Oracle Fusion Cloud ERP

Securing ERP

25C

Oracle Fusion Cloud ERP
Securing ERP

25C

G34346-01

Copyright © "2011, 2025", Oracle and/or its affiliates.

Author: Rakhi Arya

Contents

Get Help i

1 Introduction 1

Securing Oracle ERP Cloud: Overview 1
Overview of ERP Security Implementation 2
Options for Viewing a Visualization Graph 3
Role Types 5
Role Inheritance 6
Security Visualizations 6
Duty Role Components 7
Aggregate Privileges 8
Guidelines for Configuring Security in Oracle Applications Cloud 8

2 Security Console 11

Overview of Security Console 11
Configure the Security Console 12
Retrieve Latest LDAP Changes 14
Visualization Table Display Options 14
Generate a Visualization 15
Simulate Navigator Menus in the Security Console 16
Analytics for Data Resources 17
FAQs on Using the Security Console 18

3 Setting Up Application Security 19

Overview of Applications Security Setup Tasks 19
User-Name Formats 20
Password Policy 21
Role Preferences 23
User Categories 24
Add Users to a User Category 25
Enable Multifactor Authentication 26

User-Name and Password Notifications 27
How can I enable notifications for pending workers? 29
Why don't I see my user name in the forgot password email notification? 30
Why don't I see my user name in the forgot user name email notification? 30
Create a Notification Template 30
Schedule the Import User and Role Application Security Data Process 32
Schedule the Import User Login History Process 33
Why You Should Run the Send Pending LDAP Requests Process 34
Schedule the Send Pending LDAP Requests Process 35
Retrieve Latest LDAP Changes 35

4 Bridge for Microsoft Active Directory 37
Overview of Bridge for Microsoft Active Directory 37
Active Directory Synchronization 38
User Account Attribute Mapping 39
Microsoft Active Directory Bridge Setup 41
FAQs on Working with the Bridge for Microsoft Active Directory 46

5 Understanding ERP Self Service Roles 49
Before You Start 49
HCM Abstract Roles 49
ERP Self-Service Roles 49
Enterprise Resource Planning Self Service User 49
Enterprise Resource Planning Approval Duty 50
Self Service Reporting Duties 50
FAQs for ERP Self Service Roles 54

6 Enabling Basic Access to HCM Data 57
Before You Start 57
Why You Assign Security Profiles to Roles 57
Assign Security Profiles to Roles 58
Configure Employee List of Values 60

7 Implementation Users 63
Implementation Users 63
Overview of ERP Implementation Users 63

User Accounts 65
User Account Details 65
Create User Accounts for Implementation Users 66
Assign Roles to Implementation Users 67
Delete Implementation User Accounts 67
Synchronize User and Role Information 67
Reset the Cloud Service Administrator Sign-In Details 68

8 Preparing for Application Users 69
Before You Start 69
Preparing for Application Users 69
User and Role-Provisioning Setup Options 70
User Account Creation Option 71
User Account Role Provisioning Option 72
User Account Maintenance Option 72
User Account Creation for Terminated Workers Option 73
Set the User and Role Provisioning Options 74
Provision Self Service Roles to Users Automatically 74
FAQs for Preparing for Application Users 75

9 Application Users Management 77
Before You Start 77
Users 77
Users Accounts 80
FAQs on Creating and Managing Application Users 86

10 Role Provisioning 89
Role Mappings 89
Create a Role Mapping 91
Role Provisioning and Deprovisioning 92
Autoprovisioning 94
Roles That Give Workflow Administrators Access 95
Manage Roles in Custom OAuth Client Applications Using Application Extensions Page 97
FAQs on Provisioning Roles and Data to Application Users 98

11 Data Assignments 101
Data Access 101

Assign Data Access to Users 102
Revoke Data Access from Users 104
Automatic Data Provisioning 104
Creating a Data Provisioning Rule 105
Automatic Data Provisioning and Deprovisioning 106
Configure Advanced Implicit Data Security for Non-Discretionary Access 107
FAQs on Assigning Data Access to Application Users 111

12 Reporting on Application Users and Roles 113
Run the User Details System Extract Report 113
User Details System Extract Report Parameters 113
User Details System Extract Report 114
Person User Information Reports 115
User History Report 117
View Role Information Using Security Dashboard 118
LDAP Request Information Reports 118
Inactive Users Report 120
User and Role Access Audit Report 122
User Role Membership Report 124
User and Role Access Audit Report 126
User Password Changes Audit Report 128
View Locked Users and Unlock Users 129
FAQs for Reporting on Application Users and Roles 130

13 Location Based Access 133
Overview of Location-Based Access 133
How Location-Based Access Works 133
Enable and Disable Location-Based Access 134
FAQs on Location Based Access 135

14 Single Sign-On 139
Configure Single Sign-On 139
Oracle Applications Cloud as the Single Sign-On (SSO) Service Provider 141
FAQs on Single Sign-On 142

15 API Authentication 145
Configure Outbound API Authentication Using JWT Custom Claims 145

Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol 146
Configure Inbound Authentication 147
Is there a recommended format for the public certificate? 149

16 Export and Import of Security Setup Data 151
Export and Import of Security Console Data 151
Export and Import of Custom Roles 152
Export and Import a Custom Role 155
Export and Import of ERP Security Setups 156

17 Security Configuration 161
Data Security Policies 161
FAQs on Configuring Security 164

18 Roles and Role Assignments 167
Review Role Assignments 167
Review Role Hierarchies 168
Compare Roles 168

19 Role Configuration Using the Security Console 171
Custom Roles 171

20 Certificates and Keys 189
Overview of Certificates 189
Types of Certificates 189
Sign a X.509 Certificate 190
Import and Export X.509 Certificates 190
Import and Export PGP Certificates 191
Delete Certificates 192

21 Security in Oracle Financials 193
Security for Country-Specific Features 193
General Ledger 193
Payables 260

Subledger Accounting 261
Cash Management 263
Assets 265
Payments 266
Business Intelligence 270

22 Security in Oracle Project Management 281
Overview of Project Management Security 281
Creating Custom Roles for Projects 285
Project Execution Management 286
Project Financial Management 290
Project Management Work Area Security 300
Expanded View Project Plan Access for Non-Team Members 303
Business Intelligence 305

23 Security in Oracle Procurement 315
Overview of Security for Oracle Fusion Cloud Procurement 315
Procurement Requester 320
Procurement Agent 321
Supplier User 323
Supplier Administration 327
Business Intelligence 328

Get Help

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

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. 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. If the page has contextual help, help icons will appear.

Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 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

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.

Chapter	Content
Introduction	A brief overview of role-based security concepts
Using the Security Console	How to set up and manage the Security Console, and use it to view role hierarchies and Navigator menus
Managing Implementation Users	The purpose of implementation users and how you create them
Preparing for Application Users	Enterprise-wide options and related decisions that affect application users
Creating and Managing Application Users	The different ways you can create application users and maintain user accounts, with instructions for some methods
Provisioning Roles to Application Users	How to use tasks available from Setup and Maintenance to enable application users to acquire roles, with instructions for creating some standard role mappings
Configuring Security	How to create, review, and modify security components, with recommended best practices
Reviewing Roles and Role Assignments	How to use the Security Console to review roles and identify the users assigned to them
Configuring Roles in the Security Console	How to create, review, and modify roles in the Security Console, with recommended best practices

Chapter	Content
Managing Certificates and Keys	How to use the Security Console to generate, import, export, and delete digital certificates
Implementing Security in Oracle Fusion Financials	The additional security setup and configuration tasks associated with Oracle Fusion Financials
Implementing Security in Oracle Fusion Project Portfolio Management	The additional security setup and configuration tasks associated with Oracle Fusion Project Portfolio Management
Implementing Security in Oracle Fusion Procurement	The additional security setup and configuration tasks associated with Oracle Fusion Procurement

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

For information on securing reports and analytics, see the Securing Analytics Publisher Reports and Related Components in the Oracle Cloud Administering Transactional Analyses guide.

Overview of ERP Security Implementation

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

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 time cards, are granted to the abstract role **Enterprise Resource Planning Self Service User**. Abstract roles like **Employee**, **Contingent Worker** and **Line Manager** also grant access to common functionalities across a wide collection of Oracle Cloud Applications. A library of duty roles, packaging access to respective Transaction Business Intelligence subject areas and corresponding drill downs, are also available as building blocks to provide self service reporting access.

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.
- **Financial Integration Specialist**: Used to plan, coordinate, and supervise all activities related to the integration of financials information systems.

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.

Separation of Duties Considerations

Separation 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 pre-built roles that can accelerate deployment. To find out whether they could be valuable to your organization:

1. Gather your ERP stakeholders - for example, owners of business processes, IT security administrators, and internal audit / financial governance teams.
2. Identify the pre-built roles that are relevant to your ERP activities.
3. Determine whether those roles should be used as-is, or fine-tuned to suit your operational, security, and compliance requirements. For example, if a user has the **Create Payments** and **Approve Invoice** privileges, you might consider it an SoD conflict. 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 separation against reduction of risk, you might determine that the **Accounts Payable Manager** role should not be allowed to perform force approve invoices and remove that privilege.

To learn more about the SoD, see Using Advanced Controls in the Oracle Help Center (http://docs.oracle.com). To learn more about the policies and roles, see the Security Reference Manual in the Oracle Help Center.

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).

Options for Viewing a Visualization Graph

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

You can also highlight nodes that represent types of security items.

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

Node Labels

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

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

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

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

Expand or Collapse Nodes

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

Using Control Panel Tools

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

- Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.
- Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.
- Zoom to Fit: Center the image and size it so that it's as large as it can be while fitting entirely in its display window. (Nodes that you have expanded remain expanded.)
- Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area covered by the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.
- Search: Enter text to locate nodes whose names contain matching text. You can search only for nodes that the image is currently expanded to reveal.
- Control Panel: Hide or expose the Control Panel.

Using the Legend

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

- Hover over the entry for a particular item type to locate items of that type in the image. Items of all other types are grayed out.
- Click the entry for an item type to disable items of that type in the image. If an item of that type has child nodes, it's grayed out. If not, it disappears from the image. Click the entry a second time to restore disabled items.
- Hide or expose the Legend by clicking its button.

Using the Overview

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

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

Refocusing the Image

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

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

Related Topics

- Visualization Table Display Options

Role Types

Oracle Applications Cloud defines the following types of roles.

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

Let's look at the role types in detail.

Job Roles

Job roles represent the jobs that users perform in an organization. You can also create job roles.

Examples: General Accountant and Accounts Receivables Manager

Abstract Roles

Abstract roles represent users in the enterprise independent of the jobs they perform. 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.

Examples: Enterprise Resource Planning Self Service User and Project Team Member

Duty Roles

Duty roles represent a logical collection of privileges that grant access to tasks that someone performs as part of a job. You can also create duty roles. Here are some duty role characteristics:

- 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.

Examples: Budget Review and Account Balance Review

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.

Security Visualizations

A Security Console visualization graph consists of nodes that represent security items. These may be users, roles, privileges, or aggregate privileges. Arrows connect the nodes to define relationships among them.

You can trace paths from any item in a role hierarchy either toward users who are granted access or toward the privileges roles can grant.

You can select one of the following two views:

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

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

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

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

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

Related Topics

- Generate a Visualization
- Options for Viewing a Visualization Graph
- Visualization Table Display Options

Duty Role Components

A typical duty role consists of function security privileges and data security policies. 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.

These are the components of a data security policy:

- 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. You can create a General Accountant job role with no access to reporting structures. To create such a job role, copy the 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 one function security privilege with related data security policies. All aggregate privileges are predefined. This topic describes how to name and use aggregate privileges.

Aggregate Privilege Names

An aggregate privilege takes its name from the function security privilege that it includes. For example, the Promote Worker aggregate privilege includes the Promote Worker 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.

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.

Create, Edit, or Copy 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. You can copy the predefined role and edit it 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.
  - Identify roles that grant access to Navigator menu items and privileges required for that access.
- Users
  - Create user accounts.
  - Review, edit, lock, or delete existing user accounts.
  - Assign roles to user accounts.
  - Reset users' passwords.
- Analytics
  - Review statistics of role categories, the roles belonging to each category, and the components of each role.
  - View the data security policies, roles, and users associated with each data resource.
- Certificates
  - Generate, export, or import PGP or X.509 certificates, which establish encryption keys for data exchanged between Oracle Cloud applications and other applications.
  - Generate signing requests for X.509 certificates.
- Administration

- Establish rules for the generation of user names.
- Set password policies.
- Create standards for role definition, copying, and visualization.
- Review the status of role-copy operations.
- Define templates for notifications of user account events, such as password expiration.

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.

Configure the Security Console

Before you start using the Security Console, ensure that you run the background processes that refresh security data. You can use the Security Console Administration pages to select the general options, role-oriented options, and track the status of role-copy jobs.

You can also select, edit, or add notification templates.

Run the Background Processes

Here are the background processes you must run:

- **Retrieve Latest LDAP Changes** - This process copies data from the LDAP directory to the Oracle Cloud Applications Security tables. Run this process once, before you start the implementation.
- **Import User and Role Application Security Data** - This process imports users, roles, privileges, and data security policies from the identity store, policy store, and Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables.

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

1. In the Setup and Maintenance work area, go to the **Run User and Roles Synchronization Process** task in the Initial Users functional area.
2. If you want to be notified when this process ends select the corresponding option.
3. Click **Submit**.
4. Review the confirmation message and click **OK**.

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

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User and Role Application Security Data** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set Run to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Days Between Runs** to **1**.
8. Enter start and end dates and times. The start time should be after any daily run of the **Send Pending LDAP Requests** process completes.
9. Click **Submit**.
10. Click **OK** to close the confirmation message.

Configure the General Administration Options

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

Configure the Role Administration Options

1. On the Security Console, click **Administration**.
2. On the Roles tab, specify the prefix and suffix that you want to add to the name and code of role copies. Each role has a Role Name (a display name) and a Role Code (an internal name). A role copy takes up the name and code of the source role, with this prefix or suffix (or both) added. The addition distinguishes the copy from its source. By default, there is no prefix, the suffix for a role name is "Custom," and the suffix for a role code is "_CUSTOM."

3. In the **Graph Node Limit** field, set the maximum number of nodes a visualization graph can display. When a visualization graph contains a greater number of nodes, the visualizer recommends the table view.
4. Deselect **Enable default table view**, if you want the visualizations generated from the Roles tab to have the radial graph view.

View the Role Status

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

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.

Visualization Table Display Options

A visualization table contains records of roles, privileges, or users related to a security item you select.

The table displays records for only one type of item at a time:

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

Tables are all-inclusive:

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

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

Generate a Visualization

The Roles tab of the Security Console lets you generate a visualization. You can choose to view the details as a graph or as a table.

1. On the Security Console, click **Roles**.
2. Search for the security item on which you want to base the visualization.
    - In a Search field, select any combination of item types, for example, job role, duty role, privilege, or user.
    - In the adjacent field, enter at least three characters. The search returns the matching records.
    - Select a record.

      Alternatively, click **Search** to load all the items in a Search Results column, and then select a record.

3. Select either **Show Graph** or **View as Table** button.

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

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

Simulate Navigator Menus in the Security Console

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

Opening a Simulation

To open a simulated menu:

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

Working with the Simulation

In a Simulate Navigator page:

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

In either view:

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

To plan how this authorization may be altered:

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

Analytics for Data Resources

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

1. On the Analytics page, click the Database Resources tab.
2. Select the resource that you want to review in the **Data Resource** field.
3. Click **Go**.

   Results are presented in three tables.

Data Security Policies

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

Each row documents a policy, specifying by default:

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

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

Authorized Roles

The Authorized Roles table documents roles with direct or indirect access to the selected data resource. Any given role might include the following:

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

By default, each row specifies the following:

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

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

Authorized Users

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

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

Manipulating the Results

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

- Add or remove columns. Select **View - Columns**.
- Search among the results. Select **View - Query by Example** to add a search field on each column in a table.
- Export results to a spreadsheet. Select the **Export to Excel** option available for each table.

