## Contents

### Preface

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>i</td>
</tr>
</tbody>
</table>

### Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Securing Oracle ERP Cloud: Overview</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Implementing ERP Security: Overview</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Role Types</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Role Inheritance</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Duty Role Components</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Aggregate Privileges</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Guidelines for Configuring Security in Oracle Applications Cloud</td>
<td>6</td>
</tr>
</tbody>
</table>

### Security Console

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Overview of Security Console</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Administrate the Security Console</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Run Retrieve Latest LDAP Changes</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Security Visualizations</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Options for Viewing a Visualization Graph</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Visualization Table Display Options</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Generate a Visualization</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Simulate Navigator Menus in the Security Console</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Analytics for Roles</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Analytics for Database Resources</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>FAQs on Using the Security Console</td>
<td>16</td>
</tr>
</tbody>
</table>

### Bridge for Microsoft Active Directory

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Overview of Bridge for Microsoft Active Directory</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Active Directory Synchronization</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>User Account Attribute Mapping</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Microsoft Active Directory Bridge Setup</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>FAQs on Working with the Bridge for Microsoft Active Directory</td>
<td>25</td>
</tr>
</tbody>
</table>
# Implementation Users

- Implementation Users
- Overview of ERP Implementation Users
- User Accounts
- User Account Details
- Add User Accounts
- Reset Passwords
- Lock and Unlock User Accounts
- Delete User Accounts
- Create Notification Templates
- Synchronize User and Role Information
- Reset the Cloud Service Administrator Sign-In Details
- User Categories

# Application Users

- Overview
- User and Role-Provisioning Setup Options
- User Account Creation Option
- User Account Role Provisioning Option
- User Account Maintenance Option
- Set the User and Role Provisioning Options
- Provision Abstract Roles to Users Automatically
- FAQs on Preparing for Application Users

# Application Users Management

- Users
- Users Accounts
- FAQs on Creating and Managing Application Users
### 7 Role Provisioning

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Mappings</td>
<td>67</td>
</tr>
<tr>
<td>Create a Role Mapping</td>
<td>68</td>
</tr>
<tr>
<td>Role Provisioning and Deprovisioning</td>
<td>70</td>
</tr>
<tr>
<td>Autoprovisioning</td>
<td>72</td>
</tr>
<tr>
<td>User and Role Access Audit Report</td>
<td>73</td>
</tr>
<tr>
<td>Data Access</td>
<td>75</td>
</tr>
<tr>
<td>Assign Data Access to Users</td>
<td>76</td>
</tr>
<tr>
<td>Automatic Data Provisioning</td>
<td>78</td>
</tr>
<tr>
<td>Creating a Data Provisioning Rule</td>
<td>79</td>
</tr>
<tr>
<td>Automatic Data Provisioning and Deprovisioning</td>
<td>80</td>
</tr>
<tr>
<td>Access for Workflow Administrators</td>
<td>80</td>
</tr>
<tr>
<td>View Role Information Using Security Dashboard</td>
<td>83</td>
</tr>
<tr>
<td>FAQs on Provisioning Roles and Data to Application Users</td>
<td>83</td>
</tr>
</tbody>
</table>

### 8 Location Based Access

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Location-Based Access</td>
<td>87</td>
</tr>
<tr>
<td>How Location-Based Access Works</td>
<td>87</td>
</tr>
<tr>
<td>Enable and Disable Location-Based Access</td>
<td>88</td>
</tr>
<tr>
<td>FAQs on Location Based Access</td>
<td>89</td>
</tr>
</tbody>
</table>

### 9 Single Sign-On

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Single Sign-On</td>
<td>91</td>
</tr>
<tr>
<td>Oracle Applications Cloud as the Single Sign-On Service Provider</td>
<td>92</td>
</tr>
<tr>
<td>FAQs on Single Sign-On</td>
<td>93</td>
</tr>
</tbody>
</table>

### 10 Export and Import of Security Setup Data

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export and Import of Security Console Data</td>
<td>97</td>
</tr>
<tr>
<td>Export and Import of Custom Roles</td>
<td>98</td>
</tr>
</tbody>
</table>

### 11 Security Configuration

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security Policies</td>
<td>101</td>
</tr>
<tr>
<td>FAQs on Configuring Security</td>
<td>105</td>
</tr>
</tbody>
</table>
# Oracle ERP Cloud

## Securing ERP

### 12 Roles and Role Assignments
- Review Role Assignments 107
- Review Role Hierarchies 107
- Compare Roles 108

### 13 Role Configuration Using the Security Console
- Custom Roles 111
- Role Optimization 123
- FAQs on Configuring Roles in the Security Console 127

### 14 Certificates and Keys
- Overview of Certificates 129
- Types of Certificates 129
- Sign a X.509 Certificate 130
- Import and Export X.509 Certificates 130
- Import and Export PGP Certificates 131
- Delete Certificates 131

### 15 Security in Oracle Financials
- Security for Country-Specific Features 133
- General Ledger 133
- Payables 156
- Subledger Accounting 157
- Cash Management 159
- Assets 160
- Payments 161
- Business Intelligence 165

### 16 Security in Oracle Project Portfolio Management
- Overview of Project Portfolio Management Security 175
- Job or Abstract Roles Mapping to Project Roles 178
- Project Execution Management 179
- Project Financial Management 186
- Business Intelligence 193
<table>
<thead>
<tr>
<th>Chapter Number</th>
<th>Chapter Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Security in Oracle Procurement</td>
<td>203</td>
</tr>
<tr>
<td></td>
<td>Implementing Security for Procurement: Overview</td>
<td>203</td>
</tr>
<tr>
<td></td>
<td>Procurement Requester</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Procurement Agent</td>
<td>208</td>
</tr>
<tr>
<td></td>
<td>Supplier User</td>
<td>210</td>
</tr>
<tr>
<td></td>
<td>Supplier Administration</td>
<td>214</td>
</tr>
<tr>
<td></td>
<td>Business Intelligence</td>
<td>214</td>
</tr>
</tbody>
</table>
Preface

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

Using Oracle Applications

Using Applications Help

Use help icons ? to access help in the application. If you don’t see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access Oracle Applications Help.

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

You can also read Using Applications Help.

Additional Resources

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

Conventions

The following table explains the text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than symbol separates elements in a navigation path.</td>
</tr>
</tbody>
</table>

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website.

Videos included in this guide are provided as a media alternative for text-based help topics also available in this guide.
Contacting Oracle

Access to Oracle Support
Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

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

## 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 change. This topic summarizes the scope of this guide and identifies the contents of each chapter.

To manage roles, use the Security Console and other tasks available in the Setup and Maintenance work area. You may use either of these options to create or edit roles, or to view and work with them later; the choice is a matter of your preference. Some chapters in this guide discuss the use of Setup and Maintenance tasks, and later chapters discuss the use of the Security Console.

> **Note:** Any references to data roles in this guide are only applicable to Oracle HCM Cloud. Data roles are no longer used in Oracle ERP Cloud.

## Guide Structure

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

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>A brief overview of role-based security concepts</td>
</tr>
<tr>
<td>Using the Security Console</td>
<td>How to set up and manage the Security Console, and use it to view role hierarchies and Navigator menus</td>
</tr>
<tr>
<td>Managing Implementation Users</td>
<td>The purpose of implementation users and how you create them</td>
</tr>
<tr>
<td>Preparing 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 different ways 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>How to use tasks available from Setup and Maintenance to enable application users to acquire roles, with instructions for creating some standard role mappings</td>
</tr>
<tr>
<td>Configuring Security</td>
<td>How to create, review, and modify security components, with recommended best practices</td>
</tr>
<tr>
<td>Reviewing Roles and Role Assignments</td>
<td>How to use the Security Console to review roles and identify the users assigned to them</td>
</tr>
<tr>
<td>Configuring Roles in the Security Console</td>
<td>How to create, review, and modify roles in the Security Console, with recommended best practices</td>
</tr>
</tbody>
</table>
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 after creating a copy of the predefined role, 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 ERP Cloud and their intended purposes, see the Security Reference Manual in the Oracle Help Center (http://docs.oracle.com).

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 Requester.

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.
- **IT Security Manager**: Used to access the Security Console to manage roles, users, and security.

> **Note**: For the 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, see the Security Reference Manual in the Oracle Help Center (http://docs.oracle.com).

**Data Security Considerations**

- Use segment value security rules to restrict access to transactions, journal entries, and balances based on certain values in the chart of accounts, such as specific companies and cost center values, to individual roles.
- Use data access set security for Oracle Fusion General Ledger users to control read or write access to entire ledgers or portions of the ledger represented as primary balancing segment values, such as specific legal entities or companies.

For more information on securing your applications, see the Oracle ERP Cloud Securing Oracle ERP Cloud guide in the Oracle Help Center (http://docs.oracle.com).

**Role Types**

Oracle Enterprise Resource Planning (Oracle ERP) Cloud defines the following types of roles:

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

This topic introduces the role types.

**Job Roles**

Job roles represent the jobs that users perform in an organization. General Accountant and Accounts Receivables Manager are examples of predefined job roles. You can also create job roles.

**Abstract Roles**

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

All users are likely to have at least one abstract role that provides access to a set of standard functions. You may assign abstract roles directly to users.
Duty Roles
Duty roles represent a logical collection of privileges that grant access to tasks that someone performs as part of a job. Budget Review and Account Balance Review are examples of predefined duty roles. You can also create duty roles. Other characteristics of duty roles include:

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

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

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

Aggregate privileges differ from duty roles in these ways:

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

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

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

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

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

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

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

Duty Role Components
This topic describes the components of a typical duty role. Function security privileges and data security policies are granted to duty roles. Duty roles may also inherit aggregate privileges and other duty roles.
Data Security Policies
For a given duty role, you may create any number of data security policies. Each policy selects a set of data required for the
duty to be completed and actions that may be performed on that data. The duty role may also acquire data security policies
indirectly from its aggregate privileges.

Each data security policy combines:

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

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

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

Tip: The predefined duty roles represent logical groupings of privileges that you may want to manage as a

group. They also represent real-world groups of tasks. For example, the predefined General Accountant job role
inherits the General Ledger Reporting duty role. To create your own General Accountant job role with no access
to reporting structures, you could copy the predefined job role and remove the General Ledger Reporting duty
role from the role hierarchy.

Aggregate Privileges
Aggregate privileges are a type of role. Each aggregate privilege combines a single function security privilege with related data
security policies. All aggregate privileges are predefined. This topic describes how aggregate privileges are named and used.

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

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

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

Creating, Editing, or Copying Aggregate Privileges

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

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

Guidelines for Configuring Security in Oracle Applications Cloud

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

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

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

Missing Enterprise Jobs

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

Predefined Roles with Different Privileges

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

Predefined Roles with Missing Privileges

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

Related Topics

- Options for Reviewing Predefined Roles
2 Security Console

Overview of Security Console

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

Security Console Access

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

Security Console Tasks

You can do these tasks on the Security Console:

- Roles
  - Create job, abstract, and duty roles.
  - Edit custom roles.
  - Copy roles.
  - Compare roles.
  - Visualize role hierarchies and assignments to users.
  - Review Navigator menu items available to roles or users, identifying roles that grant access to Navigator items and privileges required for that access.

- Users
  - Create user accounts.
  - Review, edit, lock, or delete existing user accounts.
  - Assign roles to user accounts.
  - Reset users’ passwords.

- Analytics
  - Review statistics of role categories, the roles belonging to each category, and the components of each role.
  - View the data security policies, roles, and users associated with each database resource.

- Certificates
  - Generate, export, or import PGP or X.509 certificates, which establish encryption keys for data exchanged between Oracle Cloud applications and other applications.
• Establish rules for the generation of user names.
• Set password policies.
• Create standards for role definition, copying, and visualization.
• Review the status of role-copy operations.
• Define templates for notifications of user-account events, such as password expiration.

Administrate the Security Console

To prepare the Security Console for use, arrange to run background processes that refresh security data. You can use Security Console Administration pages to select general and role-oriented options, track the status of role-copy jobs. You can also select, edit, or add notification templates.

Run the Background Processes

Here are the background processes you must run:

• **Retrieve Latest LDAP Changes** - This process copies data from the LDAP directory to Oracle Cloud Applications Security tables. Run it once, during implementation.

• **Import User and Role Application Security Data** - This process imports users, roles, privileges, and data security policies from the identity store, policy store, and Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables.

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

1. In the Setup and Maintenance work area, search for the **Run User and Roles Synchronization Process** task and select it.
2. Click **Submit**.
3. Review the confirmation message and click **OK**.

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

1. In the Tools work area, select **Scheduled Processes**.
2. Click **Schedule New Process**.
4. Click **OK**.
5. Click **Submit**.
6. Review the confirmation message and click **OK**.

Configure the General Administration Options

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

**Configure the Role Administration Options**

1. On the Security Console, click **Administration**.
2. On the Roles tab, specify the prefix and suffix that you want to add to the name and code of role copies. Each role has a Role Name (a display name) and a Role Code (an internal name). A role copy takes up the name and code of the source role, with this prefix or suffix (or both) added. The addition distinguishes the copy from its source. By default, there is no prefix, the suffix for a role name is "Custom," and the suffix for a role code is ".CUSTOM."
3. In the **Graph Node Limit** field, set the maximum number of nodes a visualization graph can display. When a visualization graph contains a greater number of nodes, the visualizer recommends the table view.
4. Deselect **Enable default table view**, if you want the visualizations generated from the Roles tab to have the radial graph view.
5. Enable edit of data security policies: Determine whether users can enter data on the Data Security Policies page of the role-creation and role-edit trains available from the Roles tab.
6. Enable edit of user role membership: Determine whether users can enter data on the Users page of the role-creation and role-edit trains available from the Roles tab.

**View the Role Copy Status**

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

**Run Retrieve Latest LDAP Changes**

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

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

**Run the Process**

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

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.
   
   The Schedule New Process dialog box opens.
3. In the **Name** field, search for and select the **Retrieve Latest LDAP Changes** process.
4. Click **OK** to close the Schedule New Process dialog box.
5. In the Process Details dialog box, click Submit.
6. Click OK, then Close.
7. On the Scheduled Processes page, click the Refresh icon.
   Repeat this step periodically until the process completes.

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

## Security Visualizations

A Security Console visualization graph consists of nodes that represent security items. These may be users, roles, privileges, or aggregate privileges. Arrows connect the nodes to define relationships among them. You can trace paths from any item in a role hierarchy either toward users who are granted access or toward the privileges roles can grant.

You can select one of the following two views:

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

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

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

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

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

## Options for Viewing a Visualization Graph

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

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

## Node Labels

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

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

• If the image is smaller, the nodes are unlabeled.

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

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

**Expand or Collapse Nodes**

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

**Using Control Panel Tools**

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

• Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.

• Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.

• Zoom to Fit: Center the image and size it so that it is as large as it can be while fitting entirely in its display window. (Nodes that you have expanded remain expanded.)

• Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area covered by the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.

• Search: Enter text to locate nodes whose names contain matching text. You can search only for nodes that the image is currently expanded to reveal.

• Control Panel: Hide or expose the Control Panel.

**Using the Legend**

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

• Hover over the entry for a particular item type to locate items of that type in the image. Items of all other types are grayed out.

• Click the entry for an item type to disable items of that type in the image. If an item of that type has child nodes, it is grayed out. If not, it disappears from the image. Click the entry a second time to restore disabled items.

• Hide or expose the Legend by clicking its button.

**Using the Overview**

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

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

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

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

Visualization Table Display Options

A visualization table contains records of roles, privileges, or users related to a security item you select. The table displays records for only one type of item at a time:

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

Tables are all-inclusive:

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

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

Here's how you can generate a visualization:

2. Search for the security item on which you want to base the visualization.
   - In a Search field, select any combination of item types, for example, job role, duty role, privilege, or user.
   - In the adjacent field, enter at least three characters. The search returns the matching records.
   - Select a record.
   Alternatively, click Search to load all the items in a Search Results column, and then select a record.
3. Select either Show Graph or View as Table button.

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

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

Simulate Navigator Menus in the Security Console

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

Opening a Simulation

To open a simulated menu:

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

Working with the Simulation

In a Simulate Navigator page:

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

In either view:

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

To plan how this authorization may be altered:

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

### Analytics for Roles

You can review statistics about the roles that exist in your Oracle Cloud instance. On the Analytics page, click the Roles tab. Then view these analyses:

- **Role Categories.** Each role belongs to a category that defines some common purpose. Typically, a category contains a type of role configured for an application, for example, "Financials - Duty Roles."
  
  For each category, a Roles Category grid displays the number of:
  - Roles
  - Role memberships (roles belonging to other roles within the category)
  - Security policies created for those roles

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

- **Roles in Category.** Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:
  - Role memberships
  - Security policies
  - Users assigned to the role

- **Individual role statistics.** Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.
  
  Click Export to export data from this page to a spreadsheet.

### Analytics for Database Resources

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

1. On the Analytics page, click the Database Resources tab.
2. Select the resource you want to review in the **Database Resource** field.
3. Click **Go**.
Results are presented in three tables.

**Data Security Policies**

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

Each row documents a policy, specifying by default:

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

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

**Authorized Roles**

The Authorized Roles table documents roles with direct or indirect access to the selected database resource. Any given role may comprise the following:

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

By default, each row specifies the following:

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

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

**Authorized Users**

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

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

**Manipulating the Results**

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

- Add or remove columns. Select View - Columns.
FAQs on Using the Security Console

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

Private information is confidential in some contexts.

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

Some PII information is sensitive.

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

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

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

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

Overview of Bridge for Microsoft Active Directory

The bridge for Microsoft Active Directory synchronizes user account information between Oracle Applications Cloud and Microsoft Active Directory. Using the bridge, you can copy user or role details from Oracle Applications Cloud (as the source) to Active Directory (as the target), or the other way around. Depending on the direction in which data synchronization is planned, you can specify one of them as the source and the other one as the target.

The current configuration of the bridge supports single Active Directory Forest with a single domain controller topology. The bridge uses REST API (Representational State Transfer) over HTTPS to communicate with the Oracle Applications Cloud and the LDAP (Lightweight Directory Access Protocol) to communicate with the Active Directory server. The Microsoft Active Directory server may not be reachable outside the corporate firewall but must be reachable from the computer hosting the bridge.

Prerequisites

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

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

System Requirements for the Bridge:

- RAM and CPU: As per the OS requirements
- Disk Space: Minimum 10 GB of free space

Setting Up the Bridge for Microsoft Active Directory

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

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

Related Topics

- Running Bridge for Active Directory with Oracle Applications Cloud as the source
- Running Bridge for Active Directory with Active Directory as the source
Active Directory Synchronization

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

After you provide the bridge configuration details, install and run the bridge for Active Directory. Save the credentials to access Active Directory and Oracle Fusion Application, then return to Security Console AD Bridge setup to complete the user account mapping configuration. When mapping is complete, return to the bridge application and initiate the initial synchronization of users between the source and target applications.

During synchronization, the bridge extracts data from the source and target applications, compares the data, and identifies the task that must be performed on the target application for consistency.

When synchronization completes, the bridge performs the required tasks on the target application. Any errors encountered during synchronization are recorded in the log files for review and correction.

After the initial synchronization is complete, you can configure the bridge to synchronize any changes between the source and target at regular intervals or on-demand.

The bridge for active directory can perform:

- Full synchronization
- Incremental synchronization

Full Synchronization

The bridge starts full synchronization or full reconciliation when any of the following conditions are true:

- The source and target applications are synchronized for the first time.
- The bridge configuration for the active directory has changed.
- The Run Full Synchronization button is clicked.

To manually perform a full synchronization:

1. Click the Bridge for Active Directory tab on the Administration page in the Security Console.
2. Click User Attribute Mappings.
3. Expand the On Demand Synchronization section and click Run Full Synchronization.

**Note:** To disable Forced Full synchronization, click Cancel Full Synchronization.

Incremental Synchronization

The bridge starts incremental synchronization when: any of the following conditions are true:

- The source and target were previously synchronized.
- The bridge configuration for the active directory has not changed.
- The Run Full Synchronization button isn’t clicked.

Incremental synchronization can be either on-demand (manually) or at regular intervals (automatically).
User Account Attribute Mapping

After you install and configure the bridge, map the user account attributes between Oracle Applications Cloud and Microsoft Active Directory. Only when the mapping is complete, you can initiate the initial synchronization of users between the source and target applications.

⚠️ Caution: Don’t use Active Directory Bridge with SSO Chooser enabled, as it will cause synchronization issues. If you sign in to Oracle Applications Cloud locally and create new users, they will not reflect in the Active Directory after synchronization.

Map the following user attributes:

- User account attributes
- Advanced user account attributes
- Group attributes

Mapping User Attributes

The following attributes of an Oracle Fusion Applications user account are mapped to the corresponding attributes of an Active Directory user account:

- displayName: Display name of the user account
- emails.value: Primary email associated with the user account
- name.familyName: Last name of the user
- name.givenName: First name of the user
- userName: User name associated with the user account

During synchronization, the attribute values from the source are copied to the mapped target attributes. Some Active Directory attributes have size restrictions. For example, length of the sAMAccountName attribute is limited to 20 characters when used as a user attribute and can be up to 64 characters when used to name groups. Synchronization will fail if the user name has a larger value than the Active Directory attribute configured.

The following table lists a typical mapping of attributes when Oracle Fusion Application is the source.

<table>
<thead>
<tr>
<th>Oracle Cloud Application as Source</th>
<th>Microsoft Active Directory as Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>emails.value</td>
<td>Mail</td>
</tr>
<tr>
<td>Username</td>
<td>cn</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>name.familyName</td>
<td>sn</td>
</tr>
<tr>
<td>name.givenName</td>
<td>givenName</td>
</tr>
<tr>
<td>UserName</td>
<td>userPrincipalName</td>
</tr>
</tbody>
</table>
The following table lists a typical mapping of attributes when Microsoft Active Directory is the source.

<table>
<thead>
<tr>
<th>Microsoft Active Directory as Source</th>
<th>Oracle Cloud Applications as Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>emails.value</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>UserName</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>givenName</td>
<td>name.givenName</td>
</tr>
<tr>
<td>sn</td>
<td>name. familyName</td>
</tr>
</tbody>
</table>

On the Security Console, click **Administration > Bridge for Active Directory** tab > **User Attribute Mappings**. Click **Add** to add or update the mapping between attributes of the source and target applications.

### Mapping Advanced Attributes

Use this option when Active Directory is the source. Select **Synchronize User Status** to enable the account status, such as **Disabled**, to propagate to Oracle Applications Cloud.

### Microsoft Active Directory Bridge Setup

#### Prepare Oracle Applications Cloud to Connect With Microsoft Active Directory

Follow this procedure to configure the Bridge for Microsoft Active Directory. Sign in to Oracle Applications Cloud environment as an administrator with the IT Security Manager (**ORA_FND_IT_SECURITY_MANAGER_JOB**) role.

1. Click **Navigator > Security Console**.
2. On the Administration page, click the Bridge for Active Directory tab.
3. Click **Configuration**.
4. Expand the Base Configuration section and provide the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of Truth</td>
<td>Select the source, such as Oracle Fusion Applications or Active Directory.</td>
</tr>
</tbody>
</table>
### Oracle ERP Cloud

#### Securing ERP

#### Chapter 3

**Bridge for Microsoft Active Directory**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization Interval (Hours)</td>
<td>Enter the time interval (in hours) that the bridge uses to begin synchronization automatically. The default value is one hour.</td>
</tr>
<tr>
<td>Synchronization Paging Size</td>
<td>Enter the number of accounts that are synchronized in a single operation. The default value is 100 records.</td>
</tr>
<tr>
<td>Synchronization Error Threshold</td>
<td>Enter the maximum number of errors that can occur during synchronization. When the limit is reached, synchronization fails and stops. By default, synchronization stops after 50 errors have occurred.</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Specify whether you want to automatically schedule synchronizations. If enabled, the synchronizations will run automatically as per the specified schedule and interval.</td>
</tr>
<tr>
<td>Role Integration</td>
<td>Specify whether you want to use role integration. It is applicable when Active Directory is the source. When enabled, the synchronization will read groups the users are directly or indirectly assigned to in Active Directory. If a user has been assigned to or removed from a group of the group mapping, the corresponding user in Oracle Applications Cloud will be added to or removed from the corresponding mapped role in Oracle Applications Cloud.</td>
</tr>
<tr>
<td>Reset APPID Password</td>
<td>Enter a new password. During synchronization, this password is used by the bridge to connect to Oracle Applications Cloud.</td>
</tr>
</tbody>
</table>

5. Expand the Logging Configuration section and provide the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Enter the name of the log file. This file is created in the Active Directory folder on the computer where the Active Directory bridge is installed. The default value is ad_fa_synch.log</td>
</tr>
<tr>
<td>Log Level</td>
<td>Specify the level at which messages must be logged during synchronization. The default level is set to Information.</td>
</tr>
<tr>
<td>Maximum Log Size</td>
<td>Specify the maximum size of the log file. The default value is 4 GB. When the maximum size is reached, a new log file is created.</td>
</tr>
</tbody>
</table>

6. Expand the Active Directory Configuration section and provide the following details. The bridge uses this information to connect to the Active Directory server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the host address of the Active Directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port of the Active Directory server. The default non-SSL port is 389.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Select this option for secure communication with the Active Directory server. When you select this option, the default port changes to 636.</td>
</tr>
</tbody>
</table>
### Synchronization Strategy

Select the algorithm that must be used for synchronization. You can select **Directory Synchronization** or **Update Sequence Number**. The default value is **Directory Synchronization**.

*Note:* If you change the sequence number after the initial configuration, the synchronization process resets.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Base DN</td>
<td>Enter the distinguished name of the location in your Active Directory where the user accounts are created or retrieved by the bridge.</td>
</tr>
<tr>
<td>Search Base</td>
<td>Enter the same value as the User Base DN.</td>
</tr>
<tr>
<td>User Search Filter</td>
<td>Enter the LDAP query that is used by the bridge to retrieve the user account objects from the Active Directory. For example, (&amp; (objectClass=user)(!(objectClass computer))).</td>
</tr>
<tr>
<td>Group Base DN</td>
<td>Enter the distinguished name of the location in your Active Directory from where the bridge fetches the groups.</td>
</tr>
<tr>
<td>Group Search Filter</td>
<td>Enter the LDAP query that is used to fetch roles from your Active Directory server. For example, (objectClass= group).</td>
</tr>
</tbody>
</table>

*Note:* This field is applicable only when Active Directory is the source.

### Network Proxy Configuration

Expand the Network Proxy Configuration section and provide the details.

*Note:* Provide these details only when Active Directory is the source, and the bridge uses a proxy to connect to the Active Directory server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Proxy Settings</td>
<td>Select this option to enable communication through a proxy between Oracle Applications Cloud and your Active Directory bridge. Use this option when you need to connect from an isolated network host.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter a host name and address for the proxy.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a port for the proxy.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Select this option for secure communication with the proxy.</td>
</tr>
</tbody>
</table>

### Heartbeat

Expand the Heartbeat section and update the following details.

8. Expand the Heartbeat section and update the following details.
Heartbeat Interval
Enter the time interval, in seconds, at which heartbeat notifications are sent from the bridge to Oracle Applications Cloud to signal that the bridge is active. It is set to 60 seconds by default.

9. Click **Save** and click **OK**.

**Download and Install the Bridge for Active Directory**

Once you have set the configuration details for the bridge, download the bridge for Active Directory on a computer connected to your network. This computer must connect to both Oracle Applications Cloud and your Microsoft Active Directory server instance. Before you configure and install the bridge, ensure that you have the IT Security Manager role (ORA_FND_IT_SECURITY_MANAGER_JOB) access.

