rules. For example, current rules could provision the employee abstract role to every worker. Role provisioning occurs automatically unless it’s disabled for the enterprise.

Related Topics
- Uploading Data Using HCM Spreadsheet Data Loader: Explained
- User and Role-Provisioning Setup: Critical Choices

Importing Users: Worked Example
This example shows how to import worker users from legacy applications to Oracle Fusion Applications. The following table summarizes key decisions for this task.

<table>
<thead>
<tr>
<th>Decisions to Consider</th>
<th>In This Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s my spreadsheet name?</td>
<td>WorkersMMDDYYBatchnn. xlsx</td>
</tr>
<tr>
<td>You can define your own naming convention. In this example, the name is selected to make identifying the spreadsheet contents easy.</td>
<td>For example, Workers042713Batch01. xlsx.</td>
</tr>
<tr>
<td>What’s my batch name?</td>
<td>Workers042713Batchnn</td>
</tr>
<tr>
<td>You can define your own batch name, which must be unique. In this example, the batch name is the same as the spreadsheet name.</td>
<td></td>
</tr>
</tbody>
</table>

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

Prerequisites
Before you can complete this task, you must have:
1. Installed the desktop client Oracle ADF Desktop Integration Add-in for Excel
2. Enabled the Trust Center setting Trust access to the VBA project object model in Microsoft Excel
Selecting the Import Worker Users Task

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Task</td>
</tr>
<tr>
<td>Name</td>
<td>Import Worker Users</td>
</tr>
</tbody>
</table>

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

The Initiate Spreadsheet Load page opens.
Alternatively, you can select the Import Worker Users task from an implementation project.

Creating the Spreadsheet

1. On the Initiate Spreadsheet Load page, find the entry for Create Worker in the list of business objects.
2. Click Create Spreadsheet for the Create Worker entry.
3. When prompted, save the spreadsheet locally using the name Workers042713Batch01.xlsx.
4. When prompted, sign in to Oracle Fusion Applications using your Oracle Fusion user name and password.

Entering Worker Data in the Spreadsheet

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

Importing Worker Data and Correcting Import Errors

Use the default values except where indicated.

1. In the workers spreadsheet, click Upload.
2. In the Upload Options window, click OK.
   As each row of data uploads to the Load Batch Data stage tables, its status updates.
3. When uploading completes, identify any spreadsheet rows with the status Insert Failed, which indicates that the row didn't import to the stage tables.
4. For any row that failed, double-click the status value to display a description of the error.
5. Correct any import errors and click **Upload** again to import the remaining rows to the same batch. As rows import successfully to the stage tables, the data loads automatically to the application tables.

### Reviewing and Correcting Load Errors

1. In the spreadsheet, click **Refresh** to display latest load status. Any errors that occur during the load process appear in the spreadsheet.
2. Correct any load errors in the spreadsheet.
3. Repeat this process from Importing Worker Data and Correcting Import Errors until all spreadsheet rows both import and load successfully.
4. Close the spreadsheet.
   - To load a second batch of worker users on the same date, increment the batch number in the spreadsheet and batch names (for example, Workers042713Batch02).

### Inactive Users Report Reference

The Inactive Users Report identifies users who have not signed in for a period of time that you define. Run the report as a scheduled process. Use the Scheduled Processes work area, available from the Navigator.

In the Scheduled Processes work area:

1. As a prerequisite, run the Import User Login History process. (This process takes no parameters.)
2. As you run the process that generates the Inactive Users Report, set parameters:
   - Define the inactivity period, in days. This is the only required parameter, and its default value is 30.
   - Filter the users who may be included in the report, by name, department, location, or last-activity start or end date. The use of these parameters is optional.

### Report Results

The process returns an XML file that provides the following information about each inactive user:

- The number of days the user has been inactive.
- The user’s user name, given name, surname, location, and department.
- The user’s status.

### 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 and select the person whose account you're updating. The Person Management work area opens.
3. In the Tasks pane, click 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 Oracle Identity Management. 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 for which those users qualify.

Copying Personal Data to LDAP
By default, changes to personal data, such as person name and phone, are copied to the Oracle Identity Management LDAP directory periodically. To copy any changes to LDAP 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 temporary password to the user's primary work e-mail.

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**.

3. Click **Save**.

This action sends the updated user name to Oracle Identity Management. Once Oracle Identity Management has processed the request, 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, autopropose roles, and copy their personal data to LDAP by selecting **About Me - My Account** from the home page.

Line managers can add and remove roles, autopropose roles, and copy personal data to LDAP for their reports from the person gallery and the Manager Resources dashboard.

---

### 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 default formats.

<table>
<thead>
<tr>
<th>Default User-Name Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined by Oracle Identity Management</td>
<td>Oracle Identity Management generates the user name, typically using first and last names.</td>
</tr>
<tr>
<td>Person number</td>
<td>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.</td>
</tr>
<tr>
<td>Work e-mail</td>
<td>If you enter a work e-mail, then that value becomes the user name. Otherwise, the work e-mail that Oracle Identity Management defines becomes the user name.</td>
</tr>
</tbody>
</table>

#### Existing User Names

HR specialists can change an existing user name on the Manage User Account page. Select **My Workforce - Person Management** from the home page. Search for and select the worker. In the Person Management work area, select **Manage User Account**, then **Actions - Edit User Name**.

The updated name, which can be in any format, is sent automatically to Oracle Identity Management.
When you change an existing user name, the user’s password and roles remain the same. 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

Oracle Identity Management maintains Lightweight Directory Access Protocol (LDAP) user accounts for users of Oracle Fusion Applications. By default, Oracle Fusion HCM (HCM) sends some personal information about users to Oracle Identity Management. This information includes the person number, person name, phone, and manager of the person’s primary assignment. HCM sends these details to Oracle Identity Management to ensure that HCM and Oracle Identity Management hold the same information about users.

This topic describes how and when you can send personal information explicitly to Oracle Identity Management.

### Bulk Creation of Users

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

When you load person records in bulk, the order in which they’re created in HCM 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 sends no manager details for the person to Oracle Identity Management. The Oracle Identity Management information therefore differs from the information that HCM holds for the person. To correct any differences between the Oracle Identity Management and HCM versions of personal details, you run the process Send Personal Data for Multiple Users to LDAP.

### The Send Personal Data for Multiple Users to LDAP Process

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

<table>
<thead>
<tr>
<th>User Population</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All users</td>
<td>The process sends personal details for all users to Oracle Identity Management, regardless of whether they have changed since personal details were last sent to Oracle Identity Management.</td>
</tr>
<tr>
<td>Changed users only</td>
<td>The process sends only personal details that have changed since details were last sent to Oracle Identity Management (regardless of how they were sent). This option is the default setting.</td>
</tr>
</tbody>
</table>

**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 role to run this process.

### The Copy Personal Data to LDAP Action

Users can copy their own personal data to Oracle Identity Management 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 Oracle Identity Management. However, this action is available for copying changes to Oracle Identity Management immediately, if necessary.

**Related Topics**
- Synchronization of User and Role Information with Oracle Identity Management: How It’s Processed
- 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 to Oracle Identity Management 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, 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

You can’t delete a user account. However, 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** option. Human resource specialists can also suspend a user account manually, if necessary. This topic describes how automatic account suspension occurs and explains how to suspend a user account manually.

#### Work Relationship Termination

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.

Reactivation of User Accounts
If you reverse the termination of a work relationship, then:

- The user regains any role that he or she lost automatically at termination.
  
  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.

You can autoprovision roles on the Manage User Account page to update the automatic provisioning of roles for a reinstated worker.

When you rehire a worker, the user account is reactivated automatically and roles are provisioned automatically in accordance with current role provisioning rules.

In all other cases, you must reactivate suspended user accounts manually, either on the Edit User page or directly in Oracle Identity Management.

Manual Suspension of User Accounts
To suspend a user account manually, select My Team - Manage Users on the home page. On the Edit User page, set the User Account Status value to Inactive. You can reactivate the account by setting the User Account Status value back to Active. You can also manage user account status directly in Oracle Identity Management.

Note
Role provisioning isn’t affected by the manual suspension and reactivation of user accounts. For example, when you reactivate a user account, the user’s autoprovisioned roles aren’t updated unless you click Autoprovion Roles. Similarly, a suspended user account isn’t reactivated when you click Autoprovion Roles. You must explicitly reactivate the user account first.

Related Topics
- User Account Maintenance Option: Explained

Running the User Details System Extract Report: Procedure
The Oracle BI Publisher User Details System Extract Report includes details of some or all Oracle Fusion Applications user accounts.

To run this report, you must have an HCM data role that provides view-all access to person records for the Human Capital Management Application Administrator job role.

To run the report:

1. On the home page, select Tools - Reports and Analytics.

3. Select the User Details System Extract report.

4. In the report window, click More.

5. On the Oracle Business Intelligence page for the report, select Open to run the report immediately or Schedule to schedule the report.

