## Contents

### Preface

### 1 An Overview of Securing Oracle Cloud

- Securing Oracle ERP Cloud: Overview
- Security Principles: How They Are Applied
- Oracle Applications Cloud Services Security: Explained
- Security Across Access Methods: How It Is Enforced
- Role-based Security
- Oracle Applications Cloud Security Business Fit: Explained
- Security Setup

### 2 Preparing the Cloud Service for Implementation Users

- Creating Implementation Users
- Assigning Abstract and Implementation Roles
- Resetting the Cloud Service Administrator Sign-In Details: Procedure

### 3 Preparing the Cloud Service 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
8 Implementing Security in Oracle Fusion Financials

Implementing ERP Security: Overview
General Ledger
Ledger Security
Security on a Chart of Accounts
FAQs for General Ledger
Payables
Subledger Accounting
Cash Management
Assets
Payments

9 Implementing Security in Oracle Fusion Project Portfolio Management

Provisioning Access to Project Execution Management Applications: Overview
Project User Account and Role Provisioning Statuses: Explained
Provisioning Project Resources on the Manage Project User Provisioning Page: Procedure
Provisioning Project Resources on the Manage Project Enterprise Resources Page: Explained
Project Roles in Project Execution Management Applications: Explained
FAQs for Project Roles

10 Implementing Security in Oracle Fusion Procurement

Agent Security: Explained
Create Procurement Agent: Critical Choices
Supplier User Provisioning: How It Works
Supplier User Account Administration: Explained
Set Up Supplier Roles: Examples
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.
# An Overview of Securing Oracle Cloud

## Securing Oracle ERP Cloud: Overview

Oracle ERP Cloud is secure as delivered. This guide explains how to enable user access to ERP 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.

## 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>An Overview of ERP Security in the Cloud</td>
<td>A brief introduction to the concepts of role-based security</td>
</tr>
<tr>
<td>Preparing the Cloud Service for Implementation Users</td>
<td>The role of implementation users and instructions for creating 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>The ways in which you can create application users and maintain user accounts, with instructions for some methods</td>
</tr>
<tr>
<td>Provisioning Roles to Application Users</td>
<td>The ways in which 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 customize role hierarchies</td>
</tr>
<tr>
<td>Synchronizing User and Role Information with Oracle Identity Management</td>
<td>The role of the LDAP daily processes and how to schedule them</td>
</tr>
<tr>
<td>Implementing Security in Oracle Fusion Financials</td>
<td>The additional security setup and configuration tasks associated with Oracle Fusion Financials</td>
</tr>
</tbody>
</table>
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. Any exceptions are identified in relevant topics.

This guide includes discussion of the following topics:

- Function and data security
- Privacy
- Access provisioning and identity management
- Enforcement across tools, technologies, data transformations, access methods, and information life cycle
- Security reference implementation

### Function and Data Security

Functions and data are inaccessible to users unless they are provisioned with the roles necessary to gain access. Function security provides users with access to pages in application user interfaces and actions that can be performed there. Each function security privilege secures the code resources that make up the relevant UI page.

Data security allows users to view data in those pages. Some data is secured only by function security, in which case access to a user interface page gives unrestricted access to the data that is accessible from that page. For example:

- Setup data such as Receivables Receipt Method and Payment Method.
- Transaction data such as Receivables Customer Profile.
- Archive data such as Receivables Archive.

Each data security policy combines:

- A role.
- A business object being accessed.
- The condition that must be met for access to be granted.
- A data security privilege that defines the action being performed.

### Privacy

Privacy encompasses data that should not be available to other individuals and organizations. Where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.
Oracle ERP Cloud classifies data at several levels of sensitivity, and defines privacy attributes that participate in data security policies to apply appropriate protections to sensitive data. Oracle ERP Cloud secures the privacy attributes of personally identifiable information (PII) consistently across the applications, and controls the destination of privacy attributes to the fewest and most highly secured locations possible, such as limiting the attributes that the applications share with the Lightweight Directory Access Protocol (LDAP) store.

### Access Provisioning and Identity Management

The Oracle ERP Cloud services provides an initial user and provisions that user with the administration roles necessary for initial setup.

Oracle Identity Management (OIM) is available in Oracle ERP Cloud. Identity management in Oracle ERP Cloud involves creating and managing user identities, creating and linking user accounts, managing user access control through user role assignment, managing enterprise roles, and managing OIM workflow approvals and delegated administration.

Through OIM, Oracle ERP Cloud notifies the IT security manager of all of the user requests (user life cycle changes), role provisioning requests, and grants to ensure role administration is always documented, authorized, and auditable.

Provision data roles, when available, and not the job or abstract roles the data roles inherit. In the absence of data roles, provision the abstract or job roles directly.

### Enforcement Across Tools, Technologies, Data Transformations, Access Methods, and Information Life Cycle

Oracle ERP Cloud enforces security controls across tools, technology infrastructure, transformations of data, access methods and the information life cycle.

The infrastructures of an Oracle ERP Cloud coordinates transactional and analytical security so that all security policies and controls prevail across access methods and data transformations of enterprise information. Oracle ERP Cloud enforces each single statement of security policy through the multiple transformations of data necessary for transactions, dimensional analysis, and search optimization.

### Security Reference Implementation

The security reference implementation consists of predefined roles, policies, and templates for generating data roles.

The security reference implementation comprises:

- Abstract and job roles
- Duty roles and a role hierarchy for each job role and abstract role
- Privileges required to perform each duty defined by a duty role
- Data security policies for each job role, abstract role, or data role
- Policies that protect personally identifiable information
- Templates for generating data roles and data security policies defined for those data roles

An enterprise changes the reference implementation to accommodate its particular business needs, thereby creating the enterprise’s security implementation, leaving the reference implementation in place as a baseline. Upgrades preserve enterprise changes.
The security reference implementation can be viewed in the user interfaces where security tasks are performed or in the security reference manual (SRM) for each Oracle ERP Cloud offering.

**Security Principles: How They Are Applied**

Understanding how Oracle Fusion applies common security principles may be helpful in planning your Oracle Fusion Applications deployment.

**Standard Security Principles**

Oracle Fusion Applications applies the following standard security principles:

- Least privilege
- Containment and no write down
- Transparency
- Assured revocation
- Defense in depth

Adherence to these principles enhances Oracle Applications Cloud security.

**Note**

Changes and customizations required by your enterprise may reverse the protections provided by these principles.

**How Security Principles Are Applied**

Oracle Applications Cloud applies security privileges using a specific implementation of features and various supporting tools.

**Least Privilege**

Oracle Applications Cloud roles carry only required privileges. Application roles define duties that entitle access to only the functions and data necessary for performing the defined tasks of that duty.

**Containment and No Write Down**

Secured information cannot move from more to less secure stores, such as the unsecured search index, data warehouse, or a test database. Oracle Applications Cloud enforces security policies consistently across tools, access methods, and the entire information life cycle from data at rest and in transit to clones and backups.

Oracle Applications Cloud does not write sensitive information from an environment that applies restrictions to gain access to that sensitive information to one that does not. For example, Oracle Applications Cloud does not write personally identifiable information that is sensitive and private, such as national identifiers or home contact details, from Oracle Fusion Human Capital Management Cloud (Oracle Fusion HCM Cloud) to the Lightweight Directory Access Protocol (LDAP) stores. This policy extends to attachments.
Transparency

Function and data security policies are readable in plain language wherever policies are viewed or managed. Oracle Applications Cloud provides view access to implemented roles and security policies through Oracle Identity Management (OIM) and Authorization Policy Manager (APM), as well as security reference manuals and business analysis consoles.

Assured Revocation

Revoking one security policy revokes all implementations of that policy across all tools in production.

Defense In Depth

Personnel, technology, and operations are secured with multiple layers of defense across the life cycle of the information in motion, while at rest, and when accessed or used. In Oracle Fusion Applications, authentication and password security, encryption, and logging and auditing are mechanisms of redundant defense that enforce protection. A comprehensive defense-in-depth approach to protecting private and sensitive data includes securing sensitive data at rest or stored in database files and their backups, as well as in transit.

Oracle Applications Cloud Services Security: Explained

Security in Oracle Cloud Application Services is the same as for any other kind of Oracle Applications Cloud deployment. However, the experience of getting started and managing initial users is slightly different.

Aspects of security that are specific to Oracle Applications Cloud services involve the following:

- Initial environment and sign in.
- Initial user administration.
- Infrastructure.

Aspects of security that are general to Oracle Applications Cloud and Oracle Fusion Applications involve the following:

- Ongoing user administration.
- Managing roles and security policies.

Initial Environment and Sign In

Oracle provides your account administrator with a link to activate and access the service. Oracle creates one initial user for you. Sign in as the initial user to create other users, including the service administrator, the identity domain administrator, and users who must perform implementation tasks.

Initial User Administration

If your enterprise requires additional implementation users for security administration before setting up enterprise structures, the service administrator performs the Define Implementation Users tasks.

Defining implementation users can include these tasks:

- Creating users.
- Creating data roles.
• Provisioning users with roles.
The service administrator can also perform delegated administration tasks such as resetting passwords of other administrators.

**Ongoing User Administration**
After you set up basic enterprise structures, create and manage users by using the hiring processes in Human Capital Management (HCM) or performing the Manage Users task. User management includes provisioning users with roles that provide access to functions and data in Oracle Applications Cloud services. You can also set up rules that automate role provisioning according to your criteria. You set up these rules through the Manage HCM Role Provisioning Rules task.

**Managing Roles and Security Policies**
Your Oracle Applications Cloud service includes a security reference implementation. The security reference implementation provides predefined roles and policies, as well as data role templates that generate data roles based on your enterprise structures setup.

You can view the security reference implementation using the following resources:

• User interfaces where you perform application security tasks.
• Security reference manuals for each offering.
• Oracle Enterprise Repository for Oracle Applications Cloud.

To extend the security reference implementation with roles and policy modifications needed by your enterprise, use tasks such as:

• Manage Job Roles.
• Manage Role Templates.
• Manage Data Security Policies.
• Manage Duties.

**Infrastructure**

**Related Topics**
• About Creating Additional Implementation Users
• Verifying User Access: Procedure

**Security Across Access Methods: How It Is Enforced**
Oracle Fusion Applications enforce security across various access methods.

**Access Methods That Preserve Function and Data Security**
The following access methods preserve the defined security of Oracle Fusion Applications functions and data.

• Oracle Fusion Applications user interfaces
  ◦ User sign on
Authorization policies across all tools and technologies align with the Oracle Fusion Applications enterprise roles.

The following access methods in Oracle Fusion Applications are subject to entitlement, approvals, and policies.

- Menu navigation where navigation paths are subject to an entitlement
- Worklists where worklist content is subject to a privilege
- Oracle Fusion Search where the data source is subject to a privilege and security policies have been applied to the results
- Embedded analytics where the data is filtered according to security policies that apply to a role
- Tag clouds where a tag in the cloud is sized according to a count of authorized documents

These access methods are a valid way to access the data that you need and all respect the same security policies.

**How Access Security Is Enforced**

Access security is enforced using the features of the Oracle Fusion Applications security approach.

Specific enforcement details apply to the following access methods.

- Single sign on (SSO)
- Navigation paths
- Scheduled processes

**Single Sign On**

The Application Development Framework (ADF) instance running Oracle Fusion Applications supports SSO user authentication. Oracle Fusion Applications uses Oracle Access Management (OAM) for SSO.

The Policy Manager in Oracle Access Management supports the administrative tasks necessary to manage SSO and URL-based authentication and authorization policies. These policies have no relationship with OPSS policies that handle function security authorization.

SSO handles authentication in the following tools and technologies accessed by Oracle Fusion Applications.

- Oracle Business Intelligence Foundation Suite for Oracle Applications
- Oracle Enterprise Scheduler
- Oracle WebCenter Content
- Extended Spread Sheet Database (ESSbase)
- Hyperion SmartView

With SSO, a user who accesses a protected resource without having a current session cookie in the browser is redirected to the SSO server for authentication. Upon successful authentication, SSO places a session cookie in the user’s browser cache.


**Navigation Paths**

Many targets are accessed through multiple navigation paths and roles. Oracle Fusion Applications tools and technologies secure the targets of access regardless of which navigation path is used.

Entitlement privileges secure navigation paths. For example, the common component Create Item securing the business process management (BPM) task Create Items must be navigated from different Work Areas based on the roles that execute the task.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Job Role</th>
<th>Navigation to Work Area (Path)</th>
<th>BPM Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Producer</td>
<td>Product Manager</td>
<td>Product Management &gt; Items</td>
<td>Create Item</td>
</tr>
<tr>
<td>Consumer</td>
<td>Warehouse Manager</td>
<td>Warehouse Operations &gt; Inventory</td>
<td>Create Item</td>
</tr>
<tr>
<td>Consumer</td>
<td>Cost Accountant</td>
<td>Costing &gt; Cost Accounting</td>
<td>Create Item</td>
</tr>
</tbody>
</table>

In the above example, for a user provisioned with the Product Manager role, the Create Item task should appear in the Items work area under the Product Management navigation path, whereas a user provisioned with the Warehouse Manager role should see the Create Item task in the Inventory work area under the Warehouse Operations navigation path.