1. Click **Navigator > Tools > Security Console**.
2. On the Administration page, click the Bridge for Active Directory tab.
3. Click **Launch**.
4. Review the message that appears and click **OK**.
5. Accept the notification to download the bridge file (`adbridge.jnlp`).
6. Open the bridge file (`adbridge.jnlp`) from your Web browser.
7. Enter **User name** and **Password** to sign in. You can use your Oracle Applications Cloud credentials to sign in.
8. Click **OK**.
9. Click **Run** to start the bridge.
10. Enter **User name** and **Password**. You can use your Oracle Applications Cloud credentials to sign in.
11. Click **OK**.
12. Open the Bridge for Active Directory. The bridge automatically displays the necessary information configured through the Security Console.
13. Click the Configuration tab
14. In the Active Directory section, enter the **User name** and **Password** for the Active Directory server.
15. In the Oracle Applications Cloud section, enter the **Password** for the Oracle Applications Cloud host. Use the **Reset APPID Password** that you provided while configuring the bridge.
16. You can change the Oracle Applications Cloud network settings. Click **Network Settings** to update the details.
17. Click **Save** and click **Close**.

   The bridge updates the setup information from Active Directory (attributes, groups) to Oracle Applications Cloud. Use this setup information to perform mapping in the Security Console.

**Map Attributes and Groups for Synchronization**

Once you have set the configuration details for the bridge through the Security Console, download the bridge to a computer connected to your network. This computer must connect to both Oracle Applications Cloud and your Microsoft Active Directory server instance.

1. Click **Navigator > Security Console**.
2. On the Administration page, click the Bridge for Active Directory tab.
3. Click **User Attribute Mappings**.
4. Two attributes appear by default. Select source and target use attributes from the lists. Click **Add** to map more attributes between the source and target.
5. Select the source attribute from the **Source User Attribute** list.
6. Select the target attribute from the **Target User Attribute** list.
7. Click **OK**.
8. Repeat steps 4 to 7 to map more attributes.
9. Click **Save**.
10. Expand the Advanced Attribute Mappings section.
11. Set the **Synchronize User Account Status** to either enable or disable, to determine whether to synchronize the account or not.
12. Click **Save**.
13. Click **Group Mappings** to map active directory groups to Oracle Cloud Application roles.
14. Click **Add** to add new group to role mapping or select an existing mapping and click the **Actions** drop-down list.
15. On the Add Role Mapping dialog box, select the **Group** and the **Roles**. When a user account is added to or removed from a group in the Active Directory, the corresponding Oracle Cloud Application user account is added to or removed from the mapped role in Oracle Cloud Applications.
16. Click **OK**.
17. Click **Save**.

### Perform Initial Synchronization

Follow these steps to perform the initial synchronization of users:

1. Start the Bridge for Active Directory.
2. Sign in to bridge using your Oracle Fusion Applications login credentials.
3. Click the Synchronization tab.
4. Click **Run Now**.
5. Click **See Log Files** to view the log files for any errors.
6. Click **Close**.

### Run Synchronization

In the initial synchronization, data is copied from the source application to the target application. After the initial synchronization is complete, you can configure the bridge to synchronize any changes between the source and target applications, either on-demand (manually) or at regular intervals (automatically).

#### Manual Synchronization

Perform manual synchronization whenever you want to synchronize the source and target applications after the initial synchronization. To manually synchronize data, perform the following steps on the bridge:

1. Navigate to the Security Console and click the Active Directory tab.
2. Click the Synchronization tab and click **Run Now**.

#### Automatic Synchronization

You can configure the bridge to perform synchronization periodically as a Microsoft Windows service. Perform the following steps to configure automatic synchronization:

> **Note:** For setting up the Windows service, use the same domain and user credentials that you used for installing the Active Directory Bridge.

1. Start the bridge.
2. Click **Service Installation**.
3. Enter the user name and password of the account that is used to run the service. The account must have **administrative** and **Log on as a service** privileges.
4. Click **Install Windows Service**.

On successful installation, the bridge is registered as a service with the name Bridge for Active Directory.

### Specifying the Synchronization Interval

Once the bridge is set up to run as a Windows Service, it periodically performs synchronization. The synchronization interval is specified in the Security Console and must be specified before the bridge is downloaded.

1. Select **Navigator > Security Console**.
2. Click the Administration tab.
3. Click the **Bridge for Active Directory** link.
4. Go to the Configuration tab and specify the Synchronization Interval (in hours).

### FAQs on Working with the Bridge for Microsoft Active Directory

**Can the bridge support other LDAP directories?**

No, the bridge can only be used for synchronization between Oracle Cloud Applications and Microsoft Active Directory.

**How often can I synchronize information?**

Using the Microsoft Windows service, you can configure the bridge to perform synchronization periodically. The minimum interval between two synchronizations must be one hour.

**What Active Directory objects can I synchronize?**

You can synchronize Active Directory users and groups.

Use the following synchronization options:

- Synchronize users with Oracle Applications Cloud user accounts.
- Synchronize groups with Oracle Applications Cloud roles.

You can synchronize users when the source is either Oracle Applications Cloud or Active Directory. However, you can synchronize groups when the source is only Active Directory.

**What attributes can I synchronize?**

You can synchronize the following predefined attributes in Oracle Applications Cloud with any Active Directory attributes:
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayName</td>
<td>Display name of the user account.</td>
</tr>
<tr>
<td>emails.value</td>
<td>Primary email address associated with the user account.</td>
</tr>
<tr>
<td>name. familyName</td>
<td>Last name of the user.</td>
</tr>
<tr>
<td>name.givenName</td>
<td>First name of the user.</td>
</tr>
<tr>
<td>Username</td>
<td>User name (name for signing in) associated with the user.</td>
</tr>
</tbody>
</table>

You can’t change or format an attribute during synchronization.

| Note: You can synchronize only the predefined attributes, not any user-defined attribute. |

How can I view the log files?

To view the log files, click the Synchronization tab on the bridge application and click the See Log Files link. Information about each synchronization is recorded in the log files. The path to the log file on a Windows operating system is: %APPDATA%\Oracle\AD Bridge\log.
4 Implementation Users

Implementation Users

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

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

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

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

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

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

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

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

Overview of ERP Implementation Users

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

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

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

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

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

Creating Implementation Users

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task or Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create Implementation Users</td>
<td>The Application Implementation Consultant user may be your only implementation user. However, you can create the implementation users TechAdmin and ERPUser, and assign the required job roles to them if you need these implementation users and they don’t already exist in your environment. You don’t associate named workers with these users at this time because your service isn’t yet configured to onboard users in the integrated HCM core. As your implementation progresses, you may decide to replace these users or change their definitions.</td>
</tr>
<tr>
<td>2</td>
<td>Run User and Roles Synchronization Process</td>
<td>Run the process Retrieve Latest LDAP Changes to copy changes to users and their assigned roles to Oracle Fusion Human Capital Management (Oracle Fusion HCM).</td>
</tr>
<tr>
<td>3</td>
<td>Assign Security Profiles to Abstract Roles</td>
<td>Enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles.</td>
</tr>
<tr>
<td>4</td>
<td>Create a Generic Role Mapping for the Roles</td>
<td>Enable the roles created in step 3 to be provisioned to implementation users.</td>
</tr>
<tr>
<td>5</td>
<td>Assign Abstract Role and Data Access to the Implementation User</td>
<td>Assign the implementation user with the roles that enable functional implementation to proceed.</td>
</tr>
</tbody>
</table>
Once these steps are complete, you’re recommended to reset the service administrator sign-in details.

User Accounts

The User Accounts page of the Security Console provides summaries of user accounts that you select to review. For each account, it always provides:

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

It may also provide:

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

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

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

To begin working with user accounts:

1. Select the Users tab in the Security Console.
2. In a Search field, select any combination of user states and enter at least three characters.

The search returns user accounts at the states you selected, whose login, first name, or last name begins with the characters you entered.

User Account Details

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

These details always include:

- User information, which consists of user, first, and last name values, and an e-mail address. It also includes an external identifier if one has been created. This is an external-system identifier, such as a single sign-on account ID if single sign-on is enabled.
• Account information, which comprises the user’s password-expiration date, whether the account is active, and whether it is locked.

• A table listing the roles assigned to the user, including whether they are autoprovisioned or assignable. A role is assignable if it can be delegated to another user.

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

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

• You can edit values only in the User Information, Account Information, and Roles regions.

• Even in those regions, you can edit some fields only if the user is not associated with a worker or a party. If not, for example, you can modify the First Name and Last Name values in the User Information region. But if the user is associated with a worker, you would manage these values in Human Capital Management. They would be grayed out in this Edit User Details page.

• In the Roles table, Autoprovisioned check boxes are set automatically, and you cannot modify the settings. The box is checked if the user obtained the role through autoprovisioning, and cleared if the role was manually assigned. You can modify the Assignable setting for existing roles.

Click Add Autoprovisioned Roles to add any roles for which the user is eligible. Or, to add roles manually, click Add Role. Search for roles you want to add, select them, and click Add Role Membership.

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

Add User Accounts

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

To add a user account in the Security Console:

1. Select the Users tab in the Security Console to open the User Accounts page.
2. Click the Add User Account button.
3. Select a value for Associated Person Type: Worker if this account is to be linked to a worker record in HCM, or None if not.
4. By default, the account is set to be active and unlocked in the Account Information area. Typically these values are appropriate, but you may modify them.
5. Select the User Category with which you want to associate the user.

Note: If you are not sure which user category to select, you may leave it unchanged. All new users are automatically assigned to the Default user category.

6. Enter name, e-mail, and password values in the User Information region as per the following guidance.
   
   • You need not enter a User Name value. It is generated automatically according to the user name generation rule selected on the User Categories page.
   • The First Name value is not required. However, you must enter one if the selected user name generation rule makes use of the first name or the first-name initial.
The Password value must conform to the password policy established on the User Categories page. The Confirm Password value must match the Password value.

- An external identifier is the user's ID in another system, such as a single sign-on account ID if single sign-on is enabled.

7. Click Add Autoprovisioned Roles, to assign roles for which role-provisioning rules make the user eligible.
8. Click Add Roles to assign other roles. Search for roles you want to assign, select them, then click Add Role Membership. Select Done when you are finished.
9. In the Roles table, select Assignable for any role that can be delegated to another user.
10. Click Save and Close.

Reset Passwords

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

A new password must conform to your password policy. You establish this policy on the User Categories page. The page on which you reset the password displays the policy.

To reset a password:

1. On the User Accounts page, search for the user whose password you want to change.
2. For the selected user, click Action > Reset Password.
   
   As an alternative, open the user’s account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page. On that page, select Reset Password.
3. On the Reset Password dialog box, select whether to generate the password automatically or change it manually. For a manual change, also enter a new password value and a confirmation value, which must match the new value.

   Note: The option to reset a password to an automatically generated value is always available. For the manual reset option to be available, you must select the Administrator can manually reset password option on the User Categories page.
4. Click Reset Password.

Related Topics
- Administrate the Security Console

Lock and Unlock User Accounts

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

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

To complete the first procedure:

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

To complete the second procedure:

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

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

Delete User Accounts

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

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

Create Notification Templates

Users may receive Email notifications of user-account events, such as account creation or password expiration. These notifications are generated from a set of templates, each of which specifies an event. A template generates a message to a user when that user is involved in the event tied to the template.

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

Here’s how you can create a template:

1. Click the User Categories tab in the Security Console.
2. Select a user category and on the User Category Information page, click the Notifications tab.
3. Click the Edit button to make changes.
   Ensure that the Enable Notifications check box is selected.
4. Click Add Template.
5. Specify a name and description for the template.
6. Select Enabled to use the template immediately. If selected, template that had been enabled for the event which you select, is automatically disabled.
7. Select an Event from the corresponding drop-down list.
   The values for Message Subject and Message are copied from an already-configured template for which the same event is selected.
8. Update the Message Subject and Message as required.

   Note: The message text includes tokens which are replaced in runtime by literal values appropriate for a given user or account.
9. Click Save and Close.
To edit a template, select it from the templates listed in the Notification Templates table. Then follow the same process as you would to create a template. You cannot modify the event selected for a template that has been saved. You can only enable or disable an individual template when you edit it.

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

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

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

<table>
<thead>
<tr>
<th>Token</th>
<th>Meaning</th>
<th>Events</th>
</tr>
</thead>
</table>
| ${userLoginId} | The user name of the person whose account is being created or modified. | • Forgot user name  
• Password expired  
• Password reset confirmation |
| ${firstName} | The given name of the person whose account is being created or modified. | • Administration activity location based access disabled confirmation  
• Administration activity requested  
• Administration activity single sign-on disabled confirmation  
• Expiring external IDP signing certificate  
• Expiring service provider encryption certificate  
• Expiring service provider signing certificate  
• Forgot user name  
• New account created - manager  
• New user created  
• Password expired  
• Password expiry warning  
• Password generated  
• Password reset  
• Password reset - manager  
• Password reset confirmation  
• Password reset confirmation - manager |
| ${lastName}  | The surname of the person whose account is being created or modified.    | • Administration activity location based access disabled confirmation  
• Administration activity requested  
• Administration activity single sign-on disabled confirmation  
• Expiring external IDP signing certificate  
• Expiring service provider encryption certificate  
• Expiring service provider signing certificate  
• Forgot user name  
• New account created - manager  
• New user created  
• Password expired  
• Password expiry warning  
• Password generated |
<table>
<thead>
<tr>
<th>Token</th>
<th>Meaning</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(managerFirstName)</td>
<td>The given name of the person who manages the person whose account is being created or modified.</td>
<td>• New account created - manager&lt;br&gt;• Password reset confirmation - manager&lt;br&gt;• Password reset - manager</td>
</tr>
<tr>
<td>$(managerLastName)</td>
<td>The surname of the person who manages the person whose account is being created or modified.</td>
<td>• New account created - manager&lt;br&gt;• Password reset confirmation - manager&lt;br&gt;• Password reset - manager</td>
</tr>
<tr>
<td>$(loginUrl)</td>
<td>The web address to sign in to Oracle Cloud. The user can sign in and use the Preferences page to change a password that is about to expire. Or, without signing in, the user can engage a forgot-password procedure to change a password that has already expired.</td>
<td>• Expiring external IDP signing certificate&lt;br&gt;• Password expired&lt;br&gt;• Password expiry warning</td>
</tr>
<tr>
<td>$(resetUrl)</td>
<td>A one-time web address expressly for the purpose of resetting a password, used in the Password Generated, Password Reset, New Account, and New Account Manager templates.</td>
<td>• New account created - manager&lt;br&gt;• New user created&lt;br&gt;• Password generated&lt;br&gt;• Password reset&lt;br&gt;• Password reset - manager</td>
</tr>
<tr>
<td>$(CRLFX)</td>
<td>Insert line break.</td>
<td>All events</td>
</tr>
<tr>
<td>$(SP4)</td>
<td>Insert four spaces.</td>
<td>All events</td>
</tr>
<tr>
<td>$(adminActivityUrl)</td>
<td>A URL of the page in which an administrator initiates an administration activity.</td>
<td>Administration activity requested</td>
</tr>
<tr>
<td>$(providerName)</td>
<td>The name of an external Identity Provider.</td>
<td>Expiring external IDP signing certificate</td>
</tr>
<tr>
<td>$(signingCertDN)</td>
<td>The signing certificate of an external Identity Provider.</td>
<td>Expiring external IDP signing certificate</td>
</tr>
<tr>
<td>$(signingCertExpiration)</td>
<td>The expiration date of the external Identity Provider signing certificate or of the service provider signing certificate.</td>
<td>• Expiring external IDP signing certificate&lt;br&gt;• Expiring service provider signing certificate</td>
</tr>
<tr>
<td>$(encryptionCertExpiration)</td>
<td>The expiration date of the Service Provider encryption certificate.</td>
<td>Expiring service provider encryption certificate</td>
</tr>
<tr>
<td>$(adminFirstName)</td>
<td>The given name of the person who has administrator rights.</td>
<td>• Administration activity location based access disabled confirmation</td>
</tr>
</tbody>
</table>
### Synchronize User and Role Information

You run the process **Retrieve Latest LDAP Changes** once during implementation. This process copies data from the LDAP directory to the Oracle Fusion Applications Security tables. Thereafter, the data is synchronized automatically. To run this process, perform the task **Run User and Roles Synchronization Process** as described in this topic.

#### Run the Retrieve Latest LDAP Changes Process

Follow these steps:

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

### Reset the Cloud Service Administrator Sign-In Details

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

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

1. In the Setup and Maintenance work area, go to the following:
   - Functional Area: Initial Users
   - Task: Create Implementation Users
2. On the User Accounts page of the Security Console, search for your service administrator user name, which is typically your email. Your service activation mail contains this value.
3. In the search results, click your service administrator user name to open the User Account Details page.
4. Click Edit.
5. Change the **User Name** value to **ServiceAdmin**.
6. Delete any value in the First Name field.
7. Change the value in the Last Name field to ServiceAdmin.
8. Delete the value in the Email field.
9. Click Save and Close.
10. Sign out of your Oracle Applications Cloud service.

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

User Categories

Overview of User Categories

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

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

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

- Segregate users into categories
- Specify Next URL
- Set user preferences
- Define password policy
- Enable notifications

Segregate Users into Categories

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

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

Specify Next URL

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

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

Define Password Policy

Determine the number of days a password remains valid. Set the number of days before expiration that a user receives a warning to reset the password. You can define the period in which a user must respond to a notification to reset the password (Hours Before Password Reset Token Expiration). Select a password format and determine whether a previous password may be reused. You may decide whether to permit an administrator to manually modify passwords in the Reset Password dialog box, available from a given user’s record on the Users tab. This option applies only to the manual-reset capability. An administrator can always use the Reset Password dialog box to initiate the automatic reset of a user’s password.

Enable Notifications

Notifications are enabled by default, but you can disable them if required. You can also enable or disable notifications separately for each user category. If users belonging to a specific category don’t want to receive any notification, you can disable notifications for all life cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events.

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

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

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

Related Topics

- Using REST API to Add Users to a User Category

Add Users to a User Category

Using the Security Console, you can add existing users to an existing user category or create a new category and add them. When you create new users, they are automatically assigned to the default category. At a later point, you can edit the user account and update the user category. You can assign a user to only one category.

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

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

- Create a user category and add users to it
- Add users to an existing user category
- Specify the user category for an existing user
Note: You can create and delete a user category only using the Security Console. Once the required user categories are available in the application, you can use them in SCIM REST APIs and data loaders. You can’t rename a user category.

Adding Users to a New User Category

To create a user category and add users:

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

Adding Users to an Existing User Category

To add users to an existing user category:

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

Specifying the User Category for an Existing User

To add an existing user to a user category:

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

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

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

Use this task if you want to direct your users to another application or a website instead of the Oracle Applications Cloud sign in page, after they reset the password. Using the Security Console, you can specify the URL of the application or the website to which the users can be directed.

2. Select the user category and on the User Category: Details page, click **Edit**.

3. Specify the URL in the Next URL field and click **Save and Close**.

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

**How can I enable or disable notifications for users?**

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

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

2. Click the Notifications tab and click **Edit**.

3. Select the **Enable Notifications** check box to enable notifications for all users of that user category. To disable notifications, deselect the check box.

4. Click **Done**.

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

Overview

During implementation, you prepare your Oracle Applications Cloud service for application users. Decisions made during this phase determine how you manage users by default. Most of these decisions can be overridden. However, for efficient user management, you’re recommended to configure your environment to both reflect enterprise policy and support most or all users.

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

<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 a 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 Options

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

The **User Account Creation** option controls:

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

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

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

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

User Account Role Provisioning

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

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

User Account Maintenance

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

User Account Creation for Terminated Workers

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

**Related Topics**

- User Account Creation for Terminated Workers Option

User Account Creation Option

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

This table describes the **User Account Creation** option values.
### Application Users

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

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

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

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

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

### User Account Role Provisioning Option

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

This table describes the User Account Role Provisioning option values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both person and party users</td>
<td>Role provisioning and deprovisioning occur for both person and party users.</td>
</tr>
<tr>
<td></td>
<td>This value is the default value.</td>
</tr>
<tr>
<td>Party users only</td>
<td>Role provisioning and deprovisioning occur for party users only.</td>
</tr>
<tr>
<td></td>
<td>For person users, role requests are held in the LDAP requests table, where they’re identified as suppressed. They’re not processed.</td>
</tr>
<tr>
<td>None</td>
<td>For both person and party users, role requests are held in the LDAP requests table, where they’re identified as suppressed. They’re not processed.</td>
</tr>
</tbody>
</table>
Note: When a user account is created, roles may be provisioned to it automatically based on current role-provisioning rules. This provisioning occurs because user accounts without roles are suspended automatically. Automatic creation of user accounts and the associated role provisioning are controlled by the User Account Creation option.

User Account Maintenance Option

By default, a user’s account is suspended automatically when the user has no roles. This situation occurs typically at termination. The user account is reactivated automatically if you reverse the termination or rehire the worker. The User Account Maintenance option controls these actions. Use the Manage Enterprise HCM Information task to set this option.

This table describes the User Account Maintenance option values.

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

Set the User and Role Provisioning Options

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

Follow these steps:

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

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

### Provision Abstract Roles to Users Automatically

Provisioning the Employee, Contingent Worker, and Line Manager abstract roles automatically to users is efficient, as most users have at least one of these roles. It also ensures that users have basic access to functions and data when they first sign in. This topic explains how to set up automatic role provisioning during implementation using the **Manage Role Provisioning Rules** task.

#### Provision the Employee Role Automatically to Employees

Follow these steps:

1. Sign in as the TechAdmin user or another user with the IT Security Manager job role or privileges.
2. In the Setup and Maintenance work area, go to the following for your offering:
   ◦ Functional Area: Users and Security
   ◦ Task: Manage Role Provisioning Rules
3. In the Search Results section of the Manage Role Mappings page, click the **Create** icon. The Create Role Mapping page opens.
4. In the **Mapping Name** field enter **Employee**.
5. Complete the fields in the Conditions section of the Create Role Mapping page as shown in the following table.

<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>

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

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

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

Provision the Line Manager Role Automatically to Line Managers

Follow these steps:

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

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

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

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

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

FAQs on Preparing for Application Users

Can I implement single sign-on in the cloud?

Yes. Single sign-on enables users to sign in once but access multiple applications, within and across product families.
Submit a service request for implementation of single sign-on. For more information, see Oracle Applications Cloud Service Entitlements (2004494.1) on My Oracle Support at https://support.oracle.com.
Chapter 6

Application Users Management

Users

Create Users

During implementation, you can use the Create User task to create test application users. By default, this task creates a minimal person record and a user account. After implementation, you should use the Hire an Employee task to create application users. The Create User task isn’t recommended after implementation is complete. This topic describes how to create a test user using the Create User task.

Sign in and follow these steps:

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

The Create User page opens.

Completing Personal Details

1. Enter the user’s name.
2. In the E-Mail field, enter the user’s primary work e-mail.
3. In the Hire Date field, enter the hire date for a worker. For other types of users, enter a user start date. You can’t edit this date after you create the user.

Completing User Details

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

Setting User Notification Preferences

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

Completing Employment Information

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

Adding Roles

1. Click Autoprovision Roles. Any roles for which the user qualifies automatically, based on the information that you have entered so far, appear in the Role Requests table.
2. To provision a role manually to the user, click Add Role. The Add Role dialog box opens.

3. Search for and select the role. The role must appear in a role mapping for which you satisfy the role-mapping conditions and where the Requestable option is selected for the role.

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

   Repeat steps 2 and 3 for additional roles.

4. Click Save and Close.

5. Click Done.

User Data Import from Legacy Applications

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

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

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

Role Provisioning

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

Related Topics

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

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

<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.</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>
</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

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

To run the report:

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the **Import User Login History** process.

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

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

**Inactive Users Report Parameters**

All parameters except **Days Since Last Activity** are optional.

**User Name Begins With**

Enter one or more characters.

**First Name Begins With**

Enter one or more characters.

**Last Name Begins With**

Enter one or more characters.

**Department**

Enter the department from the user’s primary assignment.

**Location**

Enter the location from the user’s primary assignment.

**Days Since Last Activity**

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

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

**Last Activity Start Date**
Specify the start date of a period in which the last activity must fall.

**Last Activity End Date**

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

**Viewing the Report**

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

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

- Number of days since the user was last active
- Date of last activity
- User name
- First and last names
- Assignment department
- Assignment location
- City and country
- Report time stamp

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

**Related Topics**

- Schedule the Import User Login History Process

**Users Accounts**

**Manage User Accounts**

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

To access the user account page for a person:

1. Open the Person Management work area.
2. On the Search Person page, search for the person whose account you’re updating.
3. In the search results, select the person and select **Actions > Personal and Employment > Manage User Account**. The Manage User Account page opens.
Manage User Roles

To add a role:

1. Click Add Role.
   The Add Role dialog box opens.
2. In the Role Name field, search for the role that you want to add.
3. In the search results, select the role and click OK.
   The role appears in the Role Requests region with the status Add Requested.
4. Click Save.

To remove a role from any section of this page:

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

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

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

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

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

Copy Personal Data to LDAP

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

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

Reset Passwords

To reset a user’s password:

1. Select Actions > Reset Password.
2. In the Warning dialog box, click Yes to continue.
   This action sends a notification containing a reset-password link to the user’s work email.

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

Edit User Names

To edit a user name:

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

3. Click Save.

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

Tip: Users can add roles, autoprovion roles, and copy their personal data to LDAP by selecting Navigator > Me > Roles and Delegations. Line managers can add, remove, and autoprovion roles and copy personal data to LDAP for their reports from the Directory or by selecting Navigator > My Team > Users and Roles.

User Names

By default, user names are generated automatically in the format specified for the default user category when you create a person record. Users who have the human resource specialist (HR specialist) role can change user names for existing HCM users whose records they can access. This topic describes the automatic generation of user names and explains how to change an existing user name.

User Names When Creating Users

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

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

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

Existing User Names

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

To change a worker’s user name:

1. Search for and select the worker in the Person Management work area.
2. For the selected worker, select Actions > Personal and Employment > Manage User Account.
3. On the Manage User Account page, select **Actions > Edit User Name**.

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

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

### Why You Send Personal Data to LDAP

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

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

### Bulk Creation of Users

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

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

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

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

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

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

The process doesn’t apply to party users.

You must have the Human Capital Management Application Administrator job role to run this process.
The Copy Personal Data to LDAP Action
Users can copy their own personal data to the LDAP directory from the Manage User Account page. Human resource specialists and line managers can also perform this action for users whose records they can access. By default, personal data changes are copied periodically to the LDAP directory. However, this action is available for copying changes immediately, if necessary.

Related Topics
• User and Role-Provisioning Setup Options

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

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

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

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

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

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

Automatic Suspension of User Accounts
When you terminate a work relationship:

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

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

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

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

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

Automatic Reactivation of User Accounts

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

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

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

- The user loses any role that he or she acquired automatically at termination.

- If the user account was suspended automatically at termination, then it’s automatically reactivated.

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

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

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

Manual Suspension of User Accounts

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

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

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

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

**Related Topics**

- User Account Maintenance Option
User Details System Extract Report Parameters

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

**Parameters**

**User Population**

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

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

**From Date**

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

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

**To Date**

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

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

**User Active Status**

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

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

Chapter 6  
Application Users Management

Value | Description
--- | ---

**Related Topics**
- Run the User Details System Extract Report

**User Details System Extract Report**

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

Run the report in the Reports and Analytics work area.

**Report Results**

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

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

The information in the extract varies with the account type.

**HCM User Accounts**

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

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

- **Department**
The department from the primary assignment.

- **Worker Type**
The worker type from the user’s primary work relationship.