User Details System Extract Report Parameters

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

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCM</td>
<td>User accounts with an associated HCM person record.</td>
</tr>
<tr>
<td>TCA</td>
<td>User accounts with an associated party record.</td>
</tr>
<tr>
<td>OIM</td>
<td>Accounts for users in the PER_USERS table who have no person number or party ID. Implementation users are Oracle Identity Management users.</td>
</tr>
<tr>
<td>ALL</td>
<td>HCM, TCA, and Oracle Identity Management users accounts.</td>
</tr>
</tbody>
</table>

From Date

Accounts for HCM and Oracle Identity Management 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 Oracle Identity Management 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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Include active accounts, which belong to users with current roles.</td>
</tr>
<tr>
<td>I</td>
<td>Include inactive accounts, which belong to users with no current roles.</td>
</tr>
<tr>
<td>All</td>
<td>Include both active and inactive user accounts.</td>
</tr>
</tbody>
</table>

**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 Oracle Identity Management 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.

Oracle Identity Management User Accounts

Start Date
The account’s start date.

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

FAQs for Creating and Managing Application Users

Where do default user names come from?
By default, user names are defined in Oracle Identity Management. The format is typically the user’s first and last names, but this format can be changed in Oracle Identity Management.

The Oracle Identity Management format can also be overridden for the enterprise in Oracle Applications Cloud. Your enterprise may be using person number, party number, or primary work e-mail in place of the Oracle Identity Management format.
Why did some roles appear automatically?

Roles appear automatically for a user when:

- The user’s assignment attributes, such as person type and job, match the conditions specified for the role in a role mapping.
- In the role mapping, the role has the **Autoprov**ision option selected.

How can I create a user?

If you want to create application users, perform 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.

**Note**

If you are creating implementation users enterprise setup, use the Create Implementation Users task. It opens the integrated Oracle Identity Management pages where you can create implementation users and provision roles to them.

Related Topics

- Creating Partner User Accounts: Explained

What happens when I autoprov provision 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 autoprov provision 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, 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, 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 Oracle Identity Management 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 primary work e-mail of the user or user’s line manager, if any.
You can send these details once only for any user. If you deselect this option on the Manage User Account or Create User page, 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 from the Scheduled Processes work area.
For users for whom you haven’t so far requested an e-mail, this process resets passwords and sends out user names and passwords. The e-mail goes to the primary 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.
Role Mappings: Explained

Roles provide user 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. You provision all types of roles using role mappings. This topic describes role mappings for automatic and manual role provisioning. 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 data role Cost Accountant Finance Department, you could select the Autoprovision option and specify the following conditions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Finance Department</td>
</tr>
<tr>
<td>Job</td>
<td>Cost Accountant</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

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**

Automatic provisioning of roles to users is a request to Oracle Identity Management to provision the role. Oracle Identity Management may reject the request if it fails a custom Oracle Identity Management approval process, for example.

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.
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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>ABC Department</td>
</tr>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
</tbody>
</table>

Any user with at least one assignment that matches these conditions can request the role. The user acquires the role either immediately or after approval. 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. On the home page, click **Setup and Maintenance** to open the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Materials Management Department</td>
</tr>
<tr>
<td>Job</td>
<td>Warehouse Manager</td>
</tr>
<tr>
<td>Location</td>
<td>Seattle Distribution Center</td>
</tr>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

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 data role **Procurement Analyst Denver**.

3. Select one or more of the role-provisioning options:
### Role-Provisioning Option

<table>
<thead>
<tr>
<th>Role-Provisioning Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestable</td>
<td>Qualifying users can provision the role to other users.</td>
</tr>
<tr>
<td>Self-Requestable</td>
<td>Qualifying users can request the role for themselves.</td>
</tr>
<tr>
<td>Autoprovision</td>
<td>Qualifying users acquire the role automatically.</td>
</tr>
</tbody>
</table>

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

**Important**

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. Therefore, no further action is necessary to put new role mappings that include autoprovisioned roles into effect.

### 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 both predefined and custom data roles, abstract roles, and job roles to users.

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 (if you request immediate deprovisioning) 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.

Reversing a termination reinstates any roles that the user lost automatically at termination and removes any that the user acquired automatically at termination.

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. Oracle Identity Management processes the requests 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 and after loading person records 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.

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 LDAP Daily Processes: Procedure

Role Provisioning Status Values: Explained

The status value of a role request describes the request’s progress. This topic describes the request status values, which appear on the Manage User Account, New Person Roles, Create User, and Edit User pages.

Role Provisioning Status Values and Their Meanings

This table describes status values for role provisioning requests.
### Status  |  Meaning
--- | ---
Complete | The request completed successfully. The user has the role.
Failed | The request failed, and the role wasn’t provisioned to the user. The associated error message provides more information.
Partially complete | The request is in progress.
Pending | Oracle Identity Management received the request but processing hasn’t yet started.
Rejected | The request was rejected, and the role wasn’t provisioned to the user. An associated error message may provide more information.
Requested | The request was made but Oracle Identity Management hasn’t yet acknowledged it.

---

### User and Role Access Audit Report Reference

The User and Role Access Audit Report documents role hierarchies. Run the report to view all roles, privileges, and data security policies for:

- One user.
- All users.
- One role.
- All roles.

Run the User and Role Access Audit Report as a scheduled process. Use the Scheduled Processes work area available from the Navigator. As you run the process, set parameters that focus the report on a user you select, all users, a role you select, or all roles.

### Report Results

The process returns archive (ZIP) files. Each file name contains a prefix and a suffix that define its content. (Each file name also contains values that identify the process number, and the process run date and time.)

If you select an individual user, the process returns:
If you select an individual role, the process returns:

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ DataSec.zip</td>
<td>One XML file documenting data security policies that apply to the selected user.</td>
</tr>
<tr>
<td>USER_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ Hierarchical.zip</td>
<td>One XML file that documents functional security for the selected user. Its format depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td>USER_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ TabularFormat.zip</td>
<td>One XML file that documents functional security for the selected user. Its format is tabular (flattened).</td>
</tr>
</tbody>
</table>

If you select all users, the process returns:

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL_USERS_ [PROCESS]_ [DATE]_ [TIME]_ DataSec.zip</td>
<td>Multiple XML files, one for each user. Each documents data security policies that apply to its user.</td>
</tr>
<tr>
<td>ALL_USERS_ [PROCESS]_ [DATE]_ [TIME]_ Hierarchical.zip</td>
<td>Multiple XML files, one for each user. Each documents functional security for its user, in a format that depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td>ALL_USERS_ [PROCESS]_ [DATE]_ [TIME]_ CSV.zip</td>
<td>A comma-separated-values file that documents functional security for all users in a tabular (flattened) format.</td>
</tr>
</tbody>
</table>

If you select all roles, the process returns:
Oracle Supply Chain Management Cloud
Securing Oracle SCM Cloud

Chapter 5
Provisioning Roles to Application Users

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL_ROLES_[PROCESS]<em>[DATE]</em>[TIME]_DataSec.zip</td>
<td>Multiple XML files, one for each role. Each documents data security policies that apply to its role.</td>
</tr>
<tr>
<td>ALL_ROLES_[PROCESS]<em>[DATE]</em>[TIME]_Hierarchical.zip</td>
<td>Multiple XML files, one for each role. Each documents functional security for its role, in a format that depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td>ALL_ROLES_[PROCESS]<em>[DATE]</em>[TIME]_CSV.zip</td>
<td>A comma-separated-values file that documents functional security for all roles in a tabular (flattened) format.</td>
</tr>
</tbody>
</table>

The process also returns a diagnostic log (in the form of a ZIP file).

**FAQs for Provisioning Roles to Application Users**

**What's a role-mapping condition?**
Most are assignment attributes. At least one of a user’s assignments must match all assignment values that you specify in the role mapping if the user is to qualify for the associated roles.

**What's an associated role in a role mapping?**
Any role that you want to provision to users. Such roles can include Oracle Fusion Applications predefined roles, custom roles, and HCM data roles.

**What's the provisioning method?**
The provisioning method identifies how the user acquired the role. This table describes its values.

<table>
<thead>
<tr>
<th>Provisioning Method</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic</td>
<td>The user qualifies for the role automatically based on his or her assignment attribute values.</td>
</tr>
<tr>
<td>Manual</td>
<td>Either another user assigned the role to the user, or the user requested the role.</td>
</tr>
<tr>
<td>External</td>
<td>The user acquired the role outside Oracle Applications Cloud.</td>
</tr>
</tbody>
</table>
How can I view or change the data security policies carried by job, abstract, and data roles?

Use the Manage Data Security Policies task to view or change data security policies. To perform this task, you'll use the integrated Authorization Policy Manager.

Oracle Fusion data security stores data security policies in the policy store.

How can I view the duties included in a job role?

Use the Manage Duties task to view the duties inherited by a role. To perform this task, you'll use the Authorization Policy Manager.

Each logical partition or pillar contains a collection of application roles representing duties, and the function and data security policies carried by those roles.

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, and Oracle Fusion Suppliers.

You provision roles to implementation users in Oracle Identity Management (OIM), prior to HCM setup. After implementation is complete, the Provision Roles to Implementation Users task is no longer necessary. Use the Manage Users task to provision roles to non-implementation users.

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

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

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

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 enterprise roles provide access to tasks through the inherited duty roles.

The duty roles in a role hierarchy carry privilege to access functions and data. You don't assign duty roles directly to users. Instead, duty roles are assigned to enterprise 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

Don’t change the predefined application roles. (In the Security Console, you can identify predefined application roles by the **ORA_** prefix in the Role Code field.) Create copies and update the copies instead.