**Oracle Enterprise Scheduler Services Processes**

Function and data security policies protect batch jobs.

**Related Topics**

- Enforcement of Security Policies: Points To Consider
- Enforcement Across Tools and Technologies: Points to Consider
- Enforcement Across Tools, Technologies, Data Transformations, and Access Methods: Explained

**Role-based Security**

**Roles-Based Applications Security: Explained**

In Oracle Applications Cloud, users have roles through which they gain access to functions and data. Users can have any number of roles. Roles are grouped hierarchically to reflect lines of authority and responsibility. User access to functions and data is determined by roles arranged in hierarchies and provisioned to that user.

Role-based security in Oracle Applications Cloud controls who can do what on which data. In role-based access:
## Component

<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 Account Payable 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 Accounts Payable Manager - US data role. This role can perform any accounts payable duties that it inherits from the Accounts Payable Manager job role on the data associated with the US business unit only.

### 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. Accounts Payable Specialist 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 Payables Invoice Processing Duty. Job and abstract roles inherit duty roles that determine the access to functions appropriate to the job. For example, the job role Accounts Payable Manager inherits the Payables Invoice Processing 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.
When Linda signs in to Oracle Applications Cloud, she doesn’t have to select a role. All of these roles are active concurrently. The functions and data that Linda can access are determined by this combination of roles.

- As an employee, Linda can access employee functions and data.
- As a line manager, Linda can access line-manager functions and data.
- As an accounts payable manager (AP manager), Linda can access AP manager related functions and data for Vision Operations.

**Reviewing Predefined Roles in the Security Reference Manuals: Explained**

The security reference manuals for Oracle Applications Cloud includes descriptions of all predefined security data in your Oracle Applications Cloud services. You can access all information in these manuals from various Oracle Applications Cloud product user interface pages. For example, you can review individual job roles using the Manage Job Roles task. However, using the manuals you can compare roles and plan any changes.

You can access the security reference manuals on cloud.oracle.com. Select Resources - Getting Started - Documentation - All Books.

The security reference manual includes the following information about the security reference implementation:

- Abstract and job roles for the offering
- Duty roles and the role hierarchy for each job role and abstract role
- Privileges required to perform each duty defined by a duty role
- Data security policies for each job role, abstract role, or data role
- Policies that protect personally identifiable information
- Data security policies on fact and dimension to ensure enforcement across tools and access methods
- Segregation of duties policies respected in the design of duties for the job role
- Segregation of duties conflicts in some job role definitions
- Templates for generating data roles and data security policies defined for those data roles

Before you provision roles to users, you can use the information in the security reference manual to help you plan role customizations, if necessary, and to plan assignment of users to roles.

**Oracle Applications Cloud Security Business Fit: Explained**

You must implement security to fit your enterprise business needs.

Oracle Applications Cloud supports an extensive predefined business process model (BPM) that is secured by a reference implementation of predefined roles and security policies.
Security Reference Implementation

The security reference implementation associates a full range of predefined roles with the business process model (BPM) levels. When assigned to users, the enterprise roles guide and control access to the task flows of the BPM and associated data. At the task level, task flows define the business actions that fulfill the intent of the BPM.

A security reference manual (SRM) for each offering presents all predefined roles, role hierarchies, business objects the roles must access, segregation of duties policies, and jobs that may have conflicting duties according to those policies. The reference implementation also can be viewed using the integrated Authorization Policy Manager (APM) and Oracle Identity Management (OIM) user interface pages to manage security policies, users, and identities.

Related Topics

- Scope of the Security Reference Implementation: Explained
- Security Tasks and Oracle Fusion Applications: How They Fit Together
- Business Process Models: Explained

Security Setup

Security Setup Tasks: How They Fit Together

Set up security before and after setting up the enterprise with enterprise structures. For some Oracle Cloud Application Services implementations, security setup before enterprise structures setup may not be relevant.

Security setup and administration tasks typically use integrated user interface pages that are provided by the following products.

- Oracle Identity Manager (OIM)
- Oracle Authorization Policy Manager (APM)
- Oracle Fusion Human Capital Management (HCM) core

To define data security, administrators and implementation users additionally access integrated user interfaces provided by several products, including the following.

- Oracle Fusion Global Human Resources
- Oracle Fusion Middleware Extensions for Applications (FND)
- Oracle Fusion General Ledger (GL)
- Oracle Fusion Supplier Portal

Manage users and enterprise role hierarchies in OIM. Manage roles, including duty roles, in APM. Perform supplier role setup tasks for trading partner security in Supplier Portal. Application administrators perform user and role provisioning tasks within applications such as HCM, General Ledger, and Supplier Portal.
Initial Security Setup

The following table shows initial security setup tasks in a likely order, as well as the conditions and purposes of the tasks and where in the user interface these tasks are performed.

<table>
<thead>
<tr>
<th>Task</th>
<th>Condition</th>
<th>Purpose</th>
<th>Performed In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Implementation Users</td>
<td>The predefined Oracle Fusion Applications super user or Oracle Cloud Application Services administrator user is generally not the user who will be setting up your enterprise</td>
<td>Create user accounts for implementation users.</td>
<td>OIM</td>
</tr>
<tr>
<td>Provision Roles to</td>
<td>An implementation user has been created with the Create Implementation Users task</td>
<td>Provision implementation users with roles, such as Application Implementation Consultant, IT Security Manager, and product family Application Administrator job or data roles.</td>
<td>OIM</td>
</tr>
<tr>
<td>Implementation Users</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Preparing the Cloud Service for Implementation Users

Creating Implementation Users

About Creating Additional Implementation Users

After you sign in for the first time, you are ready to create other users who will help you with application setup. You probably want to create additional users with the type of broad setup privileges Oracle provides to the initial user you received. The initial user can not only perform all the setup tasks, but she can also perform security tasks, including resetting passwords and the granting of additional privileges to herself and to others.

The setup, or implementation, users we create in this chapter are a bit different from the Oracle Applications Cloud application users we create in the next. Usually, these setup users are not part of your Oracle Applications Cloud service organization. You don’t create them as users in Oracle Applications Cloud. 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 broad privileges required to complete application setup. You do this through role assignment.

Your application includes several categories 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, correspond to general categories of people in an organization. You will assign users with both types of roles. For the setup users, these roles are:

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

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 users are not the only users who can do setup. In the next chapter, we discuss how you can create administrators who don’t have such broad permissions, yet can configure product-specific structures and perform other related setup tasks.

Creating Oracle Applications Cloud Implementation Users: Overview

As the service administrator for the Oracle Applications 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 Applications Cloud Service

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

Sign in to the test or production Oracle Applications Cloud service using the service home URL from the service activation mail. The URL ends with either AtkHomePageWelcome or <productname>FusionHome.

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, which is the service administrator password for subsequent access to the service.

You’re recommended not to 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>You create the implementation users and product-specific user and assign the required job roles to them if these users don’t already exist in your environment. You don’t associate named workers with these users at this time because your Oracle Applications Cloud service isn’t yet configured to onboard workers. As your implementation progresses, you may decide to replace these users or change their definitions. However these three are required initially.</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 Management (OIM) to the product within Oracle Applications Cloud.</td>
</tr>
<tr>
<td>3</td>
<td>Assign roles to the Implementation User</td>
<td>Assign the application implementation consultant job role to the implementation user that enables functional implementation to proceed.</td>
</tr>
<tr>
<td>4</td>
<td>Verify User Access</td>
<td>Confirm that the implementation user can access the functions enabled by the assigned roles.</td>
</tr>
<tr>
<td>Step</td>
<td>Task or Activity</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>5</td>
<td>Import Users and Roles for Applications Security</td>
<td>Run Import Users and Roles for Application Security process to update the application security tables with any changes made in identity management or policy management.</td>
</tr>
</tbody>
</table>

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

**Creating the HCMUser Implementation User: Procedure**

This topic explains how to create the HCMUser implementation user and assign roles to the user.

Creating the HCMUser Implementation User

If you have just created the OIMAdmin or TechAdmin implementation user and are on the Oracle Identity Manager - Delegated Administration page, then follow this procedure from step 4. Otherwise, sign in as the Oracle HCM Cloud service administrator and follow these steps:

1. Select **Navigator - Tools - 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 task Create Implementation Users.
3. On the Welcome tab of the Oracle Identity Manager - Self Service page, click **Administration** in the top-right of the page.
4. In the Users section of the Welcome tab on the Oracle Identity Manager - Delegated Administration page, click **Create User**.

Complete the fields on the Create User page as shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Name</strong></td>
<td>HCMUser</td>
</tr>
<tr>
<td><strong>Display Name</strong></td>
<td>HCMUser</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Xellerate Users</td>
</tr>
<tr>
<td><strong>User Type</strong></td>
<td>Non Worker</td>
</tr>
<tr>
<td><strong>User Login</strong></td>
<td>HCMUser</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Any value that complies with the password policy</td>
</tr>
</tbody>
</table>
To view the password policy, click the Help icon by the Password field.

**Note**
Make a note of the password. The user who first signs in as HCMUser must change the password.

5. Click **Save**.

A series of tabs appears on the Create User page.

---

**Assigning Roles to HCMUser**
To assign job roles to the HCMUser implementation user, follow these steps:

1. On the Create User page, click the Roles tab.
2. On the Roles tab, click **Assign**.
3. Search for and select the following job roles:
   - Application Administrator
   - Application Implementation Consultant
   - Application Diagnostics Regular User
   - Application Diagnostics Viewer

   These four job roles now appear on the Roles tab.
4. Click **Close Single Tab** to close the Create User page and return to the Oracle Identity Manager - Delegated Administration page.

   Close the Oracle Identity Manager Delegated Administration Console tab.

---

**Important**
Application Implementation Consultant is a powerful role that has unrestricted access to a large amount of data. Once the implementation is complete, you’re recommended to revoke this role from all users using the Revoke Data Role from Implementation Users task. For ongoing maintenance of Oracle HCM Cloud setup data, use a less powerful role, such as an HCM data role based on the Human Capital Management Application Administrator role.

---

**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 - Tools - 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 task Run User and Roles Synchronization Process.
   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 Abstract and Implementation Roles

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.
Reseting 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.

Reseting 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 - Tools - 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 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 task Manage Enterprise HCM Information in the Setup and Maintenance work area. Select Navigator - Tools - Setup and Maintenance. 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 and reactivated 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.
Value | Description
--- | ---
Both person and party users | User accounts are created automatically for both person and party users. This value is the default value.

Party users only | User accounts are created automatically for party users only.
User accounts aren’t created automatically when you create HCM person records. For HCM users, account requests are held in the LDAP requests table, where they’re identified as Suppressed. They’re not passed to Oracle Identity Management.

None | User accounts aren’t created automatically.
All user account requests are held in the LDAP requests table, where they’re identified as Suppressed. They’re not passed to Oracle Identity Management.

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>Defined by Oracle Identity Management</td>
<td>The user name follows the Oracle Identity Management user-name policy. By default, Oracle Identity...</td>
</tr>
</tbody>
</table>
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 Default User Name Format option.

<table>
<thead>
<tr>
<th>Format Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Party number</td>
<td>The party number is the user name.</td>
</tr>
<tr>
<td>Person number</td>
<td>The HCM person number is the user name.</td>
</tr>
<tr>
<td></td>
<td>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>Primary work e-mail</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.

You can override default user names for individual users on the Create User, 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>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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, Oracle Identity Management suspends user accounts automatically when the user has no roles and reactivates them 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><strong>Both person and party users</strong></td>
<td>User accounts are maintained automatically for both person and party users. This value is the default value.</td>
</tr>
<tr>
<td><strong>Party users only</strong></td>
<td>User accounts are maintained automatically for party users only. For person users, account-maintenance requests are held in the LDAP requests table, where they're identified as Suppressed and not passed to Oracle Identity Management. Select this value if you maintain accounts for person users in some other way.</td>
</tr>
<tr>
<td><strong>None</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 a person record:

- 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
  - Country code
- The person's preferred language
- The person's user name, if this value has changed

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**.
### E-Mail Destination

<table>
<thead>
<tr>
<th>E-Mail Destination</th>
<th>Description</th>
</tr>
</thead>
</table>
| Alternate contact e-mail           | 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. |
| User’s primary work e-mail         | Used if:                                                                     |
|                                    | • You specify no alternate contact e-mail.                                  |
|                                    | • The user’s primary work e-mail exists.                                   |
| Primary work e-mail of the user’s line manager | Used if:                                                                     |
|                                    | • You specify no alternate contact e-mail.                                  |
|                                    | • The user’s primary work e-mail doesn’t exist.                            |
|                                    | • The primary work e-mail of the user’s line manager exists.               |
| None                               | Oracle Identity Management sends no e-mail if:                             |
|                                    | • You specify no alternate contact e-mail.                                  |
|                                    | • The user’s primary work e-mail doesn’t exist.                            |
|                                    | • The primary work e-mail of the user’s line manager doesn’t exist.        |

### 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 - Tools - Setup and Maintenance - Manage Enterprise HCM Information** to open the Enterprise page.
2. On the Enterprise page, select **Edit - Update**.
3. In the **Update Enterprise** dialog box, enter the effective date of any changes and click **OK**. The Edit Enterprise page opens.
4. Scroll down to the User and Role Provisioning Information section.