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 isn't private. It's 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's reasonable to protect such information.

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

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

3 Setting Up Application Security

Overview of Applications Security Setup Tasks

During implementation, an implementation user who has the IT Security Manager job role performs the tasks in the Initial Users functional area. This chapter describes some of these tasks in more detail.

Manage Applications Security Preferences

This task opens the Administration tab of the Security Console.

On the General subtab of the Security Console Administration tab, you:

- Specify for how long certificates remain valid by default. Certificates establish keys for the encryption and decryption of data that Oracle ERP Cloud exchanges with other applications.
- Specify how often a warning appears to remind Security Console users to import latest user and role information.

On the Roles subtab of the Security Console Administration tab, you:

- Specify default prefix and suffix values for copied roles.
- Specify a limit to the number of nodes that can appear in graphical representations of roles on the Roles tab of the Security Console.
- Specify whether hierarchies on the Roles tab appear in graphical or tabular format by default.

On the Bridge for Active Directory subtab of the Security Console Administration tab, you configure the bridge for Microsoft Active Directory.

On the User Categories tab of the Security Console, you:

- Create user categories.
- Add users to user categories.
- Specify the default format of user names for the user category.
- Manage the password policy for the user category.
- Manage the notification of user and password events to users in a selected user category.
- Create notification templates for a selected user category.

Import Users and Roles into Application Security

This task runs a process that initializes and maintains the Oracle Fusion Applications Security tables. You're recommended to schedule this process to run daily. You must also run this process after every release update.

Import User Login History

This task runs a process that imports the history of user access to Oracle Fusion Applications. This information is required by the Inactive Users Report.

User-Name Formats

During implementation, you specify the default format of user names for the default user category. This topic describes the available formats.

To select a format, you perform the Manage Applications Security Preferences task, which opens the Administration page of the Security Console. Click the User Categories tab and click the name of the default user category to open it. Click **Edit** on the Details subtab to edit the user-name format. You can change the format for any user category at any time.

Available User-Name Formats

This table describes the available user-name formats.

User-Name Format	Description
Email	The work email (or party email, for party users) is the user name. For example, the user name for john.smith@example.com is john.smith@example.com. To make duplicate names unique, a number is added. For example, john.smith2@example.com may be used if john.smith@example.com and john.smith1@example.com already exist. **Email** is the default format.
FirstName.LastName	The user name is the worker's first and last names separated by a single period. For example, the user name for John Frank Smith is john.smith. To make duplicate names unique, either the user's middle name or a random character is used. For example, John Smith's user name could be john.frank.smith or john.x.smith.
FLastName	The user name is the worker's last name prefixed with the initial of the worker's first name. For example, the user name for John Smith is jsmith.
Person or party number	The party number or person number is the user name. If your enterprise uses manual person numbering, then any number that's entered during the hiring process becomes the user name. Otherwise, the number is generated automatically and can't be edited. The automatically generated number becomes the user name. For example, if John Smith's person number is 987654, then the user name is 987654.

If you select a different user-name rule, then click **Save**. The change takes effect immediately.

System User Names

The selected user-name rule may fail. For example, a person's party number, person number, or email may not be available when the user account is requested. In this case, a system user name is generated by applying these options in the following order until a unique user name is defined:

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

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

> **Tip:** If a system user name is generated, then it can be edited later to specify a preferred value.

Password Policy

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

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

Password Policy Options

This table describes the available options for setting password policy.

Password-Policy Option	Description	Default Value
Days Before Password Expiration	Specifies the number of days for which a password remains valid. After this period, users must reset their passwords. By default, users whose passwords expire must follow the Forgot Password process.	90
Days Before Password Expiry Warning	Specifies when a user is notified that a password is about to expire. By default, users are prompted to sign in and change their passwords. This value must be equal to or less than the value of the **Days Before Password Expiration** option.	80 **Note:** This value is 10 for new installations from Update 18B.
Hours Before Password Reset Token Expiration	When users request a password reset, they're sent a password-reset link. This option specifies how long a reset-password link remains active. If the link expires before the password is reset, then reset must be requested again. You can enter any value between 1 and 9999.	4
Password Complexity	Specifies whether passwords must be simple, complex, or very complex. Password validation rules identify passwords that fail the selected complexity test. The following password complexity types are available: • Simple: Must contain at least 8 characters, 1 number. This is the default complexity type.	Simple

Password-Policy Option	Description	Default Value
	• Complex: Must contain at least 8 characters, 1 uppercase, 1 number. • Very Complex: Must contain at least 8 characters, 1 uppercase, 1 number, 1 special character. • Custom: Provides the flexibility to specify a combination of parameters to define a custom password. By default, the parameters are populated with predefined set of values to get you started. **Note:** For more information about defining custom password, see topic Configure a Custom Password Policy in the Related Topics section	
Disallow last password	Select to ensure that the new password is different from the last password. If the user requests password reset by selecting **Settings and Actions** > **Set Preferences** > **Password**, then this option determines whether the last password can be reused. However, when a user's password expires, the user can reuse the last password. This option doesn't affect password reuse after expiry. This option doesn't take affect the first time a password is reset if a user is moved from a user category that didn't have the Disallow last password option checked.	No
Administrator can manually reset password	Passwords can be either generated automatically or reset manually by the IT Security Manager. Select this option to allow user passwords to be reset manually. All passwords, whether reset manually or generated automatically, must satisfy the current complexity rule.	Yes

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

Related Topics

- Configure a Custom Password Policy

Role Preferences

During implementation, you set default role preferences for the enterprise. This topic describes the role preferences and their effects.

To set role preferences, you perform the **Manage Applications Security Preferences** task, which opens the General subtab of the Security Console Administration page. Click the Roles subtab of the Administration page. You can also set role preferences at any time on the Security Console.

Copied-Role Names

To create roles, you're recommended to copy predefined roles and edit the copied roles. When you copy a predefined role:

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

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

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

For example, if you copy the Accounts Payable Manager job role (ORA_AP_ACCOUNTS_PAYABLE_MANAGER_JOB), then the default name and code of the copied role are:

- Accounts Payable Manager Custom
- AP_ACCOUNTS_PAYABLE_MANAGER_JOB_CUSTOM

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

Graph Nodes and Default Views

On the Roles tab of the Security Console, you can display role hierarchies. By default, these hierarchies appear in tabular format. To use graphical format by default, deselect the **Enable default table view** option on the Roles subtab of the Security Console Administration tab.

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

Related Topics

- Guidelines for Copying ERP Roles
- Graphical and Tabular Role Visualizations

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 belong to different organizations within an enterprise and each organization follows a different user management policy.
- Practices related to resetting passwords are not uniform across users.
- Users have different preferences in receiving automated notifications for various tasks they perform in the application.

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

- Segregate users into categories
- Specify Next URL
- 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.

Related Topics

- User-Name and Password Notifications
- Add Users to a User Category
- 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're 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're 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:

1. On the Security Console, click **User Categories** > **Create**.
2. Click **Edit**, specify the user category details, and click **Save and Close**.
3. Click the Users tab and click **Edit**.
4. On the Users Category: Users page, click **Add**.
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**.
3. On the Users Category: Users page, click **Add**.
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:

1. On the Security Console, click **Users**.
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.

Enable Multifactor Authentication

Multifactor Authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user's identity.

With MFA enabled in OCI IAM identity domain, when a user signs in to an application, they are prompted for their user name and password, which is the first factor – something that they know. The user is then required to provide a second type of verification. This is called 2-Step Verification. The two factors work together to add an additional layer of security by using either additional information or a second device to verify the user's identity and complete the login process.

Users are increasingly connected, accessing their accounts and applications from anywhere. As an administrator, when you add MFA on top of the traditional user name and password, that helps you to protect access to data and applications. This also reduces the likelihood of online identity theft and fraud, which secures your business applications even if an account password is compromised.

With the identity service upgrade to the Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain, you can enable MFA for signing in to Oracle Fusion Cloud Applications. Oracle Fusion Cloud Applications leverages the MFA functionality available within the OCI IAM identity domain and supports six different factors. Security administrators can choose among these six factors and make them available for users to set up MFA. Users can set up MFA with the provisioned factors when they sign-in. MFA is supported only in non-federated single sign-on (SSO) environments. Here are the six factors:

- One-Time PIN over Email
- One-Time PIN over SMS
- Passcode on Oracle Mobile Authenticator
- Push-based notification from Oracle Mobile Authenticator
- FIDO Passkey Authenticator
- Bypass code

For the One-Time PIN over SMS factor, the work mobile is used as the phone number for authentication. User details such as phone number (work mobile) and email (work email) are stored in the product-specific user settings in Oracle Fusion Cloud Applications, and not on the OCI IAM identity domain.

After the identity upgrade, you can run the Send Personal Data for Multiple Users to LDAP Process to copy the phone number (work mobile) of all existing users to the OCI IAM identity domain. To manage the MFA settings in Security Console, you must be assigned a custom role based on the IT Security Manager role.

Determine the Authentication Factors Available to Users

Security administrators can assess their authentication requirements and decide on the number of factors to be enabled.

1. On the User Categories page of Security Console, select the user category that's associated with the target users.
2. Click **Two-Factor Authentication**.
3. Click **Edit**.
4. Select all the authentication options that you want for your users

   One-Time PIN over Email, One-Time PIN over SMS, and Passcode on Oracle Mobile Authenticator are selected by default, but you can modify if required.

After you enable MFA, when users of that user category sign in to Oracle Fusion Cloud Applications, they'll be redirected to the Oracle Cloud Console page and prompted to enable secure verification for themselves. See *Set Up Multifactor Authentication Methods*.

User-Name and Password Notifications

By default, users in all user categories are notified automatically of changes to their user accounts and passwords. These notifications are based on notification templates. Many templates are predefined, and you can create templates for any user category.

During implementation, you identify the notifications that you plan to use for each user category and disable any that aren't needed. This topic introduces the predefined notification templates and explains how to enable and disable notifications.

Predefined Notification Templates

This table describes the predefined notification templates. Each template is associated with a predefined event. For example, the Password Reset Template is associated with the password-reset event. You can see these notification templates and their associated events on the User Category: Notifications page of the Security Console for a user category.

Template Name	Description	Sent to Inactive Users?	Sent to Locked Users?
ORA Administration Activity Request	Notifies the user when an administrator initiates an administration activity	Yes	Yes
ORA Expiring External IDP Signing Certificate	Warns the user that an external identity provider certificate is expiring soon	No	Yes
ORA Expiring Service Provider Encryption Certificate	Warns the user that a service provider encryption certificate is expiring soon	No	Yes

Template Name	Description	Sent to Inactive Users?	Sent to Locked Users?
ORA Expiring Service Provider Signing Certificate	Warns the user that a service provider signing certificate is expiring soon	No	Yes
ORA Forgot User Name	Sends the user name to a user who requested the reminder	No	Yes
ORA Location Based Access Disabled Confirmation	Notifies the user when an administrator disables location-based access through an administration activity request	Yes	Yes
ORA New Account	Notifies a user when a user account is created and provides a reset-password link	Yes	Yes
ORA New Account Manager	Notifies the user's manager when a user account is created	Yes	Yes
ORA Password Generated	Notifies the user that a password has been generated automatically and provides instructions for resetting the password	Yes	Yes
ORA Password Expiration	Notifies the user that a password has expired and provides instructions for resetting the password	No	No
ORA Password Expiry Warning	Warns the user that a password is expiring soon and provides instructions for resetting the password	No	No
ORA Password Reset	Sends a reset-password link to a user who performed the Reset Password action on the My Account page	No	Yes
ORA Password Reset Confirmation	Notifies the user when a password has been reset	No	Yes
ORA Password Reset Manager	Sends a reset-password link to the manager of a user who performed the Reset Password action on the My Account page	No	Yes
ORA Password Reset Manager Confirmation	Notifies the user's manager when a user's password has been reset	No	Yes

Template Name	Description	Sent to Inactive Users?	Sent to Locked Users?
ORA Single Sign-On Disabled Confirmation	Notifies the user when an administrator disables Single Sign-On through an administration activity request	Yes	Yes

When you create a user category, it's associated automatically with the predefined notification templates, which are all enabled. You can update user categories using the SCIM API, and you can perform bulk updates to categories using HCM Data Loader. For information on adding users to a user category, see the topic Add Users to a User Category.

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. Each predefined event can be associated with only one enabled notification template at a time.

Note: Both pending workers and terminated workers receive emails at their personal email address.

Enabling and Disabling Notifications

For any notification to be sent to the users in a user category, notifications in general must be enabled for the user category. Ensure that the **Enable notifications** option on the User Category: Notifications page is selected. When notifications are enabled, you can disable specific templates. For example, if you disable the New Account Template, then users in the relevant user category aren't notified when their accounts are created. Other notifications continue to be sent.

To disable a template:

1. Click **Edit** on the User Category: Notifications page.
2. In edit mode, click the template name.
3. In the template dialog box, deselect the **Enabled** option.
4. Click **Save and Close**.

Related Topics

- Add Users to a User Category

How can I enable notifications for pending workers?

You can send notifications to the personal email address of pending workers and terminated workers. To send the notification, you must enable the ORA_PER_USER_ACCOUNT_NOTIFY_HOME_EMAIL profile option.

1. In the Setup and Maintenance work area, go to the **Manage Administrator Profile Values** task.
2. On the Manage Administrator Profile Values page, search for and select the ORA_PER_USER_ACCOUNT_NOTIFY_HOME_EMAIL profile option code.
3. In the Profile Values section, enter **Y** as the profile value.
4. Click **Save and Close**.

Why don't I see my user name in the forgot password email notification?

That's because there are two user names associated with your email address. The application can include only one user name in the email notification.

Why don't I see my user name in the forgot user name email notification?

That's because there are two user names associated with your email address. The application can include only one user name in the email notification.

Create a Notification Template

Predefined notification templates exist for events related to the user-account life cycle, such as user-account creation and password reset. When templates are enabled, users are notified automatically of events that affect them. To provide your own notifications, you create notification templates.

Follow these steps to create a notification template:

1. Open the Security Console and click the User Categories tab.
2. On the User Categories page, click the name of the relevant user category.
3. On the User Categories: Details page, click the Notifications subtab.
4. On the User Category: Notifications page, click **Edit**.
5. Click **Add Template**.
6. In the Add Notification Template dialog box:
    a. Enter the template name.
    b. In the **Event** field, select a value. The predefined content for the selected event appears automatically in the **Message Subject** and **Message Text** fields. Tokens in the message text are replaced automatically in generated notifications with values specific to the user.
    c. Update the **Message Subject** field, as required. The text that you enter here appears in the subject line of the notification email.
    d. Update the message text, as required.
    This table shows the tokens supported in the message text.

Token	Meaning	Events
userLoginId	User name	- Forgot user name - Password expired

Token	Meaning	Events
		- Password reset confirmation - New account created
firstName	User's first name	All events
lastName	User's last name	All events
managerFirstName	Manager's first name	- New account created - manager - Password reset confirmation - manager - Password reset - manager
managerLastName	Manager's last name	- New account created - manager - Password reset confirmation - manager - Password reset - manager
loginURL	URL where the user can sign in	- Expiring external IDP signing certificate - Password expired - Password expiry warning
resetURL	URL where the users can reset their password	- New account created - manager - New user created - Password generated - Password reset - Password reset - manager
CRLFX	New line	All events
SP4	Four spaces	All events
adminActivityUrl	URL where an administrator initiates an administration activity	Administration activity requested
providerName	External identity provider	Expiring external IDP signing certificate
signingCertDN	Signing certificate	Expiring external IDP signing certificate
signingCertExpiration	Signing certificate expiration date	- Expiring external IDP signing certificate - Expiring service provider signing certificate
encryptionCertExpiration	Encryption certificate expiration date	Expiring service provider encryption certificate

Token	Meaning	Events
adminFirstName	Administrator's first name	- Administration activity location-based access disabled confirmation - Administration activity single sign-on disabled confirmation
adminLastName	Administrator's last name	- Administration activity location-based access disabled confirmation - Administration activity single sign-on disabled confirmation

e. To enable the template, select the **Enabled** option.
f. Click **Save and Close**.