Users are generally provisioned with roles based on role provisioning rules. If a user requests a role to access a task, always review the security reference implementation to determine the most appropriate role.
6 Customizing Security

Customizing Security: Points to Consider

You can customize security and tailor it to meet business requirements that are specific to your organization. Before you perform any security customizations, familiarize yourself with the possible impact.

Security Customization Considerations

Before you make any security customizations, consider the following:

- You must not customize predefined roles. (In the Security Console, you can identify predefined application roles by the ORA_prefix in the Role Code field.) During each upgrade, predefined roles are updated to the specifications for that release, so any customizations would be overwritten.
- Instead, always make a copy of the predefined role. Then, edit the copy and save it as a custom role.
- Making your changes in a copy of a predefined role means that you can always compare to and roll back to the delivered role.
- After a maintenance update or upgrade, you can compare your customized copy to the updated predefined source role. You can see the updates to the predefined role and decide whether to incorporate them into your custom role.

Related Topics

- Reviewing Predefined Roles: Explained
- Copying Roles in the Security Console: Explained
- Comparing Roles: Procedure

Managing Resources and Roles

Creating an Authorization Policy: Procedure

The authorization policy is the mechanism that defines access rights. A user, an application role, or an external role is granted or denied the rights of the policy.

An authorization policy must have:

- At least one principal which can be a user, an external role, or an application role. Code sources are not allowed as a principal.
- At least one target that can either be a resource and action association (created within the policy) or an entitlement (created outside the policy and added to it), but not both.

Note

Entitlement-based policies correspond closely with business functions. They are recommended in cases in which a business function considers securing a collection of resources. An entitlement can be used in one or more grants.
Warning

It is recommended that you do not create target-based authorization policies. Oracle Applications Cloud supports a set of real world actions (business functions) through the use of a set of predefined entitlements that have been thoroughly tested. Each entitlement contains all the permissions a user needs to complete the real world action indicated by the entitlement name.

To create a policy:

1. From the Setup and Maintenance work area, go to the Manage Duties task. The Authorization Policy Manager opens.

2. Access the policy creation page:
   a. In the Navigation Pane, navigate to the policy domain under the appropriate application node and expand it.
   b. Right-click Authorization Policies from the resource catalog node and from the context menu, select New.

3. Enter the required policy details.
   The display name is optional and case insensitive. Specify a meaningful display name. It provides extra information to help administrators identify objects.

   The name is required and case insensitive. At runtime, this is the string that the application uses to determine whether a user is authorized to access this resource.

4. Add principals to the authorization policy:
   a. Use the Navigation Panel to search for users, external roles or application roles and see a list of the available principals in the application.
   b. Drag and drop principals from the search results tab on to the area labeled Principals. Although APM enables you to select users, external roles, and application roles as principals, for Fusion Cloud purposes you should select only application roles.
   c. Select Any or All depending upon the requirement.

   a. If you select Any, the user must match at least one of the specified principals. For example, if the principals are roles, the user must be a member of at least one of the roles for the authorization policy to apply. If you select All, the user must match all of the specified principals. For example, if the principals are roles, the user must be a member of all of them for the authorization policy to apply.

5. Add targets to the authorization policy:
   a. Use the Navigation Panel for performing a search to list the available resources or entitlements. Look for these objects in the same policy domain to which you are adding the authorization policy.
   b. Drag and drop one or more resources or entitlements from the Search Results tab into the section labeled Targets.
   c. Expand the added object in the Targets section to associate an action with it, and click Add.
6. Click **Save** to save the Authorization Policy.

## Managing Application Roles: Overview

Application roles are defined at the application or service level. You can assign application roles to external roles, users, or groups in an identity store, or another application role in the security store.

A target application may have several different roles, with each role assigned a different set of privileges for more fine-grained authorization. Membership can be granted statically to external roles or individual users.

You can use application roles to control access by establishing the following relationships:

1. Define application roles to represent the functional roles users have in the application.
2. Map each application role to external roles or individual users.
3. Create authorization policies to provide the level of access rights required to meet the goals of the application roles.
4. Add the application role as a principal to one or more authorization policies.

Application roles use role inheritance and hierarchy. The subject assigned to a role using static role assignments also inherits any child roles. When an application role is referenced as a principal in a policy, access to the resource for all users assigned to the role is governed by the policy.

## Creating an Application Role and a Role Category: Procedure

Application roles enable you to aggregate privileges to the pages and other objects necessary to perform designated operations for specific tasks in a specific application. You create application roles using Oracle Entitlements Server, which provides access to the role catalog of each application. When you create and save the application role, you can either configure it and add assignees immediately or return to the saved role later.

A role category is a tag that you can assign to a role for ease of management. You can create or delete a role category but you cannot modify it.

To create an application role, proceed as follows:

1. Use the Manage Duties task in the Setup and Maintenance work area to access the administration console of the Oracle Entitlements Server.
2. Select the parent application from the **Application Name** list on the Home tab. Under Application Roles, click **New**.
3. Use the following table as a guide to enter the required information on the General tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display Name</strong></td>
<td>Insensitive</td>
<td>Enter a meaningful display name that provides extra information to help administrators identify the object.</td>
</tr>
<tr>
<td><strong>Role Name</strong></td>
<td>Insensitive</td>
<td>At run time, the application uses this value to determine whether a user is authorized to access this resource.</td>
</tr>
<tr>
<td>Field</td>
<td>Case</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Insensitive</td>
<td>Enter useful information in the description about the entitlement.</td>
</tr>
<tr>
<td>Role Category</td>
<td>Insensitive</td>
<td>Select a tag from the list that would be helpful in organization and management.</td>
</tr>
</tbody>
</table>

In addition to the General tab, three disabled tabs appear. Saving the application role enables the disabled Application Role Hierarchy, External Role Mapping, and External User Mapping tabs.

Optionally, select the Application Role Hierarchy tab to define from which roles this application role inherits permissions (Inherits) and for which roles permissions are defined by (are Inherited By) this application role. Setting up a hierarchy is not required but if you define it, use the following sub procedure:

a. Click Inherits and click **Add**.

b. Select the radio button that corresponds to the role to which you are adding the hierarchy. You can add the roles to the role with which you are working or to a role in the Application Role Hierarchy table.

c. Complete the criteria fields in the Add a Role dialog box and click **Search**. The results display in the Search Results table. Empty strings return all roles.

d. Select the role from which this role inherits permissions in the Search Results table. To select multiple roles, use Ctrl key and mouse click together while selecting roles.

e. Click **Add**. The selected roles display in the Application Role Hierarchy tab, and the application role inherits permissions from them.

To create a role category, proceed as follows:

1. Expand the appropriate application node in the Navigation Panel and double-click the Role Categories node. The Role Categories page opens in the Home area.

2. Click New to display the New Category dialog box.

3. Provide the required details and click **Create**. The new category displays in the Role Categories list.

### Mapping External Roles to an Application Role: Procedure

To map external roles to an application role:

1. Select one of the following methods to display the desired application role:
   - Expand the information tree in the Navigation Panel to find the Role Catalog node under the appropriate Application and double click it. A search dialog box appears in the Home area.
   - In the Home area, select the Application Name under which the Application Role was created and under Application Roles, click Search. A search dialog box appears in the Home area.
2. Enter query parameters and click **Search**. The search results are displayed.

3. Select the appropriate Application Role and click **Open** to display the details. Alternately, search for Application Roles using the Navigation Panel search function and double-click the application role name on the Search Results tab to display the details.

4. Click the External Role Mapping tab, and click **Add**. The Add a Role dialog box appears.

5. Complete the query fields in the Add a Role dialog box and click **Search**. The results display in the External Role Search table.

6. Click the name of the external map in the table for mapping. To select multiple roles, press and hold the Ctrl key when you click.

7. Click **Map Roles**. The selected roles display on the External Role Mapping tab.

---

**Managing Data Roles**

**Data Role Templates: Explained**

A role template, or data role template, is a set of attributes that specify how your application constructs your data roles. The role template combines a set of base roles with a set of dimension values for a set of data security policies. You can use the Manage Role Templates task to access the integrated Authorization Policy Manager (APM) where you create and maintain data role templates that generate data roles.

**Template Attributes**

The following attributes compose data role templates:

- Template name
- Template description
- Template group ID
- Base roles
- Data dimension
- Data security policies
- Data role naming rule

---

**Note**

The integrated Oracle Identity Manager (OIM) and Authorization Policy Manager (APM) refer to abstract and data roles as external roles. APM also refers to duty roles as application roles, and scopes each to a particular application. A job role is an external role in OIM, but it also has a representation in the APM application-role hierarchy.