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 - Tools - 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:

1. In step 5, use Contingent Worker as the mapping name.

2. In step 6, set **System Person Type** to Contingent Worker.

3. 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>
</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-in in the cloud?**

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

If you’re using Oracle Human Capital Management Cloud, then you submit a service request for implementation of single sign-in.
Creating and Managing Application Users

Creating Users Using the Create User Task: 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, if it exists and sending of e-mails is enabled for the enterprise.
2. The user, if no enterprise e-mail exists.
3. The user’s line manager, if the user’s e-mail doesn’t exist.

If none of these e-mails 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 **Autoprovion 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.
Create Worker appears after other business objects such as departments, locations, and jobs. You must create those business objects before worker users, regardless of how you create them.

2. Click **Create Spreadsheet** for the Create Worker entry.

3. When prompted, save the spreadsheet locally using the name Workers042713Batch01.xlsx.

4. When prompted, sign in to Oracle Fusion Applications using your Oracle Fusion user name and password.

### Entering Worker Data in the Spreadsheet

1. In the **Batch Name** field of the spreadsheet Workers042713Batch01.xlsx, replace the default batch name with the batch name Workers042713Batch01.

2. If your data includes flexfields, then click **Configure Flexfield** to configure flexfield data. Otherwise, go to step 5 of this task.

3. In the **Configure Flexfield** window, select an attribute value and click **OK**.

4. See the Flexfields Reference tab for information about the configured flexfield.

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

### Importing Worker Data and Correcting Import Errors

Use the default values except where indicated.

1. In the workers spreadsheet, click **Upload**.

2. In the **Upload Options** window, click **OK**.

   As each row of data uploads to the Load Batch Data stage tables, its status updates.

3. When uploading completes, identify any spreadsheet rows with the status **Insert Failed**, which indicates that the row didn’t import to the stage tables.

4. For any row that failed, double-click the status value to display a description of the error.

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

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

### Reviewing and Correcting Load Errors

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

   Any errors that occur during the load process appear in the spreadsheet.

2. Correct any load errors in the spreadsheet.
3. Repeat this process from Importing Worker Data and Correcting Import Errors until all spreadsheet rows both import and load successfully.

4. Close the spreadsheet.

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

**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.

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.

**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 **Autoprovision** option selected.

## How can I create a user?

Use the Manage Users task to create new application users. Use Human Capital Management (HCM) pages to perform this task.

When you create a new worker, HCM creates a new user and identity.

The Hire Employee and Add Contingent Worker tasks also result in user creation requests.

Creating a new user automatically triggers role provisioning requests based on role provisioning rules.

### Note

If you are creating implementation users for setting up your enterprise, use the Create Implementation Users task. Use the integrated Oracle Identity Management UI pages to perform this task.

## What happens when I autoprovision roles for a user?

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

The user immediately:

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

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

## Why is the user losing roles automatically?

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

If a deprovisioned role is one that you can provision manually to users, 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.

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.
5 Provisioning Roles to Application Users

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

Role provisioning occurs automatically if:

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

For example, for the data role Sales Manager Finance Department, you could select the **Autoprov**ision 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>Sales Manager</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>
<tr>
<td>HR Assignment Status</td>
<td>Active</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.

**Related Topics**

- Role Mappings: Examples
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 - Tools - 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 task Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules. 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>
</tbody>
</table>
Role-Provisioning Option | Description
--- | ---
Self-Requestable | Qualifying users can request the role for themselves.

Autoprovision | Qualifying users acquire the role automatically.

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

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoprovision is selected by default. Remember to deselect it if you don’t want autoprovisioning.</td>
</tr>
</tbody>
</table>

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 schedule the process Autoprovision Roles for All Users to run daily. 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 into effect.

Clicking **Apply Autoprovisioning** on the Create Role Mapping and Edit Role Mapping pages has the same effect as the Autoprovision Roles for All Users process. However, for performance reasons you’re recommended to schedule the process rather than click **Apply Autoprovisioning**. In any case, you must avoid applying autoprovisioning more than once in any day. Otherwise, the number of role requests generated can slow the provisioning process.

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:

- As soon as the termination is submitted or approved
- On the day after the termination date

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.

The process creates requests to add or remove roles immediately. Oracle Identity Management processes the requests on their effective dates.

Tip
You’re recommended to schedule Autoprovision Roles for All Users to run daily at a nonpeak time and after the Send Pending LDAP Requests process completes. Send Pending LDAP Requests sends bulk requests and future-dated requests that are now current to Oracle Identity Management.

The Apply Autoprovisioning Action
Clicking Apply Autoprovisioning on the Create Role Mapping and Edit Role Mapping pages has the same effect as the Autoprovision Roles for All Users process. However, for performance reasons you’re recommended to schedule the process rather than click Apply Autoprovisioning. In any case, you must avoid applying autoprovisioning more than once in any day. Otherwise, the number of role requests generated each time you apply autoprovisioning slows the provisioning process.

Important
You must not apply autoprovisioning while the Retrieve Latest LDAP Changes or Send Pending LDAP Requests processes are running. Before you apply autoprovisioning, select Navigator - Tools - Scheduled Processes and search for both processes. Confirm that they aren’t running or scheduled to run soon.

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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>The request completed successfully. The user has the role.</td>
</tr>
<tr>
<td>Failed</td>
<td>The request failed, and the role wasn’t provisioned to the user. The associated error message provides more information.</td>
</tr>
<tr>
<td>Partially complete</td>
<td>The request is in progress.</td>
</tr>
<tr>
<td>Pending</td>
<td>Oracle Identity Management received the request but processing hasn’t yet started.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The request was rejected, and the role wasn’t provisioned to the user. An associated error message may provide more information.</td>
</tr>
<tr>
<td>Requested</td>
<td>The request was made but Oracle Identity Management hasn’t yet acknowledged it.</td>
</tr>
<tr>
<td>SOD checks in progress</td>
<td>Segregation-of-duties checks are in progress. The name of any conflicting role that the user already has appears in the <strong>Conflicting Role</strong> column.</td>
</tr>
<tr>
<td>SOD checks rejected</td>
<td>The request failed segregation-of-duties checks, and the role wasn’t provisioned to the user. The associated error message provides more information. The name of any conflicting role that the user already has appears in the <strong>Conflicting Role</strong> column.</td>
</tr>
<tr>
<td>SOD remediation in progress</td>
<td>Processing to remove segregation-of-duties conflicts is in progress.</td>
</tr>
<tr>
<td>SOD remediation rejected</td>
<td>Attempts to remove segregation-of-duties conflicts were rejected. The associated error message provides more information. The name of any conflicting role that the user already has appears in the <strong>Conflicting Role</strong> column.</td>
</tr>
</tbody>
</table>
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.

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]<em>[DATE]</em>[TIME]_</td>
<td>One XML file documenting data security policies that apply to the selected user.</td>
</tr>
<tr>
<td>DataSec.zip</td>
<td></td>
</tr>
<tr>
<td>USER_NAME_[PROCESS]<em>[DATE]</em>[TIME]_</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>Hierarchical.zip</td>
<td></td>
</tr>
<tr>
<td>USER_NAME_[PROCESS]<em>[DATE]</em>[TIME]_</td>
<td>One XML file that documents functional security for the selected user. Its format is tabular (flattened).</td>
</tr>
<tr>
<td>TabularFormat.zip</td>
<td></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]<em>[DATE]</em>[TIME]_</td>
<td>One XML file documenting data security policies that apply to the selected role.</td>
</tr>
<tr>
<td>DataSec.zip</td>
<td></td>
</tr>
<tr>
<td>ROLE_NAME_[PROCESS]<em>[DATE]</em>[TIME]_</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>Hierarchical.zip</td>
<td></td>
</tr>
<tr>
<td>ROLE_NAME_[PROCESS]<em>[DATE]</em>[TIME]_</td>
<td>One XML file that documents functional security for the selected role. Its format is tabular (flattened).</td>
</tr>
<tr>
<td>TabularFormat.zip</td>
<td></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]<em>[DATE]</em>[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]<em>[DATE]</em>[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]<em>[DATE]</em>[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:

<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 or data security pages provided by Oracle Fusion Middleware Extensions for Applications (Applications Core).

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 integrated 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.

Related Topics

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

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

Use the Manage Duties task to view the entitlement carried by the duty roles in a role hierarchy, or policies carried by enterprise roles. To perform this task, you'll use the integrated Authorization Policy Manager.

Related Topics

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

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 following tasks to view the job, abstract, and data roles provisioned to a user.

- Manage Users
- Manage User Principal
- Provision Roles to Implementation Users

Use Human Capital Management and integrated Oracle Identity Management UI pages to perform these tasks. Users, roles, and provisioning information are stored in Lightweight Directory Access Protocol (LDAP) stores.

Related Topics

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

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 different or additional roles to the user.

Access is provisioned to users based on their position or job, which consists of the duties performed in that job. Provisioned enterprise roles provide access by means of inherited duty roles.

The duty roles in a role hierarchy carry privilege to access functions and data. Duty roles are not assigned 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 add duties to or remove duties from the job role.
Important

You should not change the predefined job roles. Instead, make a copy of the predefined job role and update the duties in the copy to create a custom job role.

Users are generally provisioned with roles based on role provisioning rules. If a user requests being provisioned with a role to access a task, use the security considerations of your enterprise and the roles available in your security reference implementation to determine which roles are appropriate.

Related Topics

- Security Tasks and Oracle Fusion Applications: How They Fit Together
- Reviewing Predefined Roles in the Security Reference Manuals: Explained
Security Terminology: Explained

Oracle Identity Management is the identity store and Oracle Entitlements Server is the policy store for Oracle Fusion Applications. Both applications are available independently and each has its own terminology. The terminology that Oracle Fusion Applications uses isn’t always the same as the terminology that Oracle Identity Management and Oracle Entitlements Server use.

You must understand these terminology differences as you manage business objects in each product interface. This table shows the terminology that each product uses when referring to common business objects.

<table>
<thead>
<tr>
<th>Oracle Fusion Applications</th>
<th>Oracle Identity Management</th>
<th>Oracle Entitlements Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Role</td>
<td>Role</td>
<td>External Role</td>
</tr>
<tr>
<td>Job Role</td>
<td>Role</td>
<td>External Role</td>
</tr>
<tr>
<td>Abstract Role</td>
<td>Role</td>
<td>External Role</td>
</tr>
<tr>
<td>Duty Role</td>
<td></td>
<td>Application Role</td>
</tr>
<tr>
<td>Function Security Privilege</td>
<td></td>
<td>Entitlement</td>
</tr>
<tr>
<td>Secured Code Artifact (for example, a service, task flow, or batch program)</td>
<td></td>
<td>Resource</td>
</tr>
<tr>
<td>Database Table</td>
<td></td>
<td>Database Resource</td>
</tr>
<tr>
<td>Data Security Privilege</td>
<td></td>
<td>Action</td>
</tr>
</tbody>
</table>

Oracle Identity Management also refers to data, job, and abstract roles as enterprise roles.

Tip
Oracle Entitlements Server refers to duty roles as application roles because they’re specific to a particular grouping of applications, such as Oracle Fusion Human Capital Management.
Preparing for Security Customizations: Points to Consider

You can create custom roles and role hierarchies to tailor the security in your application.

Security Customization Considerations

Before you make any security customizations, consider the following:

- It is recommended that you do not modify the predefined roles in the security reference implementation.
- If you change a predefined role, it can affect the entire job role hierarchy and can have unintended consequences.
- Changes to predefined roles can interfere with the patching process.
- During the patching process, delivered updates can’t be merged with your changes. You must choose between your changes or updates applied during the patch.
- Applying the patch can overwrite any changes you make to predefined roles.
- Patches affect only predefined roles. Patches do not affect copies of predefined roles or custom roles.

Security Customization: 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 duties. If some of your line managers don’t handle compensation, then you can create a custom line manager role without those duties. Alternatively, if a predefined job role is too narrowly defined, then you can create a job role with a greater range of duties than its predefined equivalent.

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

**Note**

If you change the security reference implementation, then the recommendation is to create custom roles rather than modify predefined roles. Upgrade and maintenance patches to the security reference implementation preserve your changes. Therefore, if you modify predefined roles, you can’t restore them to their original state by upgrading.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren’t represented in the security reference implementation, then you create a custom job roles.

Predefined Roles with Different Duties

If the duties for a predefined job role don’t match the corresponding job in your enterprise, then you add duties to or subtract duties from the job role.

Predefined Roles with Missing Duties

If the duties for a job aren’t defined in the security reference implementation, then you create custom duty roles.