7. Click **Save** on the User Category: Notifications page.

Note: When you enable an added template for a predefined event, the predefined template for the same event is automatically disabled.

Schedule the Import User and Role Application Security Data Process

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

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

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

Schedule the Process

Follow these steps to schedule the **Import User and Role Application Security Data** process:

1. Open the **Scheduled Processes** work area.
2. In the Search Results section of the **Overview** page, click **Schedule New Process**.
3. In the **Schedule New Process** dialog box, search for and select the **Import User and Role Application Security Data** process.
4. Click **OK**.
5. In the **Process Details** dialog box, click **Advanced**.
6. On the **Schedule** tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Days Between Runs** to **1**.

8. Enter start and end dates and times. The start time should be after any daily run of the **Send Pending LDAP Requests** process completes.
9. Click **Submit**.
10. Click **OK** to close the confirmation message.

Review Synchronization Process Preferences

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

Schedule the Import User Login History Process

During implementation, you perform the Import User Login History task in the Setup and Maintenance work area. This task runs a process that imports information about user access to Oracle Fusion Applications to the Oracle Fusion Applications Security tables.

This information is required by the Inactive Users Report, which reports on users who have been inactive for a specified period. After you perform the **Import User Login History** task for the first time, you're recommended to schedule it to run daily. In this way, you can ensure that the Inactive Users Report is up to date.

Schedule the Process

Follow these steps:

1. Open the Scheduled Processes work area.
2. In the Search Results section of the Overview page, click **Schedule New Process**.
3. In the Schedule New Process dialog box, search for and select the **Import User Login History** process.
4. Click **OK**.
5. In the Process Details dialog box, click **Advanced**.
6. On the Schedule tab, set **Run** to **Using a schedule**.
7. Set **Frequency** to **Daily** and **Every** to **1**.
8. Enter start and end dates and times.
9. Click **Submit**.
10. Click **OK** to close the **Confirmation** message.

Related Topics

- Inactive Users Report

Why You Should Run the Send Pending LDAP Requests Process

You're recommended to run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to your LDAP directory server. Schedule the process in the Scheduled Processes work area. This topic describes the purpose of Send Pending LDAP Requests.

Send Pending LDAP Requests sends the following items to the LDAP directory:

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

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

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

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

  The process sends this information to the LDAP directory unless the automatic management of user accounts is disabled for the enterprise.
- Information about HCM data roles, which originate in Oracle Fusion Cloud HCM.

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

Only one instance of **Send Pending LDAP Requests** can run at a time.

Schedule the Send Pending LDAP Requests Process

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

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

Schedule the Process

Follow these steps:

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

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

Related Topics

- Why You Should Run the Send Pending LDAP Requests Process

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.

4 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.

> **CAUTION:** The bridge for Microsoft Active Directory is on limited availability only. New implementation isn't supported. As an alternative to the bridge for Microsoft Active Directory, you can use the SCIM REST resources to synchronize users onboarded in Oracle Applications Cloud with an external identity management system. For more information, see the Synchronize User Information topic (in the Related Links section) in the REST API for Common Features in Oracle Applications Cloud guide.

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 might 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:

- Windows Server Version: 2008 and 2012
- RAM and CPU: According to 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
- Synchronize User Information

Active Directory Synchronization

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

*Active Directory Synchronization*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 occurred 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 hasn't 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 won't 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.

Oracle Cloud Application as Source	Microsoft Active Directory as Target
`emails.value`	`Mail`

Oracle Cloud Application as Source	Microsoft Active Directory as Target
Username	cn
displayName	displayName
name.familyName	sn
name.givenName	givenName
UserName	userPrincipalName
UserName	sAMAccountName

The following table lists a typical mapping of attributes when Microsoft Active Directory is the source.

Microsoft Active Directory as Source	Oracle Cloud Applications as Target
Mail	emails.value
sAMAccountName	UserName
displayName	displayName
givenName	name.givenName
sn	name.familyName

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** > **Tools** > **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:

Field	Description
Source of Truth	Select the source, such as Oracle Fusion Applications or Active Directory.
Synchronization Interval (Hours)	Enter the time interval (in hours) that the bridge uses to begin synchronization automatically. The default value is 1 hour.
Synchronization Paging Size	Enter the number of accounts that are synchronized in a single operation. The default value is 100 records.
Synchronization Error Threshold	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.
Scheduler	Specify whether you want to automatically schedule synchronizations. If enabled, the synchronizations will run automatically as per the specified schedule and interval.
Role Integration	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.
Reset APPID Password	Enter a new password. During synchronization, this password is used by the bridge to connect to Oracle Applications Cloud.

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

Field	Description
File Name	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`
Log Level	Specify the level at which messages must be logged during synchronization. The default level is set to Information.
Maximum Log Size	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.

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

Field	Description
Host	Enter the host address of the Active Directory server.
Port	Enter the port of the Active Directory server. The default non-SSL port is 389.
Enable SSL	Select this option for secure communication with the Active Directory server. When you select this option, the default port changes to 636.
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.
User Base DN	Enter the distinguished name of the location in your Active Directory where the user accounts are created or retrieved by the bridge.
Search Base	Enter the same value as the User Base DN.
User Search Filter	Enter the LDAP query that's used by the bridge to retrieve the user account objects from the Active Directory. For example, `(&(objectClass=user)(!(objectClass=computer)))`.

Field	Description
Group Base DN	Enter the distinguished name of the location in your Active Directory from where the bridge fetches the groups. **Note:** This field is applicable only when Active Directory is the source.
Group Search Filter	Enter the LDAP query that's used to fetch roles from your Active Directory server. For example, (objectClass=group). **Note:** This field is applicable only when Active Directory is the source.

7. 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.

Field	Description
Enable Proxy Settings	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.
Host	Enter a host name and address for the proxy.
Port	Enter a port for the proxy.
Enable SSL	Select this option for secure communication with the proxy.

8. Expand the Heartbeat section and update the following details.

Field	Description
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**.
   The bridge for Active Directory is installed. Once the bridge is installed, you can open it.
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

After setting 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** > **Tools** > **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

In the initial synchronization, data is copied from the source application to the target application.

1. Start the Bridge for Active Directory.
2. Sign in to bridge using your Oracle Fusion Applications 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's 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

After 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** > **Tools** > **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 Applications Cloud 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:

Attribute	Description
`displayName`	Display name of the user account.
`emails.value`	Primary email address associated with the user account.
`name.familyName`	Last name of the user.
`name.givenName`	First name of the user.
`Username`	User name (name for signing in) associated with the user.

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**.

5 Understanding ERP Self Service Roles

Before You Start

This chapter provides an overview of the self-service roles provided by Oracle ERP Cloud.

HCM Abstract Roles

Oracle HCM Cloud delivers several abstract roles, including:

- Employee
- Contingent Worker
- Line Manager

These roles provide access to common functionalities across Oracle Cloud Applications such as entering expense reports, purchase requisitions, as well as advanced workforce management capabilities such as goal management, performance management suitable for workers, contingent workers, and managers.

Many of the privileges that provide access to these features may also impact subscription usage. Privileges that are assigned but remain unused can still account for subscription consumption.

The recommended process is to always make a copy of these predefined roles, remove the privileges you don't need, and assign only the required privileges.

ERP Self-Service Roles

Oracle ERP Cloud delivers a set of predefined roles that provide access to functionalities available under an Oracle Enterprise Resource Planning Self Service Cloud service subscription.

If you are not using Oracle HCM Cloud services, these roles eliminate the need for you to maintain copies of predefined HCM abstract roles to provide your users access to common functionalities.

Enterprise Resource Planning Self Service User

This abstract role provides access to common functionalities such as managing scheduled processes, as well as creating expense reports, time cards, and maintaining your skills and qualifications.

In an Oracle ERP Cloud only implementation, this role can be assigned to users in lieu of the Employee or Contingent Worker roles to provide users basic access to common functionalities not associated with their job functions.

Note: Oracle ERP Cloud does not make a distinction between employees and contingent workers. If your organization restricts certain access to contingent workers, you can use this role as a template to create a custom role suitable for contingent workers.

In addition, unlike the predefined Employee role, this role is preconfigured to provide basic access to HCM data. The following are basic access to HCM data preconfigured for this role:

Lists the object and access

Object	Access
Person Detail	View Own Record
Person Work Terms Assignment	View Own Record
Talent Profile	View Own Record
Users	View Own Record
User Role	View Own Record
Public Persons	View All People

Enterprise Resource Planning Approval Duty

This duty role includes access needed to approve transactions and access drilldown pages from approval notifications.

Self Service Reporting Duties

This set of duties provides access to both Transactional Business Intelligence subject areas and drilldown pages. They can be used as building blocks to construct reporting roles to provide self service reporting access.

The following table identifies the subject areas that predefined Financials self-service reporting duty roles can access.

Subject areas that predefined Financials or Projects self-service reporting duty roles access

Self-Service Reporting Duties	Subject Areas
Budgetary Control Self Service Reporting Duty	All Budgetary Control
Cash Management Self Service Reporting Duty	All Cash Management

Self-Service Reporting Duties	Subject Areas
Expense Self Service Reporting Duty	All Expenses
Fixed Asset Self Service Reporting Duty	All Fixed Assets
General Ledger Self Service Reporting Duty	All General Ledger, Financials Common Module - Intercompany Transactions Real Time
Payables Self Service Reporting Duty	All Payables
Receivables Self Service Reporting Duty	All Receivables
Revenue Management Self Service Reporting Duty	All Revenue Management
Projects Self Service Reporting Duty	Project Foundation, Project Costing, Project Billing, Project Control (Includes access to deeplinks for viewing project cost transaction, project overview, project plan pages)

When you create a custom job role to provide self-service reporting access, make sure you add the correct duty roles to the custom role. Transactional Business Intelligence reports, then you must give the role the correct duty roles. Your custom role must have both the **OBI** and **Financials** or **Project Management** versions of the self-service reporting duty roles. The OBI version of the self-service reporting duties provide access to the subject areas, while the Financials versions of the duties provide access to Financial Reporting Center and the relevant drilldown pages.

For example, if your role must provide self-service reporting access to the Fixed Asset subject areas and the corresponding drilldowns, then it must inherit the duty roles described in the following table:

Duty Role Name and Duty Role Code

Duty Role Name	Duty Role Code	Version
Fixed Asset Self Service Reporting	ORA_FA_SELF_SERVICE_REPORTING_DUTY	Financials
Fixed Asset Self Service Reporting Duty	ORA_FA_SELF_SERVICE_REPORTING_DUTY_OBI	OBI

These duty roles are not preconfigured with data security access. You will need to create data security policies for the custom roles to provide the necessary data access.

The following are sample data security policies to utilize Manage Data Access for Users page to manage data assignments for reporting access:

Sample Data Security Policies

Product / Family	Business Object	Conditions	Privileges
General Ledger	Data Access Set	Access the general ledger data access set for table GL_ACCESS_SETS for the general ledger data	Inquire and Analyze Oracle Fusion General Ledger Account Balance

Product / Family	Business Object	Conditions	Privileges
		access sets for which they are authorized	
	Ledger	Access the ledger for table GL_LEDGERS for the ledgers derived from data access sets for which they are authorized	Report Oracle Fusion General Ledger
	Intercompany Organization	Access the Intercompany Organization for table FUN_INTERCO_ORGANIZATIONS for the intercompany organizations for which they are authorized	View Intercompany Transaction
Payables	Business Unit	Access the business units for which the user is explicitly authorized	• Report Payables (for OTBI) • Manage Payables Invoice (for invoice drilldown) • Manage Payments by Business Unit (for payment drilldown)
Receivables	Business Unit	Access the business units for which the user is explicitly authorized	View Receivables Activities
Fixed Assets	Fixed Asset Book	Access the fixed asset book for table FA_BOOK_CONTROLS for the asset books for which they are authorized	Submit Fixed Assets Reports
Revenue Management	Ledger	Access the ledger for table GL_LEDGERS for the ledgers for which they are authorized	View Revenue Management
Budgetary Control	Control Budget	Access the control budget for table XCC_CONTROL_BUDGETS - for the Control Budgets that the current user has created	Read; Review Budgetary Control Balance; Review Control Budget;
Subledger Accounting	Subledger Accounting Ledger	• For **Business Unit** assignments - Access Ledgers Associated with Business Units • For Asset Book assignments - Access Ledgers Associated with Asset Books For deriving access from other types of assignments, please refer to the corresponding data security policies in the respective predefined job roles, such as **Cost Manager**, for details.	Manage Ledger for Subledger Data

Product / Family	Business Object	Conditions	Privileges
	Subledger Application	This policy requires the internal ID for the corresponding subledger application. Please refer to the corresponding data security policies in the respective predefined job roles, such as **Accounts Payable Manager**, for details.	Manage Subledger Application Data
	Subledger Source Transaction	This policy requires the internal ID for the corresponding subledger application. Please refer to the corresponding data security policies in the respective predefined job roles, such as **Accounts Payable Manager**, for details.	Manage Subledger Source Transaction Data
Project Management	Project Expenditure Item	Access the project expenditure items for Table PJC_EXP_ITEMS_ALL for project business unit	Manage Project Expenditure Item Data
	Project Unprocessed Expenditure Item	Access the Unprocessed Transaction for Table PJC_TXN_XFACE_ALL for business unit	Manage Project Unprocessed Expenditure Item Data
	Project Contract Invoice	Access the Invoice Lines Distributions for Table PJB_INV_LINE_DISTS for project business unit	Manage Project Contract Invoice Data
	Project Contract Revenue	Access the Revenue Distribution Lines for Table PJB_REV_DISTRIBUTIONS for business unit	Manage Project Contract Revenue Data
	Project	The project access for table PJF_PROJECTS_ALL_VL for project business units on which they are authorized as defined in Manage Data Access for Users Page	View Project Forecast Working Version Data View Project Forecast Approved Version Data
	Project	The project access for table PJF_PROJECTS_ALL_VL for project business units on which they are authorized as defined in Manage Data Access for Users Page	View Project Budget Working Version Data View Project Budget Baseline Version Data
	Project	Read only access of the project work plan for table PJF_PROJECTS_	View Project Work Plan Data

Product / Family	Business Object	Conditions	Privileges
		ALL_VL for projects where user is authorized	
	Project	The project access for table PJF_PROJECTS_ALL_VL for project business units on which they are authorized as defined in Manage Data Access for Users Page.	View Project in Project Home Data

FAQs for ERP Self Service Roles

Which roles should I be using?

If you are only implementing Oracle ERP Cloud, it is recommended that you use the Enterprise Resource Planning Self Service User role to provide common access to users instead of Employee / Contingent Worker / Line Manager roles from HCM.

If you are implementing both Oracle ERP Cloud and Oracle HCM Cloud, you can start with either, and add or remove access as required. If you choose to use Employee / Contingent Worker / Line Manager roles from HCM, be sure to create custom versions of them and remove access to functionalities that you do not need.

Should I be switching to use the ERP role if I have started my implementation?

If you have created custom versions of the Employee / Contingent Worker / Line Manager roles in your current implementation, you do not have to switch to the ERP role. You can continue using your custom roles.

If you have created custom versions of the Employee / Contingent Worker / Line Manager roles in your current implementation, you do not have to switch to the ERP role. You can continue using your custom roles.

I am using the predefined Employee / Contingent Worker / Line Manager roles today. What should I do?

At a minimum, you should plan on switching to either the predefined ERP role if it meets your business requirements, or custom versions of the Employee / Contingent Work / Line Manager roles to remove access your users do not need.

These predefined roles provide access to advanced workforce management capabilities such as goal management, performance management suitable for workers, contingent workers, and managers, many of which may also impact subscription usage. Privileges that are assigned but remain unused can still account for subscription consumption.

The recommended process is to always make a copy of these predefined roles, remove the privileges you don't need, and assign only the required privileges.

How do I switch to use the ERP role?