**Attribute Details**

This table describes components a data role template comprises.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base roles</td>
<td>Parent job or abstract roles of the data roles.</td>
<td>Financial Application Administrator</td>
</tr>
</tbody>
</table>
### Attribute Description Example

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimension</td>
<td>The stripe of data that an enterprise uses to partition transactional data.</td>
<td>Business unit = APAC</td>
</tr>
<tr>
<td>Data security policy</td>
<td>Grants an action on a database resource</td>
<td>Grant the manage payable invoice action on the PAYABLES_INVOICES business object</td>
</tr>
<tr>
<td>Role naming rule</td>
<td>How to construct the name, code, and description of the generated data roles.</td>
<td>[ROLE_CODE]:[BU_CODE]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ROLE_NAME]:[BU_NAME]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Role [ROLE_NAME] implementing Manage Payables Invoices on [BU_NAME] business unit</td>
</tr>
</tbody>
</table>

### Data Role Attributes

When you click the **Generate Roles** button, the template combines the attributes as follows:

1. Selects each of the base roles
2. Picks up the action and dimensional subset of the data granted by a data security policy
3. Names the data roles based on the naming convention

If you use the values of the previous attributes, the result is a data role like this:

<table>
<thead>
<tr>
<th>Data Role Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>FINANCIALS_APPLICATION_ADMINISTRATOR: APAC</td>
</tr>
<tr>
<td>Display Name</td>
<td>Financials Application Administrator: Asia Pacific</td>
</tr>
<tr>
<td>Description</td>
<td>Role Financials Application Administrator implementing business function Manage Payables Invoices for the Asia Pacific business unit.</td>
</tr>
</tbody>
</table>

The generated data roles are stored in the Lightweight Directory Access Protocol (LDAP) store. After a data role is generated, you provision it to users. A user provisioned with a data role is granted permission to access the data defined by the dimension and data security grant policies of the data role template.

### Related Topics

- Role Provisioning and Deprovisioning: Explained
Creating a Data Role Template: Procedure

You can use these instructions to create a new role template.

**Note**

Consider carefully before creating a custom role template. Oracle may not be able to guarantee the upgrade of your custom role templates in the future.

To create a data role template:

1. Select Global, Role Templates, in the left panel, and click New. An untitled page appears in the right panel. Six tabs appear at the top of the page: General, External Roles, Dimension, Naming, Policies, and Summary.

2. In the General tab, enter the following data for the template being created:
   - A display name (required)
   - A name (required)
   - A description (optional)
   - A template group (optional)
   
   This attribute allows searching templates by group and the simultaneous running of the templates in a group.

3. In the External Roles tab, specify the external roles for the template.
   
   a. In the Roles area, click Add to display the Add External Role dialog box where you can search for external roles matching a given pattern.
   
   b. Select roles from the results of the query and click Add.

   The roles selected are displayed in the Roles table.

4. On the Dimension tab, specify the SQL that identifies the dimensions of the template.

   The user must have access privileges to the data queried. The data returned by that SQL is displayed in the Preview Data table. Optionally, enter aliases for the column names of the returned data in the Column Display Names table at the bottom of the page.

5. In the Naming tab, specify the rule to follow to generate names of the data roles created by the template.

   These names are put together by concatenating several strings that you specify in the area Configure Role Name. Typically, one chooses an attribute of the base role and an attribute of the dimension (such as SET_ID, SET_CODE, or SET_NAME as seen in the example). The role attributes Role_Code, Role_Name, and Role_Descrip are available as the default setting. The resulting names must be unique.

   Similarly, specify the rule to generate display names for the data roles created by the template. These names are put together by concatenating several strings that you specify in the Configure Display Name area. The resulting names need not be unique, but it is recommended that you specify enough attributes to make them unique too.

   Optionally, enter a description for the roles generated.
6. On the Policies tab, specify the rules to create data set grants, as follows:
   ◦ In the Database Resource area, click **Add** to add the object to be secured by the generated data security grants.
   ◦ On the Data Sets tab, specify whether the grant uses a primary key or an instance set (the instance set is selected from the available instance sets associated with the resource, which are defined at the time of resource creation), and how the data set is mapped to a dimension attribute.
   ◦ On the Actions tab, specify the actions allowed on the database resource.

7. Save the data role template. APM validates the template. If it passes validation, the template is saved and the Summary tab is enabled.

### Running a Data Role Template: Procedure

You can preview the data roles that the template generates without creating the data roles.

**Running a Data Role Template**

To run a data role template:

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>These instructions assume that you have created and saved a valid data role template.</td>
</tr>
</tbody>
</table>

1. Open the template and select the Summary tab.
2. Click **Generate Roles**. The roles generated appear in five categories. Each external role generated by the run inherits the attributes from the corresponding parent external role.
3. Reconcile roles in the following four categories, as appropriate:
   ◦ **Invalid Roles**
     A role in this category is a role for which the base role is not found in the identity store. Delete or allow roles in this set. Deleting an invalid role removes the role, if it is not being used by any policy and removes the data security generated for that role.
   ◦ **Inconsistently Created Roles**
     A role in this category is a role with a name identical to the name of some other role already in the identity store. Typically, these roles are displayed because of a change or removal in records from where the dimensions are computed. Delete or reuse roles in this set. Reusing an inconsistently created role has the following impact:
     • Overwrites the existing role with the generated one.
     • Adds a link between the base role and the role.
     • Refreshes the role’s display name and description.
     • Adds the data security for the role.
     • Does not affect data securities defined by other templates.
○ Inconsistently Deleted Roles
  Delete or recreate roles in this set. Recreating an inconsistently deleted role has the following impact:
  • Creates the role in the identity store using the template’s naming definition.
  • Adds the data security for the role.
  • Adds a link between the base role and the role, if it was not already in place.

○ Missing Link Roles
  A role in this category misses the required link to a base role. Relinking roles in this set adds a link between the base role and the role, and updates the grant associated with that role.

After you generate the external roles and data policy grants, you can verify them by searching and opening a particular role or policy.

Running Templates Programmatically
A template or a set of templates can also be run programmatically, using web-services.

The following two functions support running a single template or the collection of templates with a given group ID using web-services:

```java
public String executeTemplate(String TemplateName)
public String executeTemplateByGroupId(String GroupId)
```

The string returns as successful or with errors. A successful run displays the templates that were run. An unsuccessful run display the error.

Updating Data Role Templates: Procedure
You might want to update data role templates and regenerate data roles for many reasons. This topic presents the steps you take to update role templates and regenerate data roles.

Procedure
To update data role templates, perform these steps.

1. Sign in using the IT Security Manager role.
2. On the home page, click the **Setup and Maintenance** tile. The Setup and Maintenance work area appears.
3. On the All Tasks tab, search for and select to the Manage Role Templates task.
   The integrated Authorization Policy Manager appears.
4. In the Navigation panel, click **Global - Role Templates - Open** (the folder icon on top of the panel).
   The Search - Role Templates page appears.
5. Perform a search and identify the template that you want to update. You can select an operator and enter a string to match for the **Template Name**, **Template Display Name**, and Template Group ID.
   You can perform a partial search.
6. Click **Search**.
   The templates that match the criteria appear in the Search Results table.

7. Double-click an item in the Search Results table to open it.
   Alternatively, select a template in the Search Results table and click **Open**.

8. Modify fields and update values as appropriate and as allowed.

9. Click **Apply** to save your changes.
   Click **Revert** to discard your changes.

10. Click the Summary tab to preview the data roles.

### Important
If you change the role template attributes, remember to regenerate the data roles so they reflect your changes.

### Updating Data Role Templates: Points to Consider
As your enterprise expands or changes, you can modify your data role templates to produce new data roles. You can make certain modifications to the data role templates to accommodate your business needs. This topic discusses the attributes that you can and can't change.

#### Changeable Attributes
You can modify the following attributes of data role templates after you run them:

- You can add or remove an external role.
  - If you add an external role and run the template, it creates external roles for the added role and for each of the dimensions.
  - If you remove an external role and run the template, then you can either deactivate the external roles associated with the deleted role or leave the roles unchanged.

- You can add or remove a dimension.
  - If you add a dimension and run the template, it creates external roles for the added dimension only.
  - If you remove a dimension and run the template, you can either deactivate the external roles associated with the deleted dimension or leave the roles unchanged.

#### Unchangeable Attributes
You cannot modify the following attributes of data role templates after you run them:

- Name of a template.
- The SQL that defines the template dimensions.

### Note
If the data that this SQL accesses changes, a new template run can return a different set of dimensions than those returned by the previous run.
• Naming rules.

**Importing and Exporting Data Role Templates: Procedure**

A data role template can be imported to or exported from the Oracle Authorization Policy Manager environment with the use of the following two utilities: `importMetadata` and `exportMetadata`. Both these utilities require establishing a connection to the Oracle WebLogic server before they can be used.

**Restriction**
The importing and exporting of data role templates is unavailable to Oracle Applications Cloud services users because you do not have access to the Oracle WebLogic server.

**Importing**
Use the following procedure to import one or more data role templates.

1. Establish a connection to the server using the following code:

   ```
   > connect ('aUser','aPassword','t5://localhost:7133')
   ```

   **Note**
   In the code, the first value is the user name, the second is the password for that user, and the third is the connection URL to the server.

2. Execute the utility `importMetadata`, as illustrated in the following sample code:

   ```
   > importMetadata(application='oracle.security.apm',
                   server='AdminServer',
                   fromLocation='/myLocation/myRoleTemplates',
                   docs='/oracle/apps/apm/**',
                   restrictCustTo='site')
   ```

   where,
   - **application** is the owner of the data role template to be imported
   - **server** is the name of the WebLogic server
   - **fromLocation** is the directory containing the templates
   - **docs** specify the templates

   **Note**
   To import all templates (including template subdirectories) in the specified directory, use `**`, as illustrated in the sample code.