Related Topics

- Reviewing Predefined Roles in the Security Reference Manuals: Explained
Managing Resources and Roles

Creating an Authorization Policy: Procedure

The authorization policy is the mechanism that defines the 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.

To create a policy, proceed as follows:

1. From the Setup and Maintenance work area, search for and go to the Manage Duties task. The integrated Authorization Policy Manager opens.
2. Access the policy creation page in one of the following ways:
   - In the Navigation Pane, navigate to the policy domain under the appropriate application node and expand it. Right-click Authorization Policies from the resource catalog node and from the context menu, select New.
   - In the Home area, select the application name under which the authorization policy will be created and from the Authorization Policies menu, click New. When using this option, the policy will be created in the Default Policy Domain.
3. Enter the required policy details.

   Note

   ◦ The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
   ◦ The name is required and case insensitive. At runtime, this is the string that the application passes to determine whether a user is authorized to access this resource.

4. Add principals to the authorization policy in one of the following ways:
   - Use the Navigation Panel for performing a search on users, external roles or application roles to list the available principals in the application. Drag and drop principals from the search results tab on to the area labelled Principals. Select Any or All depending upon the requirement.
   - In the Principals section, click Add and search for the available principals. To select multiple principals, press the Ctrl key while you mouse click, and then click Add.
5. Add Targets to the authorization policy in one of the following ways:
   - 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. Drag and drop one or more resources or entitlements from the Search Results tab into the section labeled Targets. Expand the added object in the Targets section to associate an action with it, and click Add.
   - On the Entitlements and Resources tabs, search for the available targets, select as many as you require, and click Add.

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, which have been thoroughly tested. Each entitlement contains all the permissions a user needs to complete the real world action indicated by the entitlement name.

6. Click Save to save the Authorization Policy.

Managing Application Roles: Overview

Application roles are defined at the application level and can be assigned to an external role, user, or group 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 relationships with the following:

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 inheritance pattern is such that a 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. Access the administration console of the Oracle Entitlements Server.
   You can use the Manage Duties task in the Setup and Maintenance work area to access the integrated UI pages.

2. Select the parent application from the **Application Name** list on the Home tab, and under Application Roles, click **New**.
   Alternatively, in the Search pane, browse the Applications tree nodes until you see the role catalog for the parent application. Right-click Role Catalog and select **New**.

3. Enter the required information on the General tab and save.

<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><strong>Description</strong></td>
<td>Insensitive</td>
<td>Enter useful information in the description about the entitlement.</td>
</tr>
<tr>
<td><strong>Role Category</strong></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.
Note
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. Hierarchy is not required but if you define it, use the following sub procedure:

1. Click Inherits and click **Add**.
2. 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.
3. 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.
4. 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.
5. 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, proceed as follows:

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’s 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

You use data role templates to generate data roles. Use Authorization Policy Manager (APM) to generate data roles, and create and maintain data role templates.

The attributes define a data role template.

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

The data role template specifies which base roles to combine with which dimension values for a set of data security policies. The base roles are the parent job or abstract roles of the data roles.

Note

Abstract, job, and data roles are enterprise roles in Oracle Applications Cloud. Oracle Fusion Middleware products such as Oracle Identity Manager (OIM) and Authorization Policy Manager (APM) refer to enterprise roles as external roles. Duty roles are implemented as application roles in APM and scoped to a particular application.

The dimension expresses the stripe of data, such as the territorial or geographical region you use to partition enterprise data. For example, business units are a type of dimension, and the values picked up for that dimension by the data role template as it creates data roles are the business units defined for your enterprise. The data role template constrains the generated data roles with data security grants to access specific data resources with particular actions. The data role provides provisioned users with access to a dimensional subset of the data granted by a data security policy.

An example of a dimension is a business unit. An example of a dimension value is a specific business unit defined in your enterprise, such as US. An example of a data security policy is a grant to access a business object such as a payables invoice with a manage payable invoice action (data privilege).

When you generate data roles, the template applies the values of the dimension and participant data security policies to the group of base roles.

The template generates the data roles using a naming convention specified by the template’s naming rule. 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.

For example, a data role template contains an Accounts Payable Specialist role and an Accounts Payable Manager role as its base roles, and region as its dimension, with the dimension values US and UK. The naming convention is [base-role-name]: [DIMENSION-CODE-NAME]. This data role template generates four data roles.

- Accounts Payable Specialist - US (business unit)
- Accounts Payable Specialist - UK (business unit)
- Accounts Payable Manager - US (business unit)
• Accounts Payable Manager - UK (business unit)

Making Changes To Data Role Templates
If you add a base role to an existing data role template, you can generate a new set of data roles. If the naming rule is unchanged, existing data roles are overwritten.

If you remove a base role from a data role template and regenerate data roles, a resulting invalid role list gives you the option to delete or disable the data roles that would be changed by that removal.

Making Changes to Dimension Values
If you add a dimension value to your enterprise that is used by a data role template, you must regenerate roles from that data role template to create a data role for the new dimension. For example if you add a business unit to your enterprise, you must regenerate data roles from the data role templates that include business unit as a dimension.

If you add or remove a dimension value from your enterprise that is used to generate data roles, regenerating the set of data roles adds or removes the data roles for those dimension values. If your enterprise has scheduled regeneration as an Oracle Enterprise Scheduler Services process, the changes are made automatically.

Creating a Data Role Template: Procedure
You can use these instructions to create a new role template.

To create a new template, proceed as follows:

1. Select Global, Role Templates, in the left panel, and click New to display an Untitled page in the right panel containing six tabs: 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 running simultaneously the set of templates in a group.

3. In the External Roles tab, specify the external roles for the template in one of the following ways:
   - 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. Then select roles from the results of the query and click Add. The roles selected are displayed in the Roles table.
   - Perform a regular search for external roles and drag-and-drop the desired roles from the Search Results list into 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 by default. 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 in the area Description.

6. On the Policies tab, specify the rules to create data set grants, as follows:
   - In the Database Resource area, use the button Add to add a database resource, that is, the object to be secured by the generated data security grants.
   - On the Data Sets tab, specify whether the grant is using 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. Click Save. The Oracle Authorization Policy Manager validates the information supplied and, if all data passes validation, the template is saved and the tab Summary is available.

---

### Running a Role Template: Procedure

The roles that are generated when a template is run can be previewed before the security artifacts are created. To preview the external roles that a template run generates and to run a template, follow the steps in this procedure.

**Running a Template**

To run a template, proceed as follows:

1. Open the template and bring the Summary tab to the foreground (this tab is available since the template has been saved).

2. Click Generate Roles. The roles generated are displayed in the five disjoint categories mentioned in the preceding procedure. 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.

Once external roles and data policy grants have been generated, you can verify that they have been properly created 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 returned by either of them describes the status of the run. If successful, it identifies the templates that were run. Otherwise, it identifies the error that was encountered.

Updating a Role Template: Points to Consider
Role templates can be modified or updated after they are created and run. However, there are some restrictions on updating them. You can search for the role template using the Manage Role Templates task accessible from the Tools - Setup and Maintenance work area available in the Navigator menu.

Specifics
You can make the following updates to a role template after it has been run:

• Either add an external role to a template or remove it from the template.

  When an external role is added, a template run creates external roles for the added role and for each of the dimensions. However, when it is removed, the administrator can either deactivate the external roles associated with the deleted role or leave them unchanged.

• Either add a dimension to the template dimension set or remove it from the template.

  When a dimension is added, the template run creates external roles for the added dimension only. However, when the dimension is removed, the administrator can either deactivate the external roles associated with the deleted dimension or leave them unchanged.
You cannot modify the following:

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

**Note**
However, the data that this SQL accesses may change and therefore, a new template run may return a different set of dimensions than those returned by the previous run.