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

- **Hire Date**
The enterprise hire date.
Role Name
A list of roles currently provisioned to workers whose work relationships are all terminated. This value appears for active user accounts only.

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

TCA User Accounts

Organizations
A resource group.

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

Managers
The manager of a resource group.

LDAP User Accounts

Start Date
The account's start date.

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

Related Topics

- Run the User Details System Extract Report

View Locked Users and Unlock Users

A user gets locked in the application either on entering incorrect password for multiple times or if the application hasn't been accessed for a certain period of time. The locked users report provides the list of locked users for both these scenarios.

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

View Locked Users

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

The spreadsheet shows the list of users who are locked.
The Locked Users spreadsheet contains the following two tabs:

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

**Unlock Users**

1. On the Security Console, click **Users**.
2. From the **Search** drop down list, select **Locked Users** and click the search icon.
   
   All the locked users are displayed.
3. Click the display name of a user to view the details.
4. Click **Edit**.
5. In the Account Information section, deselect **Locked**.
6. Click **Save and Close**.
7. Click **Done**.

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

**FAQs on Creating and Managing Application Users**

**Where do default user names come from?**

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

**Why did some roles appear automatically?**

In a role mapping:

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

**How can I create a user?**

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

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

When you create a new user, it automatically triggers role provisioning requests based on role provisioning rules.
What happens when I autoprov...
What happens if I send the user name and password?

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

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

What happens if I reset a user's password?

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

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

You can run the **Send User Name and Password Email Notifications** process in the Scheduled Processes work area. For users for whom you haven’t so far requested an email, this process sends out user names and reset-password links. The email goes to the work email of the user or the user’s line manager. You can send the user name and password once only to any user. A notification template for this event must exist and be enabled.
7 Role Provisioning

Role Mappings

Roles give users access to data and functions. To provision a role to users, you define a relationship, called a role mapping, between the role and some conditions. This topic describes how to provision roles to users both automatically and manually. Use the Manage Role Provisioning Rules task in the Setup and Maintenance work area.

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

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

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

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

<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 either create or update the assignment. The provisioning process also removes automatically provisioned roles from users who no longer satisfy the role-mapping conditions.

Manual Provisioning of Roles to Users

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

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

For example, for the data role Training Team Leader, you could select the Requestable option and specify the conditions shown in this table.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager with Reports</td>
<td>Yes</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

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

**Role Requests from Users**

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

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

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Finance 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. 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**

- Examples of Role Mappings
Create a Role Mapping

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

Sign in as IT Security Manager and follow these steps:

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

The Create Role Mapping page opens.

Defining the Role-Mapping Conditions

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Finance Department</td>
</tr>
<tr>
<td>Job</td>
<td>Accounts Payable Supervisor</td>
</tr>
<tr>
<td>Location</td>
<td>Redwood Shores</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 these conditions.

Identifying the Roles

1. In the Associated Roles section, click Add Row.
2. In the Role Name field, search for and select the role that you’re provisioning.
3. Select one or more of the role-provisioning options as listed in the following table:

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

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

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

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

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

5. Click **Save and Close**.

### Applying Autoprovisioning

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

### Role Provisioning and Deprovisioning

You must provision roles to users. Otherwise, they have no access to data or functions and can’t perform application tasks. This topic explains how role mappings control role provisioning and deprovisioning. Use the Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules task to create role mappings.

### Role Provisioning Methods

You can provision roles to users:

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

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

### Role Types

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

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

Role Deprovisioning

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

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

Roles at Termination

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

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

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

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

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

Reversal of Termination

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

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

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

Date-Effective Changes to Assignments

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

# Autoprosioning

Autoprosioning is the automatic allocation or removal of user roles. It occurs for individual users when you create or update assignments. You can also apply autoprosioning explicitly for the enterprise using the Autoprosion Roles for All Users process. This topic explains the effects of applying autoprosioning for the enterprise.

## Roles That Autoprosioning Affects

Autoprosioning applies only to roles that have the Autoprosion option enabled in a role mapping. It doesn’t apply to roles without the Autoprosion option enabled.

### The Autoprosion Roles for All Users Process

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

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

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

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

### When to Run the Process

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

Only one instance of Autoprosion Roles for All Users can run at a time.

### Autoprosioning for Individual Users

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

**Related Topics**

- What happens when I autoprosion roles for a user
• Schedule the Send Pending LDAP Requests Process

User and Role Access Audit Report

The User and Role Access Audit Report provides details of the function and data security privileges granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console. This report is based on data in the Applications Security tables, which you populate by running the Import User and Role Application Security Data process.

To run the User and Role Access Audit Report:

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

User and Role Access Audit Report Parameters

Population Type

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

• All roles
• Multiple users
• Role name
• User name

User Name

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

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

Role Name

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

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

From User Name Starting With

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

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

To User Name Starting With

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

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

User Role Name Starts With
Enter one or more characters from the start of a role name.

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

**Data Security Policies**

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

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

**Debug**

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

**Viewing the Report Results**

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

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

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

<table>
<thead>
<tr>
<th>Report Type</th>
<th>File Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>USER_NAME</td>
</tr>
<tr>
<td>Role name</td>
<td>ROLE_NAME</td>
</tr>
<tr>
<td>Multiple users</td>
<td>MULTIPLE_USERS</td>
</tr>
<tr>
<td>All roles</td>
<td>ALL.Roles</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Report Type</th>
<th>File Suffix</th>
<th>File Format</th>
<th>File Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>DataSec</td>
<td>CSV</td>
<td>Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only</td>
</tr>
</tbody>
</table>
### Data Access

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

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

The following table lists the elements of the enterprise structure to which users can be assigned access based on their job roles.
Assigning Data Access
Assigning data access to users is a three step process:

1. Create users using one of the following:
   - Manage Users task in Oracle Fusion Functional Setup Manager
     - Specify user attributes such as user name, assigned business unit, legal employer, department, job, position, grade, and location.
   - Security Console

2. Assign at least one job role to users. Use Oracle Fusion Human Capital Management or the Security Console to assign job roles. Alternatively, define Role Provisioning Rules to auto-provision roles to users based on the users' work assignments.

3. Assign data access to users for each applicable job role. Use the Manage Data Access for Users task in the Functional Setup Manager. For General Ledger users, you can also use the Manage Data Access Set Data Access for Users task to assign data access. Alternatively, define Data Provisioning Rules to auto-provision data access to users based on the users' work assignments.
Assign Data Access to Users

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

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

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

<table>
<thead>
<tr>
<th>Decision to Consider</th>
<th>In This Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which user role is being given data access?</td>
<td>Accounts Payable Manager</td>
</tr>
<tr>
<td>What is the security context to which access is being given?</td>
<td>Business Unit</td>
</tr>
</tbody>
</table>

Prerequisites

Before you can complete this task, you must:

1. Create users and specify the user attributes such as a user name, assigned business unit, legal employer, department, job, position, grade and location, and so on. To create users, use the Manage Users task in the Functional Setup Manager or the Create User page. If you’re implementing Oracle Fusion HCM, you can also use the Hire an Employee page. You can also use the Security Console to create the implementation users who create the setups, such as legal entities, business units, and so on, that are required to create the users in the Manage Users or Hire an Employee page.

2. Assign users their job roles. You can either use Oracle Fusion Human Capital Management or the Security Console to assign job roles.

3. Run the Retrieve Latest LDAP Changes process.

Assigning Data Access to Users Using a Spreadsheet

1. Sign in to the Functional Setup Manager as an IT Security Manager or Application Implementation Consultant and navigate to the Setup and Maintenance page.

2. Search for and select the Manage Data Access for Users task. Alternatively, you can perform this task through the product-specific task list.

3. Click **Users without Data Access** to view users who don’t have data access. Alternatively, to assign additional data access to users, use the **Users with Data Access** option.

4. Select the **Security Context**, for our example, select **Business Unit**.

5. Search for users with no data access. For our example, enter **Accounts Payable Specialist** in the **Role** field.

   ✍️ **Note:** The search fields are related to the user attributes.
6. Click **Search**. The Search Results region displays users who don't have any data access.
7. Click the **Authorize Data Access** button to export the search results to a Microsoft Excel spreadsheet. You can provide data access to a group of users through the spreadsheet.
8. Click **OK** to open the spreadsheet using Microsoft Excel.
9. Select the **Security Context** from the list for each user.
10. Enter the **Security Context Value**.
    - To provide additional data access to the user, add a new row and enter the user name, role, security context, and security context value.
    - You can click the **View Data Access** button to see what other data access the user already has even if this is outside the parameters of the search. This may help to identify users you want to grant access to because of existing access.
11. Click the **Upload** button on the spreadsheet when you have assigned data access.
12. Select the upload options on the Upload Options window and click **OK**.
13. Note the status of your upload in the **Upload** column.
    - If the status of the upload is **Successful** and there are no validation errors in the log file, you can view the data access assignment to the users using the search criteria on the Manage Data Access for Users page.
    - If the upload status is **Failed**, check the details in your upload file, correct any errors, and upload the file again.

### Automatic Data Provisioning

You can automatically assign users access to appropriate data based on their work assignments.

Automatic data provisioning occurs if:

- At least one of the user’s assignments matches all data-mapping conditions on a Data Provisioning Rule
- At least one role is automatically provisioned to the user using Role Provisioning Rules
- The matched Data Provisioning Rule includes data assignments for a role that is automatically provisioned to the user

For example, you can create a data provisioning rule to assign all current employees of the Finance Department in Seattle the following data assignments:

<table>
<thead>
<tr>
<th>Role</th>
<th>Data Security Context</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable Manager</td>
<td>Business Unit</td>
<td>US West</td>
</tr>
<tr>
<td>Accounts Payable Supervisor</td>
<td>Business Unit</td>
<td>US West</td>
</tr>
<tr>
<td>Accounts Payable Specialist</td>
<td>Business Unit</td>
<td>US West</td>
</tr>
<tr>
<td>Accounts Receivable Manager</td>
<td>Business Unit</td>
<td>US West</td>
</tr>
<tr>
<td>Accounts Receivable Specialist</td>
<td>Business Unit</td>
<td>US West</td>
</tr>
<tr>
<td>Financial Analyst</td>
<td>Data Access Set</td>
<td>US-Corporate</td>
</tr>
<tr>
<td>General Accountant</td>
<td>Data Access Set</td>
<td>US-Corporate</td>
</tr>
</tbody>
</table>
Role Provisioning

With this data provisioning rule defined, a user with a work assignment location of Seattle that has been automatically provisioned one of the job roles listed above would also get the corresponding data assignments.

Note: While role mappings and data provisioning rules use similar attributes to find a user's matching assignments, you do not need to use the same combination of attributes to drive role provisioning and the corresponding data provisioning. For example, you can use a combination of job, grade, or department or all to determine automatic provisioning of roles, and use a combination of business unit, legal employer or location or all to determine automatic provisioning of data.

Creating a Data Provisioning Rule

To automatically provision data assignments to users, you create data provisioning rules.

Before creating data provisioning rules, you first need to opt-in the feature Data Security Auto-Provisioning for ERP.

Sign in as IT Security Manager or Application Implementation Consultant and follow these steps:

1. Navigate to the Setup and Maintenance page.
2. Search for and select the Manage Data Access for Users task. Alternatively, you can perform this task through the product-specific task list.
3. Click Data Provisioning Rules.
4. In the Search Results section of the page, click Create.

The Create Data Provisioning Rules page opens.

5. Set values in the Conditions section to specify when the data provisioning rule applies. For example, use the values given in the following table to limit the data provisioning rule to current employees of the Finance Department in Seattle.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Finance Department</td>
</tr>
<tr>
<td>Location</td>
<td>Seattle</td>
</tr>
<tr>
<td>System Person Type</td>
<td>Employee</td>
</tr>
<tr>
<td>HR Assignment Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

6. In the Data Assignments section, click Add Row.
7. In the Role Name field, search for and select the role for this particular data assignment.
8. In the Security Context field, select the desired security context from the list.
Applying Automatic Provisioning
You’re recommended to run the process Autoprovison Roles for All Users after creating or editing data provisioning rules and after loading person records in bulk. This process compares all current user assignments with all current role mappings and data provisioning rules and creates appropriate autoprovisioning requests for both role and data assignments.

Automatic Data Provisioning and Deprovisioning
The process of automatic data provisioning and deprovisioning is very similar to automatic role provisioning and deprovisioning.

Automatic Data Provisioning
Users acquire a data assignment automatically when at least one of their work assignments satisfies the conditions in the relevant data provisioning rule and the corresponding role in the applicable data assignment is also automatically provisioned. For example, if a worker is hired into the Finance Department of the Seattle office, the worker acquires the relevant data assignments automatically if an appropriate role provisioning rule exists for Finance Department or Seattle office or for both, provided that at least one of the affected roles in the role provisioning rule is also automatically provisioned to the user. Provisioning occurs when you create or update worker assignments. All changes to work assignments cause review and update of a worker’s automatically provisioned roles as well as data assignments.

Data Deprovisioning
Users lose automatically provisioned data assignments when they no longer satisfy the data provisioning conditions. For example, if a worker is relocated from the Seattle office to another office, data assignments that were automatically provisioned for workers working at the Seattle office will be lost automatically. You can also manually deprovision automatically provisioned data assignments at any time.

Data Assignments at Termination
When you terminate a work relationship, the user automatically loses all automatically provisioned data assignments, similar to how the user would automatically lose all automatically provisioned roles.

Autoprovison Roles for All Users Process
The Autoprovison Roles for All Users process handles both automatic role provisioning and automatic data provisioning. The process compares all current user assignments with all current role mappings and data provisioning rules. Users with at least one work assignment that matches the conditions in a data provisioning rule and acquire those data assignments as long as the corresponding role is automatically provisioned. Users who currently have the data assignments but no longer satisfy the associated data provisioning rule conditions lose those data assignments. Users who currently have the data assignments but no longer satisfy the associated data provisioning rule conditions lose those data assignments.
Access for Workflow Administrators

Predefined roles provide workflow administration access for specific product families. These roles are assigned by default to predefined job roles. Administrators with these roles can, for example, set up approval rules and manage submitted approval tasks for corresponding product families. One predefined role gives access for all families and isn’t assigned by default to any predefined job role.

Predefined Roles

This table lists the predefined roles for workflow administration access and the predefined job roles that they’re assigned to.

<table>
<thead>
<tr>
<th>Product Family</th>
<th>Role Name</th>
<th>Role Code</th>
<th>Predefined Job Roles Assigned To</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>BPM Workflow All Domains Administrator Role</td>
<td>BPMWorkflowAllDomainsAdmin</td>
<td>None</td>
</tr>
<tr>
<td>Financials</td>
<td>BPM Workflow Financials Administrator</td>
<td>BPMWorkflowFINAdmin</td>
<td>Financial Application Administrator (ORA_FUNCION FINANCIAL_APPLICATION_ADMINISTRATOR_JOB)</td>
</tr>
<tr>
<td>Higher Education</td>
<td>BPM Workflow Higher Education Administrator</td>
<td>BPMWorkflowHEDAdmin</td>
<td>Higher Education Application Administrator (ORA_HEY_HIGHER_EDUCATION_APPLICATION_ADMINISTRATOR_JOB)</td>
</tr>
<tr>
<td>Human Capital Management</td>
<td>BPM Workflow Human Capital Management</td>
<td>BPMWorkflowHCMAdmin</td>
<td>Human Capital Management Application Administrator (ORA_HCM_HUMAN_CAPITAL_MANAGEMENT_ADMINISTRATOR_JOB)</td>
</tr>
<tr>
<td>Incentive Compensation</td>
<td>BPM Workflow Incentive Compensation Administrator</td>
<td>BPMWorkflowOICAdmin</td>
<td>Customer Relationship Management Application Administrator (ORA_ZCA_CUSTOMER_RELATIONSHIP_MANAGEMENT_ADMINISTRATOR_JOB)</td>
</tr>
<tr>
<td>Procurement</td>
<td>BPM Workflow Procurement Administrator</td>
<td>BPMWorkflowPRCAdmin</td>
<td>Procurement Application Administrator (ORA_PO_PROCUREMENT_APPLICATION_ADMINISTRATOR_JOB)</td>
</tr>
</tbody>
</table>
## Usage of the Roles

If your administrators manage workflow for more than one product family, then you or your security administrator can add the appropriate family-specific roles to custom roles for those users. If your administrators manage workflow for all product families, then add BPM Workflow All Domains Administrator Role to a custom role for those users.

**Note:**
- Assign BPM Workflow All Domains Administrator Role only if your administrators truly need access for all product families. For multiple product families, but not all, assign instead the roles for the corresponding families.
- To-do tasks are visible to all administrators no matter which role they have for workflow administration access.
Related Topics

- Edit Job and Abstract Roles
- Role Copying or Editing

View Role Information Using Security Dashboard

As an IT Security Manager, you can use the Security Dashboard to get a snapshot of the security roles and how those roles are provisioned in the Oracle Cloud Applications. The information is sorted by role category and you can view details such as data security policy, function security policy, and users associated with a role. You can also perform a reverse search on a data security policy or a function security policy and view the associated roles.

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

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

Here are the steps to view the Security Dashboard:

1. In the Reports and Analytics work area, click Browse Catalog.
   All pages of the dashboard are listed.
3. To view the Role Category Overview page, click Open.
   The page displays the number of roles in each role category in both tabular and graphical formats.
4. In the Number of Roles column, click the numeral value to view the role-related details.
5. Click View Role to view the role-specific information in the Role Dashboard.

FAQs on Provisioning Roles and Data to Application Users

What's a role-mapping condition?

Most are assignment attributes, such as job or department. At least one of a user’s assignments must match all assignment values in the role mapping for the user to qualify for the associated roles.
What's an associated role in a role mapping?

Any role that you want to provision to users. You can provision data roles, abstract roles, and job roles to users. The roles can be either predefined or custom.

What's the provisioning method?

The provisioning method identifies how the user acquired the role. This table describes its values.

<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 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 HCM Cloud, Oracle Sales Cloud, Oracle ERP Cloud, Oracle SCM Cloud, and Oracle Fusion Suppliers.

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

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

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

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

Use the Security Console to search for the user. When you select the user, the user and any roles assigned to the user appear in the visualizer. Navigate the nodes to see the role hierarchies and privileges. You must be assigned the IT Security Manager role to access the Security Console.
Why can't a user access a task?

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

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

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

Note: You cannot change predefined roles to add or remove duties. In the Security Console, you can identify predefined roles by the ORA_prefix in the Role Code field. Create copies and update the copies instead.

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

How can I autoprovison data assignments for users?

If you want to use automatic provisioning of data assignments, you need to consider the following points:

1. All users with matching work assignments would automatically get the same data assignments as specified in the data provisioning rules. While it is possible to manually deprovision undesirable data assignments, the additional manual tasks required to deprovision these undesirable data assignments would negate the benefits of automatic data provisioning and create security risks

2. Only data assignments for roles that are autoprovisioned to users can be automatically provisioned to users. However, you do not need to use the same combination of attributes to drive role provisioning in role-mappings and the corresponding data provisioning in data provisioning rules.

What happens if I autoprovison data assignments for a user?

The data assignment provisioning process is part of the role-provisioning process, and reviews the user's work assignments against all data provisioning rules.

The user immediately:

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

You are recommended to run the Autoprovision Roles for All Users process to autoprovison data assignments to users when new or changed role provisioning rules exist. Otherwise, no automatic provisioning of data assignments occurs until you next update the user's work assignments.
Why can't I see the data assignments for a user that I expect to be autoprovisioned?

Automatic provisioning of data assignments would only occur for roles that are also automatically provisioned.

What data security contexts are supported in automatic data provisioning?

All data security contexts that are supported in Manage Data Access for Users are supported. In other words, Automatic Data Provisioning is essentially rule-based Manage Data Access for Users assignments.
Location Based Access

Overview of Location-Based Access

You can use location based access to control user access to tasks and data based on their roles and computer IP addresses.

Let’s take an example to understand how location based access is useful. You want your users to have complete access to tasks or features when they’re signed into the application from your office network. But you want to restrict the access if the users are signing in from a home computer or an internet kiosk. To control the user access, you need to enable location based access and register the IP addresses of your office computers on the Security Console. Users have complete access to the tasks or features if they sign in from office computers. If they sign into the application from an unregistered computer, they can view and access only the generic tasks that aren’t tied to any particular role. From an unregistered computer, they can’t access the role-based tasks, which they could access from office.

Who Can Enable Location-Based Access

You must have the IT Security Manager role to enable location based access and make a role public. You can make a role public only when location based access is enabled. To enable location based access, you must register the IP addresses of computers from which the users usually sign in to the application.

What Happens When You Enable Location-Based Access

When you enable location based access, users signing into the application from registered IP addresses have complete access to all tasks. On the other hand, users signing in from unregistered IP addresses have no access to their role-based tasks and data. However, you can grant complete access to these users too, when required. You can also grant public access (access from all IP addresses) to certain roles. The users associated with those roles can access all tasks, no matter which IP address they sign in from.

How Location-Based Access Works

Location-based access combines the registered IP addresses of the computers and public roles to control access to the application.

Scenarios

To understand how location-based access works, consider the following scenarios and their effect on user access.

To avoid any access-related issue, carefully examine the given scenarios and plan well before you enable location-based access.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Impact on User Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>You disable location-based access.</td>
<td>All users signing into the application from their respective computers continue to have the same level of access as they had earlier.</td>
</tr>
</tbody>
</table>
Enable and Disable Location-Based Access

You can enable location based access so that you can allow users to access tasks and data based on their roles and registered IP addresses. By default, location-based access is disabled.

Before You Start
Configure location based access in a test environment and try it out before you configure it in a production environment. You must have the IT Security Manager role to enable location based access. Additionally, you must:

- Set up a valid email address. When required, the location based access control reset or recovery notification is sent to that email address.
- Add yourself to the user category for which the notification template ORA Administration Activity Requested Template is enabled.
- Keep the list of valid IP addresses ready.

Enable Location-Based Access

1. Click Navigator > Security Console.
2. On the Administration page, click the Location Based Access tab.
3. Select Enable Location Based Access.
4. In the IP Address Whitelist text box, enter one or more IP addresses separated by commas. For example, 192.168.10.12, 192.168.10.0. If you want to indicate a range of IP addresses, you may follow the Classless Inter-Domain Routing (CIDR) notation, such as 192.168.10.0/24.

Note: You can enter only up to 32 IP addresses of version IPv4 in the IP Address Whitelist text box.
Tip: Your computer’s IP address appears on the page. Add that IP address to the list so that your access to the application remains unaffected when you sign in from that computer.

5. Click **Save**.
6. Review the confirmation message and click **OK**.

After you enable location based access, make the IT Security Manager’s role public so that you can access Security Console even when signed in from an unregistered IP address.

Disable Location-Based Access

To disable location based access, deselect the **Enable Location Based Access** check box. The existing IP addresses remain in a read-only state so that you can reuse the same information when you enable the functionality again. At that point, you can add or remove IP addresses based on your need.

FAQs on Location Based Access

What is whitelisting?

Whitelisting is the process of granting trusted entities access to data or applications. When you enable location based access and register the IP addresses of computers, you are storing those IP addresses as trusted points of access. In other words, you are whitelisting those IP addresses. Users signing in from those computers will be considered as trusted users and have unrestricted access to the application.

Why can't I see the Location Based Access tab on the Administration page?

To prevent any incorrect configuration, the profile option **Enable Access to Location Based Access Control** associated with the Location Based Access tab is perhaps disabled. As a result, the tab isn’t visible. Contact your Application Implementation Consultant or Administrator to enable the profile option so that the Location Based Access tab appears on the Administration page.

How can I make a role public?

On the Security Console, identify the role that you want to make public. Except duty roles, you can make all roles public. On the Edit Role page, select the option **Enable Role for Access from All IP Addresses** and save the changes. All users associated with that role will have access to the role-based tasks, no matter which computer they’re using to sign into the application.

Note: You can make a role public only if location based access is enabled.
How can I ensure that I always have access to the Security Console?

If location based access is enabled, you must add your computer's IP address to the whitelist. Also ensure that the IT Security Manager role is granted public access. Even if you have to sign in from an unregistered computer, you can still access the Security Console and other tasks associated with the IT Security Manager role.

How can I disable Location-based Access when I am not signed in to the application?

You want to disable location-based access but you are locked out of the application and can't sign in to the Security Console. You must request access to the Administration Activity page using the URL provided to the administrators. Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

https://<podname>.fa.<datacentername>.oraclecloud.com/fscmUI/faces/FuseWelcome

Click the URL and you are directed to a secure Administrator Activity page. Select the **Disable Location Based Access** option and click **Submit**. You receive a confirmation that location-based access is disabled. Immediately, you are redirected to the Oracle Applications Cloud login page where you can sign in using your registered user name and password, and gain access to tasks and data as earlier.

How can I disable Location-based Access when I am locked out of the application?

If you are locked out of the application for some reason, use the following Administration Activity URL to disable location-based access:

https://<pod_name>.fa.<data_center>.oraclecloud.com/hcmUI/faces/AdminActivity

Only an administration user with the IT Security Manager job role can perform this unlock operation. Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Location Based Access Disabled Confirmation Template
9 Single Sign-On

Configure Single Sign-On

To configure Oracle Applications Cloud as the service provider, you must do the following:

- Add an identity provider
- Review the service provider details
- Test the identity provider
- Enable the identity provider

On the Security Console, go to the Single Sign-On tab and click **Create Identity Provider**.

Add an Identity Provider

You can add as many identity providers as required to facilitate single sign-on for all your users. However, one of them must be the default identity provider.

Before you begin:

One of the important steps in adding an identity provider is to import the metadata content of the identity provider. The metadata file contains the authentication information and also the signed and encrypted certificates of the identity provider. Make sure you have the metadata XML file or the URL readily available. Without the file, the setup isn’t complete.

> **Note:** Including encryption certificate in the metadata file is optional.

1. On the Security Console, click **Single Sign-On > Create Identity Provider**.
2. On the Identity Provider Details page, click **Edit** and enter the identity provider details:
   - Provide a **Name** and **Description** for the identity provider.
   - Select the relevant Name ID Format. If you have an email as the name of the identity provider, select **Email**. Otherwise, leave it as **Unspecified**.
   - Enter the **Sign Out URL**. This is the URL that the users are redirected to once they sign out from the application.
   - Enter the **Relay State URL**. This is the URL to which users are directed to sign and authenticate irrespective of which application they want to access.
   - Select the **Default Identity Provider** check box if you want to make this identity provider the default one.
   - Select the **Enable Chooser Login Page** check box to display the service provider's single sign-on page along with your company’s sign in page.
3. Import the identity provider metadata:
   - If it’s an XML file, click **Browse** and select it.
   - If it’s available on a web page, select the **External URL** check box and enter the URL.

> **Note:** The metadata XML file must be Base64 encoded.

4. Click **Save and Close**.
Review Service Provider Details
The Service Provider Details and the Diagnostics and Activation tabs are enabled only if the identity provider details are entered. Click the Service Provider Details tab and review the following information available on the page:

- ID of the service provider. In this case, it’s the ID of Oracle Applications Cloud.
- Service provider metadata. The URL references to an XML file that you can download and view.
- Service provider signing certificate.
- Service provider encryption certificate.

You must share these details with the identity providers so that they can use them to configure your application as the associated service provider.

Test the Identity Provider
Click the Diagnostics and Activation tab to verify if the identity provider that you added works as expected.

1. Click the Test button to run the diagnostics. The Initiate Federation SSO page appears.
2. Click the Start SSO button. You are prompted to enter the user credentials of any user registered with the identity provider. The test validates whether the federation single sign-on is successful or not. The result summary includes the following details:
   - Status of authentication: success or failure
   - The attributes passed in the assertion
   - The assertion message in XML

You can review the log messages that appear in the Federation Logs section to identify if there are any configuration issues with the identity provider.