If you are currently using Role Mapping to assign Employee role automatically to users, switching is easy. All you need to do is replace the Employee role, whether the predefined or a modified version, in the Role Mapping with the ERP role. Users that are automatically assigned the Employee role would be assigned the ERP role instead.

Oracle ERP Cloud does not make a distinction between employees and contingent workers. If your organization restricts certain access to contingent workers, you can use this role as a template to create a custom role suitable for contingent workers. Otherwise, you can re-use the Enterprise Resource Planning Self Service User role for contingent workers. You can then replace the Contingent Worker role in the Role Mapping specific for contingent workers with the appropriate role.

Lastly, Oracle ERP Cloud does not have functionalities specific to line managers. Approvals for expense reports and timecards are handled by Notifications without the need for specific privileges.

See Provision Self Service Roles to Users Automatically.

6 Enabling Basic Access to HCM Data

Before You Start

This chapter focuses on enabling basic access to HCM data if you're not using Oracle HCM Cloud service. If you're using Oracle HCM Cloud service, see the Enabling Basic Data Access for Abstract Roles chapter in the Securing HCM Cloud

Why You Assign Security Profiles to Roles

Several predefined roles can open application pages that contain HCM data in Oracle ERP Cloud. Examples of these roles are:

- Employee
- Contingent Worker
- Financial Application Administrator

Users with these roles can sign in and open application pages. However, they have no automatic access to HCM data in these pages. For example, Financial Application Administrators can open the Manage Users page but their searches return no results. To enable basic HCM data access for users with abstract roles, you assign security profiles directly to those roles.

Security Profiles to Assign to Roles

This table identifies the security profiles that you can assign directly to the Employee, Contingent Worker, and Financial Application Administrator roles. With the exception of the Transaction security profile for the Financial Application Administrator role, all of these security profiles are predefined.

Security Profile Type	Employee	Contingent Worker	Financial Application Administrator
Person	View Own Record	View Own Record	View All People
Public person	View All People	View All People	View All People
Organization	View All Organizations	View All Organizations	View All Organizations
Position	View All Positions	View All Positions	Not applicable
Legislative data group	View All Legislative Data Groups	View All Legislative Data Groups	Not applicable
Country	View All Countries	View All Countries	Not applicable

Security Profile Type	Employee	Contingent Worker	Financial Application Administrator
Document type	View All Document Types	View All Document Types	Not applicable
Transaction	Not applicable	Not applicable	Need to create a custom security profile that grants access to Financials transactions

Assign Security Profiles to Roles

In this example, you learn how to assign security profiles to roles during implementation. You perform this task to enable basic data access for the predefined Employee, Contingent Worker, and Financial Application Administrator roles.

Search for the Employee Abstract Role

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: Assign Security Profiles to Role
3. On the Manage Data Roles and Security Profiles page, enter **Employee** in the **Role** field. Click **Search**.
4. In the Search Results section, select the predefined **Employee** role and click **Edit**.

Assign Security Profiles to the Employee Abstract Role

1. On the Edit Data Role: Role Details page, click **Next**.
2. On the Edit Data Role: Security Criteria page, select the security profiles shown in the following table.

Field	Value
Organization Security Profile	View All Organizations
Position Security Profile	View All Positions
Country Security Profile	View All Countries
LDG Security Profile	View All Legislative Data Groups
Person Security Profile (Person section)	View Own Record

Field	Value
Person Security Profile (Public Person section)	View All People
Document Type Security Profile	View All Document Types

3. Click **Review**.
4. On the Edit Data Role: Review page, click **Submit**.
5. On the Manage Data Roles and Security Profiles page, search again for the predefined Employee role.
6. In the Search Results region, confirm that the **Assigned** icon appears in the **Security Profiles** column for the Employee role.

   The **Assigned** icon, a check mark, confirms that security profiles are assigned to the role.

   Repeat the steps in the Search for the Employee Abstract Role and Assign Security Profiles to the Employee Abstract Role sections for the predefined Contingent Worker role.

Search for the Financial Application Administrator Role

1. On the Manage Data Roles and Security Profiles page, enter **Financial Application Administrator** in the **Role** field. Click **Search**.
2. In the Search Results section, select the predefined **Financial Application Administrator** role and click **Edit**.

Assign Security Profiles to the Financial Application Administrator Role

1. On the Edit Data Role: Role Details page, click **Next**.
2. On the Edit Data Role: Security Criteria page, select the security profiles shown in the following table.

Field	Value
Organization Security Profile	View All Organizations
Person Security Profile (Person section)	View All People
Person Security Profile (Public Person section)	View All People
Transaction	Create New

3. Enter the name of your new transaction security profile, for example, View All Financials Transactions.
4. Click **Next** until you reach the Transaction Security Profile page.
5. Click **Add**.
6. Select FIN as the family.

7. Click **Review**.
8. On the Edit Data Role: Review page, click **Submit**.
9. On the Manage Data Roles and Security Profiles page, search again for the predefined Financial Application Administrator role.
10. In the search results, confirm that the **Assigned** icon appears in the **Security Profiles** column for the Financial Application Administrator role.

    The **Assigned** icon confirms that security profiles are assigned to the role.

Configure Employee List of Values

Fields that reference an employee or person can be found on many pages in Oracle ERP Cloud, such as preparer on a payable invoice, first approver on a payable payment request, or employee on an asset record. These lists of values show the

By default, predefined roles providing access to these pages include data security policies that allow users to choose all employees in these lists of values.

To implement restrictions in these lists of values, these predefined data security policies need to be replaced with data security policies that are more restrictive. Since predefined roles can't be modified, you make these changes to copies of the predefined roles. You can manually create the necessary data security policies using the Security Console, or assign the public person security profile for the custom role.

Restricting Access Using Security Console

In this example, you learn how to create or modify a data security policy to restrict access in employee list of values using Security Console.

1. Sign in as the TechAdmin user or another user with the IT Security Manager job role or privileges.
2. Click **Navigator**> **Tools**> **Security Console**.
3. On the Roles tab of the Security Console, search for and select your custom role.
4. In the search results, click the down arrow for the selected role and select **Edit Role**.
5. Click the **Data Security Policies** train stop.
6. Search for the data security policy with the privilege **Choose Public Person**.
7. If one exists, click on the down arrow for the selected policy and select **Edit Data Security Policy**. In the Data Set field, choose **All Values** if you don't want any restrictions, or **Select by instance set** followed by choosing a **Condition Name** that matches your needs. For example, the condition **Access Public Persons From My Own Legal Employer** would restrict employees with the same legal employer as the user.
8. If none exists, click **Create Data Security Policy**. Create a data security policy as follows:

Field	Value
Database Resource	Public Person
Data Set	Select by instance set, or All values (if no restriction is needed)
Condition Name	As desired, for example, to restrict the list of values to legal employer, use **Access Public Persons From My Own Legal Employer**

Field	Value
Actions	Choose Public Person

9. Click **OK** to close the Create or Edit Data Security window, then click the **Summary** train stop.
10. Review the summary of changes. Click **Back** to make corrections or click **Save and Close** to save the changes.

Restricting Access Using Security Profile

You can also restrict access in employee list of values using Security Profile.

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: Assign Security Profiles to Role
3. On the Manage Data Roles and Security Profiles page, enter the name of the custom role in the **Role** field. Click **Search**.
4. In the Search Results section, select the role and click **Edit**.
5. On the Edit Data Role: Role Details page, click **Next**.
6. On the Edit Data Role: Security Criteria page, proceed to the Public Person and choose the security profile as desired. You may also create a new security profile here.
7. Click **Review**.
8. On the Edit Data Role: Review page, click **Submit**.
9. On the Manage Data Roles and Security Profiles page, search again for the custom role.
10. In the search results, confirm that the **Assigned** icon appears in the **Security Profiles** column for the custom role.

    The **Assigned** icon confirms that security profiles are assigned to the role.

Related Topics

- Create ERP Roles in the Security Console
- HCM Security Profiles

7 Implementation Users

Implementation Users

The implementation or setup users are typically different from the Oracle Applications Cloud application users. They are usually not part of Oracle Applications Cloud organization.

So, you don't assign them any product-specific task or let them view product-specific data. But, you must assign them the required privileges to complete the application setup. You can assign these privileges through role assignment.

The initial user can do all the setup tasks and security tasks such as, resetting passwords and granting additional privileges to self and to others. After you sign in for the first time, create additional implementation users with the same setup privileges as that of the initial user. You can also restrict the privileges of these implementation users based on your setup needs.

You can assign job roles and abstract roles to users using the Security Console. Here are the roles that you can assign to the setup users:

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

> **Note:** The Application Implementation Consultant abstract role has unrestricted access to a large amount of data. So, assign this role to only those implementation users who do a wide range of implementation tasks and handle the setup data across environments. For users who must do specific implementation tasks, you can assign other administrator roles, such as the Financial Applications Administrator role.

If required, you can provide the same setup permissions to users that are part of your organization. You can also create administrative users with limited permissions. These users can configure product-specific settings and perform other related setup tasks.

For an implementation user, only a user account exists. No person record exists in Oracle HCM Cloud.

Overview of ERP Implementation Users

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

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

Accessing the Oracle ERP Cloud Service

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

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

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

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

Creating Implementation Users

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

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

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

User Accounts

The User Accounts page of the Security Console provides summaries of user accounts that you select to review.

For each account, it always provides:

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

It may also provide:

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

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

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

To begin working with user accounts:

1. On the Security Console, select the Users tab.
2. To perform a search, select one or more user states, select one of the user attributes (User Name, Email, First Name, or Last Name) from the drop-down list, and enter at least three characters.

   The search returns user accounts based on the selected options.

Note: On the Security Console, you can't search for users who have APPID in their user name.

User Account Details

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

These details always include:

- User information, which consists of user category, user name, first name, last name, and an email.
- Account information, which includes the user's password-expiration date, whether the account is active, and whether it's locked.
- A table listing the roles assigned to the user, including whether they're autoprovisioned or assignable. A role is assignable if it can be delegated to another user.

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

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

- You can edit values only in the User Information, Account Information, and Roles regions.
- Even in those regions, you can edit some fields only if the user isn't associated with a worker or a party. If not, for example, you can modify the First Name and Last Name values in the User Information region. But if the user is associated with a worker, you would manage these values in Human Capital Management. They would be grayed out in this Edit User Details page.
- In the Roles table, Autoprovisioned check boxes are set automatically, and you can't modify the settings. The box is checked if the user obtained the role through autoprovisioning, and cleared if the role was manually assigned. You can modify the Assignable setting for existing roles.

Note: You can edit the User Name in the Edit User Account Details page. You can update the user name irrespective of whether this account is linked to a worker record in HCM or not. All the conditions that apply for creating a user name applies while updating it. The user name can be in any format and up to a maximum length of 80 characters. The user name can include multibyte characters.

Click Add Autoprovisioned Roles to add any roles for which the user is eligible. Or, to add roles manually, click Add Role. Search for roles you want to add, select them, and click Add Role Membership. You can remove all roles that are associated with a user using the corresponding button.

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

Create User Accounts for Implementation Users

The user accounts that you add in the Security Console are used for implementation users. Depending on whether you're also using Oracle HCM Cloud, you use the Manage Users or Hire an Employee task to create application users, which include the user accounts and

Follow these steps to add a user account in the Security Console:

1. In the Security Console, click the **Users** tab.
2. On the User Accounts page, click the **Add User Account** button.
3. From the **Associated Person Type** list, select **Worker** to link this account to a worker record in HCM. Otherwise, leave it as **None**.
4. In the Account Information section, change the default settings if you don't want the account to be active or unlocked.
5. Fill in the User Information section.
    - Select the user category that you want to associate the user with. The user category includes a password policy and a rule that determines how the user name is automatically generated.
    - Enter the user's first name only if the rule from the selected user category makes use of the first name or the first name initial to generate user names.
    - Enter a password that conforms to the password policy from the selected user category.
6. In the Roles section, click the **Add Role** button.

7. Search for the role that you want to assign to the user and the click **Add Role Membership** button. The role is added to the list of existing roles.
8. Repeat the previous step to add more roles if required, or just click **Done**.
9. Click the **Add Auto-Provisioned Roles** button to add any roles that the user is eligible for, based on role provisioning rules. If nothing happens, that means there aren't any roles to autoprovision.
10. In the Roles table, click the **Assignable** check box for any role that can be delegated to another user. The **Auto-Provisioned** column displays a tick mark if the user has roles that were assigned through autoprovisioning.
11. Click the **Delete** icon to unassign any role.
12. Click **Save and Close**.

Related Topics

- Overview of User Categories

Assign Roles to Implementation Users

Use the Security Console to assign a specific role to an implementation user. Or, remove roles that were already assigned to the user.

1. In the Security Console, click the **Users** tab.
2. Search for and select the user you want to assign roles to.
3. On the User Account Details page, click the **Edit** button.
4. In the Roles section, click the **Add Role** button.
5. Search for the role that you want to assign to the user and the click **Add Role Membership** button. The role is added to the list of existing roles.
6. Repeat the previous step to add more roles if required, or just click **Done**.
7. Click the **Add Auto-Provisioned Roles** button to add any roles that the user is eligible for, based on role provisioning rules. If nothing happens, that means there aren't any roles to autoprovision.
8. In the Roles table, click the **Assignable** check box for any role that can be delegated to another user. The **Auto-Provisioned** column displays a tick mark if the user has roles that were assigned through autoprovisioning.
9. Click the **Delete** icon to unassign any role.
10. Click **Save and Close**.

Delete Implementation 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.

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.

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

    Note: If you can't see this task, make sure you've selected All Tasks in the **Show** drop-down list.
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.

8 Preparing for Application Users

Before You Start

This chapter is only applicable if you're not using Oracle HCM Cloud service. If you're using Oracle HCM Cloud service, see the Preparing for Application Users chapter in the Securing HCM Cloud guide.

Preparing for Application Users

During implementation, you prepare your Oracle Applications Cloud service for application users. Decisions made during this phase determine how you manage users by default. Most of these decisions can be overridden.

For efficient user management, you're recommended to configure your environment to both reflect enterprise policy and support most or all users.

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

Decision or Task	Topic
Whether user accounts are created automatically for application users	User Account Creation Option
How role provisioning is managed	User Account Role Provisioning Option
Whether user accounts are maintained automatically	User Account Maintenance Option
Whether user accounts are created for terminated workers that you load in bulk	User Account Creation for Terminated Workers Option
Ensuring that the Employee abstract role is provisioned automatically	Provisioning Abstract Roles to Users Automatically

Some decisions affecting application users were made when the Security Console was set up. These decisions include:

- How user names are formed by default
- How passwords are formed and when they expire
- How users are notified of their sign-in details and password events, such as expiration warnings

You may want to review these settings for each user category on the Security Console before creating application users.

Related Topics

- User-Name Formats
- Password Policy
- User-Name and Password Notifications

User and Role-Provisioning Setup Options

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

User Account Creation

The **User Account Creation** option controls:

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

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

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

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

User Account Role Provisioning

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

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

User Account Maintenance

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

User Account Creation for Terminated Workers

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

Related Topics

- User Account Creation Option
- User Account Role Provisioning Option
- User Account Maintenance Option
- User Account Creation for Terminated Workers Option

User Account Creation Option

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

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

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

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

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

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

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

User Account Role Provisioning Option

Existing users both acquire and lose roles as specified by current role-provisioning rules. For example, users may request some roles for themselves and acquire others automatically. All provisioning changes are role requests that are processed by default.

You can control what happens to role requests by setting the **User Account Role Provisioning** option. Use the **Manage Enterprise HCM Information** task to set this option. This table describes the **User Account Role Provisioning** option values.

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

Note: When a user account is created, roles may be provisioned to it automatically based on current role-provisioning rules. This provisioning occurs because user accounts without roles are suspended automatically. Automatic creation of user accounts and the associated role provisioning are controlled by the **User Account Creation** option.