## 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
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:

   ```
   > 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 implicitly 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 explicitly 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>Grants access to roles by means of entitlement</td>
</tr>
<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>
<tr>
<td>Masking</td>
<td>Hides private data on non-production database instances</td>
</tr>
<tr>
<td>Encryption</td>
<td>Scrambles data to prevent users without decryption authorization from reading secured data</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," where ‘which set of data’ is an entire object or an object instance or object instance set and ‘what’ is the object privilege.

For example, accounts payable managers can view AP disbursements for their business unit.

<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>Accounts payable managers</td>
<td>view</td>
<td>AP disbursements</td>
<td>for their business unit</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.
A business object participating in a data security policy is the database resource of the policy.

Data security policies that use job or duty roles refer to data security entitlement.

For example, the data security policy for the Accounts Payable Manager job role refers to the view action on AP disbursements as the data security entitlement.

**Important**
The duty roles inherited by the job role can be moved and job roles reassembled without having to modify the data security.

As a security guideline, data security policies based on user session context should entitle a duty role. This keeps both function and data security policies at the duty role level, thus reducing errors.

For example, a Sales Party Management Duty can update Sales Party where the provisioned user is a member of the territory associated with the sales account. Or the Sales Party Management Duty can update Sales Party where the provisioned user is in the management chain of a resource who is on the sales account team with edit access. Or the Participant Interaction Management Duty can view an Interaction where the provisioned user is a participant of the Interaction.

For example, the Disbursement Process Management Duty role includes entitlement to build documents payable into payments. The Accounts Payable Manager job role inherits the Disbursement Process Management Duty role. Data security policies for the Disbursement Process Management Duty role authorize access to data associated with business objects such as AP disbursements within a business unit. As a result, the user provisioned with the Accounts Payable Manager job role is authorized to view AP disbursements within their business unit.

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

### 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.

A data role may be granted entitlement over a set people.

For example, a Benefits Administrator A-E is allowed to administer benefits for all people that have a surname that begins with A-E.

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.

Privileged users can’t see private data such as salary details, job transactions, revenue actuals and projections, and personally identifiable information.

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.

Encryption can be enabled at the tablespace level or at the table level. 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 Custom Duty Roles: 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. This topic shows how to create a custom duty role.

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. Select Navigator - Tools - 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 hcm.
   An Untitled tab opens.
4. 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.
5. In the Role Name field, enter the duty role name. For example, enter SALES_DEPT_MANAGE_DUTY.
6. 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 a Duty Role: Procedure

This topic explains how to create a security policy for a custom duty role 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. Select **Navigator - Tools - 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 **hcm**. 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 duty role's display name and click **Search**. An Untitled tab opens.

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 Sales Department Management Duty.

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

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

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 a Duty Role: 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. 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. Select **Navigator - Tools - 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 **hcm**. 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 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 SALES_DEPT_MANAGE_DUTY in the **Role Name** field. Select your application (for example, **hcm**) 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 a Custom Duty Role: Procedure**

Once you have created a custom duty role, you’re recommended to 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 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. Select **Navigator - Tools - 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, hcm) 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.


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.

Next steps are to:

1. Add the new duty role to a job or abstract role.
2. Regenerate the data security policies for data or abstract roles that inherit this duty role.

Related Topics
- Adding Duties to a Job or Abstract Role: Procedure

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.

Restriction
Role optimization is available by separate subscription or license.

- Subscribe to the Advanced Data Security - Role Optimizer for your Oracle Applications Cloud service.
- License the Advanced Data Security - Role Optimizer for Oracle Fusion Applications for on-premise installations.

To access the role optimizer feature, you run the Role Optimization Report.
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 Diagram](image)

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.
Restriction

Role optimization is available by separate subscription or license.

- Subscribe to the Advanced Data Security - Role Optimizer for Oracle Applications Cloud services.
- License the Advanced Data Security - Role Optimizer for Oracle Fusion Applications for on-premise installations.

Navigate to the Overview page in the Scheduled Processes work area to run the report. Schedule and submit the Role Optimization Report job.

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.

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
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>

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.
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, an accounts payable manager can view invoices. The Accounts Payable Manager role provisioned to the accounts payable manager authorizes access the functions required to view invoices. Function security is also sometimes called application security and controlled by duty roles.

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

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

Related Topics

- Function Security: Explained
- Role-Based Access Control: Explained

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.

Tip
It is recommended that you do not change the predefined job and duty roles in role hierarchies. You can copy a predefined role and then 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?

You can 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
• Security Tasks and Oracle Fusion Applications: How They Fit Together

• 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
You shouldn’t remove duty roles from predefined job roles in the reference implementation. You should copy any role that doesn’t match your needs and then customize the copy.

How do I create a new job role?

Use the following tasks to view the job, abstract, and data roles provisioned to a user.

• Create Job Roles

• Manage Job Roles
Use the integrated Oracle Identity Management UI pages to perform these tasks. The Lightweight Directory Access Protocol (LDAP) identity store stores enterprise roles.

Related Topics

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

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?
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 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>User Type</td>
<td>The types of users to be processed. Values are Person, Party, and All.</td>
<td>All</td>
</tr>
<tr>
<td>Batch Size</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.
Implementing ERP Security: Overview

Oracle ERP Cloud predefines common job roles such as **Accounts Payable Manager** and **General Accounting Manager**. You can use these roles, modify them, or create new job roles as needed. A user can be assigned more than one role, so don’t define a role that includes all the accesses needed for every user.

For a listing of the predefined job roles in Oracle Fusion Financials and their intended purposes, please refer to the Security Reference Manual.

Common functionality that is not job specific, such as creating expense reports and purchase requisitions, are granted to abstract roles like **Employee**, **Line Manager**, and **Purchase Requestor**.

Oracle ERP Cloud includes the following roles that are designed for initial implementation and the ongoing management of setup and reference data:

- **Application Implementation Manager**: Used to manage implementation projects and assign implementation tasks.
- **Application Implementation Consultant**: Used to access all setup tasks.

**Note**
For ongoing management of setup and reference data, the **Financial Application Administrator**, a predefined administrator role, provides access to all financial setup tasks.

Segregation of Duties Considerations

Segregation of duties (SOD) separates activities such as approving, recording, processing, and reconciling results so you can more easily prevent or detect unintentional errors and willful fraud.

Oracle ERP Cloud includes roles that have been defined with a knowledge of a set of SOD policies that are included in the Oracle Cloud’s Access Controls Governor product. The job roles are based on those commonly defined in business and the duty definitions are defined using the Oracle Cloud SOD policies.

For example, the privilege **Create Payments** is incompatible with the privilege **Approve Invoice**. The predefined **Accounts Payable Manager** role has the privileges of **Force Approve Invoices** and **Create Payments**. When you assess and balance the cost of duty segregation against reduction of risk, you may determine that the **Accounts Payable Manager** role is not allowed to perform force approve invoices and remove this privilege.

To learn more about the policies and roles refer to the Security Reference Manual.

Data Security Considerations

- Use data security to restrict access to journal entries and balances based on certain values in the chart of accounts, such as specific companies and cost center values, to individual roles.
- Control data security to protect your organization as it grows and hires additional staff members, each responsible for only a portion of the business activities.

For more information, see:

- Oracle Enterprise Repository
- Oracle Fusion Applications Security Guide
General Ledger

General Ledger Security: Explained

Oracle Fusion General Ledger includes the following predefined roles:

- General Accounting Manager
- General Accountant
- Financial Analyst

For each of these predefined roles, the included duties grant access to application functions and data that corresponds to their responsibilities. For example, the General Accounting Manager role grants comprehensive access to all general ledger functions to both the Chief Financial Officer and the Controller.

General Ledger uses data roles to provide access to specific ledgers. Access is granted for individual ledgers or for a set of ledgers. You decide whether each role provides read-only access or read and write access. For example, grant the ability to create journal entries and modify existing journal entries or the ability to only view journals.

General Ledger automatically creates the data roles that provide single ledger access. You then manually set up the consolidated accesses to other ledgers.

Ledger Security

Data Access Set Security: Overview

Data Access Sets secure access to ledgers, ledger sets, and portions of ledgers using primary balancing segment values. If you have primary balancing segment values assigned to a legal entity, then you can use this feature to secure access to specific legal entities.

- Secures parent or detail primary balancing segment values.
- Secures the specified parent value as well as all its descendents, including midlevel parents and detail values.
- Requires all ledgers assigned to the data access set to share chart of accounts and accounting calendar.

When a ledger is created, a data access set for that ledger is automatically created; giving full read and write access to that ledger. Data access sets are automatically created when you create a new ledger set as well. You can also manually create your data access sets to give read only access or partial access to select balancing segment values in the ledger.

You can combine ledger and ledger set assignments to a single data access set you create as long as the ledgers all share a common chart of accounts and calendar. When a data access set is created, data roles are automatically created for that data access set. Three data roles are generated for each data access set, one for each of the Oracle Fusion General Ledger roles:

- General Accounting Manager
- General Accountant
- Financial Analyst
The data roles then must be assigned to your users before they can use the data access set.

- **Full Ledger Access**: Access to the entire ledger or ledger sets. For example, this could mean read only access to the entire ledger or both read and write access.

- **Primary Balancing Segment Value**: Access one or more primary balancing segment values for that ledger. You can specify read only, read and write access, or a combination of the two for different primary balancing segment values for different ledgers and ledger sets.

**Note**

Security by management segment consistent with the primary balancing segment as used above is not currently available.

### Data Access Set Security: Examples

This example shows two data access sets that secure access by using primary balancing segment values that correspond to legal entities.

**Scenario**

The figure shows the actions enabled when an access level is assigned to a balancing segment representing legal entities (LE) for one of the two access levels:

- **Read Only**
• Read and Write

InFusion USA Primary Ledger

Access Level

Balancing Segment Values (Legal Entity)

Actions

Read Only

Read and Write

131 InFusion USA Health (LE3)

View Journals
View Balances
View and Run Reports

101 InFusion USA Health (LE1)

View, Create, Post Journals
View and Update Balances
View and Run Reports

102 InFusion USA Health (LE2)

• InFusion USA Primary Ledger is assigned to this Data Access Set.

• Read only access has been assigned to balancing segment value 131 that represents the InFusion USA Health LE3.

• Read and write access has been assigned to the other two primary balancing segment values 101 and 102 that represent InFusion USA Health LE1 and LE2.

In summary, you can:

• Create a Journal Batch: In ledgers or with primary balancing segment values if you have write access.

• Modify a Journal Batch: If you have write access to all ledgers or primary balancing segment values that are used in the batch.

• View a Journal Batch: If you have read only or write access to the ledger or primary balancing segment values.

**Security on a Chart of Accounts**

**Enabling Security on a Chart of Accounts: Example**

Enabling security for a chart of accounts controls access to values in your account segments. To enable security:

• Create and assign conditions and polices to rules.

• Specific data roles to control access during journal entry, account inquiry, and reporting.
Note
Before proceeding with these steps, determine what roles are defined and assigned in Oracle Identity Manager (OIM) for each ledger and its chart of accounts. The definition of security policies requires specifying roles that are impacted by these rules.

Important: As soon as segment value security is enabled on the chart of accounts, all users are denied access to that chart of accounts. The system administrator must specifically grant security policies to the users’ roles to enable the users to access their values for that chart of accounts.

Scenario
In this example, you are responsible for creating a segment value security rule for each of your segments of your InFusion America chart of accounts.

1. Ensure that your tree and tree version definitions are properly set up.

   Note
   This step is important if you plan on using tree operators in your policy definitions since the policy may not provide the expected action if the hierarchy is not properly defined.

2. Navigate to the Setup and Maintenance page.

3. In the All Tasks tab, search for Manage Segment Value Security Rules. Click the Go to Task.

4. Enter the wanted information into the Value Set Code field. Click Search.

5. With the value set highlighted, click Edit.

6. Enable the Security enabled check box.

7. Enter the Data Security Resource Name.

8. Click Edit Data Security to begin defining the security condition and policy.

9. With the Condition tab selected, click Create to begin creating the condition.
Note
While defining each condition, you can select to specify whether it uses tree operators or regular operators. Only the following operators are supported.

- For non-tree operators select from:
  - Equal to
  - Not Equal to
  - Between
  - Not Between

- For tree operators select from:
  - Is a last descendent of
  - Is a descendent of

10. Click Save.
11. On the Policy tab, click Create in the General Information tab.
12. Enter information in the General Information tab.
13. Select the Role tab and search for the relevant data role to assign to this policy.
14. Click the Rule tab to associate the relevant condition with the policy.

Note
The Row Set field determines the range of value set values affected by the policy.

- If Multiple Values is selected, then a condition must be specified.
- If All Values is selected, then the policy grants access to all values in the value set and no condition is needed.

15. Repeat these steps for the remaining value sets in your chart of accounts.
16. Click Save and Close.
17. Click Submit.
18. The last step is to run the deploy process by clicking the Deploy Flexfield button on the Manage Key Flexfields page before security is enabled for the chart of accounts.

Related Topics
- Flexfield Deployment: Explained
Segment Value Security: Examples

Segment value security is enforced in Oracle Fusion Applications where ever the charts of accounts values are used.

Scenario

1. When entering a journal for a ledger with a secured chart of accounts, you can only use account values for which the access is granted using segment security rules.
2. When running reports against a ledger with a secured chart of accounts, you can only view balances for accounts for which the access is granted using segment security rules.
3. When viewing ledger options in an accounting configuration, if the accounts specified include references to an account with values you have not been granted access to, you can see the account but not be able to enter that secured value if you select to modify the setup.