Note: You must run the test whenever there’s a change in the identity provider configuration.

Enable the Identity Provider
If everything looks fine, you can go ahead and enable the identity provider. While you are on the Diagnostics and Activation page, click Edit and select the Enable Identity Provider check box. The identity provider is now active.

Oracle Applications Cloud as the Single Sign-On Service Provider
Your users are likely to access different internal and external applications to perform their tasks. They may require access to different applications hosted by partners, vendors, and suppliers. Certainly, users won’t like authenticating themselves each time they access a different application. This is where you as the IT Manager can make a difference. You can provide your users with a seamless single sign-on experience, when you set up Oracle Applications Cloud as a single sign-on service provider.
Your users are registered with identity providers who store and manage their identity and credentials. In Security Console, you can add those identity providers so that you can verify those users without having to store that information.

Initial Login

On a typical working day, when users sign in for the first time, they request access to an application or a web page. Oracle Applications Cloud, which is set up as a service provider, sends a verification request to the user’s identity provider who is already added to the Security Console. The identity provider verifies the user credentials and sends the authorization and authentication response back to the service provider. After successful authentication, users are granted access to the required application or web page. Because the authentication is valid across your enterprise network, users don’t have to sign in again when accessing different applications available on the same network. This entire trust chain between the service provider and the various identity providers is established using the Security Assertion Markup Language (SAML) 2.0 standards.

Final Sign-out

Single sign-on also applies to signing out of the enterprise network. When users sign out from one application, they are automatically signed out from all applications on the network. This is to prevent unauthorized access and to ensure that data remains secure all the time.

FAQs on Single Sign-On

Does the service provider store user passwords?

No. Passwords are stored with the identity providers. When a user signs in, the identity provider authenticates the password, authorizes the request to access an application, and sends that confirmation back to the service provider. The service provider then allows users to access the application or web page.

Can I set up an identity provider without enabling it?

Yes, you can set up an identity provider and test it thoroughly before enabling it. By default, an identity provider remains disabled. You can disable an identity provider at any time.

How can I allow my users to sign in using their company’s credentials?

On the Security Console, go to Single Sign-On > Identity Provider Details page and make sure that the Enable Chooser Login Page check box is selected.

When your users access the main portal page, they can sign in using one of the following options:

- The single sign-on credentials registered with the identity provider
- The single sign-on credentials registered with their company
What should I do to extend the validity of certificates provided by the identity provider?

Pay attention to the notifications you receive about certificate expiry. Request your identity provider to share with you the updated metadata file containing renewed certificate validity details. Once you upload the metadata file, the validity of the certificate is automatically renewed. You will have to monitor this information at intervals to ensure that the certificates remain valid at all times.

How can the identity provider obtain renewed certificates from the service provider?

The identity provider can submit a service request to the service provider asking for the renewed signing and encryption certificates.

How can I disable Single Sign-On when I am not signed in to the application?

You must request access to the Administration Activity page using the URL provided to the administrators. Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINISTER_SECURITY_PRIV

After you request access to the Administration Activity page, you get an email at your registered email ID containing a URL with the following format:

https://<podname>.fa.<datacentername>.oraclecloud.com/fscmUI/faces/FuseWelcome

Click the URL and you are directed to a secure Administrator Activity page. Select the Disable Single Sign On option and click Submit. You receive a confirmation that single sign-on is disabled. Immediately, you are redirected to the Oracle Applications Cloud login page where you can sign in using your registered user name and password.

What are the different events and notifications associated with the Single Sign-On functionality?

Automatic notifications are sent for the following events associated with single sign-on:

- When an administrator requests access to the Administration Activity page to disable single sign-on
- When the single sign-on functionality is disabled
- When the external identity provider’s signing certificate is about to expire
- When the service provider’s signing certificate is about to expire
- When the service provider’s encryption certificate is about to expire
Note: Notifications are sent to users who are assigned the Manage SSO privilege, as per the following schedule:
- First notification - 60 days before the expiry date
- Second notification - 30 days before the expiry date
- Last notification - 10 days before the expiry date.

How do I reimport Identity Provider metadata?
Whenever you get an updated metadata file from the Identity Provider you must reimport the file into the application to continue using SSO configuration

1. On the Identity Provider Details page, click Edit.
2. Import the identity provider metadata:
   - If it’s an XML file, click Browse and select it.
   - If it’s available on a web page, select the External URL check box and enter the URL.

Note: The metadata XML file must be Base64 encoded.

3. Click Save and Close.

Note: Remember to test the Identity Provider after reimport.

How can I disable Single Sign-On when I am locked out of the application?
If you are locked out of the application for some reason, use the following Administration Activity URL to disable single sign-on:
https://<pod_name>.fa.<data_center>.oraclecloud.com/hcmUI/faces/AdminActivity

Only an administrator user with the IT Security Manager job role can perform this unlock operation.

Ensure that the following email notification templates are enabled:
- ORA Administration Activity Requested Template
- ORA Single Sign-On Disabled Confirmation Template
Export and Import of Security Setup Data

Export and Import of Security Console Data

You can move the Security Console setup data from one environment to another using the CSV export and import functionality.

Let’s assume you have spent a lot of time and effort in configuring and setting up the Security Console in your primary environment. You test the setup and find that everything’s working as intended. Now, you want to replicate the same setup in another environment. And you want that to happen with the least effort and as quickly as possible. Well, it certainly can be done in a simple and less time-consuming way.

In the Setup and Maintenance work area, use the Manage Application Security Preferences task in the Initial Users functional area.

Before You Begin

Learn how to export business object data to a CSV file and to import business data from a CSV file. Detailed instructions are available in the Managing Setup Using CSV File Packages chapter of the Using Functional Setup Manager guide.

What Gets Exported and Imported

The Security Console setup data comprises information that you see on the Administration and User Categories tabs of the Security Console. The following business objects help in packaging those details into CSV files so that the data can be easily exported and imported.

- Security Console Administration Settings
- Security Console User Category
- Security Console User Category Notifications

Note: Lists of users or information about any specific user is never a part of this export and import process.

In this table, you will find information about the contents of each business object.

<table>
<thead>
<tr>
<th>Business Object</th>
<th>Information Included in Export and Import</th>
</tr>
</thead>
</table>
| Security Console Administration Settings| • General administration details  
• Role preferences  
• Location-based access settings       |

Note: If location-based access isn’t enabled (if the tab doesn’t appear on Security Console), nothing gets included in the export or import.

| Security Console User Category         | • User category details  
• Password policy information            |
Export and Import of Security Setup Data

When the export process successfully completes, you get the following CSV files:

- Administration Settings CSV
- User Category CSV
- User Category Notifications CSV

**Note:** If there are language packs installed on your application, additional CSV files may be generated containing the translated data.

To import data into another environment, bundle these files into a .zip file to create the CSV file package and follow the process for importing setup data.

**Related Topics**
- Exporting and Importing CSV File Packages: Procedure
- Key Information About Setup Data Export and Import Processes

Export and Import of Custom Roles

You are looking at migrating your custom role hierarchy information from a test environment to a production environment. Or, you need a quick way to replicate the role information from one production instance to another. Whatever your purpose might be, all you need is a simple spreadsheet to migrate custom role information from a source to a target.

In the Setup and Maintenance work area, use the Manage Job Roles and Manage Duties tasks in the Users and Security functional area.

**Before You Begin**

Learn how to export business object data to a CSV file and to import business data from a CSV file. Detailed instructions are available in the Managing Setup Using CSV File Packages chapter of the Using Functional Setup Manager guide.

**What Gets Exported and Imported**

When you export or import the custom roles, the following business objects containing the custom role definitions are bundled into the CSV package.

- Functional Security Custom Roles
- Functional Security Custom Role Hierarchy
Let's closely examine each business object to know what it contains.

<table>
<thead>
<tr>
<th>Business Object</th>
<th>Information Included in Export and Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Security Custom Roles</td>
<td>The custom role includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Role Code</td>
</tr>
<tr>
<td></td>
<td>• Role Name</td>
</tr>
<tr>
<td></td>
<td>• Role Description</td>
</tr>
<tr>
<td></td>
<td>• Role Category</td>
</tr>
<tr>
<td></td>
<td>• All IP Address Access - indicates that a role is granted access to the Security Control</td>
</tr>
<tr>
<td></td>
<td>irrespective of the IP address from where it's signed in.</td>
</tr>
<tr>
<td>Functional Security Custom Role Hierarchy</td>
<td>The role hierarchy includes the following details:</td>
</tr>
<tr>
<td></td>
<td>• Parent Role</td>
</tr>
<tr>
<td></td>
<td>• Member Role</td>
</tr>
<tr>
<td></td>
<td>• Add or Remove Role Membership</td>
</tr>
<tr>
<td>Functional Security Custom Role Privilege</td>
<td>The role privilege membership includes the following details:</td>
</tr>
<tr>
<td>Membership</td>
<td>• Parent Role</td>
</tr>
<tr>
<td></td>
<td>• Member Privilege</td>
</tr>
<tr>
<td></td>
<td>• Add or Remove Privilege Membership</td>
</tr>
</tbody>
</table>

When the export process successfully completes, you get the following CSV files:

- Custom Roles CSV
- Custom Role Hierarchy CSV
- Custom Role Privilege Membership CSV

To import data into another environment, bundle these files into a .zip file to create the CSV file package and follow the process for importing setup data.

Related Topics

- Exporting and Importing CSV File Packages: Procedure
- Key Information About Setup Data Export and Import Processes
11 Security Configuration

Data Security Policies

Data Security

By default, users are denied access to all data.

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

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

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

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

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

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

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

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

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

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

The following table provides an 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.

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

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

HCM Security Profiles

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

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

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

Advanced Data Security

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

Oracle Database Vault

Database Vault reduces the risk of highly privileged users such as database and system administrators accessing and viewing your application data. This feature restricts access to specific database objects, such as the application tables and SOA objects.
Administrators can perform regular database maintenance activities, but cannot select from the application tables. If a DBA requires access to the application tables, request temporary access to the Oracle Fusion schema at which point keystroke auditing is enabled.

**Transparent Data Encryption**

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

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

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

**How Database Resources and Data Security Policies Work Together**

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

The database resource defines an instance of a data object. The data object is a table, view, or flexfield.
The following figure shows the database resource definition as the means by which a data security policy secures a data object. The database resource names the data object. The data security policy grants to a role access to that database resource based on the policy’s action and condition.

**Database Resources**

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

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

**Data Security Policies**

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

- Condition identifying the instance set of values in the data object
- Action specifying the type of access allowed on the available values
Note: If the data security policy needs to be less restrictive than any available database resource for a data object, define a new data security policy.

Actions

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

Conditions

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

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

FAQs on Configuring 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.

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.

How can I design roles?

You can simulate menus that existing roles present to users to determine how the access they provide may be expanded. Create a visualization, or populate the Search Results column with a selection of roles or users. Select the user or role and click the Actions menu. A menu appears, click Simulate Navigator.

A simulated Navigator menu appears, listing menu and task entries. If the menu item appears without a lock, the menu is not authorized for the role or user. If the menu item appears with a lock, the menu is authorized for the role or user. Click
any menu item and select either of two options. One lists roles that grant access to the menu item. The other lists privileges required for access to the menu item.

How can I mask data in an environment?

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

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

How do I create a role hierarchy?

The most efficient way to create role hierarchies is to use the Security Console. You use the Edit Role action to navigate through the steps and add roles and privileges in the visualizer or table view.

Why would I need to remove duty roles from a role hierarchy?

If your custom duty roles enable actions and user interface features that your enterprise does not want users to perform in your application.

`Note:` Don’t remove duty roles from predefined job or abstract roles in the reference implementation. In the Security Console, you can identify predefined application roles by the ora_ prefix in the Role Code field. You must copy any role that doesn’t match your needs, and then edit the copy.

How do I create a new job role?

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

Review Role Assignments

You can use the Security Console to:

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

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

View the Roles Assigned to a User

Follow these steps:

1. Open the Security Console.
2. On the Roles tab, search for and select the user.

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

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

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

Identify Users Who Have a Specific Role

Follow these steps:

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

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

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

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

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

Follow these steps:

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

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

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

Compare Roles

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

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

Selecting Roles for Comparison

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

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

### Comparing Roles

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

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

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

### Adding Policies to a Role

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

Custom Roles

Create Roles in the Security Console

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

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

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

Providing Basic Information

On a Basic Information page:

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

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

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

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

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

Adding Function Security Policies

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

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

• A job or abstract role. In this case, the policy selects functional privileges specific to that role.

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

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

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

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

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

### Adding Data Security Policies

A data security policy may be explicit or implicit.

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

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

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

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

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

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

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

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

To add a role:

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

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

Adding Users

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

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

To add a user:

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

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

Completing the Role

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

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

*Related Topics*

- Options for Viewing a Visualization Graph
Role Copying or Editing

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

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

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

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

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

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

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

  You cannot:
  - Modify, add, or remove function security policies.
  - Modify or remove data security policies provided by Oracle.
  - Modify the role hierarchy.

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

- By default, the name and code of a copied role match the source role's, except a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.

- A copied role cannot inherit users from a source job or abstract role. You must select users for the copied role. (They may include users who belong to the source role.)

- When you copy a role, the Role Hierarchy page displays all roles subordinate to it. However, you can add roles only to, or remove them from, the highest role you copied.

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

**Related Topics**

- **Generate a Visualization**
Security Console Role-Copy Options

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

- Copy top role
- Copy top role and inherited roles

This topic explains the effects of each of these options.

Copy Top Role

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

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

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

The option of copying the top role is referred to as a shallow copy. This figure summarizes the effects of a shallow copy. It shows that the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.
You're recommended to create a shallow copy unless you must make changes that could affect other roles or that you couldn't make to predefined roles. To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. To copy the inherited roles, select the **Copy top role and inherited roles** option.

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

### Copy Top Role and Inherited Roles

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

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

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

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

**Related Topics**

- Guidelines for Copying HCM Roles
Copy Job and Abstract Roles

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

Copy a Role

Follow these steps:

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

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

3. In the search results, click the down arrow for the selected role and select Copy Role.
4. In the Copy Options dialog box, select a copy option.
5. Click Copy Role.
6. On the Copy Role: Basic Information page, review and edit the Role Name, Role Code, Description, and Enable Role for Access from All IP Addresses values, as appropriate. Enable Role for Access from All IP Addresses appears only if location-based access is enabled.

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

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

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

Related Topics

- Guidelines for Copying HCM Roles

Edit Job and Abstract Roles

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

Edit the Role

Follow these steps:

1. On the Roles tab of the Security Console, search for and select your custom role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.

3. On the **Edit Role: Basic Information** page, you can edit the role name and description, but not the role code. If location-based access is enabled, then you can also manage the **Enable Role for Access from All IP Addresses** option.

4. Click **Next**.

### Manage Functional Security Privileges

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

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

1. Click **Add Function Security Policy**.

2. In the Add Function Security Policy dialog box, search for and select a privilege or role.

3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from the selected role to your custom role.

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

4. If you select a single privilege, then click **Add Privilege to Role**.

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

6. Repeat from step 2 for additional privileges.

7. Click **Next**.

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

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

### Manage Data Security Policies

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

### Add and Remove Inherited Roles

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

To remove a role:

1. Select the role in the table.

2. Click the **Delete** icon.

3. Click **OK** to close the confirmation message.

   - **Note:** The role that you’re removing must be inherited directly by the role that you’re editing. If the role is inherited indirectly, then you must edit its parent role.
To add a role:

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

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

7. Click **Next**.

**Provision the Role to Users**

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

**Review the Role**

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

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

The role is available immediately.

**Create Job and Abstract Roles from Scratch**

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

**Enter Basic Information**

Follow these steps:

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

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

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

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

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

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

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

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

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

Create Data Security Policies

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

Build the Role Hierarchy

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

To add a role:

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

Provision the Role

To provision the role to users, you must create a role mapping when the role exists. Don’t provision the role to users on the Security Console.
Review the Role

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

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

Your custom role is available immediately.

Copy and Edit Duty Roles

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

Copy a Duty Role

Follow these steps:

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

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

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

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

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

Edit the Copied Duty Role

Follow these steps:

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

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

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

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

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

4. Click OK to close the confirmation message.
5. Repeat from step 2 for additional privileges.
7. Click Next.

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

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

Manage Data Security Policies

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

Add and Remove Inherited Roles

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

To remove a role:

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

To add a role:

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

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

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

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

The role is available immediately.

Related Topics
- Guidelines for Copying HCM Roles

Role Optimization

Role Optimizer

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.

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
The following figure shows how roles can proliferate or have duplicate privileges over time making your role hierarchy less efficient.

Benefits of Optimization

By using the role optimizer, you can:

- Increase user productivity.
  
  You save time that you can perform other tasks.

- Reduce 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 following figure shows how the role optimizer can suggest more efficient role hierarchies.

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.

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

Role Optimization Report

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

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

You should run this report if you:

- Make changes to the predefined role hierarchy.
- Implement your own role hierarchy instead of the predefined role hierarchy.
Note: The process makes no changes to your role hierarchies.

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

Report Files

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

The following table describes the two files that appear when you run the Role Optimization report.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterAnalysis-Job-CSVs. zip</td>
<td>Contains one CSV file for every job role. Each CSV file contains the duty roles and privileges that make up the optimized job role hierarchy. The name of a CSV file identifies the job role hierarchy data that the file contains. For example, the ClustersforJob-AR_REVENUE_MANAGER_JOB_14240.csv file contains all of the role hierarchy data for the Accounts Receivables Revenue Manager job role.</td>
</tr>
<tr>
<td>Diagnostics. zip</td>
<td>Contains a log file that provides technical details about the analysis process. You can use this file for troubleshooting purposes.</td>
</tr>
</tbody>
</table>

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

- Privilege Clusters
- Cluster Details

Role Optimization Report Results

Privilege Clusters

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

Cluster Details

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

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

The following table provides descriptions of the fields that appear in 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>
</tbody>
</table>
FAQs on Configuring Roles in the Security Console

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

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
14 Certificates and Keys

Overview of Certificates

Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications. Use the Certificates page in the Security Console functional area to work with certificates in either of two formats, PGP and X.509.

For each format, a certificate consists of a public key and a private key. The Certificates page displays one record for each certificate. Each record reports these values:

- **Type**: For a PGP certificate, "Public Key" is the only type. For an X.509 certificate, the type is either "Self-Signed Certificate" or "Trusted Certificate" (one signed by a certificate authority).
- **Private Key**: A check mark indicates that the certificate's private key is present. For either certificate format, the private key is present for your own certificates (those you generate in the Security Console). The private key is absent when a certificate belongs to an external source and you import it through the Security Console.
- **Status**: For a PGP certificate, the only value is "Not Applicable." (A PGP certificate has no status.) For an X.509 certificate, the status is derived from the certificate.

Click the Actions menu to take an appropriate action for a certificate. Actions include:

- Generate PGP or X.509 certificates.
- Generate signing requests to transform X.509 certificates from self-signed to trusted.
- Export or import PGP or X.509 certificates.
- Delete certificates.

Types of Certificates

For a PGP or X.509 certificate, one operation creates both the public and private keys. From the Certificates page, select the Generate option. In a Generate page, select the certificate format, then enter values appropriate for the format.

For a PGP certificate, these values include:

- An alias (name) and passphrase to identify the certificate uniquely.
- The type of generated key: DSA or RSA.
- Key length: 512, 1024, or 2048.
- Encryption algorithm option for key generation: AES128, AES256

For an X.509 certificate, these values include:

- An alias (name) and private key password to identify the certificate uniquely.
- A common name, which is an element of the "distinguished name" for the certificate. The common name identifies the entity for which the certificate is being created, in its communications with other web entities. It must match the name of the entity presenting the certificate. The maximum length is 64 characters.
• Optionally, other identifying values: Organization, Organization Unit, Locality, State/Province, and Country. These are also elements of the distinguished name for the certificate, although the Security Console does not perform any validation on these values.

• An algorithm by which keys are generated, MD5 or SHA1.

• A key length.

• A validity period, in days. This period is preset to a value established on the General Administration page. You can enter a new value to override the preset value.

Sign a X.509 Certificate

You can generate a request for a certificate authority (CA) to sign a self-signed X.509 certificate, to make it a trusted certificate. (This process does not apply to PGP certificates.)

1. Select Generate Certificate Signing Request. This option is available in either of two menus:
   o One menu opens in the Certificates page, from the row for a self-signed X.509 certificate.
   o The other menu is the Actions menu in the details page for that certificate.

2. Provide the private key password for the certificate, then select a file location.

3. Save the request file. Its default name is [alias]_CSR.csr.

You are expected to follow a process established by your organization to forward the file to a CA. You would import the trusted certificate returned in response.

Import and Export X.509 Certificates

For an X.509 certificate, you import or export a complete certificate in a single operation.

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.

2. In either menu, select Export, then Certificate.

3. Select a location for the export file. By default, this file is called [alias].cer.

To import, use either of two procedures. Select the one appropriate for what you want to do:

• The first procedure replaces a self-signed certificate with a trusted version (one signed by a CA) of the same certificate. (A prerequisite is that you have received a response to a signing request.)
  a. In the Certificates page, locate the row for the self-signed certificate, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
  b. Enter the private key password for the certificate.
  c. Browse for and select the file returned by a CA in response to a signing request, and click the Import button. In the Certificates page, the type value for the certificate changes from self-signed to trusted.

• The second procedure imports a new X.509 certificate. You can import a .cer file, or you can import a keystore that contains one or more certificates.
  a. In the Certificates page, click the Import button. An Import page opens.
b. Select X.509, then choose whether you are importing a certificate or a keystore.

c. Enter identifying values, which depend on what you have chosen to import. In either case, enter an alias (which, if you are importing a .cer file, need not match its alias). For a keystore, you must also provide a keystore password and a private key password.

d. Browse for and select the import file.

e. Select Import and Close.

Import and Export PGP Certificates

For a PGP certificate, you export the public and private keys for a certificate in separate operations. You can import only public keys. (The assumption is that you will import keys from external sources, who will not provide their private keys to you.)

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Public Key or Private Key.
3. If you selected Private Key, provide its passphrase. (The public key does not require one.)
4. Select a location for the export file. By default, this file is called [alias]_pub.asc or [alias]_priv.asc.

To import a new PGP public key:

1. On the Certificates page, select the Import button.
2. In the Import page, select PGP and specify an alias (which need not match the alias of the file you are importing).
3. Browse for the public-key file, then select Import and Close.

The Certificates page displays a record for the imported certificate, with the Private Key cell unchecked.

Use a distinct import procedure if you need to replace the public key for a certificate you have already imported, and do not want to change the name of the certificate:

1. In the Certificates page, locate the row for the certificate whose public key you have imported, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
2. Browse for the public-key file, then select Import.

Delete Certificates

You can delete both PGP and X.509 certificates:

1. In the Certificates page, select the menu available in the row for the certificate you want to delete. Or, in the details page for that certificate, select the Actions menu.
2. In either menu, select Delete.
3. Respond to a warning message. If the certificate’s private key is present, you must enter the passphrase (for a PGP certificate) or private key password (for an X.509 certificate) as you respond to the warning. Either value would have been created as your organization generated the certificate.
15 Security in Oracle Financials

Security for Country-Specific Features

For new implementations, you must assign the country-specific duty roles to your enterprise job roles or users before you can use the features specific to these regions. You have to assign country-specific duty roles to fscm application and obi application stripe to view the country-specific reports on the Scheduled Processes page, and to open the Parameters page of the selected process.

This table describes the duty roles for each region:

<table>
<thead>
<tr>
<th>Region</th>
<th>Duty Role</th>
<th>Role Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe, the Middle East, and Africa (EMEA)</td>
<td>EMEA Financial Reporting</td>
<td>ORA_JE_EMEA_FINANCIAL_REPORTING_DUTY</td>
</tr>
<tr>
<td>Asia Pacific (APAC)</td>
<td>APAC Financial Reporting</td>
<td>ORA_JA_APAC_FINANCIAL_REPORTING_DUTY</td>
</tr>
<tr>
<td>Asia Pacific (APAC)</td>
<td>Enterprise Financial Data Export Management for China</td>
<td>ORA_JA_CN_ENTERPRISE_FINANCIAL_DATA_EXPORT_ONLY_FOR_CHINA_DUTY_OBI</td>
</tr>
<tr>
<td>Asia Pacific (APAC)</td>
<td>Golden Tax Management for China</td>
<td>ORA_JA_GOLDEN_TAX_MANAGEMENT_FOR_CHINA_DUTY_OBI</td>
</tr>
</tbody>
</table>

General Ledger

Overview of General Ledger Security

General ledger functions and data are secured through job roles, data access sets, and segment value security rules.

Functional Security

Functional security, which is what you can do, is managed using job roles. The following job roles are predefined for Oracle Fusion General Ledger:

- General Accounting Manager
- General Accountant
- Financial Analyst

Each job role includes direct privilege grants, as well as duty role assignments, to provide access to application functions that correspond to their responsibilities. For example, the General Accounting Manager role grants comprehensive access to all General Ledger functions to the general accounting manager, controller, and chief financial officer in your organization.
Data Security

Data security, which controls what action can be taken against which data, is managed using:

- Data access sets
- Segment value security rules

Data access sets can be defined to grant access to a ledger, ledger set, or specific primary balancing segment values associated with a ledger. You decide whether each data access set provides read-only access or read and write access to the ledger, ledger set, or specific primary balancing segment values, which typically represent your legal entities that belong to that ledger. Primary balancing segment values without a specific legal entity association can also be directly assigned to the ledger.

Segment value security rules control access to data that is tagged with the value set values associated with any segment in your chart of accounts.

Security Assignment

Use the Security Console to assign users roles (job roles, as well as roles created for segment value security rules or others). Use the Manage Data Access Set Data Access for Users task to assign users data access sets as the security context paired with their General Ledger job role assignments.

For more information about security assignments and managing data access for users, see the Securing Oracle ERP Cloud guide.

Related Topics

- Data Access

Overview of Data Access Set Security

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.

You can combine ledger and ledger set assignments in single data access sets if the ledgers share a common chart of accounts and calendar. If you have primary balancing segment values assigned to a legal entity within the ledger, then you can use data access sets to secure access to specific legal entities. You can also secure access to primary balancing segments assigned directly to the ledger.

When a ledger or ledger set is created, a data access set for that ledger or ledger set is automatically created, giving full read and write access to those ledgers. You can also manually create data access sets to give read and write access, or read-only access to entire ledgers or portions of the ledger represented as primary balancing segment values.
The following figure shows that a data access set consists of an access set type and an access level. The access set type can be set to full ledger or primary balancing segment value. The access level can be read only or read and write.

![Data Access Set Diagram](image)

The **Full Ledger** access set type provides access to the entire ledger or ledger set. This could be for read-only access or both read and write access to the entire ledger.

The **Primary Balancing Segment Value** access set type provides access to one or more primary balancing segment values for that ledger. This access set type security can be specified by parent or detail primary balancing segment values. The specified parent value and all its descendants, including middle level parents and detail values are secured. You can specify read only, read and write access, or combination of both, for different primary balancing segment values for different ledgers and ledger sets.

For more information about security assignments and managing data access for users, see the Securing Oracle ERP Cloud guide.

### Examples of Data Access Set Security

This example shows a data access set that secures access by using primary balancing segment values that correspond to legal entities.

**Scenario**

The following figure shows a data access set for the US Financial Services Ledger. The access set type is Primary Balancing Segment Value, with each primary balancing segment value representing different legal entities. Read-only access has been assigned to primary balancing segment value 131, which represents the Insurance legal entity. Read and write access has been assigned to primary balancing segment values 101 and 102, which represent the Banks and Capital legal entities.
For this data access set, the user can:

- View the journals, balances, and reports for primary balancing segment value 131 for the Insurance legal entity.
- Create journals and update balances, as well as view journals, balances, and reports for primary balancing segment value 101 and 102 for legal entities Banks and Capital.