   - **restrictCustTo** is a condition that must always be set to the value `site`. 


Exporting

Use the following procedure to export one or more data role templates.

1. Ensure that the application is connected to the server.
2. Execute the utility `exportMetadata`, as illustrated in the following sample code:

   ```bash
   > exportMetadata(application='oracle.security.apm',
                     server='AdminServer',
                     toLocation='/myLocation/myRoleTemplates',
                     docs='/oracle/apps/apm/**',
                     restrictCustTo='site')
   ```

   **Note**

   `toLocation` is the directory to which the data role templates are exported.

---

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. Enterprise roles provide access to data through data security policies defined for the inherited application roles.

When setting up the enterprise with structures such as business units, data roles are automatically generated that inherit job roles based on data role templates. Data roles also can be generated based on HCM security profiles. Data role templates 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.

<table>
<thead>
<tr>
<th>Data security feature</th>
<th>Does what?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security policy</td>
<td>Defines the conditions under which access to data is granted to a role.</td>
</tr>
</tbody>
</table>
### Data security feature

<table>
<thead>
<tr>
<th>Data security feature</th>
<th>Does what?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Applies data security policies with conditions to users through role provisioning.</td>
</tr>
<tr>
<td>Data role template</td>
<td>Defines the data roles generated based on enterprise setup of data dimensions such as business unit.</td>
</tr>
<tr>
<td>HCM security profile</td>
<td>Defines data security conditions on instances of object types such as person records, positions, and document types without requiring users to enter SQL code</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Who</th>
<th>can do</th>
<th>what</th>
<th>on which set of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>warehouse managers</td>
<td>manage</td>
<td>inventory transactions</td>
<td>for the inventory organizations in which they can operate</td>
</tr>
</tbody>
</table>

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.
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.

Data Roles
Data roles are implemented as job roles for a defined set of data.

A data role defines a dimension of data within which a job is performed. The data role inherits the job role that describes the job. For example, a data role entitles a user to perform a job in a business unit.

The data role inherits abstract or job roles and is granted data security privileges. Data roles carry the function security privileges inherited from job roles and also the data security privilege granted on database objects and table rows.

For example, an accounts payables specialist in the US Business Unit may be assigned the data role Accounts Payables Specialist - US Business Unit. This data role inherits the job role Accounts Payables Specialist and grants access to transactions in the US Business Unit.

Data roles are created using data role templates. You create and maintain data roles in the Authorization Policy Manager (APM). Use the Manage Data Roles and Security Profiles task to create and maintain HCM data roles in Oracle Fusion HCM.

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 an enterprise role such as Manager. The resulting data role with its role hierarchy and grants operates in the same way as any other data role.

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

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

Advanced Data Security: 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.

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.

Creating Custom Duty Roles

Creating Duty Roles in Authorization Policy Manager: Procedure

Duty roles are made up of function security privileges and data security policies. You can create custom duty roles if the predefined duty roles don't meet your needs. For example, a predefined duty role may have more or fewer function security privileges or data security policies than you need.

Duty roles exist in Oracle Entitlements Server and you can manage them there using the Authorization Policy Manager console. Alternatively, you can create duty roles on the Security Console, either from scratch or by copying and editing an existing duty role. This topic shows how to create a duty role in Authorization Policy Manager.

Once the duty role exists, you:

1. Add function security privileges to the duty role.
2. Add data security policies to the duty role.
3. Verify the duty role.

Creating a Duty Role

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

1. On the home page, click **Setup and Maintenance** to open the Setup and Maintenance work area.
2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task. The Oracle Entitlements Server Authorization Management page opens.
3. In the Application Name section of the Home tab, select your application. For example, select `fscm`.
4. Under the Application Roles heading on the Home tab, select **New**. An Untitled tab opens.
5. In the **Display Name** field on the Untitled tab, enter the display name of the new duty role. For example, enter `Sales Department Management Duty`.
6. In the **Role Name** field, enter the duty role name. For example, enter `AR_DEPT_MANAGE_DUTY_CUSTOM`.
7. Select the relevant role category. For example, select `ERP_DUTY`.
8. Click **Save**. The duty role’s display name now appears as the tab name.
The next step is to add function security privileges to the duty role.

**Adding Function Security Privileges to Duty Roles in Authorization Policy Manager: Procedure**

This topic explains how to create a security policy for a custom duty role in Authorization Policy Manager and add an existing function security privilege to it. Typically, you perform this task immediately after creating a custom duty role.

Adding Function Security Privileges to a Duty Role

If you have just created a duty role and the duty role tab is still open, then:

- Select **Create Policy - Default Policy Domain** in the top-right corner of the tab to open an Untitled tab.
- Continue from step 5.

Otherwise, sign in with the IT Security Manager job role and follow these steps:

1. On the home page, click **Setup and Maintenance** to open the Setup and Maintenance work area. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

   The Oracle Entitlements Server Authorization Management page opens.

2. In the Application Name section of the Home tab, select your application. For example, select **fscm**. Under the Application Roles heading on the Home tab, click **Search**.

   The Role Catalog page opens.

3. In the **Display Name** field in the Search Roles section, enter the display name and click **Search**.

4. In the Search Results section, select the duty role and select **New Policy - Default Policy Domain**.

   An Untitled tab opens.

5. In the **Display Name** field on the Untitled tab, enter the policy name. For example, enter Policy for AR Department Management Duty Custom.

   **Tip**
   
   Names of predefined security policies begin with the words Policy for.

6. In the **Name** field, enter the policy name. For example, enter AR_DEPT_MNG_DUTY_POLCUS.

7. In the Targets section, click **Add Targets**.

   The **Search Targets** dialog box opens.

   **Tip**
   
   In this context, a target is a function security privilege and a principal is a role. When a target is granted to the principal, a function security privilege is granted to the duty role.
8. In the Display Name field on the Entitlements tab, enter the name of the function security privilege. For example, enter Manage Department. Click Search.

The Manage Department function security privilege secures access to the Manage Departments page.

9. In the search results, select the function security privilege and click Add Selected.

This action adds the function security privilege to the Selected Targets section.

10. Click Add Targets to close the dialog box.

11. On the Untitled tab, click Save.

This action updates the Untitled tab with the name of the new policy.

The next step is to assign data security policies to your custom duty role.

Adding Data Security Policies to Duty Roles in Authorization Policy Manager: Procedure

This topic explains how to find the data security policies assigned to an existing duty role and add them to a custom duty role in Authorization Policy Manager. Adding data security policies to a custom duty role is part of the process of creating the duty role. Typically, you perform this task immediately after adding function security privileges to a duty role.

Adding Data Security Policies to a Duty Role

If you are on the Authorization Management page, then click the Home tab and continue from step 3. Otherwise, sign in with the IT Security Manager job role and follow these steps:

1. On the home page, click Setup and Maintenance to open the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

The Oracle Entitlements Server Authorization Management page opens.

3. In the Application Name section of the Authorization Management Home tab, select your application. For example, select fscm. Click Search under the Application Roles heading.

The Role Catalog page opens.

4. In the Display Name field in the Search Roles section, enter the name of the predefined duty role from which you want to copy the data security policies. For example, enter Department Management Duty. Click Search.

5. Select the role in the search results and click Open.

The Department Management Duty page opens.

6. In the top-right corner of the page, click Find Policies - Default Policy Domain.

The Search Authorization Policies tab opens.

The data security policies for this duty role appear on this tab.

8. Select the first data security policy of interest and click **Edit**.


   The **Select and Add: Roles** dialog box opens.

   Search for your duty role. For example, enter AR_DEPT_MANAGE_DUTY_CUSTOM in the **Role Name** field. Select your application (for example, **fscm**) as the **Application**, and click **Search**.

10. Select the duty role and click **OK**.

    A copy of this data security policy now exists against your custom duty role.

11. Click **Save**. Click **OK** to close the **Confirmation** dialog box.

Repeat steps 8 through 11 to add additional data security policies to your duty role.

### Verifying Custom Duty Roles: Procedure

After you create a custom duty role, you must verify it. Typically, you perform this task immediately after adding function security privileges and data security policies to the duty role. This topic describes how to verify a custom duty role.

#### Verifying a Custom Duty Role

If you’re on the Authorization Management page, then click the Home tab and continue from step 3. Otherwise, sign in with the IT Security Manager job role and follow these steps:

1. On the home page, click **Setup and Maintenance** to open the Setup and Maintenance work area.

2. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

   The Oracle Entitlements Server Authorization Management page opens.

3. On the Home tab, select your application (for example, **fscm**) in the Application Name section. Click **Search** under the Application Roles header.

   The Role Catalog page opens.

4. Search for your duty role.

   In the search results, select the duty role and click **Open**. The duty role page opens.

5. Click **Find Policies - Default Policy Domain**.

   The Search Authorization Policies tab opens.

6. In the Policies For: section, the:

   a. Functional Policies tab shows your function security privileges.

   b. Data Security tab shows your data security policies.
7. Click Close Multiple Tabs to close the open tabs and return to the Home tab.

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. Since inventory transactions are secured objects, and a data role template exists for limiting the Warehouse Manager role to the inventory organizations in which they can operate, a data role inherits the job role to limit access to those inventory transactions that are in the M1 Inventory Organization. Objects not secured explicitly with a data role are secured implicitly by the data security policies of the job role.