User Account Maintenance Option

By default, a user's account is suspended automatically when the user has no roles. This situation occurs typically at termination. The user account is reactivated automatically if you reverse the termination or rehire the worker. The User Account Maintenance option controls these actions.

Use the **Manage Enterprise HCM Information** task to set this option. This table describes the **User Account Maintenance** option values.

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

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

User Account Creation for Terminated Workers Option

The User Account Creation for Terminated Workers option controls whether user accounts are created for terminated workers. It applies only when you run Send Pending LDAP Requests.

Typically, you run Send Pending LDAP Requests after loading workers in bulk using HCM Data Loader, for example. This option doesn't apply to workers created in the user interface unless they're future-dated. Use the Manage Enterprise HCM Information task to set this option.

This table describes the **User Account Creation for Terminated Workers** option values.

Value	Description
No (or not set)	User account requests generated for terminated workers are suppressed when you run the Send Pending LDAP Requests.
Yes	User account requests generated for terminated workers are processed when you run the Send Pending LDAP Requests.

This option determines whether user account requests for terminated workers are processed or suppressed. A user account request is generated for a worker created by bulk upload only if:

- The **User Account Creation** enterprise option is set to **Both person and party users**.
- The **GeneratedUserAccountFlag** attribute for the Worker object isn't set to **N**.

Otherwise, user account requests for workers are suppressed and **User Account Creation for Terminated Workers** has no effect.

Related Topics

- Why You Should Run the Send Pending LDAP Requests Process

Set the User and Role Provisioning Options

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

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

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

Related Topics

- User and Role-Provisioning Setup Options

Provision Self Service Roles to Users Automatically

Provisioning the Enterprise Resource Planning Self Service User role automatically to users is efficient, as most users have this role. It also ensures that users have basic access to functions and data when they first sign in.

Provision the Self-Service 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.

Field	Value
System Person Type	Employee
HR Assignment Status	Active

6. In the Associated Roles section of the Create Role Mapping page, add a row.
7. In the **Role Name** field of the Associated Roles section, click **Search**.
8. In the Search and Select dialog box, enter **Enterprise Resource Planning Self Service User** in the **Role Name** field and click **Search**.
9. Select **Enterprise Resource Planning Self Service User** 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**.

    If you're currently using a modified version of the predefined Employee role, you can continue to do so by entering the name of your modified role instead of the predefined Enterprise Resource Planning Self Service User role in the **Role Name** field.

FAQs for Preparing for Application Users

Can I implement single sign-on in the cloud?

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

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

Related Topics

- Oracle Applications Cloud Service Entitlements (Doc ID 2004494.1)

9 Application Users Management

Before You Start

This chapter is only applicable if you're not using Oracle HCM Cloud service. If you're using Oracle HCM Cloud service, see the Creating Application Users and the Managing Application Users chapters in the Securing HCM Cloud guide.

Users

Options for Creating Application Users

When you create person records, user accounts can be created automatically. The User and Role Provisioning options control whether user accounts are created and maintained automatically. You set these options for the enterprise during implementation using the **Manage Enterprise HCM Information** task.

Some enterprises use applications other than Oracle ERP Cloud to manage user and role provisioning. In this case, you set the User and Role Provisioning options to prevent automatic creation of user accounts. Oracle ERP Cloud user accounts don't provide access to other enterprise applications.

Creating Person Records

You can create person records:

- Individually, using the **Manage Users** task
- In bulk, uploading them using HCM Data Loader

When Oracle HCM Cloud is implemented, ERP users won't create person records. This activity is performed by HCM users who use tasks such as Hire an Employee, rather than Create User.

Uploading Workers Using HCM Data Loader

To load workers using HCM Data Loader, use the **Import and Load Data** task in the Data Exchange work area. The enterprise option **User Account Creation** controls whether user accounts are created for all workers by default. You can prevent user accounts from being created for individual workers by setting the **GeneratedUserAccountFlag** attribute of the User Information component to **N**. If you're creating user accounts for uploaded workers, then you can provide a user name in the uploaded data. This value overrides the default user-name format for the default user category. You run the process **Send Pending LDAP Requests** to send bulk user-account requests for processing.

> **Note:** If appropriate role mappings don't exist when you load new workers, then user accounts are created but no roles are provisioned. User accounts without roles are automatically suspended when **Send Pending LDAP Requests** completes. To avoid this suspension, always create a role mapping for the workers you're loading before you load them. Having the recommended role mapping to provision abstract roles automatically to employees, contingent workers, and line managers is sufficient in most cases.

Related Topics

- Provision Abstract Roles to Users Automatically

Create Application Users

This topic describes how you create an application user using the Manage Users task. By default, this task creates a minimal person record and a user account.

Sign in and follow these steps:

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page. You can also search for the **Manage Users** task in the Setup and Maintenance work area.
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 **Email** field, enter the user's primary work email.

   > **Tip:** If email validation is enabled, then a warning appears if the email already exists.

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 either create a user account or link an existing standalone user account.

To create a user account, select **Enter user name**. If you leave the **User Name** field blank, then the user name is generated automatically in the enterprise default format. In this case, automatic creation of user accounts must be enabled for the enterprise. If you enter a user name, that name is used if it's valid.

Alternatively, you may have created a standalone user account on the Security Console or using SCIM (REST) APIs. These types of user accounts aren't linked to person records. To link such an account to the new person record:

1. Select **Link user account**.
2. Click the **Link** icon to open the Link User Account dialog box.
3. In the Link User Account dialog box, search for and select the user account. Accounts that are already linked to person records don't appear here. The account can be in any status. Its status isn't changed when you link it.
4. Click **OK** to link the account.

> **Tip:** On the Edit User page, you can edit the user details and link a different user account, if required. The link to the existing user account is removed automatically.

Defaulting User Names

By default, user names are generated automatically in the format specified for the default user category when you create a user. This table summarizes the effects of the available formats for Oracle ERP Cloud users.

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

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

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
- An appropriate notification template exists

For example, if the predefined notification template New Account Template is enabled for the default user category, then a notification is sent to the new user.

If you deselect this option, then you can send the notification later by running the Send User Name and Password Email Notifications process. The notification is sent to the user's work email. 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.

   Note: If you linked an existing user account, then any roles that were already assigned externally and manually to the account appear in the Roles section. When you click Autoprovision Roles, the user's entitlement to those roles is reviewed. If the user doesn't qualify for the roles based on the employment information entered so far, then their removal is requested.

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 selected 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**.

Enable Validation of Work Email for Users and Roles

You can enable validation of the email that you enter on the Manage Users task. When validation is enabled, a warning message appears if you enter a duplicate value. The message provides the name, the user name, or both of the email owner.

This warning enables you to enter a unique email before saving. Validation of the email on the Manage Users task is disabled by default. This topic explains how to enable validation of the email value on the Manage Users task.

Enable Email Validation

Follow these steps to enable validation using the profile option, PER_MANAGE_USERS_EMAIL_VALIDATION.

1. In the Setup and Maintenance work area, use the **Manage Administrator Profile Values** task.
2. On the Manage Administrator Profile Values page, enter **PER_MANAGE_USERS_EMAIL_VALIDATION** in the **Profile Option Code** field and click **Search**.
3. In the Profile Values section of the search results, enter **Y** in the **Profile Value** field.
4. Click **Save and Close**.

> **Note:** When validation of the work email is enabled, it only applies to the Manage Users task. It doesn't apply to user accounts that you manage on the Security Console.

Users Accounts

Manage Application Users

Once you create users and provision them with access to the application, there are various user management tasks you have to perform on an ongoing basis. Here are examples of some of the tasks you might have to do:

- Terminating user accounts when users leave the organization
- Acting as a proxy for users so you can troubleshoot issues

This chapter describes how to perform these and other use management tasks. But you can also use the file import functionality to perform user management tasks such as::

- Enabling or disabling user accounts

- Promoting, demoting, or transferring an employee

User Management Using Manage Users

ERP administrators can use the Manage Users task to manage user accounts when Oracle HCM Cloud service isn't being used. When Oracle HCM Cloud is being used, HR Specialists and Line Managers can manage user accounts with the Manage User Accounts task.

This topic describes how to update an application user account.

To access the user account page for a person:

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page. You can also search for the **Manage Users** task in the Setup and Maintenance 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 click the person's name. The **Edit User** page will open.

User Management Using Security Console

IT Security Managers can manage user accounts from the Security Console.

To access the User Account Details page for a person:

1. Select **Navigator** > **Tools** > **Security Console** to open the Security Console.
2. Click the **Users** tab.
3. Search for the user using one of the following:
    - First Name
    - Last Name
    - User Name
    - Email
4. Click on either the display name or user name link.

On the User Accounts page of the Security Console, IT Security Managers can:

- Create and manage user accounts. Typically, only accounts for implementation users are created and managed in this way.
- Delete the account of an implementation user, if required. User accounts of application users should not be deleted.
- Lock and unlock user accounts. Users can't sign in to locked accounts.
- Make user accounts active or inactive.
- Provision rules to users.
- Reset user passwords, provided that the Administrator can manually reset password option is selected for the relevant user category.

On the User Categories page of the Security Console, IT Security Managers can create and manage user categories. For any category, they can:

- Define the default format of user names.
- Set the password policy.

- Manage notifications.
- Add users to and remove users from the category.

Tip: Users can add roles, autoprovision roles, and copy their personal data to LDAP by selecting **Navigator** > **Me** > **Roles and Delegations**.

Change 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: When you change an existing user name, the user receives no automatic notification of the change. Therefore, you're recommended to send details of the updated user name to the user.

Reset Passwords

Passwords can only be reset using the User Account Details page in the Security Console. ERP administrators can't reset a user's password using the Manage Users task.

To reset a user's password:

1. Navigate to the User Account Details page in the Security Console, and search for the user as discussed in the User Management Using Security Console section.
2. Select **Actions** > **Reset Password**.
3. You have the option to either automatically generate a new password or manually change the password, provided that the Administrator can manually reset password option is selected for the relevant user category. If the option to manually change the password is available and you choose it, enter the new password in the **New Password** field and again in the **Confirm New Password** field. Then click **Reset Password**.

   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.

Change a User's Email Address

To change a user's email address:

1. Navigate to the User Account Details page in the Security Console, and search for the user as discussed in the User Management Using Security Console section.
2. Click on either the display name or user name link.
3. On the User Account Details page, click **Edit**.
4. On the Edit User Account page, edit the email address.

5. Click **Save and Close**.

Manage User Roles

You can manage user roles from both the Edit User page inside the Manage Users task or the Edit User Account page.

To add a role:

1. Click **Add Role**.

   The Add Role dialog box opens.
2. Search for the role that you want to add.
3. In the search results, select the role and click **OK**.

   If you're using the Manage Users task, the role appears in the Role Requests region with the status **Add Requested**. If you're using the Edit User Account page, the role appears in the Roles region
4. Click **Save**.

To remove a role from any section of this page:

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

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

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

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

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

Terminate User Accounts

This topic describes how you can terminate a user account when an employee leaves your enterprise. The process outlined in this topic applies if you're using Oracle ERP Cloud service only. If your enterprise also uses Oracle HCM Cloud service, then a different process

Manually Suspend User Accounts

When an employee leaves your enterprise, in most cases it's best practice to inactivate the user account. Inactivating the user's account prevents the user from being able to log in to the application.

To manually suspend a user account, ERP administrators follow these steps:

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.

   You can also search for the **Manage Users** task in the Setup and Maintenance work area.
2. Search for and select the user whose account you want to inactivate to open the Edit User page.

3. In the User Details section of the Edit User page, set the **Active** field to **Inactive**. You can reactivate the account by setting the **Active** value back to **Active**.
4. Click **Save and Close**.

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.

> **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.

Remove Roles from a User

Instead of inactivating a user account, you can remove some or all of the roles assigned to the user. You might want to do this if you want to keep some roles active. For example, maybe you want to keep the user account valid to allow the user access to specific pages you have created.

These are the steps to selectively remove roles from a user.

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page.

   You can also search for the **Manage Users** task in the Setup and Maintenance work area.
2. Search for and select the user whose roles you want to remove.

   The Edit User page for the user opens.
3. In the Current Roles section, select the role you want to remove, then click the **Remove** icon. Repeat this process for each role assigned to the user that you want to remove.
4. Click **Save and Close**.

Automatically Suspend User Accounts

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.

Users can acquire roles automatically at termination, if an appropriate role mapping exists. In this case, the user account remains active.

Related Topics

- User Account Maintenance Option

Link an Existing User Account to a Person Record

By default, when you create person records, user accounts are created automatically in your LDAP directory and linked to those person records. However, this automatic creation of user accounts can be disabled for the enterprise.

For example, you may have some other way of managing user accounts, or user accounts may already exist in your LDAP directory. In this case, you must link the existing user account manually to the person record. This topic explains how to link an existing user account to a person record in Oracle HCM Cloud. You must have access to the person record to perform this task.

Follow these steps:

1. Select **Navigator** > **My Team** > **Users and Roles** to open the Search Person page. You can also search for the **Manage Users** task in the Setup and Maintenance work area.
2. Search for and select the user whose user account you want to link. The **Edit User** page will open.
3. In the User Details section, click **Link User Account**.
4. In the Link User Account dialog box, search for and select the user name.

   The list contains only those user accounts that aren't already linked to an Oracle HCM Cloud person record.
5. Click **OK** to close the Link User Account dialog box.
6. Click **Save**.

Any roles that were already assigned externally and manually to the linked user account appear in the Current Roles section. If the user doesn't qualify for those roles, based on current employment information, then their removal is requested. The Role Requests section of the Manage Users task shows the roles for which the user qualifies. You can add roles, as appropriate, before clicking **Save**.

Get User Sign-in Sign-out Information

You can get the last seven days of user sign-in sign-out information using a setting available on the Add User Account page in Security Console. To view the setting, you must enable a profile option.

You can access the sign-in sign-out information through REST APIs. For more information, see the topic Sign In and Sign Out Audit REST Endpoints in *REST API for Common Features in Oracle Fusion Cloud Applications* on the Oracle Help Center.

Here's how you enable the profile option:

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search the following **Profile Option Code**:

   ASE_ADVANCED_USER_MANAGEMENT_SETTING
3. In the **Profile Value** drop-down list, select **Yes**.
4. Click Save and Close.

Note: The audit data is available for seven days.

The profile option is enabled. On the Add User Account page in Security Console, the setting to get user sign-in sign-out information appears now in the Advanced Information section.

On the Security Console, click **Users**. On the User Accounts page, click **Add User Account** and select **Enable Administration Access for Sign In-Sign Out Audit REST API**. You can also enable this option on the User Account Details Edit page.

FAQs on Creating and Managing Application Users

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.

What happens when I autoprovision roles for a user?

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

The user immediately:

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

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

Why is the user losing roles automatically?

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

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

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

You can see the roles that you want to assign, if the role satisfies all of the following conditions:

- A role mapping exists for the role. For more information on creating a role mapping, see the topic *Create a Role Mapping*.
- The Requestable option is selected for the role in the role mapping. For more information, see the topic *How do I provision HCM data roles to users?*.
- At least one of your assignments satisfies the role-mapping conditions.

What happens if I deprovision a role from a user?

The user loses the access to functions and data that the removed role was providing exclusively. The user becomes aware of the change when he or she next signs in.

If the user acquired the role automatically, then future updates to the user's assignments may mean that the user acquires the role again.

What happens if I edit a user name?

The updated user name is sent to your LDAP directory for processing when you click Save on the Manage User Account or Edit User page. The account status remains Active, and the user's roles and password are unaffected. As the user isn't notified

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.

10 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 to provision roles.

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

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

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

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

Attribute	Value
Department	Finance Department
Job	Sales Manager
HR Assignment Status	Active

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

Manual Provisioning of Roles to Users

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

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

For example, for the data role Training Team Leader, you could select the **Requestable** option and specify the conditions shown in this table.

Attribute	Value
Manager with Reports	Yes
HR Assignment Status	Active

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

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

Role Requests from Users

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

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

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

Attribute	Value
Department	Finance Department
System Person Type	Employee
HR Assignment Status	Active

Any user with at least one assignment that matches these conditions can request the role. Self-requested roles are defined as manually provisioned.