**Note:** In financial reporting, the list of ledgers isn’t secured by data access sets when viewing a report in Preview mode. Users can view the names of ledgers they don’t have privileges to view. However, the data from a secured ledger doesn’t appear on the report.

For more information about security assignments and managing data access for users, see the Securing Oracle ERP Cloud guide.

## Segment Value Security

Set up segment value security rules on value sets to control access to parent or detail segment values for chart of accounts segments, also called flexfield segments. Segment value security rules restrict data entry, online inquiry, and reporting.

### Secured Value Sets

When you enable security on a value set, access to all values for that value set is denied. To control access to value set values, you enable security on the value set, create conditions, and then assign the conditions to roles. The roles should be created solely for the purpose of segment value security. The roles are then assigned to users.
If a value set is secured, every usage of that value set in a chart of accounts structure instance is secured. For example the same security applies if that value set is:

- Used for two or more segments in the same chart of accounts, such as the primary balancing and intercompany segments
- Shared across different segments of different charts of accounts

**Secured Segment Values**

Segment value security applies mainly when data is created or updated, and when account combinations are queried. When you have access to secured account values, you can view and use those secured values across all modules of the applications where there are references to accounting flexfields including:

- Transaction entry pages
- Balances and transactions inquiry pages
- Setup pages
- Reports

On setup pages, you can still view referenced account combinations with secured account values, even if you haven't been granted access to those secured values. However, if you try to update such references, you can't use those secured values. On reports, you can view balances for secured account values only if you have access to those secured values.

> **Note:** You can enforce segment value security for inquiries and reporting based on any hierarchy, even hierarchies that aren’t published to the reporting cube.

**Segment Value Security Implementation**

You implement segment value security using the Security Console and these pages: Manage Value Sets, Manage Chart of Accounts Structures, Publish Account Hierarchies.
The following figure shows the steps for defining and implementing security rules for segment values.

To define segment value security roles:

1. Create segment value security roles.
2. Enable security on the value set.
3. Create conditions for the rule.
4. Create policies to associate the conditions with the role.
5. Deploy the accounting flexfield.

>Note: You can enable security only on value sets with a type of Independent.
6. Publish the account hierarchies.
7. Assign the role to users.

Whenever you assign segment value security roles to a user, the rules from the user’s assigned roles can be applied together. All of the segment value security roles assigned to a user pertaining to a given value set are simultaneously applied when the user works with that value set. For example, one rule provides access to cost center 110 and another rule provides access to all cost centers. A user with both of these segment value security rules has access to all cost centers when working in a context where that value set matters.

Segment Value Security Conditions

When you create a condition, you specify an operator. The following table describes the operators that you can use.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal to</td>
<td>• Provides access to a specific detail or child value.</td>
</tr>
<tr>
<td></td>
<td>• Don’t use to provide access to a parent value.</td>
</tr>
<tr>
<td>Not equal to</td>
<td>• Provides access to all detail and child values, except the one that you specify.</td>
</tr>
<tr>
<td></td>
<td>• Don’t use to provide access to a parent value.</td>
</tr>
<tr>
<td>Between</td>
<td>• Provides access to a detail range of values.</td>
</tr>
<tr>
<td>Is descendant of</td>
<td>• Provides access to the parent value itself and all of its descendants including middle level parents and detail values.</td>
</tr>
<tr>
<td>Is last descendant of</td>
<td>• Provides access to the last descendants for example, the detail values of a parent value.</td>
</tr>
</tbody>
</table>

**Tip:** For the operators Is descendant of and Is last descendant of:
- Specify an account hierarchy (tree) and a tree version to use these operators.
- Understand that the security rule applies across all the tree versions of the specified hierarchy, as well as all hierarchies associated with the same value set of the specified hierarchy.

Example of Segment Value Security

You can set up segment value security rules on value sets to control access to parent or detail segment values for chart of accounts segments. Segment value security rules restrict data entry, online inquiry, and reporting. The following example describes why and how you might want to use segment value security.

Securing Values for the Cost Center and Account Segments

For this scenario, only certain users should have access to the Accounting cost center and the US Revenue account. To create a complete data security policy that restricts segment value access to those users:

1. Plan for the number of roles that represent the unique segment value security profiles for your users. For this scenario, you can create two roles, one for the cost center segment and one for the account segment.
2. Use the Security Console to create the roles. Append the text SVS-role to the role names so it’s clear the roles are solely for segment value security. For this scenario, you create roles Accounting Cost Center-SVS Role and US Revenue Account-SVS Role.
3. Use the Manage Segment Value Security Rules task to enable security on the cost center and account value sets associated with the chart of accounts.

4. Create a condition for each value set. For example, the condition for the Accounting cost center is that the cost center is equal to Accounting.

5. Create a policy to associate the conditions to the roles. For example, create a policy to assign the condition for the Accounting cost center to the role Accounting Cost Center-SVS Role.

6. Use the Security Console to assign the appropriate role to the appropriate user. For example, assign the role Accounting Cost Center-SVS Role to the users who should have access to the Accounting cost center.

Enable Security on a Chart of Accounts

This example demonstrates how to enable security on a chart of accounts to control access to specific segment values. The following table summarizes the key decisions for this scenario.

<table>
<thead>
<tr>
<th>Decisions to Consider</th>
<th>In This Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which segment in the chart of accounts must be restricted?</td>
<td>Cost center</td>
</tr>
</tbody>
</table>
| Which cost center values have to be granted to different users? | • Child values 110 to 120  
• Child value 310  
• Parent value 400 and all its children  
• All cost centers |
| What’s the name of the value set for the segment with the Cost Center label? | Cost Center Main |
| What’s the name of the user who can access cost centers 110 to 120? | Casey Brown |
| What’s the name of the tree for the accounting flexfield? | All Corporate Cost Centers |
| What version of the tree hierarchy does the condition apply to? | V5 |

Summary of the Tasks and Prerequisites

This example includes details of the following tasks you perform when defining and implementing segment value security.

1. Define roles for segment value security rules.
2. Enable segment value security for the value set.
3. Define the conditions.
4. Define the policies.
5. Deploy the accounting flexfield.
6. Publish the account hierarchies.
7. Assign segment value security roles to users.

Perform the following prerequisites before enabling security on a chart of accounts:

• To work with the Security Console, you need the IT Security Manager role assigned to your user setup.
• To work with value sets and profile options, you need the Financial Application Administrator role.
• Set the Enable Data Security Policies and User Membership Edit profile to Yes.

### Defining Roles for Segment Value Security Rules

To create a complete data security policy, create the roles first so that they’re available for assignment to the segment value security rules.

1. In the Tools work area, open the Security Console.
2. Perform the following steps four times to create four roles.
3. Click **Create Role**.
4. On the Create Role page, complete the fields as shown in this table, and then click **Next, Next, Next, Next, Save and Close**.
5. Click **OK** and complete the fields, as shown in this table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Role 1</th>
<th>Role 2</th>
<th>Role 3</th>
<th>Role 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Name</td>
<td>Cost Center 110-120 SVS Role</td>
<td>Cost Center 310 SVS Role</td>
<td>Cost Center 400 SVS Role</td>
<td>Cost Center All SVS Role</td>
</tr>
<tr>
<td>Role Code</td>
<td>CC_110_120_SVS_ROLE</td>
<td>CC_310_SVS_ROLE</td>
<td>CC_400_SVS_ROLE</td>
<td>CC_ALL_SVS_ROLE</td>
</tr>
<tr>
<td>Role Category</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Description</td>
<td>Access to cost centers 110 to 120.</td>
<td>Access to cost center 310.</td>
<td>Access to parent cost center 400 and all its children.</td>
<td>Access to all cost centers.</td>
</tr>
</tbody>
</table>
The following figure shows the Create Role page for the first role, which is Cost Center 110-120 SVS Role. The role code, role category, and description fields are complete.

Enabling Segment Value Security for the Value Set

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Financials
   - Functional Area: Financial Reporting Structures
   - Task: Manage Segment Value Security Rules

2. In the **Value Set Code** field, enter Cost Center Main and click **Search**.
3. In the Search Results section, click **Edit** to open the Edit Value Set page.
4. Select the **Security enabled** option.
5. In the **Data Security Resource Name** field, enter Secure_Main_Cost_Center_Values.
6. Click **Save**.
The following figure shows the Edit Value Set page for the Cost Center Main value set. Security is enabled and a data security resource name has been entered.

### Defining the Conditions

Use conditions to specify the segment values that require security.

Segment value security rules that provide access to all segment values, and segment value security rules that provide access to single nonparent segment values, don’t need a condition. Instead, you can define the policy to cover all values, and you can define a policy to cover a single nonparent segment value provided that you know the internal ID for that segment value. If you don’t know the internal ID, you can create a condition for that single segment value.

In this scenario, the internal ID for segment value 310 isn’t known, so the following steps create all of the conditions, except for the access to all cost centers, which the policy definition can cover.

1. Click [Edit Data Security](#) to open the Edit Data Security page.
2. On the Condition tab, click [Create](#) to open the Create Database Resource Condition window.
3. Enter CC 110 - 120 in the Name field.
4. Enter Cost Centers 110 to 120 in the Display Name field.
5. Accept the default value of All for the Match field.

Matching to All means that all of the condition rows apply simultaneously and all of them must be met in identifying the values.

Matching to Any means that any of the condition rows could apply. For example, if you create multiple condition rows, each of which on its own is an alternative scenario for identifying the values that apply, you would select Match to Any.
Because this example only has one condition row, the Match selection doesn't matter. If however, you define multiple condition rows for segment value security, you would have to select Match to Any, because a single account value can't satisfy multiple account value-based conditions.

6. Click **Add** in the Conditions section.
7. Select **VALUE** for the **Column Name** field.
8. Select **Between** for the **Operator** field.

> **Note:** You can select one of the following operators: Equal to, Not equal to, Between, Is descendant of, Is last descendant of.

9. Enter 110 in the first **Value** field and 120 in the second **Value** field.
The following figure shows the Create Database Resource Condition page for the condition named CC 110 - 120. The display name is Cost Centers 110 to 120, and one condition is defined. The condition has a column name of VALUE, an operator of Between, and the specified values are 110 and 120.

10. Click **Save**.
11. To create the next database resource condition for segment value 310, click **Create** on the Condition tab.
12. Enter CC 310 in the **Name** field.
13. Enter Cost Center 310 in the **Display Name** field.
14. Click **Add** in the Conditions section.
15. Select **VALUE** for the **Column Name** field.
16. Select **Equal to** for the **Operator** field.
17. In the **Value** field, enter 310.
The following figure shows the definition of the second condition.
The following figure shows the Create Database Resource Condition page for the condition named CC 310. The display name is Cost Center 310, and one condition is defined. The condition has a column name of VALUE, an operator of Equal to, and the specified value is 310.

18. Click **Save**.
19. To create the next database resource condition for parent value 400, click **Create** on the Condition tab.
20. Enter CC 400 in the **Name** field.
21. Enter Parent Cost Center 400 in the **Display Name** field.
22. In the Condition section, click **Add**.
23. Select VALUE for the **Column Name** field.
24. Select the **Tree Operators** option.
25. For the **Operator** field, select Is a last descendant of, which restricts access to the parent cost center 400 and all of its children, including intermediary parents.

**Note:** For the **Tree Operators** field, you can only select Is a last descendant of or Is a descendant of.

26. In the **Value** column, click the **Select Tree Node** icon to open the Select Tree Node window.
The following figure shows the Select Tree Node window. Values are required for the Tree Structure, Tree, and Active Tree Version fields. The window also includes these Tree Node options: Specify primary keys, Select from hierarchy.

27. In the Tree Structure field, select Accounting Flexfield Hierarchy. This signifies that you are choosing among trees that are used as accounting flexfield, or charts of accounts, hierarchies.
28. In the Tree field, select All Corporate Cost Centers.
29. In the Active Tree Version field, select V5.
30. In the Tree Node field, select the Select from hierarchy button. The Tree Node section opens.
31. In the Tree Node section, expand the nodes and select 400.
The following figure shows the Select Tree Node window after completing the fields in steps 27 through 31.

32. Click **OK**.
The following figure shows the resulting Create Database Resource Condition page for the condition named CC 400. The display name is Parent Cost Center 400 and one condition is defined. The condition has a column name of VALUE, an enabled Tree Operators option, an operator called Is a last descendant of, and a value of 400.

![Create Database Resource Condition](image)

33. Click **Save**.

### Defining the Policies

Create policies to assign conditions to segment value security roles.

1. On the Edit Data Security page, click the Policy tab.
2. Click **Create** to open the Create Policy window.
3. On the General Information tab, enter Policy for 110-120 in the **Name** field.
4. Accept the default value of General Ledger in the **Module** field.
5. Enter 9/1/16 in the **Start Date** field.
The following figure shows the General Information tab on the Create Policy page for the policy named Policy for 110-120. The start date for the policy is 9/1/16.

6. Select the Role tab and click **Add** to open the Select and Add window.
7. Enter 110 in the **Role Name** field.
8. Select hcm in the **Application** field.
   Roles with the Default category are created in the hcm application.
9. Click **Search**.

The following figure shows the Select and Add Roles window with the search results. The role retrieved by the search results is named Cost Center 110-120 SVS Role.

10. Select Cost Center 110-120 SVS Role and click **OK**.
The following figure shows the Role tab on the Create Policy page with the role that was populated by the search results.

11. Select the Rule tab.
12. Accept the default setting of Multiple Values in the Row Set field.

Note: The Row Set field determines the range of value set values affected by the policy.
   - If Multiple Values is selected, 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.
   - If Single Value is selected, then the internal Value ID for the segment value must be specified and no condition is needed.

13. Click Search on the Condition field.
14. Select Cost Centers 110 to 120 for the Condition field and click OK.

The following figure shows the Rule tab on the Create Policy page. The selected row set is Multiple Values and the condition is Cost Centers 110 to 120.

15. Click Save and Close.
16. Click OK to confirm.
17. Repeat steps 2 through 13 to create the rest of the policies, using the values in the following table.
Field | Policy 2 | Policy 3 | Policy 4
--- | --- | --- | ---
General Information tab, Name | Policy for 310 | Policy for 400 | Policy for all cost centers
General Information tab, Start Date | 9/1/16 | 9/1/16 | 9/1/16
Role tab, Role Name | Cost Center 310 SVS Role | Cost Center 400 SVS Role | Cost Center All SVS Role
Rule tab, Row Set | Multiple Values | Multiple Values | All Values
Rule tab, Condition | Cost Center 310 | Parent Cost Center 400 | Not Applicable

18. Click **Done**.

Deploying the Accounting Flexfield

You must deploy the accounting flexfield for the segment value security changes to take effect.

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Financials
   - Functional Area: Financial Reporting Structures
   - Task: Manage Chart of Accounts Structures
2. In the **Module** field, select General Ledger and click **Search**.
3. Select the row for the Accounting Flexfield and click **Deploy Flexfield**.

The following figure shows the Manage Chart of Accounts Structure page after searching for General Ledger modules. The search results display a row with a key flexfield named Accounting Flexfield.

4. Click **OK**.
Publishing the Account Hierarchies

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Financials
   - Functional Area: Financial Reporting Structures
   - Task: Publish Account Hierarchies

2. In the Hierarchy field, select All Corporate Cost Centers.
3. In the Hierarchy Version field, select V5.
4. Click Search.
5. In the Search Results section, expand the hierarchy row.
6. Select the row for the hierarchy version V5.
7. Click Publish.
8. Click OK.

Assigning Segment Value Security Roles to Users

1. In the Tools work area, open the Security Console.
2. Enter Cost Center 110-120 SVS Role in the Search field and click Search.
3. In the Search Results section, select the down arrow icon and select Edit Role.

The following figure shows the Roles page and the available menu options, including Edit Role, for the role named Cost Center 110-120 SVS Role.

4. Click Next four times to navigate to the Edit Role: Users page.
5. Click Add User.
6. Enter Casey in the Search field and click Search.
7. Click Add User to Role to add Casey Brown to the role.
8. Click OK to confirm.

The following figure shows the Edit Role page for the Cost Center 110-120 SVS Role with the user Casey Brown selected.

9. Repeat steps 2 through 8 to add the other roles to different users as needed.

Related Topics
• Update Existing Setup Data

Data Security Differences in GL Features Based on Balance Cubes

In certain cases, differences in data security can appear depending on whether the GL feature being used is directly or indirectly based on the balances cube. For example, this can occur when a user is assigned multiple data access sets for the same balances cube with different security specifications for ledger or primary balancing segment value access, or when segment value security rule assignments are involved.

General Ledger features based directly on the balances cube are:

• Inquire on Detail Balances
• Account Monitor
• Account Inspector
• Financial Reporting
• Smart View
• Allocations

All other General Ledger features are indirectly based on the balances cube.

When using features indirectly related to the balances cube, you select a specific data access set and you work only with that one data access set at a time. The defined ledger and primary balancing segment value access for the selected data access set are enforced.

When using features directly related to the balances cube, the cumulative effects of your combined data access sets for that balances cube are enforced. From your combined data access sets for that cube, balances cube security separately
constructs the access filter for the ledger dimension and primary balancing segment values dimension independently of the other dimensions. This means the specific combination of ledger and primary balancing segment values access as defined in each distinct data access set are not enforced as such. Instead, you have access simultaneously to all the ledgers and all the primary balancing segment values granted to you through your combined data access sets.

**Note:** Balances cube security grants access to all values of the balancing segment value set for a data access set defined as either of the following:

- Full ledger
- All Values: Specific Balancing Segment Values Access Type

With segment value security rules assigned to you through your various roles, the security rules are in effect simultaneously whether working directly or indirectly with the balances cube.

Segment value security rules are specified for a particular value set. Therefore, as you are working on anything that references the secured value set, all segment value security rules for that value set that are assigned to you through any of your roles are in effect at the same time, regardless of the specific role the rule was assigned to. In other words, segment value security rules are cumulative, or the union of all the segment value security rules you have assigned to you through your roles. If you have one role assigned to your user that only grants access to cost center 200, and another role that grants access to cost centers 300 through 500, then you have access to cost centers 200 and 300 through 500.

When using features indirectly based on the balances cube, such as journal entry pages, the primary balancing segment values you can access are based on the intersection of:

- Primary balancing segment values granted to you through your current selected data access set.
- All of your assigned segment value security rules pertaining to the primary balancing segment value set across all of your assigned segment value security roles.

So, if a balancing segment value is only granted in either of the selected data access set or a segment value security role, that balancing segment value isn’t available to you.

In contrast, for features directly based on the balances cube, your access is based on the cumulative union of:

- Primary balancing segment values granted to you through all your assigned data access sets related to the balances cube that you’re working with.
- Any segment value security rule grants to that primary balancing segment value set across all of your segment value security role assignments.

**Example**

This setup is used to more clearly and comprehensively illustrate the difference in how security works for features directly and indirectly related to the balances cube with respect to data access sets and segment value security, though this might not generally reflect a real-life example.

In this example, your job role is assigned two different data access sets for the Vision Corporation ledger. The Vision Corporation 01 data access set is assigned primary balancing segment value 01, and the Vision Corporation 02 data access set is assigned primary balancing segment value 02. You are also assigned segment value security roles SVS 01 and SVS 03.

The following table lists the job role, data access set, and primary balancing segment value assignments for this example.

<table>
<thead>
<tr>
<th>Job Role</th>
<th>Data Access Set</th>
<th>Primary Balancing Segment Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Accounting Manager</td>
<td>Vision Corporation 01</td>
<td>01</td>
</tr>
<tr>
<td>General Accounting Manager</td>
<td>Vision Corporation 02</td>
<td>02</td>
</tr>
</tbody>
</table>
The following table lists the primary balancing segment values that are assigned to you through the segment value security roles.

<table>
<thead>
<tr>
<th>Segment Value Security Role</th>
<th>Primary Balancing Segment Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVS 01</td>
<td>01</td>
</tr>
<tr>
<td>SVS 03</td>
<td>03</td>
</tr>
</tbody>
</table>

Select Vision Corporation 01 Data Access Set

For features indirectly based on the balances cube, you can access primary balancing segment value 01. This segment value represents the intersection of the Vision Corporation 01 data access set and the SVS 01 and SVS 03 segment value security roles.

Neither your selected data access set, nor your segment value security roles provide access to Company 02, and your selected data access set Vision Corporation 01 and your cumulative segment value security roles SVS01 and SVS03 only intersect on primary balancing segment value 01, and not on 03.

For features directly based on the balances cube, you can access primary balancing segments 01, 02, and 03. These segment values represent the union of your assigned data access sets and segment value security roles. With the balances cube, all data access sets assigned to you that are related to the balances cube you’re working with apply simultaneously, regardless of the data access set you selected to work with in the application.

Select Vision Corporation 02 Data Access Set

For features indirectly based on the balances cube, you can’t access any primary balancing segment value because none of the values from the Vision Corporation 02 data access set and SVS 01 and SVS 03 segment value security roles intersect.

For features directly based on the balances cube, you can access primary balancing segments 01, 02, and 03. These values represent the union of your assigned data access sets and segment value security roles.

FAQs for General Ledger

What happens when changes are made to an account hierarchy that's referenced in segment value security rules?

The tree is set from an active to a draft state. The rules referencing the account hierarchy become ineffective.

After making changes to your hierarchy, you can submit the Process Account Hierarchies process to automatically run the required steps for processing account hierarchies updates in one submission, including:

- Tree audit
- Tree activation
- Row flattening
- Column flattening
- Maintain value set
• Maintain account hierarchy
• Publish hierarchy

With a successful audit process, the hierarchy is set back to an active status. The rules referencing the account hierarchy go back to being effective using the updated hierarchy.

Run the row and column flattening processes for the updated hierarchy as the flexfield component in the application as well as other hierarchy processes rely on the flattened hierarchy data to come up with the list of values available to the user to properly secure the correct account values.

Run the Maintain Value Sets and Maintain Chart of Account Hierarchies processes, particularly for hierarchy changes to the primary balancing segment value set if such values are referenced in your primary balancing segment value based data access sets. These processes update the data that is required to regulate ledger and data access security by storing:

• Primary balancing segment values assigned to a ledger.
• Specific child balancing segment values assigned to a data access set through parent value assignments.

When does security take effect on chart of accounts value sets for balances cubes?
To enforce segment value security according to defined security policies, you must enable security on the value set before you publish the affected account hierarchies to the balances cube. Likewise, to stop enforcing segment value security for a previously secured value set, you must disable security on the value set and then republish the account hierarchies.

Once segment value security is enforced, you don’t have to republish account hierarchies if you define new security policies or modify existing policies for the secured value set, even if the security definition has hierarchical conditions that use parent values.

Note: If you change an account hierarchy that’s already published, you must republish to reflect the updated hierarchy in the balances cube. Use the Publish Account Hierarchy task to republish the tree version. Republishing the account hierarchy also ensures proper enforcement of security policies that are based on parent values included in the changed hierarchy.

How can I secure the data in GL balances cubes?
Use data access set and segment value security to secure dimension values such as ledger and chart of account values. For chart of accounts dimension values, security restricts the display of data associated with the secured values, but not the selection of the values themselves. For example, when submitting a report, you can select company value 100 in your report definition when selecting the Point of View, even if you weren’t granted access to that company value. However, you can’t see the data associated with company 100 in your report.

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.

You assign users to the appropriate security context, such as a business unit, for job roles using the Manage Data Access for Users page.
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
- Accounts Payable Invoice 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

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. This role provides the access to configure your accounting rules.

- For more information about available setup job roles, duty roles and privileges, see the Oracle Financial Security Reference Manual.
Security to Perform Transactional Tasks

To create and view subledger journal entries, you must have the necessary access to perform the tasks in the relevant subledger work areas. Predefined subledger job roles include the entitlement to create and view subledger journal entries for subledger transactions you are authorized to access.

Security for Accounting Transformations in Accounting Hub

Accounting transformations require both function and data security privileges.

Oracle Accounting Hub security for accounting transformations includes:

- Setup task security
  - Security to register source systems into Accounting Hub.
  - 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 source system with the Accounting Hub.

To register your external source system and configure accounting rules, the setup user must be provisioned with a role that includes the following duty roles:

- Application Implementation Consultant
- Accounting Hub Integration

- In the security reference implementation, the Financial Application Administrator job role hierarchy includes the Accounting Hub Administration Duty role. This role provides the access to integrate your external source systems with accounting transformations.

Security to Perform Transactional Tasks

To import transaction data for accounting and posting in general ledger, the user must be provisioned with a job role that is associated with the Accounting Hub Integration duty role.

- The Import Subledger Accounting Transactions privilege is assigned to the Accounting Hub Integration duty role. This role enables the user to submit the Import Subledger Accounting Transactions process. This process also creates accounting entries and posts them in the general ledger.

To create and view subledger journal entries as an independent task, you must have the access necessary to perform the tasks. These tasks can be opened from the Oracle General Ledger, Journals work area. You must have access to the work area, as well as all of 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 the entitlement to manage general accounting functions. This entitlement provides access to the general ledger, Journals work area.

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

- Accounting Hub Integration 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

For more information about available setup job roles, duty roles, and privileges, see the Oracle Financials Cloud Security Reference guide on the Oracle Help Center.

Related Topics
- Data Security

Cash Management

Considerations When You Create Accounts

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.

The Bank Account Model can explicitly grant account access to multiple business units, functions, and users. Consider the following when you set up bank accounts:

- Assign 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.
- Grant bank account security. Bank account security consists of bank account use security, bank account access security, and user and role security.

Account Use

Account Use refers to accounts created for:

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

Select the appropriate use or uses when creating an account in one or more of these applications.
Account Access

Payables and Receivables account access is secured by business unit. Before the bank account is ready for use by Payables or Receivables, you must:

1. Select the appropriate use for the application.
2. Grant access to one or more business units.

Note: You can only assign access to the business units that use the same ledger as the bank accounts owning the legal entity.

User and Role Security

You can 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. For Payables and Receivables, you must have the proper business unit assigned to access a bank account even if the secure bank account by users and roles is No. 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.

- You must assign the security duty role Cash Management Administration to the Cash Manager job role to provide access for setting up banks, branches, and accounts. You must have the assigned Manage Bank Account Security privilege to modify the User and Role Security.
- If you want to restrict the access to the Security tab, you must create a customized role and remove the privilege Manage Bank Account Security. For example, you would copy the Cash Management Administration duty role, rename it, and remove the privilege.

Assets

Assets Data Security Components

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
- Submit Fixed Assets Reports
Asset Book Security Context

After you have completed your Assets setup, you can assign job roles to users using the Security Console and then grant explicit data access for asset books using the Manage Data Access for Users task from the Setup and Maintenance work area.

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. The default book value must be set using the Default Book profile option. You set the value at the site, product, or user level. Usually, the default book is automatically entered in the Book field when you perform transactions and run reports. You can override the default value and enter another value from the list of values.

Related Topics

- Assets Profile Options

Payments

System Security Options: Critical Choices

You can implement application security options on the Manage System Security Options page as part of a complete security policy that’s 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.

Note: Credit card services are currently not available in Oracle Financials Cloud implementations.

Note: Before you can import credit cards into Expenses, you must enable encryption or tokenization of credit cards in Payments.

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

- Which security practices do you want to employ?
- 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?

In the Setup and Maintenance work area, use the following to set up application security options:

- Offering: Financials
- Functional Area: Payments
- Task: Manage System Security Options
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). PCI DSS 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.
- Create the master encryption key.
  - Rotate the master encryption key periodically.