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

How can I secure a common object such as an attachment category or a profile option?

Use the Manage Data Security Policies task to secure objects. To perform this task, you’ll use the integrated Authorization Policy Manager or data security pages.

How can I view, create, or change a data role template?

Use the Manage Role Templates task to view, create, or change data role templates. Use the integrated Authorization Policy Manager to perform the Manage Role Templates task.

Related Topics

- Data Role Templates: Explained

How do I change the roles in a role hierarchy?

An enterprise role is a role that users can be members of. Jobs are implemented as enterprise roles. Use the Manage Job Roles task to change a hierarchy of enterprise roles. You perform the task in the integrated Oracle Identity Management.

An application role is a collection of permissions. Duties are implemented as an application roles. In Oracle Fusion Applications, a duty corresponds to a line on a job description. For example, a duty of an accounts payable manager might be supplier master management. Use the Manage Duties task to change a hierarchy of duty roles. You perform this task in the integrated Authorization Policy Manager.

The LDAP directory stores the role hierarchy and the spanning of roles across multiple pillars or logical partitions. The policy store stores duty roles. The identity store stores enterprise roles.
Important
Don’t change the predefined job, abstract, and duty roles in role hierarchies. (In the Security Console, you can identify predefined application roles by the ORA_ prefix in the Role Code field.) Instead, copy a predefined role, and make your required changes. You can then provision your custom role as you would the predefined roles.

Related Topics
- Security Tasks and Oracle Fusion Applications: How They Fit Together

How do I create a role hierarchy?
The most efficient way to create role hierarchies is the use the Security Console. You navigate through the steps and add roles and privileges in the visualizer.

You can also use the Manage Job Roles task to create a hierarchy of enterprise roles. Use the integrated Oracle Identity Management UI pages to perform this task. You can use the Manage Duties task to create a hierarchy of applications roles. Use the integrated Authorization Policy Manager to perform this task.

Related Topics
- Role Inheritance: Explained

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 on the Security Console to create job roles. Enter the information on 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.

You can also use the Create Job Roles task to create job roles.

This task opens the integrated Oracle Identity Management (OIM) pages to perform these tasks. The Lightweight Directory Access Protocol (LDAP) identity store stores the job role, or enterprise role as OIM refers to it..

How do I create a new data role?
Use the Manage Role Templates task to define which data roles are generated. To perform this task, you’ll use the integrated Authorization Policy Manager.
Use the Manage Data Roles and Security Profiles task to define which HCM data roles are generated. To perform this task, you'll use Oracle Fusion Human Capital Management (HCM).

These tasks may trigger the need for revised role provisioning rules to ensure that new data roles are appropriately provisioned to users.

**Related Topics**

- Creating an HCM Data Role: Worked Example
- Role Provisioning and Deprovisioning: Explained
- Data Role Templates: Explained

**Can I create a new duty role?**

Yes. Use the Manage Duties task to create a duty role. To perform this task, use the integrated Authorization Policy Manager.

**Related Topics**

- How can I tell which roles are provisioned to a user?
7 Using the Security Console

Setting Up the Security Console: Explained


Profile Options

To set the profile options, search for and select the Manage Administrator Profile Values task in the Setup and Maintenance work area. Then search for and select each option.

- The Security Console Working App Stripe profile option (ASE_WORKING_APP_STRIPE) specifies a policy stripe within the policy store. In effect, this option selects an application whose roles are available to be worked with in the Security Console. For example, if you copy a job role in the Security Console, then you see inherited duty roles belonging to the application designated by your policy-stripe selection.

  The default policy-store application is HCM. To see roles inherited from another application, update the profile option to change to that application. (Note that some roles inherit from multiple applications.) Defining user-level values for this profile option allows different users to view different application stripes.

- The Enable Data Security Policies and User Membership Edit profile option (ASE_ROLE_MGMT_PREF) determines whether users can enter data in the Data Security Policies page and the User page of the Security Console role-creation and role-edit trains.

Import User and Role Process

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.

Run the process to populate Applications Security tables. Then 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.

You are recommended to schedule the Import User and Role Application Security Data process to run at the same frequency as the Retrieve Latest LDAP Changes and Send Pending LDAP Requests processes. With each scheduled run, the process copies only changes made since its previous run.

Administration Options

Within the Security Console, select the Administration tab to set these options:

- Role Copy Preferences: 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). When a user copies a role, the copy adopts the name and code of the source role, with this prefix or suffix (or both) added to distinguish 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."

- Certificate Preferences: Set the 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.)
Security Visualizations: Explained

A Security Console visualization consists of nodes representing 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 that roles can grant.

In a visualization, 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.

For example, a job role might consist of several duty roles. If you were to select the job role as the focus of a visualization (and if you set the Security Console to display paths leading toward privileges), an initial image would show nodes representing the duty roles encircling a node representing the job role. You could then manipulate the image (as described in the following sections).

Expand or Collapse Nodes

You can expand nodes or collapse them. To expand a node is to reveal roles, privileges, or users to which it connects. To collapse a node is to hide those items.

In the earlier example, you might expand one of the duty-role nodes. It would then occupy the center of its own circle of nodes. Each would represent a subsidiary duty role or a privilege belonging to the duty role you expanded.

To expand or collapse nodes:

1. Make a selection in the **Expand Toward** option to determine whether nodes expand toward privileges or toward users. (In the example, the expand toward privileges option would have been selected.)

2. Select a node and right-click.

3. 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.

   These options appear only when appropriate. For example, a Collapse option appears only when the selected node is already expanded.

Enlarge or Reduce the Image

You can enlarge or reduce a visualization. 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 signifies user, R signifies role, P signifies privilege, and A signifies aggregate privilege. If the image is smaller still, the nodes are unlabeled.

Use tools located at the upper right of a visualization:

- **Plus**: Zoom in (enlarge the image). You can also use the mouse wheel to zoom in.
- **Minus**: Zoom out (reduce the image). You can also use the mouse wheel to zoom out.
- **Circle**: Click to activate a magnifying glass. When this feature is active, hover 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 the circle button again to deactivate the magnifying glass.
• **Square**: Click to center the image and size it so that it is as large as it can be and still fit entirely in its display window. (Nodes that you have expanded remain expanded.)

### Enhance Your View

Use these techniques to enhance your view of a visualization, or of nodes within it:

- If nodes are labeled with symbols or are unlabeled, hover over any node to display the name of the user, role, or privilege it represents.
- Click the background of the visualization, then drag the entire image in any direction.

### Create Related Visualizations

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**.

### 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, or determine how you can alter that access to create new roles.

#### Opening a Simulation

Open a simulated menu from the Security Console:

1. Create a visualization, or populate the Search Results column with a selection of roles or users.

2. In a visualization, right-click on a role or user. Or, in the Search Results column, left-click on the button near the lower right corner of the listing for a role or user.

3. Select **Simulate Navigator**.

#### Working with the Simulation

A simulated Navigator panel lists menu and task entries. A padlock icon next to an entry indicates that it can be, but is not currently, authorized for the role or user. An entry without a padlock icon is already authorized for the role or user.

To plan how this authorization may be altered:

1. Click on 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)
  - Function security policies and data 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. List the roles belonging to a category that you select by clicking on that category in the Role Categories grid. For each role, the Roles in Category grid also shows the number of:

  - Role memberships
  - Function security policies and data security policies
  - Users assigned the role

- Individual role statistics. Click the name of a role in the Roles in Category grid to open a page that lists the function security policies, data 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.

FAQs for Using the Security Console

How can I select security items to visualize?

Enter text in the Search field. A search-suggestions dialog box lists roles, privileges, or users whose names contain the text you entered. Select one of these items in either of two ways.

- Select an item directly from the search-suggestions dialog box.
- Click the Search button (next to the Search field). The search-suggestions dialog box closes, and all items that occupied it appear in the Search Results column. Select an item there.

You can filter the Search Results column before you select an item from it. Click Refine and, in a Refine Search Results window, select an item type. The column then shows only items of the selected type whose names contain the search text.
Chapter 8
Reviewing Roles and Role Assignments

Reviewing Roles and Role Assignments on the Security Console: 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

1. On the home page, click **Tools - Security Console**.
2. On the Security Console, search for and select the user.

A visualization appears showing 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**.

Identifying Users Who Have a Specific Role

To identify all users who have a specific role:

1. On the Security Console, search for and select the role.
   
   A visualization appears showing the role and its hierarchy.
2. Set **Expand Toward** to **Users**.

   **Tip**

   Set the **Expand Toward** option to control whether the visualization moves up the hierarchy from the selected role (toward users) or down the hierarchy from the selected role (toward privileges).

In the refreshed visualization, solid blue circles identify users. User names appear on hover.

Users may inherit roles either directly or indirectly from other roles, which appear as solid green circles. Expand a role to view its hierarchy.
Reviewing Job and Abstract Roles on the Security Console: Explained

You can use the Security Console to review the role hierarchy of a job role or abstract role. You must have the IT Security Manager job role to perform this task.