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

Role-Mapping Names

Role-mapping names must be unique in the enterprise. Devise a naming scheme that shows the scope of each role mapping. For example, the role mapping Autoprovisioned Roles Sales could include all roles provisioned automatically to workers in the sales department.

Related Topics

- Autoprovisioning
- Examples of Role Mappings

Create a Role Mapping

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

Sign in as IT Security Manager and follow these steps:

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

    The Create Role Mapping page opens.

Defining the Role-Mapping Conditions

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

Field	Value
Department	Finance Department
Job	Accounts Payable Supervisor
Location	Redwood Shores
System Person Type	Employee
HR Assignment Status	Active

Users must have at least one assignment that meets all these conditions.

Identifying the Roles

1. In the Associated Roles section, click **Add Row**.
2. In the **Role Name** field, search for and select the role that you're provisioning.

3. Select one or more of the role-provisioning options as listed in the following table:

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

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

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

   The **Delegation Allowed** option indicates whether users who have the role or can provision it to others can also delegate it. You can't change this value, which is part of the role definition. When adding roles to a role mapping, you can search for roles that allow delegation.
4. If appropriate, add more rows to the Associated Roles section and select provisioning options. The role-mapping conditions apply to all roles in this section.
5. Click **Save and Close**.

Applying Autoprovisioning

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

Role Provisioning and Deprovisioning

You must provision roles to users. Otherwise, they have no access to data or functions and can't perform application tasks. This topic explains how role mappings control role provisioning and deprovisioning.

Use the **Manage Role Provisioning Rules** or **Manage HCM Role Provisioning Rules** task to create role mappings.

Role Provisioning Methods

You can provision roles to users:

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

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

Role Types

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

Automatic Role Provisioning

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

Role Deprovisioning

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

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

Roles at Termination

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

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

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

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

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

Reversal of Termination

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

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

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

Date-Effective Changes to Assignments

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

Autoprovisioning

Autoprovisioning is the automatic allocation or removal of user roles. It occurs for individual users when you create or update assignments. You can also apply autoprovisioning explicitly for the enterprise using the Autoprovision Roles for All Users process.

Roles That Autoprovisioning Affects

Autoprovisioning applies only to roles that have the **Autoprovision** option enabled in a role mapping.

It doesn't apply to roles without the **Autoprovision** option enabled.

The Autoprovision Roles for All Users Process

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

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

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

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

When to Run the Process

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

Options for the Process

When processing a large number of requests, you can enable bulk mode for this process to improve performance. In the bulk mode, the process groups all users for the same role into one request, and assigns multiple users to single role at once. In the default non-bulk mode, one user is assigned to a role at a time.

To enable bulk mode, follow these steps:

1. In the Setup and Maintenance work area, search and open the task **Manage Profile Options**.
2. In the **Search Results** section, click the + (New) icon.
3. On the **Create Profile Option** page, enter the following values:
    - Profile Option Code = PER_AUTO_PROVISION_ROLES_ENABLE_BULK
    - Profile Display Name = PER_AUTO_PROVISION_ROLES_ENABLE_BULK
    - Application = Global Human Resources
    - Module = Users
    - Start Date = <Today's date>

    Click **Save and Close**.
4. On the **Manage Profile Options** page, select the **Enabled** and **Updateable** check boxes for Site Level. Click Save and Close.
5. In the Setup and Maintenance work area, search and open the **Manage Administrator Profile Values** task.
6. Search for the profile option code PER_AUTO_PROVISION_ROLES_ENABLE_BULK. In the Profile Value text box, enter 'Y'. Note that this value is for one-time use, and you need to reset the value again for the next run of the process. Click **Save and Close**.

You can enable multithreading for the process by setting the profile option ORA_PER_AUTO_PROVISION_ROLES_ENABLE_MULTITHREADING to 'Y'. This creates child jobs, which help in improving the performance.

For more information, see the topic Best Practices for User and Role Provisioning in HCM.

Autoprovisioning for Individual Users

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

Related Topics

- What happens when I autoprovision roles for a user?
- Schedule the Send Pending LDAP Requests Process
- Best Practices for User and Role Provisioning in HCM

Roles That Give Workflow Administrators Access

Workflow administrators for a specific product family need a predefined, family-specific workflow role to access tasks and manage submitted tasks for that family. To configure workflow tasks, they also need BPM Workflow System Admin Role (BPMWorkflowAdmin).

For example, administrators with the family-specific roles can do things like reassign submitted tasks, but they also need BPM Workflow System Admin Role to define approval rules. Other than the family-specific workflow roles, there's

also BPM Workflow All Domains Administrator Role (BPMWorkflowAllDomainsAdmin). This gives administrators access to all product families. Assign to the administrators a role that contains the workflow roles appropriate for their needs.

Workflow Roles

Here are the roles that give access to workflow administration.

Product Family	Role Name	Role Code
All	BPM Workflow All Domains Administrator Role	BPMWorkflowAllDomainsAdmin
All	BPM Workflow System Admin Role	BPMWorkflowAdmin
Financials	BPM Workflow Financials Administrator	BPMWorkflowFINAdmin
Higher Education	BPM Workflow Higher Education Administrator	BPMWorkflowHEDAdmin
Human Capital Management	BPM Workflow Human Capital Management	BPMWorkflowHCMAdmin
Incentive Compensation	BPM Workflow Incentive Compensation Administrator	BPMWorkflowOICAdmin
Procurement	BPM Workflow Procurement Administrator	BPMWorkflowPRCAdmin
Project Management	BPM Workflow Project Administrator	BPMWorkflowPRJAdmin
Sales	BPM Workflow Customer Relationship Management Administrator	BPMWorkflowCRMAdmin
Supply Chain Management	BPM Workflow Supply Chain Administrator	BPMWorkflowSCMAdmin

Things to Know About the Roles

Here are some things to know about how these workflow roles should be used and what the roles let administrators do.

- If your administrators manage workflow for multiple product families, you should give those users a custom role with the appropriate family-specific workflow roles added.
- If your administrators manage workflow for all product families, give them a custom role with BPM Workflow All Domains Administrator Role.

  > **CAUTION:** Assign BPM Workflow All Domains Administrator Role only if your administrators really do need access to workflow tasks from all product families. For access in multiple product families, but not all, use the workflow roles for the corresponding families instead.

- All administrators can see to-do tasks, no matter which role they have for workflow administration.

- Only administrators with either BPM Workflow All Domains Administrator Role or BPM Workflow System Admin Role would have Skip Current Assignment as an action to take on workflow tasks.

Related Topics

- Role Copying or Editing
- Assign Roles to an Existing User
- Edit Job Role and Abstract Role
- Actions and Statuses for Workflow Tasks
- Create Roles in the Security Console

Manage Roles in Custom OAuth Client Applications Using Application Extensions Page

You can manage user assignments and role assignments for platform applications and custom applications respectively from the Security Console.

In environments provisioned with an Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain, the Security Console displays the Application Extensions page. On this page, you can view all the available Platform Applications and Custom OAuth Client Applications.

- Platform Applications are provisioned by default in an OCI IAM identity domain environment. The roles assigned to these applications are the ones created in Oracle Fusion Cloud Applications. You can add or remove users to roles that are associated with a platform application.
- Custom OAuth Client Applications are those that the users create in an OCI IAM identity domain. The roles assigned to these applications have permission groups enabled. You can add or remove roles to a custom application.

Add User to Role Associated with Platform Application

1. On the **Application Extensions** page, in the Platform Applications section, click an application.
2. Click **Roles** (These roles are application-specific service roles available in the OCI IAM identity domain).
3. From the roles that are listed, click a role to which you want to add users to.
4. Click **Add** to search for and add users to the role.
5. Click **Done**.

Add Role to Custom OAuth Client Application

1. On the **Application Extensions** page, in the Custom OAuth Client Applications section, click an application.
2. Click **Roles** (These roles are permission groups enabled roles).
3. On the Roles page, click **Add** to search for and add roles to the application.
4. Click **Done**.

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.

Provisioning Method	Meaning
Automatic	The user qualifies for the role automatically based on his or her assignment attribute values.
Manual	Either another user assigned the role to the user, or the user requested the role.
External	The user acquired the role outside Oracle Applications Cloud.

How do I provision roles to users?

Use the following tasks to provision roles to users.

- Manage Users
- Provision Roles to Implementation Users

The Manage Users task is available in Oracle Fusion Cloud HCM, Oracle CX Sales, Oracle ERP Cloud, Oracle SCM Cloud, and Oracle Fusion Suppliers.

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

Related Topics

- Role Provisioning and Deprovisioning

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 can't change predefined roles to add or remove duties. In the Security Console, you can identify predefined roles by the ORA_ prefix in the Role Code field. Create copies and update the copies instead.

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

11 Data Assignments

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's 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's 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.

Product	Security Context
Oracle Fusion Cloud Financials	Business Unit Data Access Set Ledger Asset Book Control Budget Intercompany Organization Reference Data Set Legal Entity
Oracle Fusion Cloud Supply Chain Management	Inventory Organization Reference Data Set Cost Organization Inventory Organization Manufacturing Plant
Oracle Fusion Cloud Procurement	Business Unit
Oracle Fusion Cloud Project Portfolio Management	Project Organization Classification

Product	Security Context
Oracle Fusion Cloud Incentive Compensation	Business Unit

Assigning Data Access

Assigning data access to users is a three step process:

1. Create users using one of the following:
    - Manage Users task in Oracle Fusion Cloud 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 Cloud 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.

Related Topics

- Assign Data Access to Users

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 only one user at a time.

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

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

Prerequisites

Before you can complete this task, you must:

1. Create users and specify the user attributes such as a user name, assigned business unit, legal employer, department, job, position, grade and location, and so on. To create users, use the Manage Users task in the Functional Setup Manager or the Create User page. If you're implementing Oracle Fusion Cloud 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 Cloud 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.

Related Topics

- Data Access

Revoke Data Access from Users

Use the Manage Data Access for Users page to revoke data access from users.

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 the **Users with Data Access** option.
4. Search for existing data access assignments you want to revoke by entering either a user name or a role name.
5. Click **Search**. The Search Results region displays data access assignments that match the search criteria.
6. Select the data access assignment you wish to revoke.
7. On the **Actions** menu, click **Revoke Data Access Assignments**.
   The selected data access assignment is revoked.

Revoking Data Access from Users Using a Spreadsheet

On the Manage Data Access for Users page, you can revoke access of multiple 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 the **Authorize Data Access** button which would generate the security data access template spreadsheet. Save the spreadsheet and open it with Microsoft Excel.
4. To revoke a data access assignment, specify the assignment by providing the **Security Context**, **Security Context Value**, **User Name**, and **Role** in the spreadsheet, then select the value **No** in the **Active** column. Create a new row for each data access assignment you wish to revoke.
5. Click the **Upload** button when you have entered all the assignments you need to revoke in the spreadsheet.
   - If the status of the upload is Successful, it means the data access assignment is successfully revoked.
   - If the upload status is Failed, check the details in your upload file, correct any errors, and upload the file again.
   - If you see the following message, then the assignment for the entered combination of Security Context, Security Context Value, User Name, and Role can't be found or is no longer active:
     “This assignment doesn't exist. Enter an active assignment.”

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:

Role	Data Security Context	Value
Accounts Payable Manager	Business Unit	US West
Accounts Payable Supervisor	Business Unit	US West
Accounts Payable Specialist	Business Unit	US West
Accounts Receivable Manager	Business Unit	US West
Accounts Receivable Specialist	Business Unit	US West
Financial Analyst	Data Access Set	US-Corporate
General Accountant	Data Access Set	US-Corporate
General Accounting Manager	Data Access Set	US-Corporate

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.

Field	Value
Department	Finance Department
Location	Seattle
System Person Type	Employee
HR Assignment Status	Active

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 **Autoprovision 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.

Autoprovision Roles for All Users Process

The Autoprovision 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.

Configure Advanced Implicit Data Security for Non-Discretionary Access

In Oracle Fusion Cloud ERP, you can use the Manage Data Access for Users page to control who can see specific data. You do it by explicit data assignment. However, many predefined self-service roles include implicit data security assignments for non-discretionary access. Some job roles, like Procurement Requester, come with built-in access to data for the part of the business that they work in. This implicit data management has many benefits. Let's look at why implicit data management is useful for an organization.

Sometimes, you may need to give many people the same access to certain data, especially for self-service roles like Procurement Requester. This role gives people access to data for the business unit they work in by default. For example, someone who works in the US business unit will be able to manage requisitions in that unit when given the Procurement Requester role. However, if they need access to data in other business units, you will have to specifically give them that access on the Manage Data Access for Users page. If many people in the same business unit need the same access to another business unit, it might be easier to set up a new data security policy instead of giving everyone access individually. For example, if all people in the US business unit need access to the Canada business unit, it is more efficient to set up a new policy rather than giving everyone access individually.

Advanced Implicit Data Security for Non-Discretionary Access helps you configure implicit data security. Let's look at an example of setting up implicit data security for Vision Corporation. Vision Corporation is headquartered in Germany with operations in Spain and Italy. The operations in each country are set up as their own business units – Vision Germany, Vision Italy, and Vision Spain.

In this example, the employees in Germany can manage requisitions for all three business units, but employees in Italy and Spain can only manage requisitions for their own business units.

If the business unit on primary worker assignment is:	Users can manage requisitions in:
Vision Germany	Vision Germany Vision Italy Vision Spain
Vision Italy	Vision Italy
Vision Spain	Vision Spain

Suppose that George is an employee from the German office with the predefined Procurement Requester role that grants him access to manage requisitions in Vision Germany. Similarly, Braun is an employee from the Spain office, so the predefined Procurement Requester role grants her access to manage requisitions in Vision Spain. Now, to configure additional data security policies to allow non-discretionary access for users in Vision Germany, you must configure a new database resource condition and then configure a new data security policy.

Configure New Database Resource Condition

To set up a new data security policy that lets other business units access your data, you need to create a database resource condition, also called an instance set. This will allow you the access you need.