Implementation Process of Master Encryption Key and Encryption
Before you can enable encryption for credit card or bank account data, you must automatically create a master encryption key. The master encryption key exists on the file system of Oracle Platform Security Services (OPSS). OPSS stores your master encryption key. The application uses your master encryption key to encrypt your sensitive data.

Automatic creation of the master encryption key ensures that it is created and stored in the proper location and with all necessary permissions.

Credit Card Tokenization
If you tokenize your credit card data, you are complying with PCI DSS requirements. PCI DSS requires companies to use payment applications that are PCI DSS compliant.

Tokenization is the process of replacing sensitive data, such as credit card data, with a unique number, or token, that isn’t considered sensitive. The process uses 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 mathematically reversed to derive the actual credit card number.

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

Credit Card Data Encryption
You can 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 Receivables and Oracle Collections are automatically encrypted. Encryption is based on the credit card encryption setting you specify on the Manage System Security Options page.

Note: If you bring card numbers into Payments through import, it’s 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.

Bank account encryption doesn’t affect internal bank account numbers. Internal bank accounts are set up in Oracle Cash Management. They are used as disbursement bank accounts in Oracle Payables and as remit-to bank accounts in Receivables.
Supplier, customer, and employee bank account numbers entered in Oracle applications are automatically encrypted. Encryption is 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, it’s 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.

The master encryption key is stored on OPSS. OPSS stores data in an encrypted format. The master encryption key can be rotated, or generated, which also encrypts subkeys, but doesn’t result in encrypting the bank account numbers again.

If your installation has an existing master encryption key, you can automatically generate a new one by clicking Rotate.

Note: To secure your payment instrument data, you’re advised to annually rotate the master encryption key or rotate it according to your company’s security policy.

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

Note: 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:

- OPSS
- Payments master encryption key
- Payments subkeys
- Sensitive data encryption and storage
The following figure illustrates the security architecture of the OPSS repository, the master encryption key, and the subkeys.

Credit Card and Bank Account Number Masking
Payments serves as a payment data repository for 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 bank account numbers.

On the Manage System Security Options page, you can mask credit card numbers and external bank account numbers. To do it, select the number of digits to mask and display. For example, a bank account number of XXXX012 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.

Enable Encryption of Sensitive Payment Information
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. To enable encryption, you must create a master encryption key. Oracle Platform Security Services is a repository that stores your master encryption key. The application uses your master encryption key to encrypt your sensitive data.

† Note: Before you can import credit cards into Expenses, you must enable encryption or tokenization of credit cards in Payments. If you are using credit card data anywhere other than Expenses, you must enable tokenization in Payments.
To secure your credit card or bank account data, complete these steps:

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Financials
   - Functional Area: Payments
   - Task: Manage System Security Options
2. On the Manage System Security Options page, click **Apply Quick Defaults**.
3. Select all the check boxes:
   - Automatically create wallet file and master encryption key
   - Encrypt credit card data
   - Encrypt bank account data
4. Click **Save and Close**.

---

**Business Intelligence**

**Overview of Financial Reporting Security**

Security for financial reporting uses Role Based Access Control, which has the following components:

- Users with roles.
- Roles that grant access to functions and data.
- Functions and data access that is determined by the combination of role.

> **Note:** Users can have any number of roles.

Data security, which controls what action can be taken against which data, can also be applied to financial reporting. Data security is managed using:

- Data Access Sets:
  - Are defined to grant access to a ledger, ledger set, or specific primary balancing segment values associated with a ledger.
  - Permit viewing of journals, balances, and reports.
- Segment Value Security Rules:
  - Are set up on value sets to control access to parent or detail segment value for chart of accounts segments.
  - Restrict data entry, online inquiry, and reporting.

> **Note:** For more information about security, see the Securing Oracle ERP Cloud guide.
Oracle Fusion Transactional Business Intelligence Security

Oracle Fusion Transactional Business Intelligence is a real-time, self-service reporting solution. All application users with appropriate roles can use Transactional Business Intelligence to create analyses that support decision making. In addition, business users can perform current-state analysis of their business applications using a variety of tools. These include Oracle Business Intelligence Enterprise Edition as the standard query and reporting tool, Oracle Business Intelligence Answers, and Oracle Business Intelligence Dashboard tools. This topic summarizes how access is secured to Transactional Business Intelligence subject areas, Business Intelligence Catalog folders, and Business Intelligence reports.

Subject Areas

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

The following table identifies the subject areas that predefined Financials job roles can access.

<table>
<thead>
<tr>
<th>Financials Job Role</th>
<th>Subject Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable Manager</td>
<td>All Payables</td>
</tr>
<tr>
<td>Accounts Payable Specialist</td>
<td>All Payables</td>
</tr>
<tr>
<td>Accounts Payable Supervisor</td>
<td>Payables Invoices - Installments Real Time, Payables Payments - Disbursements Real Time, Payables Payments - Payment History Real Time</td>
</tr>
<tr>
<td>Accounts Receivable Manager</td>
<td>All Receivables</td>
</tr>
<tr>
<td>Accounts Receivable Specialist</td>
<td>All Receivables</td>
</tr>
<tr>
<td>Asset Accounting Manager</td>
<td>All Fixed Assets</td>
</tr>
<tr>
<td>Budget Manager</td>
<td>Budgetary Control - Transactions Real Time</td>
</tr>
<tr>
<td>Cash Manager</td>
<td>All Cash Management</td>
</tr>
<tr>
<td>Expense Manager</td>
<td>All Expenses</td>
</tr>
<tr>
<td>Financial Analyst</td>
<td>All Financials</td>
</tr>
<tr>
<td>Financial Application Administrator</td>
<td>All Financials</td>
</tr>
<tr>
<td>Financial Integration Specialist</td>
<td>All Financials</td>
</tr>
</tbody>
</table>
Analyses fail if the user can’t access all subject areas in a report.

**Business Intelligence Catalog Folders**

Business Intelligence Catalog folders are functionally secured using the same duty roles that secure access to the subject areas.

The following table identifies the folders that predefined Financials job roles can access.

<table>
<thead>
<tr>
<th>Financials Job Role</th>
<th>Business Intelligence Catalog Folders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable Manager</td>
<td>Transactional Business Intelligence Payables</td>
</tr>
<tr>
<td>Accounts Payable Specialist</td>
<td>Transactional Business Intelligence Payables</td>
</tr>
<tr>
<td>Accounts Payable Supervisor</td>
<td>Transactional Business Intelligence Payables</td>
</tr>
<tr>
<td>Accounts Receivable Manager</td>
<td>Transactional Business Intelligence Receivables</td>
</tr>
<tr>
<td>Accounts Receivable Specialist</td>
<td>Transactional Business Intelligence Receivables</td>
</tr>
<tr>
<td>Asset Accountant</td>
<td>Transactional Business Intelligence Fixed Assets</td>
</tr>
<tr>
<td>Asset Accounting Manager</td>
<td>Transactional Business Intelligence Fixed Assets</td>
</tr>
<tr>
<td>Budget Manager</td>
<td>Transactional Business Intelligence Budgetary Control</td>
</tr>
<tr>
<td>Cash Manager</td>
<td>Transactional Business Intelligence Cash Management</td>
</tr>
</tbody>
</table>
Business Intelligence Reports

Analyses are secured based on the folders in which they’re stored. If you haven’t secured Business Intelligence reports using the report privileges, then they’re secured at the folder level by default. You can set permissions against folders and reports for Application Roles, Catalog Groups, or Users.

You can set permissions to:

- Read, Execute, Write, or Delete
- Change Permissions
- Set Ownership
- Run Publisher Report
- Schedule Publisher Report
- View Publisher Output

How Reporting Data Is Secured

The data that’s returned in Oracle Transactional Business Intelligence reports is secured in a similar way to the data that’s returned in application pages. Data access is granted by roles that are linked to security profiles. This topic describes the part played by Transaction Analysis Duty Roles in securing access to data in Transactional Business Intelligence reports. It also describes how to enable this access in custom job roles.

Transaction Analysis Duty Roles

Each of the Transaction Analysis Duty roles providing access to subject areas and Business Intelligence Catalog folders is granted one or more data security policies. These policies enable access to the data.
Custom Job Roles

If you create a custom job role with access to Transactional Business Intelligence reports, then you must give the role the correct duty roles. Your custom role must have both the OBI and Financials versions of the Transaction Analysis Duty roles. These duty roles ensure that your custom job role has the function and data security for running the reports.

For example, if your role must access the Fixed Asset Transaction Analysis subject areas, then it must inherit the duty roles described in the following table:

<table>
<thead>
<tr>
<th>Duty Role</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed Asset Transaction Analysis Duty</td>
<td>OBI</td>
</tr>
<tr>
<td>Fixed Asset Transaction Analysis</td>
<td>Financials</td>
</tr>
</tbody>
</table>

The Fixed Asset Transaction Analysis Duty role is granted relevant data security policies and inherits Business Intelligence Consumer Role.

Business Intelligence Roles: Explained

Oracle Business Intelligence roles apply to both Oracle Business Intelligence Publisher and Oracle Fusion Transactional Business Intelligence. They grant access to Business Intelligence functionality, such as the ability to run or author reports. These roles are in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and Financials data. This topic describes the Business Intelligence roles.

This table lists the Business Intelligence roles.

<table>
<thead>
<tr>
<th>Business Intelligence Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Intelligence Consumer Role</td>
<td>Allows reporting from Business Intelligence Applications, Business Intelligence Publisher, Real Time Decisions, Enterprise Performance Management and Business Intelligence Office. This role allow you to run reports from the web catalog but it will not allow a report to be authored from a subject area.</td>
</tr>
<tr>
<td>Business Intelligence Authoring</td>
<td>Allows authoring within Business Intelligence Applications, Business Intelligence Publisher, Real Time Decisions, Enterprise Performance Management and Business Intelligence Office.</td>
</tr>
<tr>
<td>Business Intelligence Applications Analysis Management</td>
<td>Performs Business Intelligence Applications Analysis generic duty.</td>
</tr>
<tr>
<td>Fixed Asset Business Intelligence Management</td>
<td>Manages access to Fixed Assets OBIA Dashboard.</td>
</tr>
<tr>
<td>Business Intelligence Applications Administrator</td>
<td>Provides access to the BI Applications Configuration Manager and to the BI Data Warehouse Administration Console.</td>
</tr>
</tbody>
</table>
Delivered Roles for Financials Subject Areas

Access to subject areas in the Oracle Business Intelligence Catalog is secured by OTBI Transactional Analysis Duty roles. The following table lists subject areas and the corresponding job role and OTBI Transactional Analysis duty role that are required for creating user-defined reports using the subject areas. The OTBI Transactional Analysis duty role is inherited by the job role. Use this table to verify that your users have the job roles necessary to create reports using subject areas.

**Note:** The Business Intelligence Consumer role allows users to view reports, but not create new ones. All other job roles inherit the Business Intelligence Author role, enabling users with those job roles to create new reports. The following table lists subject areas for Financials and the default security roles needed for each one.

<table>
<thead>
<tr>
<th>Subject Areas</th>
<th>Job Role</th>
<th>OTBI Transactional Analysis Duty Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budgetary Control - Transactions Real Time</td>
<td>Budget Manager</td>
<td>Budgetary Control Analysis Duty</td>
</tr>
<tr>
<td>Cash Management - Bank Statement Balances Real Time</td>
<td>Cash Manager</td>
<td>Cash Management Transaction Analysis Duty</td>
</tr>
<tr>
<td>Cash Management - Bank Statement Line Charges Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Management - Bank Statements Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Management - External Cash Transactions Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expenses - Employee Expense Overview Real Time</td>
<td>Expense Manager</td>
<td>Expenses Summary Transaction Analysis Duty</td>
</tr>
<tr>
<td>Expenses - Expense Transactions Real Time</td>
<td></td>
<td>Expense Transactions Transaction Analysis Duty</td>
</tr>
<tr>
<td>Financials Common Module - Intercompany Transactions Real Time</td>
<td>Intercompany Accountant, General Accountant</td>
<td>Inter Company Transaction Analysis Duty</td>
</tr>
<tr>
<td>Fixed Assets - Asset Assignments Real Time</td>
<td>Asset Accountant</td>
<td>Fixed Asset Transaction Analysis Duty</td>
</tr>
<tr>
<td>Fixed Assets - Asset Balances Real Time</td>
<td></td>
<td>Fixed Asset Details Transaction Analysis Duty</td>
</tr>
<tr>
<td>Fixed Assets - Asset Depreciation Real Time</td>
<td></td>
<td>Fixed Depreciation Transaction Analysis Duty</td>
</tr>
<tr>
<td>Fixed Assets - Asset Financial Information Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Assets - Asset Retirements and Reinstatements Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Assets - Asset Source Lines Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Assets - Asset Transactions Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Assets - Asset Transfer Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Ledger - Balances Real Time, General Ledger - Journals Real Time</td>
<td>General Accountant</td>
<td>General Ledger Transaction Analysis Duty</td>
</tr>
<tr>
<td>Subject Areas</td>
<td>Job Role</td>
<td>OTBI Transactional Analysis Duty Role</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• General Ledger - Period Status Real Time</td>
<td>• Payables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• General Ledger - Transactional Balances Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Payables Invoices - Installments Real Time</td>
<td>• Accounts Payable Manager</td>
<td>• Payables to Ledger Reconciliation Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Payables Invoices - Prepayment Applications Real Time</td>
<td>• Accounts Payable Specialist</td>
<td>• Payables Invoice Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Payables Invoices - Transactions Real Time</td>
<td>• General Accountant</td>
<td>• Payables Payment Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Payables Invoices - Trial Balance Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Payables Invoices - Withholding Real Time</td>
<td>• Payables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Payables Payments - Disbursements Real Time</td>
<td>• Payables Invoice Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Payables Payments - Payment History Real Time</td>
<td>• Payables Payment Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Adjustments Real Time</td>
<td>• Accounts Receivable Manager</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Receivables - Bills Receivable Real Time</td>
<td>• Accounts Receivable Specialist</td>
<td>• Receivables Customer Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Receivables - Credit Memo Applications Real Time</td>
<td>• General Accountant</td>
<td>• Receivables Transaction Analysis Duty</td>
</tr>
<tr>
<td>• Receivables - Credit Memo Requests Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Customer Account Site Tax Profile Real Time</td>
<td>• Receivables Receipts Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Customer Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Customer Tax Profile Real Time</td>
<td>• Receivables Receipts Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Miscellaneous Receipts Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Payment Schedules Real Time</td>
<td>• Receivables Receipts Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Receipt Conversion Rate Adjustments Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Receipts Details Real Time</td>
<td>• Receivables Receipts Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Revenue Adjustments Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Standard Receipts Application Details Real Time</td>
<td>• Receivables Receipts Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>• Receivables - Transactions Real Time</td>
<td>• Receivables to Ledger Reconciliation Transaction Analysis Duty</td>
<td></td>
</tr>
</tbody>
</table>

- Subledger Accounting - Journals Real Time
- Subledger Accounting - Payables Summary Reconciliation Real Time
- Subledger Accounting - Receivables Summary Reconciliation Real Time
- Subledger Accounting - Supporting References Real Time
- Cash Manager
- Accounts Payable Manager
- Accounts Receivable Manager
- Asset Accountant
- Subledger Accounting Transaction Analysis Duty
Reporting Roles and Permissions

Viewing reporting roles and permissions can help you to understand how Oracle Transactional Business Intelligence security works.

This topic explains how to view:

- The reporting roles that a job role inherits
- The permissions for sample Oracle Transactional Business Intelligence reports in the Business Intelligence Catalog

Viewing Inherited Reporting Roles on the Security Console

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

2. On the Security Console, search for and select a job role. For example, search for and select the Accounts Payable Manager job role.

   Depending on the enterprise setting, either a graphical or a tabular representation of the role appears. Switch to the tabular view if it doesn’t appear by default.

3. Accounts Payable Manager inherits many duty roles, such as Payables Balance Analysis and Payables Invoice Processing. These roles (without the word Duty in their names) are Financials roles. Their role codes start with the characters ORA_. Find these roles in the table.

4. Notice also the many Transaction Analysis Duty roles (with the word Duty in their names) that appear at the console. For example, Accounts Payable Manager inherits the Transactional Analysis Duty. These roles are OBI roles. Their role codes start with the characters FBI_. Find these roles in the table.

5. Notice that the Payables Invoice Transaction Analysis Duty role inherits BI Consumer Role. Most of the OBI duty roles inherit BI Consumer Role.

   Tip: You can export the role hierarchy to a spreadsheet for offline review.

Viewing Permissions in the Business Intelligence Catalog

To view these permissions, you must have a role that inherits BI Administrator Role. None of the predefined Financials job roles inherits BI Administrator Role.

1. Select Navigator > Tools > Reports and Analytics to open the Reports and Analytics work area.
2. In the Contents pane, click the Browse Catalog icon. The Business Intelligence Catalog page opens.
3. In the Folders pane, expand Shared Folders.
   Expand the Financials folder and then the Bill Management folder.
4. Click the Customers Export Report folder.

   A list of reports appears on the BI Catalog page.

5. Click Costing Reports > More > Permissions.

   The Permissions dialog box opens. Scroll if necessary to see the complete list of permissions, which includes the role BI Administrator Role.
6. Click the Oracle Applications tab to return to the home page.
Configure Security for Oracle Transactional Business Intelligence

Oracle Transactional Business Intelligence secures reporting objects and data through a set of delivered Transaction Analysis Duty roles. You can't configure the Transaction Analysis Duty roles provided with Oracle Financials Cloud, or the associated security privileges. However, you can configure reporting security according to your security requirements as described in this topic.

Oracle Transactional Business Intelligence secures reporting objects and data through the following types of roles:

- Reporting objects and data are secured through the predefined OTBI Transactional Analysis Duty roles. The Transaction Analysis Duty roles control which subject areas and analyses a user can access and what data a user can see.

- Business Intelligence roles, for example, BI Consumer Role, or BI Author Role. These roles grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports and subject areas to create and run reports and view analytics.

You can't copy or modify the Business Intelligence roles or the Transaction Analysis Duty roles provided with Oracle Financials, or the associated security privileges. In addition, any role with a role code prefix of OBIA, for example, Business Intelligence Applications Analysis Duty (OBIA_ANALYSIS_GENERIC_DUTY), can also not be copied. However, you can configure reporting security according to your security requirements as described in this topic.

Modifying Transaction Analysis Duty Role Assignments

To configure the subject areas that users have access to create a custom job role and provide the role with the Oracle Transactional Business Intelligence duty roles that provide the required access.

For example, you can create a role that provides access to both general ledger and fixed assets subject areas by assigning both the General Ledger Transaction Analysis Duty and the Fixed Asset Transaction Analysis Duty to the role.

Modifying Business Intelligence Role Assignments

The Business Intelligence roles enable users to perform tasks within Business Intelligence tools such as Oracle Business Intelligence Publisher. The default Business Intelligence roles used in Oracle Financials Cloud are BI Consumer and BI Author.

The delivered Transaction Analysis Duty roles inherit the BI Consumer Role, which provides view-only access to analyses and reports. You assign the BI Author Role at the job role level, giving you flexibility in granting the BI Author privilege to only those job roles that you want to have access to create and edit analyses and reports.

All predefined Financials Cloud job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default. You can optionally create copies of the predefined job roles and add or remove the BI Author Role from the roles as required.

Business Intelligence Publisher Secured List Views

Oracle Business Intelligence Publisher is a set of tools for creating formatted reports based on data models. You can access Business Intelligence Publisher from Business Intelligence Composer or the Business Intelligence Catalog by clicking New > Report. This topic describes how you can use secured list views to secure access to data in Business Intelligence reports.
Some reporting tools combine the data model, layout, and translation in one report file. With that approach, business-intelligence administrators must maintain multiple copies of the same report to support minor changes. By contrast, Business Intelligence Publisher separates the data model, layout, and translation. Therefore, reports can be:

- Generated and consumed in many output formats, such as PDF and spreadsheet
- Scheduled for delivery to e-mail, printers, and so on
- Printed in multiple languages by adding translation files
- Scheduled for delivery to multiple recipients

Business Intelligence Publisher Data Security and Secured List Views

When you create a Business Intelligence Publisher data model with physical SQL, you have two options.

You can:

1. Select data directly from a database table, in which case the data you return isn’t subject to data-security restrictions. Because you can create data models on unsecured data, you’re recommended to minimize the number of users who can create data models.

2. Join to a secured list view in your select statements. The data returned is determined by the security profiles that are assigned to the roles of the user who’s running the report.
16 Security in Oracle Project Portfolio Management

Overview of Project Portfolio Management Security

Oracle Project Portfolio Management Cloud predefines common job roles such as Project Manager and Project Accountant. You can use these roles or create new ones if the predefined roles don’t fully represent your enterprise. For example, the predefined Project Manager role includes project budget management privileges. If some of your project managers don’t manage budgets, you can copy the predefined project manager role and remove the appropriate privileges to create a custom role. A user can have more than one role, so don’t define a role that includes all the accesses needed for every user.


The aspects of security that are discussed in this topic include:

- Securing common functionality
- Securing Project Financial Management and Grants Management applications
- Securing Project Execution Management applications

Securing Common Functionality

Common functionality that is not job-specific, such as creating time cards, expense reports, and purchase requisitions, are granted to the Employee abstract role that is automatically provisioned to each employee.

Oracle Project Portfolio Management Cloud provides the following roles that are designed for initial implementation and the ongoing management of setup and reference data:

- Application Implementation Manager: Manages implementation projects and assigns implementation tasks.
- Application Implementation Consultant: Accesses all setup tasks.
- Project Integration Specialist: Plans, coordinates, and supervises all activities related to the integration of project management information systems.
- Project Application Administrator: Accesses all Project Portfolio Management setup tasks for ongoing management of setup and reference data. Also, uses the Application Composer to extend the application.

Securing Project Financial Management and Grants Management Applications

Project Financial Management and Grants Management applications require both function and data security privileges.
You can secure access to data in one of the following ways:

- **Manage Projects in Organization Hierarchy**
  
  - Not part of seeded role, but can be used to extend the access to projects that belong to organizations in a hierarchy.
  
  - For example, Consulting West consists of organizations, Consulting South West and Consulting North West. A user assigned as administrator to Consulting West organization node is automatically able to access projects in Consulting West, Consulting South West, and Consulting North West.

- **Manage Data Access for Users**
  
  - **Explicit using Data Assignment Model Access**
    
    Data security is explicitly assigned to users through the Manage Data Access for Users page. User role assignment is done separately using the Security Console.
    
    For example, the user Abraham Mason with Project Accountant job role can be assigned access to costing data in the US business unit by selecting the appropriate security context of Business Unit and context value of US on Manage Data Access for Users page.
  
  - **Implicit Using Product-Specific Access**
    
    Data security is determined by product-specific logic.
    
    For Project Financial Management application, the role on the project determines the access to the project.
    
    For Grants Management application, the role on the award determines the access of a principal investigator to the award.
    
    For example, if you are assigned the Project Manager role on a project, you can edit budgets for that project.

You can be assigned data access in one of the following ways:

- During implementation, you can be assigned roles with appropriate data security assignment.
- During the project life cycle you can be assigned to one or more projects.

These data roles and project assignments authorize you to navigate, access, and perform business functions in work areas or dashboards.

The following table lists predefined job or abstract roles and the type of security that grants the role access to data in a work area or dashboard.

<table>
<thead>
<tr>
<th>Job or Abstract Role</th>
<th>Work Area or Dashboard</th>
<th>Data Security Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Accountant</td>
<td>Asset</td>
<td>Project business unit</td>
</tr>
<tr>
<td>Project Accountant</td>
<td>Costs</td>
<td>Project expenditure business unit</td>
</tr>
<tr>
<td>Project Accountant</td>
<td>Revenue</td>
<td>Contract business unit</td>
</tr>
<tr>
<td>Project Administrator</td>
<td>Project Financial Management</td>
<td>Project business unit Project organization</td>
</tr>
</tbody>
</table>
Securing Project Execution Management Applications

Project Execution Management applications use implicit, product-specific logic to authorize access to data in various business functions.

During the project life cycle you can be assigned to one or more projects or tasks. These assignments authorize you to navigate, access, and perform business functions in work areas or dashboards.

The following table lists predefined job or abstract roles and the type of security that grants access to data in a work area or dashboard.

<table>
<thead>
<tr>
<th>Job or Abstract Role</th>
<th>Work Area or Dashboard</th>
<th>Data Security Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Billing Specialist</td>
<td>Invoices</td>
<td>Contract business unit</td>
</tr>
<tr>
<td>Project Management Duty</td>
<td>Project Management Infolet Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Management Duty</td>
<td>Project Performance Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Project Management Infolet Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Project Performance Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Project Management</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Project Manager Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Team Member</td>
<td>Project Financial Management</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Grants Accountant</td>
<td>Invoices</td>
<td>Contract business unit</td>
</tr>
<tr>
<td>Grants Accountant</td>
<td>Revenue</td>
<td>Contract business unit</td>
</tr>
<tr>
<td>Grants Administrator</td>
<td>Awards</td>
<td>Contract business unit</td>
</tr>
<tr>
<td>Grants Administrator</td>
<td>Contracts</td>
<td>Contract business unit</td>
</tr>
<tr>
<td>Grants Administrator</td>
<td>Project Financial Management</td>
<td>Project business unit</td>
</tr>
<tr>
<td>Principal Investigator</td>
<td>Awards</td>
<td>Award assignment</td>
</tr>
<tr>
<td>Principal Investigator</td>
<td>Contracts</td>
<td>Award assignment</td>
</tr>
<tr>
<td>Principal Investigator</td>
<td>Project Financial Management</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Job Role or Abstract Role</td>
<td>Work Area or Dashboard</td>
<td>Data Security Based On</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Project Execution</td>
<td>Project Management</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Execution</td>
<td>Project Management Infolet Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Execution</td>
<td>Project Manager Dashboard</td>
<td>Project assignment</td>
</tr>
<tr>
<td>Project Execution</td>
<td>Requirements</td>
<td>No data security required</td>
</tr>
<tr>
<td>Project Execution</td>
<td>My Work - Tasks</td>
<td>Task assignment or task follower</td>
</tr>
<tr>
<td>Project Execution</td>
<td>My Work - Change Orders</td>
<td>Change order role</td>
</tr>
<tr>
<td>Project Execution</td>
<td>My Work - Deliverables and Issues</td>
<td>No data security required</td>
</tr>
<tr>
<td>Team Collaborator</td>
<td>My Work - Tasks</td>
<td>Task assignment or task follower</td>
</tr>
<tr>
<td>Team Collaborator</td>
<td>My Work - Change Orders</td>
<td>Change order role</td>
</tr>
<tr>
<td>Team Collaborator</td>
<td>My Work - Deliverables and Issues</td>
<td>No data security required</td>
</tr>
<tr>
<td>Team Collaborator</td>
<td>Team Member Dashboard</td>
<td>Task assignment</td>
</tr>
<tr>
<td>Project Executive</td>
<td>Project Hierarchy</td>
<td>Project hierarchy element assignment</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>Project Resources</td>
<td>No data security required</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>Resource Manager Dashboard</td>
<td>No data security required</td>
</tr>
</tbody>
</table>

**Note:** If you change a to do task to a project task, security is based on project assignment.

---

**Job or Abstract Roles Mapping to Project Roles**

When you assign a project role to a project team member, the associated job or abstract role determines the operations, such as viewing or managing, that the team member can perform in pages and task flows. Each project role is associated with an job or abstract role.

If the predefined security reference implementation doesn’t fully represent your enterprise, then you can make changes. For example, your enterprise may require additional roles with specific constraints on accessing application functions.
Rather than create a role from scratch, you can copy a role, then edit the copy to create a new role.