Example

Create conditions and assign them to specific data roles to control access to your segment values. For example:

1. Enable security on both the cost center and account value sets that are associated with your chart of accounts.
2. Assign the General Accountant - InFusion USA data role to have access to cost center Accounting and account US Revenue.
3. Deny all other users access to the specified cost center and account values.

Segment Value Security Operators

Use any of the following operators in your conditions to secure your segment values:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal to</td>
<td>• Secures a detail specific value.</td>
</tr>
<tr>
<td></td>
<td>• Don't use this operator to secure a parent value.</td>
</tr>
<tr>
<td>Not equal to</td>
<td>• Secures all detail values except the one that you specify.</td>
</tr>
<tr>
<td></td>
<td>• Don't use this operator to secure a parent value.</td>
</tr>
</tbody>
</table>
### Operator

<table>
<thead>
<tr>
<th>Operator</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between</td>
<td>Secures a detail range of values.</td>
</tr>
<tr>
<td>Is descendent of</td>
<td>Secures the parent value itself and all of its descendents including mid level parents and detail values.</td>
</tr>
<tr>
<td>Is last descendent of</td>
<td>Secures the last descendents, for example the detail values of a parent value.</td>
</tr>
</tbody>
</table>

**Tip:**

For Is descendent of and Is last descendent of:

- Specify an account hierarchy (tree) and a tree version to use this operator.
- Understand that the security rule applies across all the tree versions of the specified hierarchy, as well as all hierarchies associated with the value set.

-----

## FAQs for General Ledger

### How do I view, create, or update accounting flexfield segment security rules?

Use the Manage Security Segments task, which is available in Oracle Fusion General Ledger.

### How do I view, create, or update data access sets used to secure ledgers and ledger sets?

Use the Manage Data Access Sets task, which is available in Oracle Fusion General Ledger.

### When does security take effect on chart of accounts value sets?

New security policies must be defined before the ledger is created and account hierarchies are published to be effective.

### How can I secure GL balances cubes?

Secure GL balances cubes with chart of accounts dimension values, which use data access set and segment value security. Security restricts the display of data, not the selection of dimensions. For example, you can select the Company dimension for your report definition, but may not be able to display company 100 if your data access set or segment value security does not allow you access to that value.
What's the difference between balance cube security and other General Ledger security?

Balance cube security applies only to the Account Monitor, Account Inspector, Financial Reporting, Smart View, and Allocations. Balance cube security is based on the data access security plus the security rules rather than just the current data access set. When you create or change existing data access security or security rules, you must republish any tree version affected by the change. Use the Publish Account Hierarchies page. Republishing is required for the security to become effective in the cube.

All other General Ledger security, such as detail balances and journal entries, are based on current selected data access set.

Payables

Payables Security: Explained

In Oracle Fusion Payables you secure access to invoices and payments by business unit. You can access invoices and payments for viewing or processing only in the business units to which you have permission. The permission must be explicitly granted to each user using data roles.

Payables is integrated to the document repository for processing scanned invoices. Edit access to the document repository is granted to the following predefined roles:

- Accounts Payable Manager
- Accounts Payable Specialist
- Accounts Payable Supervisor

The following predefined roles have view-only access to the document repository:

- Financial Application Administrator
- Cost Accountant
- Project Accountant

Subledger Accounting

Security for Subledger Accounting: Explained

Oracle Fusion Subledger Accounting features require both function and data security privileges.

Overview

Security for Subledger Accounting includes:

- Setup task security
  - Security to configure accounting rules to define accounting treatments for transactions.
• Transaction task security
  ◦ Security to create subledger journal entries (manual subledger journal entries or those generated by the Create Accounting process or Online Accounting)
  ◦ Security to review and generate reports of subledger journal entries and lines.

Security to Perform Setup Tasks
Use the Define Subledger Accounting Rules task in the Setup and Maintenance work area to configure subledger accounting rules.

To configure subledger accounting rules, the setup user must be provisioned with a role that includes the Subledger Accounting Administration duty role.

• In the security reference implementation, the Financial Application Administrator job role hierarchy includes the Subledger Accounting Administration duty role, which provides the access to configure your accounting rules.
• For more information on available setup job roles, duty roles and privileges, see the Oracle Fusion Financial Security Reference Manual.

Security to Perform Transactional Tasks
To create and view subledger journal entries, you must have the access necessary to perform the tasks, which can be accessed from the relevant subledger work areas. Predefined subledger job roles and data roles include entitlement to create and view subledger journal entries for subledger transactions that you are authorized to access.

**Security for Accounting Transformations: Explained**

Accounting transformations require both function and data security privileges.

Oracle Fusion Accounting Hub security for accounting transformations include:

• Setup task security
  ◦ Security to integrate your external systems with accounting transformations, indicating what types of transactions or activities require accounting from those systems.
  ◦ Security to configure accounting rules to define accounting treatments for transactions.

• Transactional task security
  ◦ Security to create subledger journal entries (manual subledger journal entries or those generated by the Create Accounting process).
  ◦ Security to review and generate reports of subledger journal entry headers and lines.

Security to Perform Setup Tasks
Use the Define Accounting Transformation Configuration task in the Setup and Maintenance work area to integrate your external systems with the Accounting Hub.

To register your external systems and configure accounting rules, the setup user needs to be provisioned with a role that includes the Accounting Hub Administration Duty role.

• In the security reference implementation, the Financial Application Administrator job role hierarchy includes the Accounting Hub Administration Duty role, which provides the access to integrate your external systems with accounting transformations.
For more information on available setup job roles, duty roles and privileges, see the Oracle Fusion Accounting Hub Security Reference Manual.

Security to Perform Transactional Tasks

To create and view subledger journal entries, you must have the access necessary to perform the tasks. These tasks can be accessed from the Oracle Fusion General Ledger, Journals work area, therefore you must have access to the work area, and the ledgers (primary, secondary and reporting currency) in which the journal entry is posted.

The following are defined in the security reference implementation:

- The General Accounting Manager job role hierarchy includes duty roles that provide entitlement to manage your general accounting functions. This entitlement provides access to General Ledger Journals work area.
- The General Accounting Manager data role hierarchy includes data security policies that provide entitlement to access ledger and subledger journal entries.
  - Ledger access is provided through Data Access Sets.

The following duty roles need to be assigned directly to the General Accounting Manager job role to provide access to create and view subledger journal entries:

- Subledger Accounting Duty
- Subledger Accounting Reporting Duty

Alternatively, you can assign the Subledger Accounting Duty and Subledger Accounting Reporting Duty roles to any of the following General Ledger job roles:

- Chief Financial Officer
- Controller
- Financial Analyst
- General Accountant

Related Topics

- Data Security: Explained

Cash Management

Creating Accounts: Points to Consider

Banks, branches and accounts fit together on the premise of the Bank Account model. The Bank Account model enables you to define and keep track of all bank accounts in one place and explicitly grant account access to multiple business units, functions, and users. Consider the following when you set up bank accounts:

- Assigning a unique general ledger cash account to each account and use it to record all cash transactions for the account. This facilitates book to bank reconciliation.
- Granting bank account security; bank account security consists of bank account use security, bank account access security, and user and role security.
Account Use
Refers to accounts created for:

- Oracle Fusion Payables
- Oracle Fusion Receivables
- Oracle Fusion Payroll

When creating an account to be used in one or more of these applications you must select the appropriate use or uses.

Account Access
Payables and Receivables account access is secured by business unit. In addition to selecting the appropriate application use or uses, one or more business units must be granted access before the bank account can be used by Payables and Receivables. Only business units that use the same ledger as the bank accounts owning legal entity can be assigned access.

User and Role Security
You have the option to further secure the bank account so that it can only be used by certain users and roles. The default value for secure bank account by users and roles is No. In Payables and Receivables even if the secure bank account by users and roles is No, you must have the proper business unit assigned to access a bank account. If the secure bank account by users and roles is set to Yes, you must be named or carry a role assigned to the bank account to use it.

Note
The security role Bank and Branch Management Duty is used to set up banks and branches.
The security role Bank Account Management Duty is used to set up accounts.

Assets

Assets Data Security Components: How They Work Together
In Oracle Fusion Assets, you can secure access to assets to perform transactions and view their information by asset book. Every asset book created in Assets is automatically secured. You can perform transactions or view asset data only in the books to which you have permission. The permission must be explicitly granted to each user based on his or her duty requirements.

Data Privileges
Each activity is individually secured by a unique data privilege. In other words, when you provide access to a book, you actually provide permission to perform a particular activity in that book. For example, you can allow user X to perform only tasks related to asset additions in book AB CORP and restrict the same user from performing asset retirements in this book.

The data accesses for different asset activities are secured for the book with the following data privileges:

- Add Fixed Asset Data
- Change Fixed Asset Data
- Retire Fixed Asset Data
- Track Fixed Asset Data
Data Roles
An asset book creation event is created when ever you set up an asset book during initial implementation or subsequent maintenance. The asset book creation event automatically invokes the data role generation service, which runs the Assets template for the asset book data role template and generates at least one data role for each applicable role and asset book combination. The data role generated automatically inherits the function privileges from the base role and grants data access as per its data policies.

You can update the Assets template for the asset book data role template definition or create a new template in Oracle Identity Management to meet your various data security requirements. For example you may want to create more than one data role for an asset book with each role having different data security policies or privileges. You can update the data role’s polices any time after its creation to add new policies or remove an existing policy.

Default Asset Books
Since the data access is secured by book, you must provide or select the book to perform transactions and view asset details. If you have access to only one book, you can set up this book as the default book. In this case, the default book is automatically entered in the Book field when you perform transactions and run reports. You can override the default and enter another value from the list of values. If the default book is not valid in the given context, then the Book field is left blank. In some transaction flows this defaulting behavior does not apply. The default book value must be set using the Default Book profile option. You set the value at the site, product or user level.

Related Topics
- Oracle Fusion Assets Profile Options: Critical Choices
- Data Role Templates: Explained

Payments

System Security Options: Critical Choices
You can implement system security options on the Manage System Security Options page as part of a complete security policy that is specific to your organization. Security options can be set for encryption and tokenization of credit cards and bank accounts, as well as for payment instrument masking. Security options are used for both funds capture and disbursement processes.

To secure your sensitive data, consider your responses to the following security questions:

- Which security practices do you want to employ?
- Do you want to automatically create a wallet file and master encryption key, and automatically implement encryption or do you want to use some combination of an automatic and manual process?
- Do you want to tokenize your credit card data?
- Do you want to encrypt your bank account data?
- Do you want to encrypt your credit card data?
• How frequently do you want to rotate the master encryption key and the subkeys?

• Do you want to mask credit card and bank account numbers, and if so, how?

To set up system security options, navigate as follows: Setup and Maintenance work area > All Tasks tab > Search field: Task Lists and Tasks > Name field: Payments > Search button > Define Payments Security folder > Manage System Security Options task > Go to Task icon > Manage System Security Options page.

Best Security Practices
The following actions are considered best security practices for payment processing:

• Comply with the Payment Card Industry Data Security Standard (PCI-DSS), which is the security standard that is required for processing most types of credit cards.
  ◦ Comply with all requirements for accepting credit card payments.
  ◦ Minimize the risk of exposing sensitive customer data.
  ◦ Work with a PCI-DSS auditor to ensure compliance with the required security standards and to avoid potential violations.

• Encrypt and mask customer credit card and supplier bank account numbers and card holder names before importing or entering data into Payments.

• Create a wallet.
  ◦ Store the wallet file in a very secure, limited access file system location.
  ◦ Obtain a master encryption key and subkeys externally or let Payments generate them automatically.
  ◦ Rotate the master encryption key periodically.

Implementation Process of Wallet File, Master Encryption Key, and Encryption
Before you can enable encryption for credit card or bank account data, you must automatically or manually create a wallet file that exists on the file system of the Oracle Enterprise Storage Server. A wallet file is a digital file that stores your master encryption key, which the application uses to encrypt your sensitive data.

Important
Oracle Cloud customers can only use the automatic process to create the wallet file, the master encryption key, and implement encryption. On-premise customers can optionally use some combination of an automatic and manual process or an entirely manual process to take the same actions.

Automatic creation of the wallet file ensures that the wallet file is created in the proper location and with all necessary permissions.

Manual creation of the wallet file and use of your own master encryption key requires a file that contains your binary (3DES) encryption key. Both files must be placed in the same directory. The directory must be readable and writable by the Weblogic Server (WLS) container hosting the Financials Domain.

Tip
If you manually create a wallet, ensure that you enter the full path of the ewallet.p12 in the New Wallet File Location field of the Master Encryption Key dialog box.
Credit Card Tokenization

By choosing to tokenize your credit card data, you are complying with Payment Card Industry Data Security Standard (PCI-DSS) requirements that companies must use payment applications that are PA-DSS compliant.

Tokenization is the process of replacing sensitive data, such as credit card data, with a unique number, or token, that is not considered sensitive. The process uses the service of a third-party payment system that stores the sensitive information and generates tokens to replace sensitive data in the applications and database fields. Unlike encryption, tokens can’t be reversed mathematically to derive the actual credit card number.

You can set up your tokenization payment system by clicking the Edit Tokenization Payment System button on the Manage System Security Options page and selecting your tokenization payment system. Then, to activate tokenization for credit card data, click the Tokenize button in the Credit Card Data section.

Credit Card Data Encryption

You can choose to encrypt your credit card data to assist with your compliance of cardholder data protection requirements with the following:

- Payment Card Industry (PCI) Data Security Standard
- Visa’s PCI-based Cardholder Information Security Program (CISP)

Credit card numbers entered in Oracle Fusion Receivables and Oracle Fusion Collections are automatically encrypted based on the credit card encryption setting you specify on the Manage System Security Options page.

Tip
If you bring card numbers into Payments through import or customization, it is advisable to run the Encrypt Credit Card Data program immediately afterward.

Bank Account Data Encryption

You can encrypt your supplier and customer bank account numbers.

Important
Bank account encryption doesn’t affect internal bank account numbers. Internal bank accounts are set up in Oracle Fusion Cash Management and are used as disbursement bank accounts in Oracle Fusion Payables and as remit-to bank accounts in Receivables.

Supplier, customer, and employee bank account numbers entered in Oracle applications are automatically encrypted based on the bank account encryption setting you specify on the Manage System Security Options page.

Note
If you bring bank account numbers into Payments through import or customization, it is advisable to run the Encrypt Bank Account Data program immediately afterward.

Master Encryption Key and Subkey Rotation

For payment instrument encryption, Payments uses a chain key approach. The chain key approach is used for data security where A encrypts B and B encrypts C. In Payments, the master encryption key encrypts the subkeys and the subkeys encrypt the payment instrument data. This approach allows easier rotation of the master encryption key.