Follow these steps:

1. On the home page, click **Tools - Security Console**.

2. On the Security Console, ensure that **Expand Toward** is set to **Privileges**.

3. Search for the role.

   In the Oracle Entitlements Server Authorization Policy Manager, job and abstract roles have both an external role and an application role. Both roles appear in the Security Console search results. Application roles have the suffix (**Application role**).

4. Select the external role to view the complete role hierarchy.

   A visualization appears showing any roles that the role inherits directly.

5. To expand the hierarchy of any inherited role, select it, right-click, and select **Expand**.

   In the visualization, single-letter labels have the following meanings:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Security Artifact</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Aggregate privilege</td>
</tr>
<tr>
<td>P</td>
<td>Function security privilege</td>
</tr>
<tr>
<td>R</td>
<td>Role</td>
</tr>
</tbody>
</table>

Role and privilege names appear on hover.

**Tip**
To review any function security privileges granted directly to a job or abstract role, review its application role rather than its external role on the Security Console.

**Related Topics**

- Managing Job and Abstract Roles on the Security Console: Explained
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, to determine whether you want to incorporate upgrade changes into your custom role.

1. Begin the process from the Security Console, in either of two ways:
   - Click the **Compare Roles** button.
   - Create a visualization, right-click one of its roles, and select the **Compare Roles** option.

2. 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 from a visualization, the First Role field displays the name of the role you selected in the visualization. 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.

3. Filter for any combination of these artifacts in the two roles:
   - Function security policies
   - Data security policies
   - Inherited roles

4. 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

5. 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 Reference

The User and Role Access Audit Report documents role hierarchies. Run the report to view all roles, privileges, and data security policies for:

- One user.
- All users.
- One role.
Run the User and Role Access Audit Report as a scheduled process. Use the Scheduled Processes work area available from the Navigator. As you run the process, set parameters that focus the report on a user you select, all users, a role you select, or all roles.

**Report Results**

The process returns archive (ZIP) files. Each file name contains a prefix and a suffix that define its content. (Each file name also contains values that identify the process number, and the process run date and time.)

If you select an individual user, the process returns:

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ DataSec.zip</td>
<td>One XML file documenting data security policies that apply to the selected user.</td>
</tr>
<tr>
<td>USER_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ Hierarchical.zip</td>
<td>One XML file that documents functional security for the selected user. Its format depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td>USER_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ TabularFormat.zip</td>
<td>One XML file that documents functional security for the selected user. Its format is tabular (flattened).</td>
</tr>
</tbody>
</table>

If you select an individual role, the process returns:

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROLE_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ DataSec.zip</td>
<td>One XML file documenting data security policies that apply to the selected role.</td>
</tr>
<tr>
<td>ROLE_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ Hierarchical.zip</td>
<td>One XML file that documents functional security for the selected role. Its format depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td>ROLE_ NAME_ [PROCESS]_ [DATE]_ [TIME]_ TabularFormat.zip</td>
<td>One XML file that documents functional security for the selected role. Its format is tabular (flattened).</td>
</tr>
</tbody>
</table>

If you select all users, the process returns:

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL_ USERS_ [PROCESS]_ [DATE]_ [TIME]_ DataSec.zip</td>
<td>Multiple XML files, one for each user. Each documents data security policies that apply to its user.</td>
</tr>
<tr>
<td>File Name</td>
<td>File Content Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>ALL_USERS_[PROCESS]<em>[DATE]</em>[TIME]_Hierarchical.zip</strong></td>
<td>Multiple XML files, one for each user. Each documents functional security for its user, in a format that depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td><strong>ALL_USERS_[PROCESS]<em>[DATE]</em>[TIME]_CSV.zip</strong></td>
<td>A comma-separated-values file that documents functional security for all users in a tabular (flattened) format.</td>
</tr>
</tbody>
</table>

If you select all roles, the process returns:

<table>
<thead>
<tr>
<th>File Name</th>
<th>File Content Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALL_ROLES_[PROCESS]<em>[DATE]</em>[TIME]_DataSec.zip</strong></td>
<td>Multiple XML files, one for each role. Each documents data security policies that apply to its role.</td>
</tr>
<tr>
<td><strong>ALL_ROLES_[PROCESS]<em>[DATE]</em>[TIME]_Hierarchical.zip</strong></td>
<td>Multiple XML files, one for each role. Each documents functional security for its role, in a format that depicts hierarchical relationships among security artifacts.</td>
</tr>
<tr>
<td><strong>ALL_ROLES_[PROCESS]<em>[DATE]</em>[TIME]_CSV.zip</strong></td>
<td>A comma-separated-values file that documents functional security for all roles in a tabular (flattened) format.</td>
</tr>
</tbody>
</table>

The process also returns a diagnostic log (in the form of a ZIP file).
9 Customizing Roles Using the Security Console

Creating Custom Roles

Copying 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. (Note however that the Security Console prevents you from copying some roles because they support middleware components.)

**Note**

Never edit predefined roles. (You can identify a predefined role by the ORA prefix in the Role Code field). During each upgrade, predefined roles are updated to the specifications for that release, so any customizations would be overwritten.

To initiate the copy, create a visualization and select a role in it. Right-click and select **Copy Role**. Then select one of two options:

- **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 will 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 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.)

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

- By default, the name and code of the copied role are the same as those of the source role, except that a prefix, suffix, or both are appended. In the 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.)

- Although the Role Hierarchy page displays all roles subordinate to the role you copied, you can add roles only to (or remove them from) the top role you copied.

Creating Roles in the Security Console: Procedure

You can use the Security Console to create duty, job, or abstract roles. (Alternatively, you can use Oracle middleware applications to create roles, but this topic is limited to the use of the Security Console.)

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

To create a role from scratch, select the Create Role button in the Security Console. 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 Accounts Receivable Specialist.

2. In the Role Code field, create an internal name for the role, such as AR_ACCOUNTS_RECEIVABLE_SPECIALIST_JOB.

   For role name and role code, it’s recommended that you develop a naming convention to distinguish custom roles from seeded roles. (In the Administration page, you can configure a prefix or suffix that is added to role copies for this purpose. Establish a similar convention for roles you create from scratch.)

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."

   In subsequent pages, you will be limited to options appropriate for the category you select here. For example, as you create function security policies, a given privilege (such as View All Sales Accounts) might be available to you if you select one category (one involving Sales), but not if you select another (such as one that applies to the SCM application).

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

Adding Functional 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 Functional 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 other duty roles, job roles, or abstract roles to which the duty role 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:


2. In a Search field, enter text to search for a privilege or role. Click the Search icon to see all results that include your search text, then use the Refine option to filter entries by type.

3. Select a privilege or role. If you select a privilege, click Add Privilege to Role. If you select a role, click Add All Privileges.

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

- Click on a privilege to view details of the code resource that it secures.
- Delete a privilege. If, for example, you have added all the privileges associated with a role, but want to use only some of them, you’ll need to 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 an element of a data role.
• 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.

(Note that a data privilege, which specifies what a user can do with a piece of data, differs from a functional privilege. The latter, appropriate for a function security policy, grants access to a UI feature.)

You can use a Data Security Policies page to manage implicit policies. First, however, an Enable Data Security Policies and User Membership Edit profile option must be set to Yes. (If this option is set to No, the Data Security Policies page is view-only; a Create Data Security Policies button is removed from the page. In that case, you must use middleware applications to manage data security policies and apply them to roles. The profile option is available from the Manage Administrator Profile Values task in the Setup and Maintenance work area.)

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. You can use Authorization Policy Manager to create new conditions.
  
  ◦ 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’ve 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 a visualization, with the role you are creating as its focus. Link it to other roles from which it will 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 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, enter text to search for the role you want to add. Click the Search icon to see all results that include your search text, then use the Refine option to filter roles by type.

3. Select the role you want, and click Add Role Membership. You add not only the role you’ve selected, but also its entire hierarchy.

You can use visualization tools to enlarge, reduce, magnify, or recenter the nodes that define your role hierarchy. (See the related topic, “Security Visualizations: Explained.”) Or, right-click on an added node to expand, collapse, or delete it.
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.) You can use this page, however, only if the Enable Data Security Policies and User Membership Edit profile option is set to Yes. (If the option is set to No, the page is view-only.) To add a user:

1. Select Add User.

2. In a Search field, enter text to search for the user you want to add. Click the Search icon to see all results that include your search text. The search automatically refines itself to include users, but not roles.

3. Select a user among the search results, then click Add User to Role.

Completing the Role

On a Summary and Impact Report page, review the selections you’ve made. Summary listings show the numbers of function security policies, data security policies, roles, and users you’ve 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 need to make changes, navigate back to the appropriate page and do so. If you’re satisfied with the role, select Save and Close.

Related Topics

- Security Visualizations: Explained
- Setting Up the Security Console: Explained

Running Retrieve Latest LDAP Changes: Procedure

After creating a custom job role or abstract role on the Security Console, you must run the Retrieve Latest LDAP Changes process. This process makes the role available elsewhere in Oracle Fusion Human Capital Management (Oracle Fusion HCM). This topic describes how to run Retrieve Latest LDAP Changes.

**Note**

Once implementation is complete, you’re recommended to schedule Retrieve Latest LDAP Changes to run daily. Once the process is scheduled, you can’t run it on an as-needed basis.