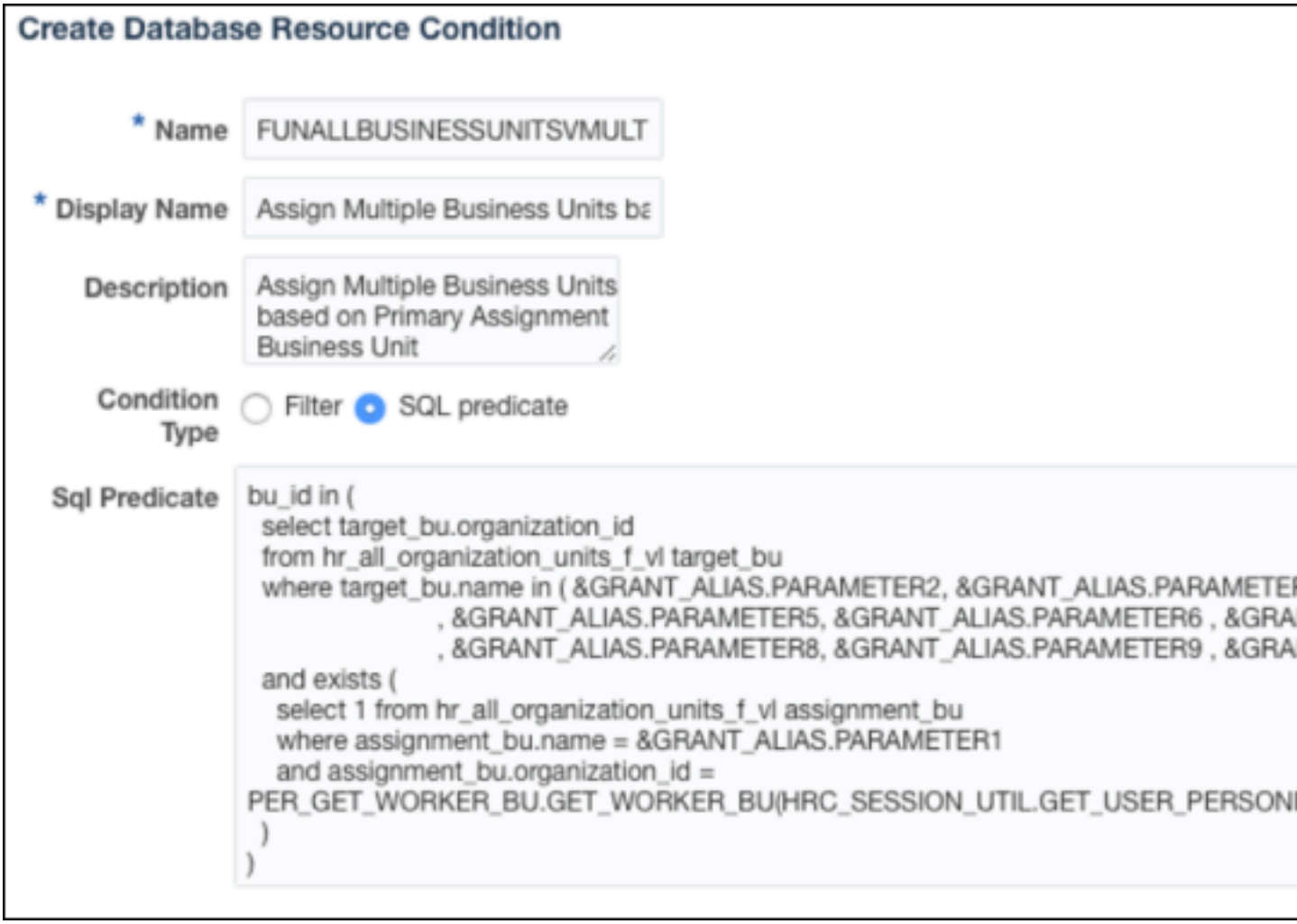
To create the condition, use a specific kind of statement called a predicate.

```
BU_ID IN (
SELECT TARGET_BU.ORGANIZATION_ID
FROM HR_ALL_ORGANIZATION_UNITS_F_VL TARGET_BU
WHERE TARGET_BU.NAME IN
( &GRANT_ALIAS.PARAMETER2, &GRANT_ALIAS.PARAMETER3, &GRANT_ALIAS.PARAMETER4
, &GRANT_ALIAS.PARAMETER5, &GRANT_ALIAS.PARAMETER6, &GRANT_ALIAS.PARAMETER7
, &GRANT_ALIAS.PARAMETER8, &GRANT_ALIAS.PARAMETER9, &GRANT_ALIAS.PARAMETER10 )
AND EXISTS (
SELECT 1 FROM HR_ALL_ORGANIZATION_UNITS_F_VL ASSIGNMENT_BU
WHERE ASSIGNMENT_BU.NAME = &GRANT_ALIAS.PARAMETER1
AND ASSIGNMENT_BU.ORGANIZATION_ID = PER_GET_WORKER_BU.GET_WORKER_BU(HRC_SESSION_UTIL.GET_USER_PERSONID ,
 NULL)
)
)
```

This predicate is a way to use different values for the primary business unit and the desired target business units. The primary business unit's value is in PARAMETER1, and the desired target business unit's values are in PARAMETER2 through PARAMETER10. Use the Security Console to set up conditions for the database. Only the IT Security Manager can use the Security Console, which you can find in the Navigator menu.

To configure a new database resource condition:

1. Navigate to the Security Console.
2. On the Administration tab, click **Manage Database Resources**.
3. Search a database resource. In this example, enter **Business Unit**, and select **Edit**.
4. On the Condition tab, click **Add**.
5. In the Name field, enter a familiar name that you can distinguish from the predefined ones.
6. In the Display Name field, enter a display name.
7. In the Description field, enter a description of the condition.
8. In the Condition Type field, select **SQL predicate** and then enter the predicate in the SQL predicate field as shown in the figure.



9. Click **Save**.
10. Click **Submit** to save your changes. The new condition is ready for use.

If you don't need to reuse the condition for different scenarios, you can create a simpler condition with hardcoded values as shown below:

```
BU_ID IN (
SELECT TARGET_BU.ORGANIZATION_ID
FROM HR_ALL_ORGANIZATION_UNITS_F_VL TARGET_BU
WHERE TARGET_BU.NAME IN ( 'Vision Italy' , 'Vision Spain' )
AND EXISTS (
SELECT 1 FROM HR_ALL_ORGANIZATION_UNITS_F_VL ASSIGNMENT_BU
WHERE ASSIGNMENT_BU.NAME = 'Vision Germany'
AND ASSIGNMENT_BU.ORGANIZATION_ID = PER_GET_WORKER_BU.GET_WORKER_BU(HRC_SESSION_UTIL.GET_USER_PERSONID ,
 NULL)
)
)
```

You can make the predicate even simpler and faster if you already know the internal ID numbers for the business units. That way, you don't have to look them up every time in the runtime code.

```
BU_ID IN ( 1016 /* Vision Spain */ , 1017 /* Vision Italy */ )
```

```
AND PER_GET_WORKER_BU.GET_WORKER_BU(HRC_SESSION_UTIL.GET_USER_PERSONID , NULL) = 911 /* Vision Germany */
```

Configure New Data Security Policy

You can set up new data security rules for both predefined roles and roles you create yourself. In this example, we're making a rule for the predefined role of the Procurement Requester.

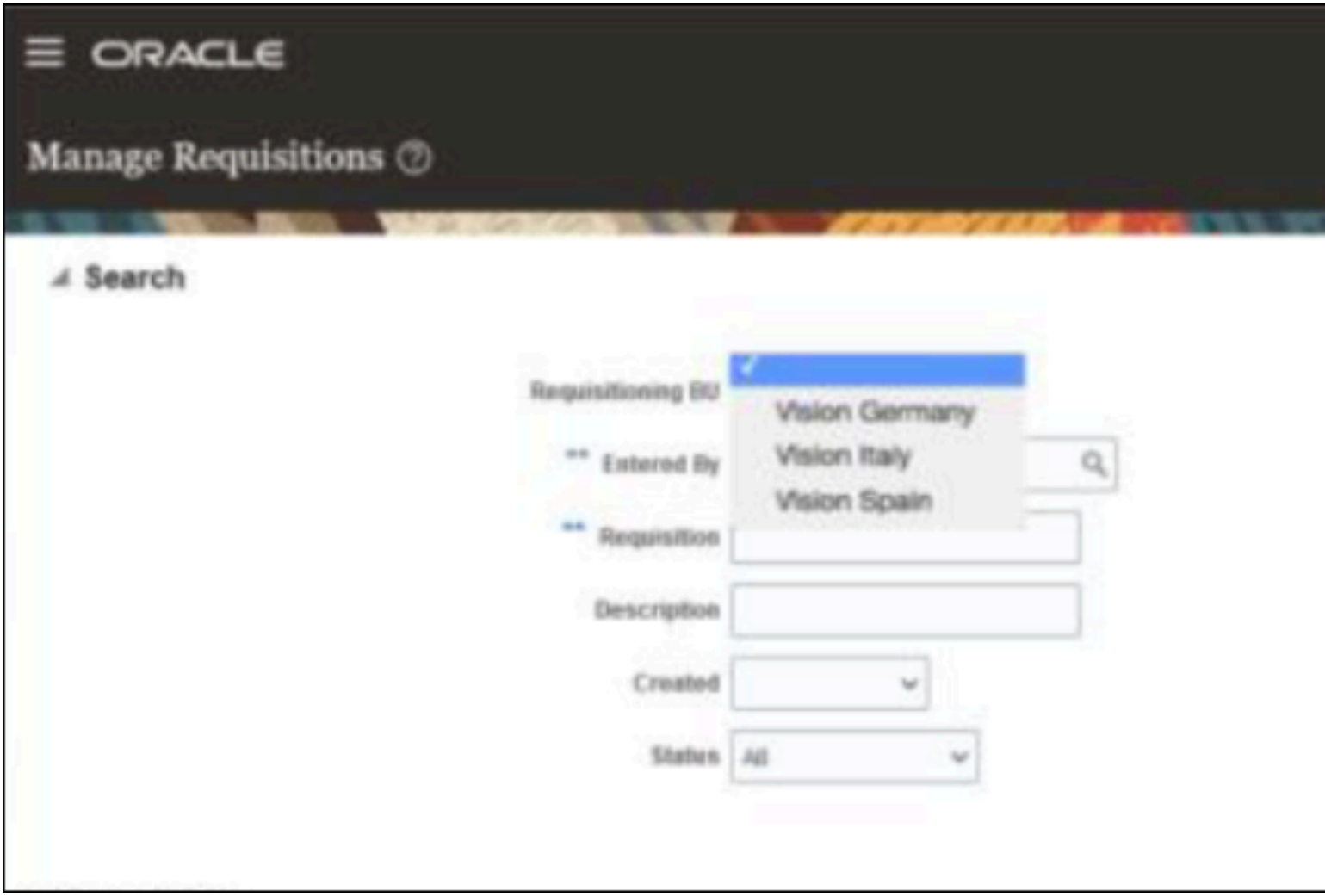
To configure a new data security policy:

1. On the Roles tab of the Security Console, search for the role that you want to configure.
2. In the search results, click the down arrow for the selected role and select **Edit Rol**e.
3. Go to **Data Security Policies**.
4. Click **Create Data Security**. In this example, you must create a new data security policy for the **Business Unit** resource and the **Manage Requisition** action, using the condition you created.
5. In the Database Resource field, select **Business Unit**.
6. In the Data Set field, select **Select by instance set**.
7. In the Select data by condition field, select the condition that you created.
8. In the PARAMETER1 field, enter the primary worker assignment business unit that's driving the data assignment.
9. In PARAMETER2 through PARAMETER10, enter the target business units to be assigned when the primary worker assignment business unit for a user matches the value in PARAMETER1. You don't have to fill in all nine parameters. In this example, in PARAMETER1, you should enter Vision Germany, and in PARAMETER2 and PARAMETER3, you should enter Vision Italy and Vision Spain.

   Note: If you choose to use simple predicates with hardcoded values when setting up the database resource condition, you don't have to enter any parameter values here. The parameter values will be hidden.
10. From the Actions drop-down list, select **Manage Requisition**.
11. Click **OK**.
12. Go to the Summary and Impact Report step to review the changes.
13. Click **Save and Close**.

Verify New Data Security Policy

You can verify the new data security policy that you configured. Notice that users from Vision Germany can now manage requisitions in Vision Italy and Vision Spain.



FAQs on Assigning Data Access to Application Users

How can I autoprovision 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 autoprovision 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 autoprovision 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.

12 Reporting on Application Users and Roles

Run the User Details System Extract Report

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

To run the report:

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

Related Topics

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

User Details System Extract Report Parameters

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

Parameters

User Population

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

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

From Date

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

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

To Date

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

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

User Active Status

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

Value	Description
A	Include users with active accounts.
I	Include users with inactive accounts.
All	Include both active and inactive user accounts.

Related Topics

- Run the User Details System Extract Report
- User Details System Extract Report

User Details System Extract Report

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

Run the report in the Reports and Analytics work area.

Report Results

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

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

The information in the extract varies with the account type.

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

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

Department
The department from the primary assignment.

Worker Type
The worker type from the user's primary work relationship.

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

Hire Date
The enterprise hire date.

Role Name
A list of roles currently provisioned to workers whose work relationships are all terminated. This value appears for active user accounts only.

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

Organizations
A resource group.

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

Managers
The manager of a resource group.

Start Date
The account's start date.

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

Related Topics

- Run the User Details System Extract Report
- User Details System Extract Report Parameters

Person User Information Reports

This topic describes the Person User Dashboard and Person User Information Oracle Business Intelligence Publisher reports. Use these reports to extract the history of a specified Oracle Fusion Cloud HCM user account. To run the reports, you must inherit the ORA_PER_MANAGE_USER_AND_ROLES_DUTY_OBI duty role.

Several predefined job roles, including IT Security Manager and Human Resource Specialist, inherit this duty role. To run the reports:

1. Open the Reports and Analytics work area.
2. Select **All Folders** > **Shared Folders** > **Human Capital Management** > **Workforce Management** > **Human Resources Dashboard**.

Both reports appear in the Human Resources Dashboard folder.

Running the Person User Information Reports

Use the Person User Dashboard report to display user account information, specifically the person ID, of a specified user. Follow these steps:

1. Click the **Person User Dashboard** entry.
2. On the Person User Summary page, complete the parameters shown in this table to filter the report and click **Apply**.

Parameter	Description
Display Name	The user's display name, for example, John Gorman
Last Name	The user's last name, for example, Gorman
Start Date	The user's start date. Users with start dates equal to or later than this date may appear in the report.

3. When you have identified the user of interest, copy the person ID from the Person User Information table in the report. You use this person ID in the Person User Information report.

Use the Person User Information report to display the detailed history of a specified user account. Follow these steps:

1. In the Human Resources Dashboard folder, click **Person User Information**.
2. On the Person User Detail page, complete either or both of the parameters shown in this table and click **Apply**:

Parameter	Description
Start Date	The user's start date. Users with start dates equal to or later than this date may appear in the report.
Person ID	The person ID copied from the Person User Dashboard report.

The report output includes:

- Person information
- User history
- Assigned roles and details of the associated role mappings

- Role delegation details
- LDAP request details
- Work relationship and assignment information

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

Related Topics

- User History Report

User History Report

This topic describes the User History report, which extracts and formats the history of a specified Oracle Fusion Cloud HCM user account. Oracle Support may ask you to run this report to help diagnose user-related errors.

To run the report, you must inherit the ORA_PER_MANAGE_USER_AND_ROLES_DUTY_OBI (Manage Users) duty role. Several predefined job roles, including IT Security Manager and Human Resource Specialist, inherit this duty role. Follow these steps to run the report.

1. Select **Navigator** > **My Team** > **Users and Roles**.
2. On the Search Person page, search for the person of interest.
3. In the search results, click the person name to open the Edit User page.
4. On the Edit User page, click **Print User History**. In the User History dialog box, you can review the report.

   You can either print the report or download a PDF file by clicking relevant icons in the User History dialog box.
5. Click **Cancel** to close the User History dialog box.

> **Tip:** You don't have to view the report. You can select **Print User History** > **Download** to download the PDF file. The file name is in the format **<person ID>_UserHistory.pdf**.

This report is identical to the Person User Information report, which authorized users can run in the Reports and Analytics work area.

Report Contents

For the selected user, the report includes:

- Person information
- User history
- Provisioned roles and details of any associated role mappings
- Role delegation details
- LDAP request details
- Work relationship and assignment information

View Role Information Using Security Dashboard

As an IT Security Manager, you can use the Security Dashboard to get a snapshot of the security roles and how those roles are provisioned in the Oracle Cloud Applications.

The information is sorted by role category and you can view details such as data security policy, function security policy, and users associated with a role. You can also perform a reverse search on a data security policy or a function security policy and view the associated roles.

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

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

Here are the steps to view the Security Dashboard:

1. In the Reports and Analytics work area, click **Browse Catalog**.
2. On the Oracle BI page, open **Shared Folders** > **Security** > **Transaction Analysis Samples** > **Security Dashboard**.

   All pages of the dashboard are listed.
3. To view the Role Category Overview page, click **Open**.

   The page displays the number of roles in each role category in both tabular and graphical formats.
4. In the **Number of Roles** column, click the numeral value to view the role-related details.
5. Click **Role Overview** to view the role-specific information in the Role Dashboard.

LDAP Request Information Reports

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

To run the reports:

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

Both reports appear in the Human Resources Dashboard folder.

Running the LDAP Request Information Reports

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

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

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

The report output includes:

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

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

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

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

Parameter	Description
Within the Last N Days	Enter a number of days. The report includes LDAP requests updated within the specified period.

Parameter	Description
Request Type	Select an LDAP request type. The value can be one of Create, Update, Suspend, Activate, UserRoles, Terminate, and All.
Request Status	Select an LDAP request status. The value can be one of Complete, Faulted, In Progress, Request, Part Complete, Suppressed, Rejected, Consolidated, and All.