Whether you create the master encryption key automatically or manually, it is stored in the wallet. The wallet is an Oracle Applications program module that protects stored data in an encrypted format. The master encryption key can be rotated, or generated, which re-encrypts the subkeys, but does not result in a re-encryption of the credit card or bank account numbers.
If your installation already has an existing master encryption key, you can rotate, or generate, a new one by clicking the Edit Master Encryption Key button and creating it automatically or manually.

**Tip**

To secure your payment instrument data, you are advised to schedule regular rotation of the master encryption key once a year or according to your company’s security policy.

You can also choose the frequency with which new subkeys are automatically generated, based on usage or on the maximum number days. To specify a subkey rotation policy, click the **Edit Subkey Rotation Policy** dialog box.

**Tip**

To secure your payment instrument data, you are advised to schedule regular rotation of the subkeys.

The security architecture for credit card data and bank account data encryption is composed of the following components:

- Oracle Wallet
- Payments master encryption key
- Payments subkeys
- Sensitive data encryption and storage

The following figure illustrates the security architecture of the wallet, the master encryption key, and the subkeys.

**Credit Card and Bank Account Number Masking**

Payments serves as a payment data repository on top of the Oracle Fusion Trading Community Architecture (TCA) model. TCA holds customer and supplier information. Payments stores all of the customer and supplier payment information and their payment instruments, such as credit cards and bank accounts. Payments provides data security by allowing you to mask payment instrument numbers.

On the Manage System Security Options page, you can mask credit card numbers and external bank account numbers by selecting the number of digits to mask and display. For example, a bank account number of XXXX8012 displays the last...
four digits and masks all the rest. These settings specify masking for payment instrument numbers in the user interfaces of multiple applications.

### Enabling Encryption of Sensitive Payment Information: Procedures

Financial transactions contain sensitive information, which must be protected by a secure, encrypted mode. To protect your credit card and external bank account information, you can enable encryption. Encryption encodes sensitive data, so it can’t be read or copied. Before enabling encryption, you must create a wallet file. A wallet file is a digital file that stores your master encryption key, which the application uses to encrypt your sensitive data.

**Note**

For Oracle Cloud customers, only method 1, completely automatic, is applicable. For on-premise customers, methods 2 to 4 are applicable.

To secure your credit card or bank account data, you can use any one of the methods shown in the table.

<table>
<thead>
<tr>
<th>Method</th>
<th>Create Wallet File</th>
<th>Generate Master Encryption Key</th>
<th>Enable Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Automatically</td>
<td>Automatically</td>
<td>Automatically</td>
</tr>
<tr>
<td>2</td>
<td>Automatically</td>
<td>Automatically</td>
<td>Manually</td>
</tr>
<tr>
<td>3</td>
<td>Manually</td>
<td>Automatically</td>
<td>Manually</td>
</tr>
<tr>
<td>4</td>
<td>Manually</td>
<td>Manually</td>
<td>Manually</td>
</tr>
</tbody>
</table>

**Tip**

For all methods, navigate to the Setup and Maintenance work area and search for the Manage System Security Options task.

**Method 1**

To use method 1, perform the following steps:

1. Open the Manage System Security Options page.
2. Click **Apply Quick Defaults**.
3. Select all the check boxes:
   - Automatically create wallet file and encryption key
   - Encrypt credit card data
   - Encrypt bank account data
4. Click **Apply**.

**Method 2**

To use method 2, perform the following steps:

1. Open the Manage System Security Options page.
2. Click **Edit Master Encryption Key**.
3. Select **Automatically create wallet file and master encryption key**.
4. Click **Save and Close**.
5. On the Manage System Security Options page, click **Encrypt** in either the Credit Card Data section or the Bank Account Data section or in both sections.

**Methods 3 and 4**

To use method 3 or 4, perform the following steps:

1. Using the Oracle Wallet Manager utility, create an empty wallet file called ewallet.p12.
2. Open the Manage System Security Options page.
3. Click **Edit Master Encryption Key**.
4. Take one of the following actions:
   - In the **New Wallet File Location** field, enter the path to the master encryption key, click **Save and Close**, and then click **Done**.
   - Generate a secure, custom key by copying a file containing the bits of the key to the same directory as the empty Oracle wallet, ewallet.p12.

   **Important**
   After manually creating the wallet file, delete the file containing the key bits using a utility that supports secure deletion.

5. For the Master Encryption Key, select **Application-generated** for method 2 or select **User-defined** for method 3.
6. Click **Save and Close**.
7. On the Manage System Security Options page, click **Encrypt** in either the Credit Card Data section or the Bank Account Data section or in both sections.
Implementing Security in Oracle Fusion Project Portfolio Management

Provisioning Access to Project Execution Management Applications: Overview

Use the Manage Project User Provisioning page to request user accounts and assign enterprise roles for project enterprise labor resources. This action enables resources to sign into Project Execution Management applications to plan projects, manage resources, review, track, and collaborate on work.

You can also request user accounts and assign enterprise roles when you create or edit resources on the Manage Project Enterprise Resources page.

During implementation you can provision a set of users and assign the Project Application Administrator role so that these administrators can initiate the provisioning process for the rest of the project enterprise labor resources.

Resources to Provision

A resource that you provision typically falls into one of these categories:

- Resource is an employee or contingent worker in Oracle Fusion HCM and is a project enterprise labor resource in Oracle Fusion Project Management.

  User accounts for these resources are typically created in Oracle Fusion HCM. You can associate the employee or contingent worker with a project enterprise labor resource and assign project-related roles when you create the resource in Oracle Fusion Project Management.

  Important
  You can't create a user account in Oracle Fusion Project Management for an existing HCM employee or contingent worker. HCM persons are registered in Oracle Fusion HCM.

- Resource is a project enterprise labor resource in Oracle Fusion Project Management, but isn’t an HCM employee or contingent worker.

  You can maintain resource details and add resources to projects even if the resources aren’t HCM employees or contingent workers. Create user accounts to register the resources in Oracle Identity Management, and assign project-related enterprise roles to the resources.

- Resource is an HCM employee or contingent worker, but isn’t a project enterprise labor resource in Oracle Fusion Project Management.

  You can assign project-related enterprise roles to resources who have user accounts that were created in Oracle Fusion HCM. However, you must create the resources in Oracle Fusion Project Management before you can assign them to projects, or before the resources can open project or resource management pages in the application.
Enterprise Roles

You can provision the following predefined enterprise roles to resources:

- Project Application Administrator: Collaborates with project application users to maintain consistent project application configuration, rules, and access.
- Project Execution: Manages projects in Project Execution Management applications. Manages issues, deliverables, changes, and the calendar.

**Note**
The Project Manager job role doesn’t include the Project Execution enterprise role by default.

- Resource Manager: Manages a group of project enterprise labor resources. Monitors the utilization of resources and manages the assignment of resources to work on projects. Collaborates with project managers to find suitable resources to fulfill project resources requests.
- Team Collaborator: Performs, tracks, and reports progress on project and nonproject work. Collaborates with other team members or project managers to perform project tasks and to-do tasks. Manages issues, deliverables, changes, and the calendar.

In addition, you can provision custom job roles for resources. For example, you can provision a Custom Team Member role that contains a different set of security permissions than the Project Team Member role.

Default Role Assignments

You can select project-related predefined and custom roles to provision by default. The application assigns the default roles to project enterprise labor resources that you create using any of the following methods:

- Import Project Enterprise Resource process for Oracle Cloud
- Project Enterprise Resource External Service
- Import HCM Persons as Project Enterprise Resources process
- Export Resources and Rates process that moves resources from the planning resource breakdown structure in Project Financial Management applications to Oracle Fusion Project Management
- Maintain Project Enterprise Labor Resources process in Oracle Fusion Project Resource Management

**Important**
Default role assignments apply only to resources who are employees or contingent workers.

Go to the Manage Project User Provisioning page - Default Provisioning Attributes tab - Default Role Assignment section to select the default roles. Then select the Automatically Provision Roles When MassCreating Project Enterprise Labor Resources option.

Project User Account and Role Provisioning Statuses: Explained

This topic describes project user account and role provisioning statuses in Project Execution Management applications.
Project User Account Statuses

The user account status indicates whether a project enterprise labor resource can access Project Execution Management applications based on assigned roles. The following table lists the project user account statuses.

<table>
<thead>
<tr>
<th>User Account Status</th>
<th>Description</th>
</tr>
</thead>
</table>
| Active              | The user is active and can access the application. A project user account is active for a resource in either of these scenarios:
  - You create a user account for the resource in Oracle Fusion Project Management.
  - The resource is an employee or contingent worker with an active account in Oracle Fusion Human Capital Management (HCM). |
| Inactive            | The user is inactive and cannot access the application. A project user account is inactive for a resource in either of these scenarios:
  - The resource is an employee or contingent worker who is no longer active in HCM, such as when the employee is terminated.
  - The resource isn’t an employee or contingent worker and you disable the resource in Oracle Identity Management. |

Role Provisioning Statuses

When you create a user account in Oracle Fusion Project Management and assign project enterprise roles to the resource, the application sends a provisioning request to Oracle Identity Management. The role provisioning status indicates the processing status of the request. The following table lists the role provisioning statuses.

<table>
<thead>
<tr>
<th>Role Provisioning Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>Role provisioning is requested for a resource.</td>
</tr>
<tr>
<td>Completed</td>
<td>Role provisioning completed without errors or warnings.</td>
</tr>
<tr>
<td>Failed</td>
<td>Role provisioning failed because of errors or warnings.</td>
</tr>
<tr>
<td>Partially completed</td>
<td>Role provisioning is partially complete.</td>
</tr>
<tr>
<td>Role Provisioning Status</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Pending</td>
<td>Role provisioning is in progress.</td>
</tr>
<tr>
<td>Provisioned</td>
<td>The role is provisioned in Oracle Identity Management.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The role provisioning request is rejected by Oracle Identity Management.</td>
</tr>
</tbody>
</table>

You can view project user account and role provisioning statuses on the Manage Project User Provisioning page and Manage Project Enterprise Resources page.

## Provisioning Project Resources on the Manage Project User Provisioning Page: Procedure

Use the Manage Project User Provisioning page to create and update project users, request user accounts, and assign enterprise roles to resources. This action enables resources to sign into Project Execution Management applications to plan projects, manage resources, and review, track, and collaborate on work.

### Creating and Provisioning a User

Perform these steps to create a project user, request a user account, and provision roles on the Manage Project User Provisioning page.

1. In the Navigator, click **Setup and Maintenance**.
2. Search for the Manage Project User Provisioning task.

   **Note**
   The Manage Project User Provisioning task is included in the Project Execution Management offering in Oracle Fusion Functional Setup Manager.

3. Click the **Go to Task** icon to open the **Manage Project User Provisioning page - User Provisioning tab**.
4. Click the **Create** icon to open the **Create Project User** window.
5. Enter the required fields and click the **Request User Account** option. When you select the **Request User Account** option, the roles that you specified to provision by default appear in the Role Details table for the resource.
6. Select the **Assign Administrator Role** option to assign the Project Application Administrator role to the resource. This action adds the Project Application Administrator role to the Role Details table.
7. Add predefined or custom roles to the Role Details table, as needed. The predefined roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team Collaborator</td>
<td>Performs, tracks, and reports progress on project and nonproject work. Manages issues, deliverables, changes, and the calendar.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Project Execution</td>
<td>Manages projects in project management applications and is not assigned the project manager job role. Manages issues, deliverables, changes, and the calendar.</td>
</tr>
<tr>
<td>Project Application Administrator</td>
<td>Collaborates with project application users to maintain consistent project application configuration, rules, and access.</td>
</tr>
</tbody>
</table>

**Note**
The Team Collaborator and Project Execution roles appear in the Role Details table by default. You can change the default roles on the Manage Project User Provisioning page - Default Provisioning Attributes tab.

8. Click **Save and Create Another** or **Save and Close**.

This action:
- Sends a request for a user account to Oracle Identity Management
- Sends the resource an e-mail notification when the provisioning process is successful

**Additional points to consider:**

- You can add or remove roles for a resource with an existing user account. Use the **Edit** feature to add roles. Use the **Actions** menu to remove roles.

**Note**
You must wait until the previous provisioning request is complete for a resource before you add or remove roles for the resource.

- Use the **Assign Resource as Project Manager** action in the Search Results region to add a resource to a project as a project manager. When you add a project manager with the **Assign Resource as Project Manager** action, the application provisions the Project Execution role for the resource.
- Click the link in the **Last Request Status** column to view the details of the most recent provisioning action for a resource.
- On the **Manage Project User Provisioning page - Default Provisioning Attributes tab**, you can:
  - Select project-related predefined and custom roles to provision by default when you create project users.
Select the **Automatically Provision Roles When Mass Creating Project Enterprise Labor Resources** option to assign the default roles when creating users with import processes and services for employees and contingent workers.

---

### Provisioning Project Resources on the Manage Project Enterprise Resources Page: Explained

You can provision a resource on the Manage Project Enterprise Resources page when you create or edit a resource who is not an employee or contingent worker in Oracle Fusion Human Capital Management.

#### Provisioning a Resource

You can request a user account from the Create Project Enterprise Resource window or Edit Project Enterprise Resource window.

- On the Create Project Enterprise Resource window, select the **Request User Account** option.
- On the Edit Project Enterprise Resource window, click **Activate User Account**.

When you request a user account from the Create or Edit Project Enterprise Resource window, the application:

- Provisions the default role assignments for the resource
- Sends a request for a user account to Oracle Identity Management
- Sends the resource an e-mail notification when the provisioning process is successful

Click the link in the **User Account Status** column to view the role provisioning status of the most recent provisioning action for a resource.

---

### Project Roles in Project Execution Management Applications: Explained

A project role is a classification of the relationship that a person has to a project, such as project manager, functional consultant, or technical lead. A project role defines the type of work that a person performs on a project, and allows access to project management information for the project manager role.

Project manager and project team member are predefined project roles that you cannot edit or delete. You can create additional project roles to meet the needs of your organization. However, you cannot delete a project role that is designated as a resource's primary project role, specified on a project resource request, or assigned to a resource on a project.

Project roles are used for the following purposes:

- To identify the type of work that a person performs on project assignments
- To set up default resource qualifications
- As criteria when searching for resources to fulfill project resource requests
- As a resource's primary project role
Project Assignments

When you add a resource to a project, you select a project role to identify the type of work that the resource will perform on the project. The default project role is Project Team Member for resources or resource placeholders that you add directly to the Manage Project Resources page in the Project Management work area.

When you fulfill a project resource request in the Project Resources work area and create an assignment for the resource, the project role specified on the request is the default project role on the assignment. You can change the project role on the Assign Resource page before you submit the assignment for approval.

Default Resource Qualifications

On the Manage Project Roles page, select a set of default qualifications, proficiencies, and keywords for each project role. Default qualifications, proficiencies, and keywords that you associate with a project role automatically appear as requirements on a project resource request when you select the project role for the request.

Project Resource Requests

When searching for resources to fulfill a project resource request on the Search and Evaluate Resources page, you can filter the resource search results by project role to focus the results. Resources that have the selected project role filter as their primary project role will appear in the results. The number next to the filter indicates the number of resources in the results that have the primary project role.