1. Use the Security Console to:
   - Copy an existing job or abstract role
   - Modify the function security policies
   - Modify the data security policies
   - Modify the role hierarchy

2. Then use the Manage Project Roles page to associate the new job or abstract role with a project role.

Tip: Never edit the predefined roles. Instead, either copy the predefined roles and edit the copies, or create custom roles from scratch. You can perform both tasks on the Security Console.

Example: Project Manager Role in Project Financial Management
For example, the predefined Project Manager role in Project Financial Management includes project budget management privileges. If some of your project managers don’t manage budgets:

1. In the Security Console:
   - Copy the role that is the closest to the role that you want to create, such as the Project Management Duty role. Give the role a unique name, such as Junior Project Manager.
   - Edit the functional policies to remove budget management.
   - Edit the data security policies to remove any policy that refers to budget management.
   - Save the role to create the new security grants.

2. On the Manage Project Roles page, create a Junior Project Manager project role and map it to the new Junior Project Manager job or abstract role.

Now any person who is added to the project as a Junior Project Manager can perform the functions based on the duties under the new job or abstract role.

Project Execution Management

Overview of Provisioning Access to Project Execution Management Applications

Use the Manage Project User Provisioning page to request user accounts and assign job or abstract 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 job or abstract 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.

Note: 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 the identity management system, and assign project-related job or abstract 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 job or abstract 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.

Job or Abstract Roles

You can provision the following predefined job or abstract 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.

- **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.

- **Project Executive**: Establishes key performance indicators and other project performance criteria for a business area or organization. Manages business area performance. Owns profit and loss results for an organization, service line, or region.

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 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 Project Management
- Maintain Project Enterprise Labor Resources process in Project Resource Management

Go to the Manage Project User Provisioning page > Default Provisioning Attributes tab > Default Role Assignments section to select the default roles. Then select the option to Automatically provision roles when mass creating project enterprise labor resources.

Project User Account and Role Provisioning Statuses

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 the identity management system. |

Role Provisioning Statuses

When you create a user account in Oracle Fusion Project Management and assign project job or abstract roles to the resource, the application sends a provisioning request to the identity management system. The role provisioning status indicates the processing status of the request. The following table lists the role provisioning statuses.
Role Provisioning Status | Description
--- | ---
Requested | Role provisioning is requested for a resource.
Completed | Role provisioning completed without errors or warnings.
Failed | Role provisioning failed because of errors or warnings.
Partially completed | Role provisioning is partially complete.
Pending | Role provisioning is in progress.
Provisioned | The role is provisioned in the identity management system.
Rejected | The role provisioning request is rejected by the identity management system.
Suppressed | Status used in HCM for user accounts aren’t created automatically.

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

### Provision Project Resources from the Manage Project User Provisioning Page

Use the Manage Project User Provisioning page to create and update project users, request user accounts, and assign job or abstract 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. Navigate to the Setup and Maintenance work area and search for the Manage Project User Provisioning task.
2. On the Search page, click the Manage Project User Provisioning link to open the Manage Project User Provisioning page > User Provisioning tab.
3. Click the Create icon to open the Create Project User window.
4. 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.
5. 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.
6. Add predefined or custom roles to the Role Details table, as needed. The following table lists the predefined roles.
### Role Description

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Application Administrator</strong></td>
<td>Collaborates with project application users to maintain consistent project application configuration, rules, and access.</td>
</tr>
<tr>
<td><strong>Project Execution</strong></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><strong>Resource Manager</strong></td>
<td>Performs functions in Oracle Fusion Project Resource Management.</td>
</tr>
<tr>
<td><strong>Team Collaborator</strong></td>
<td>Performs, tracks, and reports progress on project and nonproject work. Manages issues, deliverables, changes, and the calendar.</td>
</tr>
<tr>
<td><strong>Project Executive</strong></td>
<td>Establishes key performance indicators and other project performance criteria for a business area or organization. Manages business area performance. Owns profit and loss results for an organization, service line, or region.</td>
</tr>
</tbody>
</table>

**Tip:** 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.

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

This action:
- Sends a request for a user account to the identity management system
- 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.
Provision Project Resources from the Manage Project Enterprise Resources Page

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

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.

Following are examples of predefined project roles that you can’t edit or delete:

• Project manager
• Team member
• Staffing owner

You can create additional project roles to meet the needs of your organization. However, you can’t delete a project role that’s designated as a resource's primary project role, specified on a project resource request, or assigned to a resource on a project.

Use project roles 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
• To allow access to project management information for project managers
• To identify the default staffing owner of project resource requests for a project
Project Assignments
You select a project role when you add a resource to a project. The primary project role for a project enterprise resource is the default project role when you add the resource to the Manage Project Resources page.

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 assignment before you submit the assignment for approval.

Default Resource Qualifications
On the Manage Project Roles page, select a set of default qualifications, proficiency, and keywords for each project role. Default qualifications, proficiency, 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 the resource’s primary project role to focus the results.

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:

- 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
- When sorting 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 project management or resource management pages, you must be a project enterprise labor resource with an active user account. In addition, you must have a job or abstract role with the security privilege to access specific pages in Project Execution Management applications.

For more information, refer to the Securing Project Execution Management Applications section in the Implementing Project Portfolio Management Security: Overview topic.

Project Financial Management

Security Privileges for Budgets and Forecasts
Budget and forecast security is determined by a combination of project role, security roles (job and duty roles) and privileges, and workflow setup.

The following sections describe the privileges required to perform various steps in the budget creation, submission, and approval process. They also describe the impact of using workflow to manage status changes.

> Note: The privileges and workflow setup for forecasting mirrors that for budgeting.

Creating and Submitting a Budget Version
The following table describes the access required to create and submit a budget version.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access budget versions for a project</td>
<td>Manage Project Budget</td>
</tr>
<tr>
<td>2</td>
<td>Create a budget version</td>
<td>Create Project Budget</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The privilege required for editing budget versions in Excel is Manage Project Budget Excel Integration.</td>
</tr>
<tr>
<td>3</td>
<td>Submit working version</td>
<td>Manage Project Budget Working Version</td>
</tr>
<tr>
<td>4</td>
<td>Create baseline directly</td>
<td>Create Baseline Version Data</td>
</tr>
</tbody>
</table>
As a project application administrator, you can configure the financial plan approval rules to support integration with other Oracle cloud services. For example, you can add workflow rules to validate that the total budget amount does not exceed that of the strategic budget imported from the Enterprise Planning and Budgeting Cloud Service. The application auto-rejects the budget version if its total amount exceeds that of the Enterprise Planning and Budgeting Cloud Service (EPBCS) budget version with current baseline status.
This following figure describes the steps for creating and submitting a budget version for creation of a baseline.

Creating a Baseline for a Budget Version
The following table describes the access required to create a baseline for a budget version or reject it.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>If using workflow, receive notification of budget submission</td>
<td>NA (Approver e-mail ID is entered manually by users)</td>
</tr>
</tbody>
</table>
This following figure describes the steps for creating a baseline for a budget version.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Access budget versions for a project</td>
<td>Manage Project Budget</td>
</tr>
<tr>
<td>3</td>
<td>Create baseline or reject budget</td>
<td>Create Baseline Version Data</td>
</tr>
</tbody>
</table>
Reworking a Rejected Budget Version

The following table describes the access required to rework a rejected version (set it back to Working status) or delete it, if it is no longer required.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access budget versions for a project</td>
<td>Manage Project Budget</td>
</tr>
<tr>
<td>2</td>
<td>Rework working version</td>
<td>Manage Project Budget Working Version</td>
</tr>
<tr>
<td>3</td>
<td>Delete working version</td>
<td>Manage Project Budget Working Version</td>
</tr>
</tbody>
</table>
The following figure describes the steps for reworking a rejected budget version.

```
Rejected Version

Privilege
Manage Project
Budget available?

No
No access to project budgets

Yes

Privileges
Manage Project Budget
Working Version, Create Baseline Version
Data available?

Yes

Delete version

Rework version

Working Version

Submit version

Deleted Version

End
```

**Related Topics**

- Workflow of Budget and Forecast Approvals

**Project Roles in Budgeting and Forecasting**

Default project roles, including project application administrator, project manager, and project administrator can perform specific budgeting and forecasting tasks.
### Default Access for Roles

The following table describes the default access for each role.

<table>
<thead>
<tr>
<th>Privilege Area</th>
<th>Project Application Administrator</th>
<th>Project Manager</th>
<th>Project Administrator</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit budget and forecast planning options</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Project application administrators set planning options for financial plan types. Project managers and accountants can view planning options at the version level.</td>
</tr>
<tr>
<td>Create versions</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Generate versions</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Applies to budgets generated when setting a baseline for the project plan. Project administrators can’t generate forecasts from progress (they don’t have access to publish progress.)</td>
</tr>
<tr>
<td>Edit versions in Excel</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Submit versions</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Approve versions</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>A team member with project manager security role access must be manually designated as the project manager for the project. If workflow is enabled, then approval occurs through a notification. Menu actions aren’t available on the budgeting and forecasting pages.</td>
</tr>
<tr>
<td>Review versions</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>
FAQs for Project Roles

What's a project role?
Project roles represent either a requirement or an assignment on a project, such as a project manager or project team member.

You associate an job or abstract role with each project role. When you assign a project role to a project team member, the associated job or abstract role determines the type of access the team member has to project information. For example, project managers can manage project progress or create budgets and forecasts. Project team members may only have access to view progress or financial plans.

When you create a project role, you assign it to one or more reference data sets so that only project roles that are relevant to the project unit are available to assign to project team members.

Persons who are directly assigned job or abstract roles such as Project Manager or Project Application Administrator may have access to certain project information even if they aren’t project team members or don’t have a specific project role assignment.

What's the difference between a job title and a project role?
A job title represents the function of a person within an organization and the position within a reporting hierarchy. For example, your organization may have designations or job titles such as software developer, sales representative, or accounts manager.

Project roles represent either a requirement or an assignment on a particular project, for example, project manager. Project roles may differ from project to project.

Business Intelligence

Security for Subject Areas

Oracle Project Portfolio Management OTBI organizes reporting metadata into functional areas called subject areas. Subject areas contain folders that include metrics and attributes which are secured by the Oracle Business Intelligence Applications duty roles. Oracle Project Portfolio Management application job roles are mapped to these business intelligence application duty roles. This ensures that you see only the subject areas based on their business functions. For example, a project billing specialist sees only the Project Billing - Invoices Real Time subject area.

The following table lists the subject area and the corresponding Business Intelligence Applications duty role that is used to secure the subject area:

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Business Intelligence Applications Duty Role</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projects - Period Close Exceptions</td>
<td>Project Costing Transaction Analysis Duty</td>
<td>You must have access to the business unit or projects to view data for this subject area.</td>
</tr>
<tr>
<td></td>
<td>Grants Management Transaction Analysis Duty</td>
<td></td>
</tr>
<tr>
<td>Project Billing - Event Real Time</td>
<td>Project Contract Billing Event Transaction Analysis Duty</td>
<td>You must have business unit access to view the data for this subject area.</td>
</tr>
<tr>
<td>Subject Area</td>
<td>Business Intelligence Applications Duty Role</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Project Billing - Funding Real Time | Project Contract Invoice Transaction Analysis Duty  
Project Contract Revenue Transaction Analysis Duty | You must have business unit access to view the data for this subject area.                                                                                     |
| Project Billing - Invoices Real Time | Grants Management Transaction Analysis Duty  
Project Contract Invoice Transaction Analysis Duty | The folders Award, Primary Sponsor, and Institution within this subject area are visible only if you have access to the Grants Management Transaction Analysis Duty role.  
You must have business unit access to view the data for this subject area. |
| Project Billing - Revenue Real Time | Grants Management Transaction Analysis Duty  
Project Contract Revenue Transaction Analysis Duty | The folders Award, Primary Sponsor, and Institution within this subject area are visible only if you have access to the Grants Management Transaction Analysis Duty role.  
You must have business unit access to view the data for this subject area. |
| Project Control - Budgets Real Time | Grants Management Transaction Analysis Duty  
Project Budget Transaction Analysis Duty | The folders Award, Primary Sponsor, and Institution within this subject area are visible only if you have access to the Grants Management Transaction Analysis Duty role.  
You must have access to the business unit or projects to view data for this subject area. |
| Project Control - Forecasts Real Time | Project Forecast Transaction Analysis Duty | You must have access to the business unit or projects to view data for this subject area.                                                                 |
| Project Control - Progress Real Time | Project Progress Transaction Analysis Duty | You must have access to the business unit or projects to view data for this subject area.                                                                 |
| Project Costing - Actual Costs Real Time | Grants Management Transaction Analysis Duty  
Project Costing Transaction Analysis Duty  
Project Journals Transaction Analysis Duty | The folders Award, Primary Sponsor, and Institution within this subject area are visible only if you have access to the Grants Management Transaction Analysis Duty role.  
You must have access to the business unit or projects to view data for this subject area. |
| Project Costing - Assets Real Time | Project Costing Transaction Analysis Duty  
Project Journals Transaction Analysis Duty | You must have business unit access to view the data for this subject area.                                                                                     |
| Project Costing - Commitments Real Time | Grants Management Transaction Analysis Duty  
Project Costing Transaction Analysis Duty | The folders Award, Primary Sponsor, and Institution within this subject area are visible only if you have access to the Grants Management Transaction Analysis Duty role.  
You must have access to the business unit or projects to view data for this subject area. |
<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Business Intelligence Applications Duty Role</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Costing - Expenditure Item Performance Real Time</td>
<td>Project Costing Transaction Analysis Duty Project Journals Transaction Analysis Duty</td>
<td>You must have access to the business unit or projects to view data for this subject area.</td>
</tr>
<tr>
<td>Project Costing - Unprocessed Transactions Real Time</td>
<td>Grants Management Transaction Analysis Duty Project Costing Transaction Analysis Duty</td>
<td>You must have access to the business unit or projects to view data for this subject area.</td>
</tr>
<tr>
<td>Project Management - Opportunity Integration Real Time</td>
<td>Project Planning Transaction Analysis Duty</td>
<td>You can view the projects data for which you are the project manager on the Manage Project Resources page for the project.</td>
</tr>
<tr>
<td>Project Management - Planning Real Time</td>
<td>Project Planning Transaction Analysis Duty</td>
<td>You can view the projects data for which you are the project manager on the Manage Project Resources page for the project.</td>
</tr>
<tr>
<td>Project Management - Change Management Real Time</td>
<td>Project Change Management Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you are the creator or owner of the change order.</td>
</tr>
<tr>
<td>Project Management - Project Hierarchy Real Time</td>
<td>Project Hierarchy Transaction Analysis Duty</td>
<td>You can view all the data in this subject area for the projects connected to elements that you own or for which you can delegate rights.</td>
</tr>
<tr>
<td>Project Management - Project Resources Real Time</td>
<td>Project Planning Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you have access to the subject area.</td>
</tr>
<tr>
<td>Project Management - Project Work Items Real Time</td>
<td>Project Work Items Transaction Analysis Duty</td>
<td>You can view the projects data for which you are the project manager on the Manage Project Resources page for the project.</td>
</tr>
<tr>
<td>Project Management - Requirements Real Time</td>
<td>Project Requirements Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you have access to the subject area.</td>
</tr>
<tr>
<td>Project Management - Task Management Real Time</td>
<td>Task Management Transaction Analysis Duty</td>
<td>You can view data in this subject area if you are the owner or the creator of the tasks.</td>
</tr>
<tr>
<td>Project Resource Management - Resource Management Real Time</td>
<td>Project Resource Management Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you have access to the subject area.</td>
</tr>
<tr>
<td>Projects - Cross Subject Area Analysis Real Time</td>
<td>Project Budget Transaction Analysis Duty Project Contract Invoice Transaction Analysis Duty Project Contract Revenue Transaction Analysis Duty Project Costing Transaction Analysis Duty Project Foundation Transaction Analysis Duty</td>
<td>You must have access to the business unit or projects to view data for this subject area.</td>
</tr>
<tr>
<td>Subject Area</td>
<td>Business Intelligence Applications Duty Role</td>
<td>Additional Information</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Grants Management Transaction Analysis Duty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Projects - Grants Management - Award Analysis Real Time</td>
<td>Grants Management Transaction Analysis Duty</td>
<td>You must have access to the contract or award business unit, or awards to view data for this subject area.</td>
</tr>
<tr>
<td>Projects - Grants Management - Award Funding Real Time</td>
<td>Grants Management Funding Analysis Duty</td>
<td>You must have access to the contract or award business unit, or awards to view data for this subject area.</td>
</tr>
<tr>
<td>Project Management - Project Issues Real Time</td>
<td>Project Issue Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you have access to the subject area.</td>
</tr>
<tr>
<td>Project Resource Management - Resource Pool Real Time</td>
<td>Project Resource Management Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you have access to the subject area.</td>
</tr>
<tr>
<td>Project Management - Baseline Versions Real Time</td>
<td>Project Planning Transaction Analysis Duty</td>
<td>You can view the projects data for which you are the project manager on the Manage Project Resources page for the project.</td>
</tr>
<tr>
<td>Projects - Performance Reporting Real Time</td>
<td>Project Performance Reporting Transaction Analysis Duty</td>
<td>You can view all the data in this subject area if you have access to the subject area.</td>
</tr>
</tbody>
</table>

**Mapping Business Intelligence Duty Roles and Oracle Application Job Roles**

Oracle Project Portfolio Management application job roles inherit Oracle Transactional Business Intelligence application duty roles so that correct data is visible to relevant users. For example, project accountants can view project cost data for the expenditure organization that they’re responsible for.

The following table lists the Oracle Transactional Business Intelligence application duty roles and corresponding Oracle Project Portfolio Management application job roles that inherit these duties.

<table>
<thead>
<tr>
<th>Business Intelligence Application Duty Role</th>
<th>Oracle Application Job Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grants Management Funding Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td>Grants Management Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td>Business Intelligence Application Duty Role</td>
<td>Oracle Application Job Role</td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Project Budget Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
<tr>
<td>Project Change Management Transaction Analysis Duty</td>
<td>Project Execution</td>
</tr>
<tr>
<td></td>
<td>Team Collaborator</td>
</tr>
<tr>
<td>Project Contract Invoice Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Billing Specialist</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
<tr>
<td>Project Contract Revenue Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
<tr>
<td>Project Costing Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
<tr>
<td>Business Intelligence Application Duty Role</td>
<td>Oracle Application Job Role</td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Project Manager</td>
<td></td>
</tr>
<tr>
<td>Project Foundation Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td>Project Hierarchy Transaction Analysis Duty</td>
<td>Project Executive</td>
</tr>
<tr>
<td>Project Journals Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td>Project Planning Transaction Analysis Duty</td>
<td>Project Execution</td>
</tr>
<tr>
<td>Project Progress Transaction Analysis Duty</td>
<td>Grants Administrator</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
<tr>
<td></td>
<td>Team Collaborator</td>
</tr>
<tr>
<td>Project Requirements Transaction Analysis Duty</td>
<td>Project Manager</td>
</tr>
<tr>
<td>Project Resource Management Transaction Analysis Duty</td>
<td>Resource Manager</td>
</tr>
<tr>
<td>Project Work Items Transaction Analysis Duty</td>
<td>Project Execution</td>
</tr>
<tr>
<td>Task Management Transaction Analysis Duty</td>
<td>Team Collaborator</td>
</tr>
<tr>
<td>Project Contract Billing Event Transaction Analysis Duty</td>
<td>Grants Accountant</td>
</tr>
<tr>
<td></td>
<td>Grants Administrator</td>
</tr>
<tr>
<td>Business Intelligence Application Duty Role</td>
<td>Oracle Application Job Role</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>Grants Department Administrator</td>
</tr>
<tr>
<td></td>
<td>Principal Investigator</td>
</tr>
<tr>
<td></td>
<td>Project Accountant</td>
</tr>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Billing Specialist</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Issue Transaction Analysis Duty</th>
<th>Project Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Team Collaborator</td>
</tr>
<tr>
<td></td>
<td>Project Executive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Performance Reporting Transaction Analysis Duty</th>
<th>Project Accountant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Project Administrator</td>
</tr>
<tr>
<td></td>
<td>Project Manager</td>
</tr>
</tbody>
</table>

Set Up Security Profile to View Employee Names in Analyses

Use the Manage Data Role and Security Profiles task to gain access to employee names in your analysis. Following steps help you to get the required access.

Setting Up Security Profile

> Note: Only an application administrator can access the Manage Data Role and Security Profiles task.

1. Navigate to the Setup and Maintenance work area and click **Search**.
2. On the Search page, search for the Manage Data Role and Security Profiles task.
3. Click the **Manage Data Role and Security Profiles** link.
4. Search for the user role, such as project manager or project accountant, to grant the access.
5. In the Search Results region, select the role and click **Edit**.
6. Select **View All People** or **View All Workers** when prompted for a Public Person security profile.
7. Click **Review**.
8. Click **Submit**.

View Reporting Roles and Permissions

Viewing reporting roles and permissions can help you to understand how Oracle Transactional Business Intelligence security works.
This topic explains how to view:

- The reporting roles that a job role inherits
- The permissions for sample Oracle Transactional Business Intelligence reports in the Business Intelligence Catalog

### Viewing Inherited Reporting Roles on the Security Console

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

1. Select **Navigator > Tools > Security Console**.
2. On the Security Console, search for and select a job role. For example, search for and select the Project Manager job role.

   Depending on the enterprise setting, either a graphical or a tabular representation of the role appears. Switch to the tabular view if it doesn’t appear by default.

   Project Manager inherits many duty roles, such as Project Plan Management and Project Budget Management. These roles (without the word Duty in their names) are **Projects** roles. Their role codes start with the characters `ORA_`. Find these roles in the table.

   Notice also that Project Planning Transaction Analysis Duty roles (with the word Duty in their names) appear in the view. For example, Project Manager inherits the Project Management Duty. These roles are **OBI** roles. Their role codes start with the characters `FBI_`. Find these roles in the table.

   Notice that the Project Management Analysis duty role inherits BI Consumer Role. Most of the **OBI** duty roles inherit BI Consumer Role.

   **Tip:** You can export the role hierarchy to a spreadsheet for offline review.

### Viewing Permissions in the Business Intelligence Catalog

To view these permissions, you must have a role that inherits BI Administrator Role. None of the predefined Projects job roles inherits BI Administrator Role.

1. Select **Navigator > Tools > Reports and Analytics** to open the Reports and Analytics work area.
2. In the Contents pane, click the **Browse Catalog** icon. The Business Intelligence Catalog page opens.
3. In the Folders pane, expand `Shared Folders > Projects > Project Billing`. The reports are listed.
4. Select **Preview Invoice Report** and click **More > Permissions**.
5. View the permissions.

### Oracle Transactional Business Intelligence Security Configuration

Oracle Transactional Business Intelligence secures reporting objects and data through a set of delivered Transaction Analysis Duty roles. You can’t configure the Transaction Analysis Duty roles provided with Oracle Project Portfolio Management, or the associated security privileges. However, you can configure reporting security according to your security requirements as described in this topic.

### Modifying Transaction Analysis Duty Role Assignments

To configure the subject areas that users have access to create a custom job role and provide the role with the Oracle Transactional Business Intelligence duty roles that provide the required access.
For example, you can create a role that provides access to both Project Resource Management - Resource Pool Real Time and Project Management - Project Issues Real Time subject areas by assigning both the Project Resource Management Transaction Analysis Duty and Project Planning Transaction Analysis Duty to the role.

Modifying Business Intelligence Role Assignments

The Business Intelligence roles enable users to perform tasks within Business Intelligence tools such as Oracle Business Intelligence Publisher. The default Business Intelligence roles used in Oracle Project Portfolio Management are BI Consumer and BI Author.

The delivered Transaction Analysis Duty roles inherit the BI Consumer Role, which provides view-only access to analyses and reports. You assign the BI Author Role at the job role level, giving you flexibility in granting the BI Author privilege to only those job roles that you want to have access to create and edit analyses and reports.

All predefined Project Portfolio Management job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default. You can optionally create copies of the predefined job roles and add or remove the BI Author Role from the roles as required.

Business Intelligence Publisher Secured List Views

Oracle Business Intelligence Publisher is a set of tools for creating formatted reports based on data models. You can access Business Intelligence Publisher from Business Intelligence Composer or the Business Intelligence Catalog by clicking New > Report. This topic describes how you can use secured list views to secure access to data in Business Intelligence reports.

Some reporting tools combine the data model, layout, and translation in one report file. With that approach, business-intelligence administrators must maintain multiple copies of the same report to support minor changes. By contrast, Business Intelligence Publisher separates the data model, layout, and translation. Therefore, reports can be:

- Generated and consumed in many output formats, such as PDF and spreadsheet
- Scheduled for delivery to e-mail, printers, and so on
- Printed in multiple languages by adding translation files
- Scheduled for delivery to multiple recipients

Business Intelligence Publisher Data Security and Secured List Views

When you create a Business Intelligence Publisher data model with physical SQL, you have two options.

You can:

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

Oracle Procurement Cloud applications use the standard role-based security model. Predefined security roles are delivered for in the security reference implementation.

Some types of delivered roles are:

- Common job roles.
- Abstract roles, for common functionality that is not job-specific.
- Duty roles, that can carry both function and data security grants.
- Discretionary roles, are like duty roles but can be provisioned to users independent of job or abstract roles.

For each of the predefined roles, the included or inherited duties grant access to application functions that correspond to their responsibilities. In some areas of Procurement you must also grant data access directly to specific users. For example, you must directly set up users such as buyers, category managers and procurement managers as procurement agents.