If the process is scheduled when you create a custom job or abstract role, then you can wait for the process to complete its daily run. Once that run completes, the custom role is available in Oracle Fusion HCM. Alternatively, if you can’t wait for the daily process, then you can end the scheduling temporarily and run the process as described here. When the process completes, you can schedule it again.

Running Retrieve Latest LDAP Changes

Sign in to Oracle Fusion HCM 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**.

---

**Oracle Supply Chain Management Cloud**
Securing Oracle SCM Cloud

Chapter 9

Customizing Roles Using the Security Console

98
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.


   Repeat this step periodically until the process completes.

Once the process completes successfully, you can select your custom role in Oracle Fusion HCM interfaces, such as Manage Data Roles and Security Profiles.

Related Topics

- Copying and Editing Job or Abstract Roles Using the Security Console: Procedure
- Creating Job or Abstract Roles Using the Security Console: Procedure

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 duplicative 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.

Report Usage
To optimize your roles based on the report, navigate to the Setup and Maintenance work area. Use the Manage Duties task and the Manage Job Roles tasks to update your role hierarchy, as necessary.

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:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterAnalysis-Job-CSVs.zip</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Diagnostics. zip</td>
<td>Contains a log file that provides technical details about the analysis process. You can use this file for troubleshooting purposes.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>The name of the optimized cluster, usually in this format: Cluster ###</td>
</tr>
<tr>
<td>Primary, Secondary, Tertiary Candidate Role</td>
<td>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.</td>
</tr>
<tr>
<td>Jobs in Cluster</td>
<td>The number of job roles that inherit the privilege cluster. A list of job names and descriptions is also included.</td>
</tr>
<tr>
<td>Privileges in Cluster</td>
<td>The number of privileges that make up the cluster. A list of privilege names and descriptions is also included.</td>
</tr>
</tbody>
</table>

Using the Role Optimization Report

Privilege Clusters

After you select the duty role to map to each privilege cluster, use the Manage Duties task and assign the privileges to the role.
Job Roles

Adding, removing, and replacing roles might be suggested as part of the role optimization report. You use the Manage Job Roles task to update job role hierarchies.
10 Synchronizing User and Role Information with Oracle Identity Management

Synchronization of User and Role Information with Oracle Identity Management: How It's Processed

Oracle Identity Management maintains Lightweight Directory Access Protocol (LDAP) user accounts for users of Oracle Fusion Applications. Oracle Identity Management also stores the definitions of abstract, job, and data roles, and holds information about roles provisioned to users.

Most changes to user and role information are shared automatically by Oracle Applications Cloud and Oracle Identity Management. No action is necessary to make this exchange of information happen.

However, you must run the processes Send Pending LDAP Requests and Retrieve Latest LDAP Changes to manage some types of information exchange between Oracle Applications Cloud and Oracle Identity Management.

The table summarizes the role of each process.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Pending LDAP Requests</td>
<td>Sends bulk requests and future-dated requests that are now active to Oracle Identity Management. The response to each request from Oracle Identity Management to Oracle Applications Cloud indicates transaction status (for example, Completed).</td>
</tr>
<tr>
<td>Retrieve Latest LDAP Changes</td>
<td>Requests updates from Oracle Identity Management that may not have arrived automatically because of a failure or error, for example.</td>
</tr>
</tbody>
</table>
This figure summarizes the information flow of the daily processes between Oracle Fusion Human Capital Management and Oracle Identity Management. The flow is the same for all Oracle Fusion applications.

Scheduling the Processes

You must run both processes at least daily to identify and process future-dated changes as soon as they take effect.

Retrieve Latest LDAP Changes must complete before Send Pending LDAP Requests runs. For this reason, leave a gap between the scheduled start times of the processes. Depending on the size of your enterprise and the number of updates, a gap of 1 or 2 hours may be enough.

Send Pending LDAP Requests has two required parameters, **User Type** and **Batch Size**. You’re recommended to use the default values of these parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Type</strong></td>
<td>The types of users to be processed. Values are Person, Party, and All.</td>
<td>All</td>
</tr>
<tr>
<td><strong>Batch Size</strong></td>
<td>The number of requests in a single batch. For example, if 400 requests exist and you set batch size to 25, then the process creates 16 batches of requests to process in parallel. The value A means that the batch size is calculated automatically.</td>
<td>A</td>
</tr>
</tbody>
</table>
Scheduling the LDAP Daily Processes: Procedure

You’re recommended to schedule these processes to run daily:

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Pending LDAP Requests</td>
<td>Sends bulk requests and future-dated requests that are now active to Oracle Identity Management.</td>
</tr>
<tr>
<td>Retrieve Latest LDAP Changes</td>
<td>Requests updates from Oracle Identity Management that may not have arrived automatically because of a failure or error, for example.</td>
</tr>
</tbody>
</table>

**Important**

Schedule the processes only when your implementation is complete. Once you schedule the processes, you can’t run them on an as-needed basis, which is necessary during implementation.

This procedure explains how to schedule the processes.

**Scheduling the Retrieve Latest LDAP Changes Process**

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Scheduled Processes work area.
3. Search for and select the process Retrieve Latest LDAP Changes in the **Schedule New Process** dialog box.
4. In the **Process Details** dialog box, click **Advanced**.
5. On the Schedule tab, select Using a schedule.
6. In the **Frequency** field, select Daily.
7. Enter the start and end dates and times.
   
   Plan for Retrieve Latest LDAP Changes to complete before Send Pending LDAP Requests starts.
8. Click **Submit**.

**Scheduling the Send Pending LDAP Requests Process**

1. Click **Schedule New Process** in the Search Results section of the Scheduled Processes work area.
2. Search for and select the process Send Pending LDAP Requests in the **Schedule New Process** dialog box.
3. In the **Process Details** dialog box, select a user type value and enter a batch size. You’re recommended to leave **User Type** set to All and **Batch Size** set to A. Click **Advanced**.

4. On the Schedule tab, select Using a schedule.

5. In the **Frequency** field, select Daily.

6. Enter the start and end dates and times.

   Leave a gap between the start times of the two processes so that Retrieve Latest LDAP Changes completes before Send Pending LDAP Requests starts.

7. Click **Submit**.

---

### Send Pending LDAP Requests: Explained

You’re recommended to run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to Oracle Identity Management. Schedule the process in the Scheduled Processes work area.

Send Pending LDAP Requests sends the following items to Oracle Identity Management:

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

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

- Work e-mails.

  If you include work e-mails when you create person records, then the process sends those e-mails to Oracle Identity Management, which owns them. They’re usable only when Oracle Identity Management returns them to Oracle Applications Cloud.

- Role provisioning and deprovisioning requests.

  The process sends these requests to Oracle Identity Management unless automatic role provisioning is disabled for the enterprise.

- Changes to person attributes for individual users.

  The process sends this information to Oracle Identity Management unless the automatic management of user accounts is disabled for the enterprise.

- Information about HCM data roles, which originate in Oracle Fusion Human Capital Management.
Note
All of these items are sent to Oracle Identity Management automatically unless they’re either future-dated or generated by bulk data upload. You run the process Send Pending LDAP Requests to send future-dated and bulk requests to Oracle Identity Management.

Retrieve Latest LDAP Changes: Explained


You’re recommended to run Retrieve Latest LDAP Changes daily. Schedule the process in the Scheduled Processes work area.

Retrieve Latest LDAP Changes delivers the following information to Oracle Applications Cloud from Oracle Identity Management:

- Names of user accounts.
  
  The globally unique identifier (GUID) from the LDAP directory user account is added automatically to the person record.

- Latest information about abstract, job, and data roles.

  Oracle Identity Management stores latest information about all abstract, job, and data roles, including HCM data roles.

  Note
  Oracle Fusion Human Capital Management keeps a local copy of all role names and types so that lists of roles in user interfaces are up to date. HCM data roles are available only after Oracle Identity Management returns them to Oracle Fusion HCM.

- Work e-mails.

  A worker can have only one work e-mail, which Oracle Identity Management owns. Once the e-mail exists, you manage it in Oracle Identity Management. Retrieve Latest LDAP Changes sends any changes to Oracle Fusion HCM.
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 via 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. 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 defaults to a value set on the Administration page. You can enter a new value to override the default.

### 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 opens in the Certificates page, from the row for a self-signed X.509 certificate. The other 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.

**There are two types of import:**

- The first 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 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’ve 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: Explained

You can delete both PGP and X.509 certificates.

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. In either menu, select Delete, then respond to a warning message.
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. A type of enterprise role.

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.

application role
A role specific to applications and stored in the policy store.

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 accessed by a data role, such as the data controlled by a business unit.

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 role template**
A set of instructions that specifies which base roles to combine with which dimension values to create a set of data security policies.

**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.

**enterprise role**
Abstract, job, and data roles are shared across the enterprise. An enterprise role is an LDAP group. An enterprise role is propagated and synchronized across Oracle Fusion Middleware, where it is considered to be an external role or role not specifically defined within applications.
**entitlement**
Grant of access to functions and data. Oracle Fusion Middleware term for privilege.

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

**gallery**
A searchable collection of portraits that combines the functions of the person directory with corporate social networking and self-service applications for both workers and managers.

**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**

**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 employment-terms or assignment level.
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 deprovisioning
The automatic or manual removal of a role from a user.

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.

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.