Primary Project Roles

You can designate a primary project role for a resource that represents the work that the resource typically performs on project assignments.

You can use the resource’s primary project role in the following areas in Oracle Fusion Project Resource Management:

- As a resource search option filter when viewing resources on the Search and Evaluate Resources page
- When viewing resource information on the Resource Details page
- When comparing the attributes of multiple resources against the requirements specified in the project resource request on the Compare Resources page
- As an attribute value to assign to new resources that the Maintain Project Enterprise Labor Resources process creates
- As search criteria when searching for a project enterprise labor resource to designate as a resource pool owner on the Manage Resource Pools page
- As advanced search criteria when searching for resource pool members on the Manage Resource Pools page
- As column to sort open project resource requests on the Resource Manager Dashboard

FAQs for Project Roles

How can I assign project roles by default when I import project enterprise labor resources?

Go to the Manage Project User Provisioning page, Default Provisioning Attributes tab, Default Project Role Provisioning for Project Execution Management Labor Resources section. Select the option to **Automatically provision roles when mass**
creating project enterprise labor resources. The application automatically assigns the predefined and custom roles that you selected on the Define Role Assignments table to each resource when you create project users using any of these methods:

- Import HCM Persons as Project Enterprise Resources process
- Import Project Enterprise Resource process for Oracle Cloud
- Project Enterprise Resource External Service
- Maintain Project Enterprise Labor Resources
- Export Resources and Rates process from the planning resource breakdown structure in Oracle Project Financial Management to Oracle Fusion Project Management

Why can't I view project management or resource management pages?

To view the following project management or resource management pages, you must be a project enterprise labor resource with an active user account. In addition, you must have an enterprise role with the security privilege to access these pages:

- Manage Project Plan page in the Project Management work area
- Manage Tasks page in the My Work work area
- Overview page in the Project Resources work area
- Project Manager Dashboard
- Resource Manager Dashboard
- Team Member Dashboard
Agent Security: Explained

Use the Manage Procurement Agent page to maintain a procurement agent's access to procurement functionality for a business unit. You can implement document security for individual document types such as purchase orders, purchase agreements, and requisitions. You can also control a procurement agent’s access to activities such as suppliers, approved supplier list entries, and business intelligence spend data through the settings on this page.

Implementing Document Security
The key elements for document security are the procurement business unit, enabling agent access to document types, and the access levels to other agents’ documents.

Create Procurement Agent: Critical Choices

The Manage Procurement Agent page is used to create or edit a procurement agent and define that agent's access to procurement functionality within a procurement business unit.

Note
The following Fusion predefined roles are controlled by procurement agent access configuration: Buyer, Category Manager, Procurement Manager, Procurement Contracts Administrator, Supplier Administrator, and Catalog Administrator.

Procurement BU
Assign the agent to one or more procurement business units (BU).

Action
Enable the agent to access one or more procurement action for each procurement business unit.

- Manage Requisitions
- Manage Purchase Orders
- Manage Purchase Agreements: Enable access to blanket purchase agreements and contract agreements.
- Manage Negotiations: Enable access to Sourcing negotiations, if implemented by your organization.
- Manage Catalog Content: Enable access to catalog content. This action allows an agent to manage catalog content such as local catalogs, punchout catalogs, content zones, smart forms, information templates, and collaborative authoring.
- Manage Suppliers: Enable access to create and update supplier information.
- Manage Approved Supplier List Entries: Enable access to create and update approved supplier lists.
- Analyze Spend: Used by the business intelligence functionality to view invoice spend information.
**Access to Other Agents' Documents**

Assign an access level to documents owned by other procurement agents for each procurement business unit. Note that an agent can perform all actions on their own documents as long as they have procurement BU access.

- **None**: The agent cannot access documents owned by other agents.
- **View**: Permits the agent to search and view other agents’ documents.
- **Modify**: Permits the agent view, modify, delete, and withdraw other agents’ documents.
- **Full**: Permits the agent full control of other agents’ documents which include view, modify, delete, withdraw, as well as perform document actions including freeze, hold, close, cancel, and finally close.

**Supplier User Provisioning: How It Works**

Supplier User Provisioning refers to the process of establishing suppliers with access to Oracle Fusion Supplier Portal. It enables the buying organization to create and maintain user accounts, job roles, and data access controls for supplier contacts. An important part of supplier user provisioning is to provision job roles, which give users the ability to perform online business tasks and functions with the buying organization which are associated with their job.

The content Supplier Users can access and tasks they can perform are tightly controlled by the buying organization. However, a key feature of Oracle Fusion Supplier Portal allows supplier users to assume the responsibility for user account management on behalf of the buying organization by creating and maintaining user accounts for their fellow employees that require access to the Supplier Portal application. The buying organization maintains control by granting provisioning access to their trusted suppliers, significantly reducing their administrative burden.

**User Provisioning Job Roles**

The seeded job roles that can perform supplier user provisioning are:

- **Supplier Administrator**: This is an internal job role to the buying organization. Users with this role are responsible for maintaining supplier profile information as well as administering user accounts for supplier contacts.
- **Supplier Manager**: This is an internal job role responsible for authorizing a new supplier for spending. The role controls the addition of new spend authorized suppliers into the supply base. This job role and Supplier Administrator can be assigned to the same individual which may be appropriate in smaller organizations.
- **Supplier Self Service Clerk (SSC)**: This is a supplier job role. Supplier users with this role can maintain contact profiles and request user accounts for their fellow employees. All contact profile updates and user account requests made by the SSC require approval by the buying organization.
- **Supplier Self Service Administrator (SSA)**: This is a supplier job role. Supplier users with this role can maintain contact profiles and provision user accounts to their fellow employees, without requiring buying organization approval.

There are several flows in where user provisioning can be performed:

- Supplier registration review and approval.
- Supplier contact change request review and approval.
- Suppliers work area, Edit Supplier flow where supplier contacts are maintained.
- Oracle Fusion Supplier Portal work area where suppliers can perform user provisioning on behalf of their company using the Manage Profile task.

In each of these flows the user can create a user account, assign job roles and set data security access for a supplier contact.

**Manage Supplier User Roles Setup Page**

The Manage Supplier User Roles setup page is used by the buying organization to define the job roles that can be provisioned to supplier users for accessing Oracle Fusion Supplier Portal. This page also controls options for how the supplier
job roles are used in the various provisioning flows. These two distinct setup tasks are intended to be performed by two different internal job roles.

The Manage Supplier User Roles page serves two important setup tasks:

1. The core task is to define the list of roles that can be provisioned to supplier users in Oracle Fusion Supplier Portal provisioning flows. The supplier roles are added from the central Oracle LDAP roles repository which stores all Oracle Fusion application job roles. Once the role is added to the table, it is immediately available for provisioning to supplier contacts by the Supplier Administrator. Only the IT Security Manager job role can add and remove roles to avoid the risk of adding an internal application job role inadvertently which could result in suppliers gaining unauthorized access to internal data. This security risk is the reason only the IT Security Manager has the privilege to manage the list of supplier job roles that can be provisioned.

2. Define the supplier role usages. The Procurement Application Administrator is responsible for this setup task, which manages settings for how the supplier job roles are exposed in provisioning flows. The first column controls whether the supplier job role can be provisioned by suppliers in Oracle Fusion Supplier Portal, specifically supplier users with the SSA role.

Additionally, default roles can be established which expedite supplier user account requests by allowing the buying organization to identify the minimum set of job roles that a supplier contact can be granted. This prevents approvers from having to explicitly review and assign job roles for each user account request.

The IT Security Manager can also set supplier role usages as they can access all functions on the setup page, however this is typically performed by the Procurement Application Administrator. The Procurement Application Administrator cannot add or remove roles from the table.

When the role default setup is done correctly, the Supplier Administrator (or approver) can review supplier contact user account requests with job roles selected based on the source of the request, and proceed to approve user account requests with appropriate role assignments.

The three role usages relevant to supplier user provisioning include:

- **Allow Supplier to Provision:** If selected, the role can be provisioned by the SSA, assuming the role is also assigned to the SSA user.

- **Default for Oracle Fusion Supplier Portal:** If selected, the role is automatically added to supplier user requests in the core user provisioning flows, such as supplier registration and supplier profile maintenance.

- **Default for Oracle Fusion Sourcing:** If selected, the role is automatically added to supplier user requests generated in sourcing flows such as Create Negotiation.

A role in the table can be marked for one or more of the three usages.
The figure below shows the flow for managing supplier user roles.

The IT Security Manager and the Procurement Application Administrator access the Manage Supplier User Roles page through the following respective setup tasks in the Oracle Fusion Setup Manager, under Define Supplier Portal Configuration:

- Manage Supplier User Roles
- Manage Supplier User Roles Usages

**Note**
SSA users should be careful when removing roles from their account because they are not able to add additional roles to their own user account.

To ensure the SSA provisions proper roles to the supplier users in their company, users with the SSA job role are able to provision roles based on those roles checked in the Allow Supplier to Provision column and the set of roles they have already been assigned. This intersection, as depicted in the figure below, determines what roles they can grant to their fellow employees.
Related Topics

- User Account: Explained

Supplier User Account Administration: Explained

User accounts need to be provisioned to allow supplier contacts to access the Oracle Fusion Supplier Portal application. User account maintenance is performed for a specific supplier contact under the Contacts tab. A user account is assigned roles that determine what functions a supplier contact can perform when logging into the application.

Below are Fusion flows where a user account can be requested and managed as part of a supplier contact:

- Create Supplier Contact: When creating a supplier contact, the administrator can also request to create a user account for the contact, request roles and grant data access.

  Note
  Creating a user account for a supplier contact cannot be reversed. Once a user account is created, it cannot be deleted from the system, but it can be inactivated

- Edit Supplier Contact: The supplier administrator can make changes to supplier contact information as well as create or maintain the user account for the contact.

- Approve supplier registration request: When an approver is approving a supplier registration, the approver can create and edit supplier contacts. Since a user account is part of a supplier contact, the approver has the ability to create a user account and assign roles within this flow.
The Supplier Administrator is responsible for:

- Creating and inactivating supplier user accounts

When Create User Account is selected for a contact, a request is initiated to Oracle Fusion Identity Management (OIM) to provision the account. Status is displayed to the user to communicate provisioning status during this process.

When the process is complete, OIM sends notification to the supplier contact with the username and temporary password to access Oracle Fusion Supplier Portal. If the process fails, a notification is sent to the Supplier Administrator alerting them that a user account was not successfully provisioned for the supplier contact.

- Assigning supplier job roles.

The Roles subtab controls function security which determines the business objects and task flows the supplier user can access. Supplier job roles should be assigned based on the job that the contact performs within the supplier organization, such as Customer Service Representative or Accounts Receivable Specialist.

- Assigning data access

The Data Access tab controls data security, or which transactions the user can access for the specific business objects their job role is associated with. There are two levels of data security; Supplier and Supplier Site. By default all supplier user accounts start with supplier level, meaning they can access all transactions belonging to their supplier company only. For more restrictive access, Supplier Site level, limits user access to transactions for specific Supplier Sites only.

**Set Up Supplier Roles: Examples**

The following simple examples illustrate selecting and managing roles for supplier user provisioning.

**Selecting Roles for Supplier User Provisioning:**

Company ABC decides to expand supplier portal deployment and allow suppliers to access orders and agreements. The IT security manager navigates to the Manage Supplier User Roles page, searches for the supplier job role, supplier customer service representative. The IT security manager adds supplier customer service representative to the table. The procurement application administrator then navigates to the Manage Supplier User Roles page and sets supplier customer service representative as Default for Supplier Portal, and Allow Supplier to Provision.

**Managing Default Roles and Defining Roles that the Self Service Administrator (SSA) can Provision:**

Company ABC determines that all supplier users can be granted access to orders, shipments, receipts, invoices and payments information by default, but access to agreements will only be granted to select supplier users. The sales representative role will not be marked as a default role.

Company ABC recently implemented Oracle Fusion Sourcing and needs to provision the supplier bidder role to specific suppliers invited to sourcing events. The SSA should not be allowed to provision this role as it needs to be controlled by Company ABC. When supplier bidder is added to the table, Allow Supplier to Provision should not be checked, but Default Roles for Sourcing is checked.

**Related Topics**

- User Account: Explained
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 named in a security policy, such as view or edit.

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
An XML filter or SQL predicate WHERE clause in 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.

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 template used to generate data roles by specifying which base roles to combine with which dimension values for a set of data security policies.

**data security**
The control of access to data. Data security controls what action a user can taken 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 that represents one of the duties of a job.

**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 widget or functionality within a page. Function security controls what a user can do.
**HCM data role**
A job role, such as benefits administrator, associated with instances of HCM data, such as all employees in a department.

**identity**
A person representing a worker, supplier, or customer.

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

**job role**
A role for a specific job consisting of duties, such as an accounts payable manager or application implementation consultant. A type of enterprise role.

**keyword**
A word or phrase, entered as free-form, unstructured text on a project resource request, that does not exist as a predefined qualification content item. Keywords are matched against the resource’s qualifications and the results are included in the qualification score calculation.

**offering**
A comprehensive grouping of business functions, such as Sales or Product Management, that is delivered as a unit to support one or more business processes.

**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.

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

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

**privilege cluster**
A group of privileges that you can map to a duty role; usually referenced in the output of the Role Optimization Report.
project resource request
List of criteria used to find a qualified resource to fulfill an open resource demand on a project. Project resource requests include qualifications, keywords, requested date range, and other assignment information, such as project role and work location.

qualification
Items in structured content types such as competencies, degrees, and language skills that have specific values and proficiency ratings.

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 in Oracle Fusion Applications, including 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.

segregation of duties
An internal control to prevent a single individual from performing two or more phases of a business transaction or operation that could result in fraud.
**SQL predicate**
A type of condition using SQL to constrain the data secured by a data security policy.

**subledger journal entry**
A detailed journal entry generated for a transaction in a subledger application.

**subledger journal entry line**
An individual debit or credit line that is part of a subledger journal entry.

**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.

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