Predefined Roles for Procurement

Predefined roles for Procurement are provided in the security reference implementation for these functional areas:

- Requisitioning
- Purchasing
- Supplier
- Supplier Portal
- Sourcing
- Supplier Qualification
- Setup and Administration
- Business Intelligence

The following table lists predefined requisitioning security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Procurement Requester</td>
<td>Abstract</td>
<td>Creates requests for goods or services for themselves and for others. Also has access to the Add Requisition Lines function which supports the quick creation of multiple requisition lines. This role must be directly assigned to a user.</td>
</tr>
<tr>
<td>Procurement Catalog Administrator</td>
<td>Abstract</td>
<td>Manages agreements and catalog content. This includes catalogs, category hierarchies, content zones, information templates, map sets, public shopping lists and smart forms.</td>
</tr>
</tbody>
</table>
## Security in Oracle Procurement

### The following table lists predefined purchasing security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement Preparer</td>
<td>Abstract</td>
<td>Creates requests for goods or services for themselves and for others. This role must be directly assigned to a user.</td>
</tr>
<tr>
<td>Procurement Requester</td>
<td>Abstract</td>
<td>Creates requests for goods or services for themselves. This role is inherited by users whose primary worker assignment is Employee or Contingent Worker.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buyer</td>
<td>Job</td>
<td>Performs transactional functions in procurement applications, such as for processing purchase agreements and purchase orders.</td>
</tr>
<tr>
<td>Category Manager</td>
<td>Job</td>
<td>Identifies savings opportunities. Determines negotiation strategies. Creates requests for quote, information, proposal or auction events on behalf of their organization. Awards future business, typically in the form of agreements and orders with suppliers.</td>
</tr>
<tr>
<td>Procurement Contracts Administrator</td>
<td>Job</td>
<td>Creates, manages and administers procurement contracts.</td>
</tr>
<tr>
<td>Procurement Manager</td>
<td>Job</td>
<td>Manages a group of buyers in an organization.</td>
</tr>
</tbody>
</table>

### The following table lists predefined buying organization supplier security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier Administrator</td>
<td>Abstract</td>
<td>Manages supplier information and user provisioning.</td>
</tr>
<tr>
<td>Supplier Manager</td>
<td>Abstract</td>
<td>Manages supplier information and authorizes promotion of prospective suppliers to spend authorized status.</td>
</tr>
</tbody>
</table>

### The following table lists predefined supplier portal security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier Accounts Receivable Specialist</td>
<td>Job</td>
<td>Submits invoices and tracks invoice and payment status for the supplier organization.</td>
</tr>
<tr>
<td>Role</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supplier Bidder</td>
<td>Abstract</td>
<td>Represents a potential supplier. Responds to requests for quote, proposal, information and reverse auctions.</td>
</tr>
<tr>
<td>Supplier Customer Service Representative</td>
<td>Job</td>
<td>Manages inbound purchase orders. Communicates shipment activities for the supplier organization. Tracks, acknowledges or requests changes to new orders. Monitors the receipt activities performed by the buying organization.</td>
</tr>
<tr>
<td>Supplier Demand Planner</td>
<td>Job</td>
<td>Manages supplier scheduling, supplier managed inventory, and consigned inventory for the supplier organization.</td>
</tr>
<tr>
<td>Supplier Inventory Manager</td>
<td>Job</td>
<td>Manages inventory process control from beginning to end. Monitors available supplies, materials and products to ensure that customers, employees and production have access to the materials they need.</td>
</tr>
<tr>
<td>Supplier Product Administrator</td>
<td>Job</td>
<td>Uses retail external portal, and uploads and maintains supplier product and catalog data with the retailer. This catalog data is for both sell-side and buy-side transactions.</td>
</tr>
<tr>
<td>Supplier Product Design Engineer</td>
<td>Job</td>
<td>Views items and their related details such as a bill of material, attachments or approved manufacturers list. Reviews and acknowledges change orders, and initiates change requests against items they are providing or manufacturing for the customer.</td>
</tr>
<tr>
<td>Supplier Sales Representative</td>
<td>Job</td>
<td>Manages agreements and deliverables for the supplier organization. Acknowledges or requests changes to agreements. Adds catalog line items with customer-specific pricing and terms. Updates contract deliverables that are assigned to the supplier. Updates progress on contract deliverables for which the supplier is responsible.</td>
</tr>
<tr>
<td>Supplier Self Service Administrator</td>
<td>Abstract</td>
<td>Manages the profile information for the supplier company. Primary tasks include updating supplier profile information and requesting user accounts to grant employees access to the supplier application.</td>
</tr>
<tr>
<td>Supplier Self Service Clerk</td>
<td>Abstract</td>
<td>Manages the profile information for the supplier company. Primary tasks include updating supplier profile information and requesting user accounts to grant employees access to the supplier application.</td>
</tr>
</tbody>
</table>
The following table lists predefined sourcing security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Manager</td>
<td>Job</td>
<td>Identifies savings opportunities. Determines negotiation strategies. Creates requests for quote, information, proposal or auction events on behalf of their organization. Awards future business, typically in the form of contracts or purchase orders to suppliers.</td>
</tr>
<tr>
<td>Sourcing Project Collaborator</td>
<td>Abstract</td>
<td>Helps determine negotiation strategies, award decision criteria, and perform objective scoring. The role can be assigned to a key organization member helping to do these tasks.</td>
</tr>
</tbody>
</table>

The following table lists predefined supplier qualification security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier Qualification</td>
<td>Discretionary</td>
<td>Allows a user to define the requirements a supplier should meet. Can qualify a supplier by performing verification and audits. Can assess and maintain supplier qualifications.</td>
</tr>
</tbody>
</table>

The following table lists predefined setup and administration security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement Application Administrator</td>
<td>Job</td>
<td>Performs most setup tasks. Performs the technical aspects of keeping the procurement application functions available. Configures the applications to meet the business needs of the organization.</td>
</tr>
<tr>
<td>Procurement Catalog Administrator</td>
<td>Abstract</td>
<td>Manages agreements and catalog content. This includes catalogs, category hierarchies, content zones, information templates, map sets, public shopping lists and smart forms.</td>
</tr>
<tr>
<td>Procurement Contract Administrator</td>
<td>Job</td>
<td>Creates, manages and administers procurement contracts.</td>
</tr>
<tr>
<td>Procurement Integration Specialist</td>
<td>Job</td>
<td>Plans, coordinates, and supervises all activities related to the integration of the procurement applications.</td>
</tr>
<tr>
<td>Procurement Manager</td>
<td>Job</td>
<td>Manages a group of buyers in an organization.</td>
</tr>
</tbody>
</table>
The following table lists predefined business intelligence security roles and their descriptions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier Administrator</td>
<td>Abstract</td>
<td>Manages supplier profile and user provisioning.</td>
</tr>
<tr>
<td>Supplier Manager</td>
<td>Abstract</td>
<td>Manages supplier information and authorizes promotion of prospective suppliers to spend authorized status.</td>
</tr>
<tr>
<td>Purchase Analysis</td>
<td>Abstract</td>
<td>Allows a user to perform line-of-business analysis on requisitions, purchase orders and suppliers. This role is only used to grant access to Oracle Business Intelligence, not the Oracle Procurement Cloud applications. The user is not a procurement agent. They are a person who owns the line-of-business and wants to do business intelligence analysis on procurement data. The user who has this role has data access to the business unit associated with their primary worker assignment. You can assign additional business units to their data access. Use the Manage Data Access for Users task, in the Setup and Maintenance work area.</td>
</tr>
</tbody>
</table>

**Procurement Requester**

**Procurement Requester Data Security**

Your ability to create or view purchase requisitions is controlled by role-based data security. Three abstract roles define procurement requester security:

- Procurement Requester
- Procurement Preparer
- Advanced Procurement Requester

**Procurement Requester**

With the Procurement Requester role you can create requests for goods or services for yourself. This abstract role is inherited by the Employee and Contingent Worker job roles. As a procurement requester you can:

- Create purchase requisitions.
- View requisitions that have your name listed as the requester on the requisition line.
- Edit requisitions that have your name listed as the person who entered the requisition.
With the Procurement Requester role you have implicit access to data for the business unit associated with your primary worker assignment. This determines the requisitioning business unit you belong to.

**Procurement Preparer**

With the Procurement Preparer role you can create requests for goods or services for yourself and for others. This role must be provisioned directly to you.

**Advanced Procurement Requester**

With the Advanced Procurement Requester role you can create requests for goods or services for yourself and for others. You also have access to the Add Requisition Lines function, which supports the quick creation of multiple requisition lines. This role must be provisioned directly to you.

**Additional Business Units**

To provide you requester access to additional business units, beyond your primary worker assignment, you must be provisioned explicit data access to them. A security administrator can do this using the Manage Business Unit Data Access for Users task, in the Setup and Maintenance work area, Users and Security functional area. For example, consider the following scenario:

- Your primary employee assignment is to US business unit.
- You have also been directly provisioned with data access to the France business unit.

As a result, you have access to data for both the US and France business units.

**View Requisitions Owned by Other Users**

By default, you can only see:

- Requisitions you create.
- Requisitions you did not create, in which you are listed as the requester on one of the lines.

A security administrator can use function security to provide you the ability to view requisitions owned by other users. They can assign you the privilege View Requisitions - All. This provides you access to requisitions for which you are not the preparer or requester, in the business units you have access to.

Some additional purchase requisition-related privileges are available in the security reference implementation, are not assigned to predefined roles, but can be assigned as needed.

- Edit Requisition as Approver: Allows you to modify requisitions as an approver.
- Reassign Requisition: Allows you to reassign requisitions entered by others.
- Reassign Requisition Data: Allows you data access for reassigning requisitions entered by others.

**Note:** Never edit the predefined roles. You can make a copy of a predefined role to create a custom role, if needed.

For more information about procurement requester security roles refer to the Oracle Procurement Cloud Security Reference guide in the Oracle Help Center.

---

**Procurement Agent**
Manage Procurement Agent Security

Use the Manage Procurement Agents task to create and maintain a procurement agent’s access to procurement functionality for a business unit. Find the task in the Procurement Foundation and Payables functional areas.

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 manage activities for suppliers, negotiations, catalog content, and business intelligence spend data.

Key aspects for managing procurement agents are:

- Understanding what a procurement agent is.
- Implementing document security.
- Navigating to the Manage Procurement Agents task.

What is a Procurement Agent?

Procurement agents are typically users with procurement roles such as:

- Buyer
- Catalog Administrator
- Category Manager
- Procurement Contract Administrator
- Procurement Manager
- Supplier Administrator
- Supplier Manager
- Supplier Qualification

They have procurement job responsibilities in the buying organization, such as creating purchase agreements, purchase orders, and related procurement functions. You must set up these users as procurement agents for them to manage procurement documents and perform other procurement actions.

Implement Document Security

The key elements for setting up procurement agent document security are:

- Assigning the agent to a procurement business unit.
- Enabling the agent’s access to procurement actions.
- Defining the agent’s access levels to other agents’ documents.

Procurement Agents

Use the Manage Procurement Agents task to manage procurement agents, including defining an agent’s access to procurement functionality within a procurement business unit.

Find the task in the Procurement Foundation and Payables functional areas.

The following predefined procurement roles are controlled by procurement agent access configuration:

- Buyer
- Catalog Administrator
• Category Manager
• Procurement Contracts Administrator
• Procurement Manager
• Supplier Administrator
• Supplier Manager
• Supplier Qualification

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

**Action**
Enable the agent with access to one or more procurement actions for each procurement business unit.

- Manage Requisitions: Enable access to purchase requisitions.
- Manage Purchase Orders: Enable access to 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 Sourcing Programs: Enable access to track and manage sourcing programs.
- Manage Catalog Content: Enable access to catalog content. This includes local catalogs, punchout catalogs, content zones, smart forms, information templates, and collaborative authoring.
- Manage Suppliers: Enable access to create and update supplier information.
- Manage Supplier Qualifications: Enable access to initiatives, qualifications, and assessments, if Supplier Qualification is implemented by your organization.
- Manage Approved Supplier List Entries: Enable access to create and update approved supplier lists.
- Analyze Spend: Used by the business intelligence functionality to enable access 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:** An agent can perform all actions on their own documents as long as they have procurement BU access.

- None: The agent has no access to documents owned by other agents.
- View: Permits the agent to search and view other agents’ documents.
- Modify: Permits the agent to view, modify, delete, and withdraw other agents’ documents.
- Full: Permits the agent full control of other agents’ documents. This includes the view, modify, delete, withdraw, freeze, hold, close, cancel, and finally close actions.

**Supplier User**

**How Supplier User Provisioning Works**
Supplier user provisioning refers to the process of establishing supplier users with access to the Supplier Portal work area. Your buying organization can create and maintain user accounts, job roles, and data access controls for supplier contacts.
The content supplier users can access, and tasks they can perform, are controlled by your buying organization. You can allow trusted supplier users to request and manage user accounts for their fellow employees that require access to the Supplier Portal work area.

User Provisioning Job Roles

You provision supplier users with job roles, giving them the ability to perform business tasks and functions using the Supplier Portal work area. The predefined job roles that can perform supplier user provisioning are:

- **Supplier Administrator**: This is a buying organization job role. Users with this role are responsible for maintaining supplier profile information as well as administering user accounts for supplier contacts.
- **Supplier Manager**: This is a buying organization job role. Users with this role are responsible for authorizing new suppliers for spending. They control the addition of new spend authorized suppliers into the supply base. In smaller organizations, you can assign this job role and the Supplier Administrator role to the same individual.
- **Supplier Self Service Administrator**: This is a supplier organization job role. Supplier users with this role can maintain company profiles and request user accounts for their fellow employees. All profile changes and user account requests made by the supplier self service administrator require approval by the buying organization.
- **Supplier Self Service Clerk**: This is a supplier organization job role. Supplier users with this role can maintain company profiles and request user accounts for their fellow employees. All profile changes and user account requests made by the supplier self service clerk require approval by the buying organization.

You can perform user provisioning from the following procurement flows:

- Supplier registration review and approval.
- Supplier profile change request review and approval.
- Suppliers work area, Manage Suppliers task, Edit Supplier flow where supplier profiles are maintained.
- 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 a user with one of the appropriate job roles can:

- Create or request a user account.
- Assign job roles.
- Set data security access for supplier contacts.

Manage Supplier User Roles Setup Page

The IT security manager can go to the **Setup and Maintenance** work area and use the **Manage Supplier User Roles** task in the **Procurement** offering and **Supplier Portal** functional area.

The Procurement Application Administrator can go to the **Setup and Maintenance** work area and use the **Manage Supplier User Role Usages** task in the **Procurement** offering and **Supplier Portal** functional area.

Your buying organization uses the Manage Supplier User Roles page to perform the following setup actions. These actions are performed by two different job roles: IT Security Manager, and Procurement Application Administrator.

- **IT Security Manager**: Define the list of roles that can be granted to supplier users in Supplier Portal provisioning flows. Only the IT Security Manager job role can add and remove roles. This helps your organization avoid the risk of adding an internal application job role inadvertently. It prevents suppliers from gaining unauthorized access to internal data. The supplier roles are added from the central Oracle LDAP roles repository which stores all Oracle Fusion application job roles. Once they add a role to the table, the role is immediately available for provisioning to supplier contacts by the Supplier Administrator.
• Procurement Application Administrator: Define the supplier role usages. The Procurement Application Administrator is responsible for this setup task. They manage settings for how the supplier job roles are exposed in provisioning flows.

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

Your buying organization can establish default roles which expedite supplier user account requests. To do this, identify the minimum set of job roles that a supplier contact can be granted. Use default roles so that approvers don’t have to explicitly review and assign job roles for each user account request.

When the role default setup is done correctly, the Supplier Administrator (or approver) can review supplier contact user account requests. This allows them to:

• Review requests with job roles selected based on the source of the request.
• Approve user account requests with appropriate role assignments.

The two role usages relevant to supplier user provisioning are:

• 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 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 two usages.

Related Topics

• Supplier User Account Request

Supplier User Account Administration

The buying organization’s supplier administrator provisions user accounts to provide supplier contacts access to the Supplier Portal work area. The administrator performs user account maintenance for a specific supplier contact in the Suppliers work area, on the Edit Supplier page, Contacts tab. The administrator assigns a user account with roles that determine what functions the supplier contact can perform in the Supplier Portal work area.

The following are Oracle Procurement Cloud flows where a supplier administrator can request and manage a user account for 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. A supplier user can also request for a supplier contact and user account to be created.
• 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. A supplier user can also request a user account to be created for an existing contact.
• Approve supplier registration request: When approving a supplier registration, an approver can create and edit supplier contacts. 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.

Note: Creating a user account for a supplier contact cannot be reversed. Once a user account is created it cannot be deleted, but it can be inactivated.
The Supplier Administrator is responsible for:

- Creating and inactivating supplier user accounts.
- Assigning job roles.
- Assigning data access.

Create and Inactivate Supplier User Accounts

Select the Create User Account option for a contact to send a request to the identity management system to provision the account. Status is displayed to communicate provisioning status during this process. When the process is complete, the identity management system sends notification to the supplier contact with the user name and temporary password for the Supplier Portal work area. If the process fails, a notification is sent to the Supplier Administrator that a user account was not successfully provisioned.

Assign Job Roles

Use the Roles subtab to control function security. This 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. For example, Customer Service Representative or Accounts Receivable Specialist.

Assign Data Access

Use the Data Access tab to control data security. This determines which transactions the user can access for the specific business objects their job role is associated with. The two levels of data security are: 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, the Supplier Site level limits user access to transactions for specific supplier sites only.

Set Up Supplier Roles

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

Select Roles for Supplier User Provisioning:

Vision Corporation decides to expand their Supplier Portal work area deployment and allow supplier customer service representatives to access orders and agreements.

The IT security manager navigates to the Setup and Maintenance work area and uses the Manage Supplier User Roles task in the Procurement offering and Supplier Portal functional area. They search for the supplier job role Supplier Customer Service Representative, and add the role to the table.

The Procurement Application Administrator then navigates to the Setup and Maintenance work area and uses the Manage Supplier User Role Usages task in the Procurement offering and Supplier Portal functional area. For the Supplier Customer Service Representative role, they select the following option: Default for Supplier Portal.

Manage Default Roles for Supplier Users and Supplier Bidders:

Vision Corporation decides the Supplier Sales Representative role should not be marked as a default role for the Supplier Portal work area. The Procurement Application Administrator navigates to the Manage Supplier User Role Usages task. They ensure the Default for Supplier Portal option is not selected for that role.

Vision Corporation also recently implemented Oracle Fusion Sourcing. They must provision the Supplier Bidder role to suppliers invited to sourcing events. The IT Security Manager navigates to the Manage Supplier User Roles page. They add the Supplier Bidder role to the table. For the newly added role, they select the Default for Sourcing option.
Supplier Administration

Security for Individual Supplier Information

Use the Personally Identifiable Information (PII) framework to protect tax identifiers for suppliers classified as individuals. PII refers to the framework in Oracle Fusion Applications for protecting sensitive data for an individual. Additional security privileges are required for users to view and maintain such data.

The predefined job roles Supplier Administrator and Supplier Manager include data security polices to maintain tax identifiers for suppliers classified as individuals. Only users with these roles can view and maintain the following tax identifiers for individual suppliers:

- Taxpayer ID
- Tax Registration Number
- National Insurance Number

Individual suppliers are defined as suppliers with a Tax Organization Type of Individual or Foreign Individual.

Other users without these roles can still search and access individual suppliers. They are restricted from viewing or updating the tax identifiers for these suppliers.

Similar PII data security is also enforced in the Supplier Registration flows. Only users with the Supplier Administrator and Supplier Manager roles can view or maintain the tax identifier information for an individual supplier’s registration approval request.

How can I view and update a supplier contact’s mobile phone?

To view, but not edit, a supplier contact’s mobile phone, you must have the View Trading Community Person Mobile Phone Number data security privilege. To view and edit a supplier contact’s mobile phone, you must have the Manage Trading Community Person Mobile Phone Number data security privilege.

If you have neither privilege, and if there is a mobile phone, the number is masked with asterisks. If there is no mobile phone, the field is blank.

Business Intelligence
Security for Oracle Procurement Cloud Business Intelligence: Overview

Users with the appropriate roles can view, create or edit business intelligence analytics and reports in Oracle Procurement Cloud.

Security for viewing, creating, and editing business intelligence analytics and reports includes these concepts:

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

Business Intelligence Roles

Business intelligence security roles apply to both Oracle Business Intelligence Publisher and Oracle Transactional Business Intelligence. They grant access to business intelligence functionality, such as the ability to run or author analytics and reports. Users need one or more of these roles. In addition, users need the roles that grant access to the following:

- Functional folders, analytics and reports
- Subject areas
- Oracle Procurement Cloud data

Access to Subject Areas in the Business Intelligence Catalog

Access to subject areas in the Business Intelligence Catalog is secured by OTBI Transactional Analysis Duty roles. The following table lists the procurement subject areas by functional area, and the corresponding job roles and OTBI Transactional Analysis Duty role needed for each subject area.

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Job Role</th>
<th>OTBI Transactional Analysis Duty Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement - Implemented Change Orders Real Time</td>
<td>• Category Manager</td>
<td>Implemented Change Order Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Buyer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Procurement - Pending Change Orders Real Time</td>
<td>• Category Manager</td>
<td>Pending Change Order Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Buyer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Procurement - Procure To Pay Real Time</td>
<td>• Accounts Payable Manager</td>
<td>Spend Transaction Analysis Duty Role</td>
</tr>
<tr>
<td></td>
<td>• Accounts Payable Specialist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accounts Payable Supervisor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buyer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Procurement - Purchasing Agreements Real Time</td>
<td>• Category Manager</td>
<td>Agreement Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Buyer</td>
<td></td>
</tr>
<tr>
<td>Subject Area</td>
<td>Job Role</td>
<td>OTBI Transactional Analysis Duty Role</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Procurement - Purchasing Real Time</td>
<td>• Category Manager</td>
<td>Purchase Order Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Buyer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Purchase Analysis</td>
<td></td>
</tr>
<tr>
<td>Procurement - Requisitions Real Time</td>
<td>• Buyer</td>
<td>Purchase Requisitions Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Purchase Analysis</td>
<td></td>
</tr>
<tr>
<td>Procurement - Spend Real Time</td>
<td>• Accounts Payable Manager</td>
<td>Spend Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Accounts Payable Specialist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accounts Payable Supervisor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buyer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Sourcing - Supplier Awards Real Time</td>
<td>• Category Manager</td>
<td>Sourcing Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Sourcing - Supplier Negotiations Real Time</td>
<td>• Category Manager</td>
<td>Sourcing Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Sourcing - Supplier Responses Real Time</td>
<td>• Category Manager</td>
<td>Sourcing Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Procurement Contract Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Procurement Manager</td>
<td></td>
</tr>
<tr>
<td>Supplier - Profile Change Request Real Time</td>
<td>• Supplier Administrator</td>
<td>Supplier Master Data Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Supplier Manager</td>
<td></td>
</tr>
<tr>
<td>Supplier - Supplier Real Time</td>
<td>• Purchase Analysis</td>
<td>Supplier Master Data Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Supplier Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supplier Manager</td>
<td></td>
</tr>
<tr>
<td>Supplier Import - Supplier Real Time</td>
<td>• Purchase Analysis</td>
<td>Supplier Master Data Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Supplier Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supplier Manager</td>
<td></td>
</tr>
<tr>
<td>Supplier Qualification - Qualifications and</td>
<td>• Supplier Qualification</td>
<td>Supplier Qualification Analysis Duty</td>
</tr>
<tr>
<td>Assessments Real Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier Qualification - Question Responses</td>
<td>• Category Manager</td>
<td>Supplier Question and Responses Analysis Duty</td>
</tr>
<tr>
<td>Real Time</td>
<td>• Supplier Qualification</td>
<td></td>
</tr>
<tr>
<td>Supplier Registration - Supplier Real Time</td>
<td>• Purchase Analysis</td>
<td>Supplier Master Data Transaction Analysis Duty</td>
</tr>
<tr>
<td></td>
<td>• Supplier Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supplier Manager</td>
<td></td>
</tr>
</tbody>
</table>
Access to Reports in the Business Intelligence Catalog

Access to functional folders in the Business Intelligence Catalog is secured using the same duty roles that secure access to the subject areas. Functional folders contain delivered analytics and reports. For example, a user who inherits the Purchase Order Transaction Analysis Duty has access to the:

- Purchasing folder in the Business Intelligence Catalog
- Procurement-Purchasing Real Time subject area

Reports are secured based on the folders in which they’re stored. You can set permissions against folders and reports for Application Roles, Catalog Groups, or Users. The following table lists the procurement functional area folders, and the corresponding job roles and OTBI Transactional Analysis Duty role for each folder.

<table>
<thead>
<tr>
<th>Functional Area Folder</th>
<th>Job Role</th>
<th>OTBI Transactional Analysis Duty Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procure To Pay</td>
<td>• Accounts Payable Manager&lt;br&gt;• Accounts Payable Specialist&lt;br&gt;• Accounts Payable Supervisor&lt;br&gt;• Buyer&lt;br&gt;• Procurement Manager</td>
<td>Spend Transaction Analysis Duty Role</td>
</tr>
<tr>
<td>Purchasing</td>
<td>• Category Manager&lt;br&gt;• Buyer&lt;br&gt;• Procurement Contract Administrator&lt;br&gt;• Procurement Manager&lt;br&gt;• Purchase Analysis</td>
<td>Purchase Order Transaction Analysis Duty</td>
</tr>
<tr>
<td>Sourcing</td>
<td>• Category Manager&lt;br&gt;• Buyer&lt;br&gt;• Procurement Manager</td>
<td>Sourcing Transaction Analysis Duty</td>
</tr>
<tr>
<td>Spend</td>
<td>• Accounts Payable Manager&lt;br&gt;• Accounts Payable Specialist&lt;br&gt;• Accounts Payable Supervisor&lt;br&gt;• Buyer&lt;br&gt;• Procurement Manager</td>
<td>Spend Transaction Analysis Duty Role</td>
</tr>
<tr>
<td>Supplier</td>
<td>• Supplier Administrator&lt;br&gt;• Supplier Manager</td>
<td>Supplier Master Data Transaction Analysis Duty</td>
</tr>
<tr>
<td>Supplier Qualification</td>
<td>• Category Manager&lt;br&gt;• Supplier Qualification</td>
<td>Supplier Question and Responses Analysis Duty, and Supplier Qualification Analysis Duty</td>
</tr>
</tbody>
</table>

For a list of predefined analytics and reports, see Oracle Procurement Cloud View Procurement Reports and Analyses on the Oracle Help Center.
Reporting Data

The data that's returned in reports is secured in a similar way to the data that's returned in Oracle Procurement Cloud pages. Each of the transaction analysis duty roles grants access to subject areas and Business Intelligence Catalog folders. To view the roles click **Navigator > Security Console**.

If you cannot see buyer or requester names in analyses or reports, add the View All Workers security profile to your user role. Use the Assign Security Profiles to Role task, in the Setup and Maintenance work area.

Secured List Views

You have two options to obtain access to data using a data model that uses a SQL Query as the data source:

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

PII Data

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

For more information about delivered roles, see the Oracle Procurement Cloud Security Reference guide in the Oracle Help Center.

For more information about business intelligence, see the Oracle Procurement Cloud Creating and Administering Analytics and Reports guide in the Oracle Help Center.

Setting Up Security Profile to View Employee Names in Procurement Analyses: Procedure

Use the Assign Security Profiles to Role task to obtain access to buyer and requester names in your analyses.

Setting Up Security Profile

If you create or run a report and cannot see buyer or requester names in the report, check your person data security profile. Follow these steps to add the View All Workers security profile to your user role.

> **Note:** A Security Manager can open and use the Assign Security Profiles to Role task.

1. From the Navigator, click **Setup and Maintenance**.
2. In the Setup and Maintenance work area, search for and open the **Assign Security Profiles to Role** task.
3. On the Manage Data Roles and Security Profiles page, search for the user role to which you want to grant access. For example, Buyer.
4. In the Search Results region, select the role and click **Edit**.
5. On the Edit Data Role: Role Details page, click Next.
6. Select **View All Workers** when prompted for a Public Person security profile.
7. Click **Review**.
8. Click **Submit**.
Glossary

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

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

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

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

balances cube
A multidimensional database that holds accounting financial data. The cube allows different views of the balances to be quickly displayed.

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

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

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

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

dashboard
A collection of analyses and other content, presented on one or more pages to help users achieve specific business goals. Each page is a separate tab within the dashboard.
**data dimension**
A stripe of data accessible by a user. Sometimes referred to as data security context.

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

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

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

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

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

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

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

**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 having common control over one or more legal entities.

**enterprise role**
Enterprise roles provide users with access both to the application functions they need to perform their jobs as well as the permissions to access the data where they need to perform those functions. There are two types of enterprise roles: job roles...
and abstract roles. Job roles permit users to perform activities specific to their job. Abstract roles permit users to perform functions that span the different jobs in the enterprise.

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

**flexfield**
A flexible data field that you can configure such that it contains one or more segments or stores additional information. Each segment has a value and a meaning.

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

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

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

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

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

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

**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.

**LDAP**

**party**
A physical entity, such as a person, organization or group, that the deploying company has an interest in tracking.
**person number**
A person ID that is unique in the enterprise, allocated automatically or manually, and valid throughout the enterprise for all of a person’s work and person-to-person relationships.

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

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

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

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

**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.

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

**role**
Controls access to application functions and data.

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

**role mapping**
A relationship between one or more roles and one or more assignment conditions. Users with at least one assignment that matches the conditions qualify for the associated roles.
role provisioning
The automatic or manual allocation of a role to a user.

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

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

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

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.

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

workflow
An automated process that passes a task from one user (or group of users) to another to view or act on. The task is routed in a logical sequence to achieve an end result.
**XML filter**

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