The report includes a table showing for each request:

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

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

Inactive Users Report

Scheduling the Import User Login History process to run daily is a prerequisite to get a valid report about inactive users.

The Import User Login History process imports information that the Inactive Users Report process uses to identify inactive users. The Inactive Users Report process helps to identify users who haven't signed in for a specified period.

Before you run the inactive users report for a certain period, make sure that the Import User Login History data exists for that period. It's important to know when the user last signed in. That's why it's recommended to always run the Import User Login History process for a longer duration to offer greater flexibility with the date range.

1. In the Scheduled Processes work area, click **Schedule New Process**.
2. Search for and select the **Inactive Users Report** process.
3. In the Process Details dialog box, set parameters to identify one or more users.
4. Click **Submit**.

Inactive Users Report Parameters

All parameters except Days Since Last Activity are optional.

User Name Begins With

Enter one or more characters.

First Name Begins With

Enter one or more characters.

Last Name Begins With

Enter one or more characters.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Days Since Last Activity

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

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

Last Activity Start Date

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

Last Activity End Date

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

Viewing the Report

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

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

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

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

Related Topics

- Schedule the Import User Login History Process

User and Role Access Audit Report

The User and Role Access Audit Report provides details of the function and data security privileges granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console.

This report is based on data in the Applications Security tables, which you populate by running the **Import User and Role Application Security Data** process. To run the User and Role Access Audit Report:

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

Note: Only the roles at the top of a role hierarchy are included in the Role Name column of the All roles report. If you want to review a role that is lower down the role hierarchy, then apply a filter for the role in which you're interested, to the Inherited Role Hierarchy column.

User and Role Access Audit Report Parameters

Population Type

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

- All roles
- Multiple users
- Role name
- User name

User Name

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

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

Role Name

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

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

From User Name Starting With

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

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

To User Name Starting With

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

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

User Role Name Starts With

Enter one or more characters from the start of a role name.

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

Data Security Policies

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

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

Debug

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

Viewing the Report Results

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

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

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

Report Type	File Prefix
User name	USER_NAME
Role name	ROLE_NAME
Multiple users	MULTIPLE_USERS
All roles	ALL_ROLES

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

Report Type	File Suffix	File Format	File Contents
Any	DataSec	CSV	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when **Data Security Policies** is selected.

Report Type	File Suffix	File Format	File Contents
			Note: Extract the data security policies only when necessary, as generating this report is time consuming.
Any	Hierarchical	CSV	Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.
• **Multiple users** • **All roles**	CSV	CSV	Functional security policies in a comma-separated, tabular format.

The process also produces a .zip file containing a diagnostic log.

For example, if you report on a job role at 13.30 on 17 December 2015 with process ID 201547 and the **Data Security Policies** option selected, then the report files are:

- **ROLE_NAME_201547_12-17-2015_13-30-00_DataSec.zip**
- **ROLE_NAME_201547_12-17-2015_13-30-00_Hierarchical.zip**
- **Diagnostic.zip**

User Role Membership Report

The User Role Membership Report lists role memberships for specified users.

To run the report process:

1. Open the Scheduled Processes work area.
2. Search for and select the **User Role Membership Report** process.

User Role Membership Report Parameters

You can specify any combination of the following parameters to identify the users whose role memberships are to appear in the report.

> **Note:** The report might take a while to complete if you run it for all users, depending on the number of users and their roles.

User Name Begins With

Enter one or more characters of the user name.

First Name Begins With

Enter one or more characters from the user's first name.

Last Name Begins With

Enter one or more characters from the user's last name.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Viewing the Report

The process produces a **UserRoleMemberships_processID_CSV.zip** file and a **Diagnostics_processID.zip** file. The **UserRoleMemberships_processID_CSV.zip** file contains the report output in CSV format. The report shows the parameters that you specified, followed by the user details for each user in the specified population. The user details include the user name, first and last names, user status, department, location, and role memberships.

The following table lists a brief description of these columns:

Column Name	Description
User Name	User ID assigned to the user.
First Name	First name of the user.
Last Name	Last name of the user.
LDAP User	Indicates whether the user exists in the Identity Store.
Department	Department of the user.
Location	Location of the user.
Policy Stripe	The policy store's application stripe where the user to role membership exists.
Assigned Role Name	Role code of the role assigned to the user.
Assigned Role Display Name	Role display name of the role assigned to the user.
Assigned Role Description	Description of the role assigned to the user.

Tip: First Name, Last Name, Department, and Location column values are applicable only to users that are linked to a person/worker.

User and Role Access Audit Report

The User and Role Access Audit Report provides details of the function and data security privileges granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console.

This report is based on data in the Applications Security tables, which you populate by running the **Import User and Role Application Security Data** process. To run the User and Role Access Audit Report:

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

Note: Only the roles at the top of a role hierarchy are included in the Role Name column of the All roles report. If you want to review a role that is lower down the role hierarchy, then apply a filter for the role in which you're interested, to the Inherited Role Hierarchy column.

User and Role Access Audit Report Parameters

Population Type

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

- All roles
- Multiple users
- Role name
- User name

User Name

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

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

Role Name

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

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

From User Name Starting With

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

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

To User Name Starting With

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

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

User Role Name Starts With

Enter one or more characters from the start of a role name.

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

Data Security Policies

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

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

Debug

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

Viewing the Report Results

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

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

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

Report Type	File Prefix
User name	USER_NAME
Role name	ROLE_NAME
Multiple users	MULTIPLE_USERS
All roles	ALL_ROLES

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

Report Type	File Suffix	File Format	File Contents
Any	DataSec	CSV	Data security policies. The .zip file contains one file for all users or roles. The data security policies file is generated only when **Data Security Policies** is selected.

Report Type	File Suffix	File Format	File Contents
			Note: Extract the data security policies only when necessary, as generating this report is time consuming.
Any	Hierarchical	CSV	Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.
• **Multiple users** • **All roles**	CSV	CSV	Functional security policies in a comma-separated, tabular format.

The process also produces a .zip file containing a diagnostic log.

For example, if you report on a job role at 13.30 on 17 December 2015 with process ID 201547 and the **Data Security Policies** option selected, then the report files are:

- **ROLE_NAME_201547_12-17-2015_13-30-00_DataSec.zip**
- **ROLE_NAME_201547_12-17-2015_13-30-00_Hierarchical.zip**
- **Diagnostic.zip**

User Password Changes Audit Report

This report identifies users whose passwords were changed in a specified period. You must have the ASE_USER_PASSWORD_CHANGES_AUDIT_REPORT_PRIV function security privilege to run this report. The predefined IT Security Manager job role has this privilege by default.

To run the User Password Changes Audit Report:

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

User Password Changes Audit Report Parameters

Search Type

Specify whether the report is for all users, a single, named user, or a subset of users identified by a name pattern that you specify.

User Name

Search for and select the user on whom you want to report. This field is enabled only when **Search Type** is set to **Single user**.

User Name Pattern

Enter one or more characters that appear in the user names on which you want to report. For example, you could report on all users whose user names begin with the characters **SAL** by entering **SAL%**. This field is enabled only when **Search Type** is set to **User name** pattern.

Start Date

Select the start date of the period during which password changes occurred. Changes made before this date don't appear in the report.

To Date

Select the end date of the period during which password changes occurred. Changes made after this date don't appear in the report.

Sort By

Specify how the report output is sorted. The report can be organized by either user name or the date when the password was changed.

Viewing the Report Results

The report produces these files:

- **UserPasswordUpdateReport.csv**
- **UserPasswordUpdateReport.xml**
- **Diagnostics_[process ID].log**

For each user whose password changed in the specified period, the report includes:

- The user name.
- The first and last names of the user.
- The user name of the person who changed the password.
- How the password was changed:
    - ADMIN means that the change was made for the user by a line manager or the IT Security manager, for example.
    - SELF_SERVICE means that the user made the change by setting preferences or requesting a password reset, for example.
    - FORGOT_PASSWORD means that the user clicked the **Forgot Password** link when signing in.
    - REST_API means that the change was made for the user by SCIM REST APIs.
- The date and time of the change. The format of date and time of the change is "dd/MM/yyyy HH:mm:ss".

View Locked Users and Unlock Users

A user gets locked in the application on entering incorrect password for multiple times. The locked users report provides the list of locked users for both these scenarios.

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

View Locked Users

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

   The spreadsheet shows the list of users who are locked.

The Locked Users spreadsheet contains the following two tabs:

- LOCKED_USERS_<Request ID> - 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_<Request ID> - 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 for Reporting on Application Users and Roles

Can I extract details of all Oracle Fusion Applications users?

Yes. The Oracle BI Publisher report User Details System Extract provides details of user accounts. For example, you can produce a report showing all user accounts, inactive user accounts, or accounts created between specified dates.

To run the report, you need a data role that provides view-all access to person records for the Human Capital Management Application Administrator job role.

Related Topics

- User Details System Extract Report

How can I find out which roles a user has?

Search for and select the user on the Roles tab of the Security Console. In the visualization area, you can see the user's role hierarchy in tabular or graphical format.

Alternatively, you can run the User Role Membership Report for one or more users.

13 Location Based Access

Overview of Location-Based Access

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

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

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

What Happens When You Enable Location-Based Access

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

Prerequisite

To make sure that an administrator can regain access to Oracle Applications Cloud if an accidental account lock out occurs, the administrator must have the following settings configured:

- A valid email
- The IT Security Manager role
- Email notifications are enabled

Related Topics

- How Location-Based Access Works
- Enable and Disable Location-Based Access

How Location-Based Access Works

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

Scenarios

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

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

Scenario	Impact on User Access
You disable location-based access.	All users signing into the application from their respective computers continue to have the same level of access as they had earlier.
You enable location-based access and register few IP addresses, but don't grant public access to any role.	• Users who sign into the application from the registered IP addresses have access to their tasks as usual. • Users signing in from unregistered IP addresses can access only the generic tasks that aren't tied to any particular role.
You enable location-based access, register a few IP addresses, and grant public access to certain roles.	• Users signing in from the registered IP addresses have complete access. • Users signing in from unregistered IP addresses can't access any role-based tasks unless you grant public access to those roles. If you have made a role public, users can access all the tasks tied to that role.
You enable location-based access, but don't register any valid IP address, and don't grant public access to any role.	Users can sign in with valid credentials but can access only the generic tasks that aren't assigned to a specific role. **CAUTION:** Try and avoid this scenario. Register at least one valid IP address and grant public access (access from all IP addresses) to IT Security Manager role when you enable location-based access.

Related Topics

- How can I make a role public?
- How can I ensure that I always have access to the Security Console?

Enable and Disable Location-Based Access

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

Before You Start

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

- Set up a valid email address. When required, the location-based access control reset or recovery notification is sent to that email address.

- Add yourself to the user category for which the notification template **ORA Administration Activity Request Template** is enabled.
- Keep the list of valid IP addresses ready.

Enable Location-Based Access

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

   > **Note:** You can enter the IP address (IPv4 only) range suffix only up to 32 in the **IP Address Allowlist** text box. For example, 168.1.192.0/32 to 168.1.192.32/32.

   > **Tip:** Your computer's IP address appears on the page. Add that IP address to the list so that your access to the application remains unaffected when you sign in from that computer.

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

After you enable location-based access, make the IT Security Manager's role public to access Security Console even from an unregistered IP address.

Disable Location-Based Access

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

Related Topics

- What is allowlisting?
- Why can't I see the Location Based Access tab on the Administration page?

FAQs on Location Based Access

What is allowlisting?

Allowlisting is the process of granting trusted entities access to data or applications. When you enable location-based access and register the IP addresses of computers, you're storing those IP addresses as trusted points of access.

You can include IP Addresses of all computers hosting cloud applications that require access to Oracle Applications Cloud. In other words, you're allowlisting those IP addresses. Users signing in from those computers are considered as trusted users and have unrestricted access to the application.

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

To prevent any incorrect configuration, the profile option Enable Access to Location Based Access Control associated with the Location Based Access tab is perhaps disabled. As a result, the tab isn't visible.

Contact your Application Implementation Consultant or Administrator to enable the profile option so that the Location Based Access tab appears on the Administration page.

How can I make a role public?

On the Security Console, identify the role that you want to make public. Except duty roles, you can make all roles public. On the Edit Role page, select the option Enable Role for Access from All IP Addresses and save the changes.

Note: You can make a role public only if location based access is enabled.

How can I ensure that I always have access to the Security Console?

If location-based access is enabled, you must add your computer's IP address to the allowlist. Also ensure that the IT Security Manager role is granted public access.

Even if you have to sign in from an unregistered computer, you can still access the Security Console and other tasks associated with the IT Security Manager role.

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

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

Make sure you have the following privileges:

- ASE_ADMINISTER_SSO_PRIV
- ASE_ADMINSTER_SECURITY_PRIV

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

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

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

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

If you're locked out of the application for some reason, use the following Administration Activity URL to disable location-based access. Only an administration user with the IT Security Manager job role can perform this unlock operation.

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Location Based Access Disabled Confirmation Template

14 Single Sign-On

Configure Single Sign-On

To enable single sign-on in your environment, complete the settings in the Single Sign-on Configuration section on the Security Console. This configuration lets you enable a login page and a page to which users must be redirected to after logging out of the application.

Do these steps:

1. On the Security Console, click the **Single Sign-On** tab.
2. In the Single Sign-On Configuration section, click **Edit**.
3. Enter the **Sign Out URL**. Users are redirected to this page once they sign out from the application.

   Note: The Sign Out URL is the same for all the identity providers that you configure.

4. If **Enable Chooser Login Page** isn't enabled already, select it to display the service provider's single sign-on page along with your company's login page.
5. Click **Save**.

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

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

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

Note: Oracle Cloud Applications support all SAML 2.0 compatible federation servers.

Review Service Provider Details

- Service provider metadata. The URL references to an XML file that you can download and view.
- Service provider signing certificate.
- Service provider encryption certificate.

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

Add an Identity Provider

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

Before you begin:

One of the important steps in adding an identity provider is to import the metadata content of the identity provider. The metadata file contains the authentication information and also the signed and encrypted certificates of the identity

provider. Make sure you have the metadata XML file or the URL readily available. Without the file, the setup isn't complete.

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

1. On the Security Console, click **Single Sign-On** > **Create Identity Provider**.
2. On the Identity Provider Details page, click **Edit** and enter the identity provider details:
    - Provide a **Name** and **Description** for the identity provider. Ensure that the identity provider name is unique for the partnership.
    - Select the relevant Name ID Format. If you have an email as the name of the identity provider, select **Email**. Otherwise, leave it as **Unspecified**.
    - Enter the **Relay State URL**. Users are directed to this URL to sign and authenticate irrespective of which application they want to access.
    - Select the **Default Identity Provider** check box to make this identity provider the default one.
3. Import the identity provider metadata:
    - If it's an XML file, click **Browse** and select it.
    - If it's available on a web page, select the **External URL** check box and enter the URL. External URL isn't stored in this configuration and is used only for importing the identity provider metadata during identity provider creation or modification.

    Note: The metadata XML file must be Base64 encoded.
4. Click **Save and Close**.

    Note: Oracle Applications Cloud can't be used as an identity provider.

Test the Identity Provider

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

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

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

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

Enable the Identity Provider

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

Note: You can enable an identity provider only after you import service provider metadata into the identity provider.

Oracle Applications Cloud as the Single Sign-On (SSO) Service Provider

Your users are likely to access different internal and external applications to perform their tasks. They might require access to different applications hosted by partners, vendors, and suppliers.

Certainly, users won't like authenticating themselves each time they access a different application. This is where you as the IT Manager can make a difference. You can provide your users with a seamless single sign-on experience, when you set up Oracle Applications Cloud as a single sign-on service provider.

Your users are registered with identity providers who store and manage their identity and credentials. In Security Console, you can add those identity providers so that you can verify those users without having to store that information.

Note: The identity service associated with your Oracle Fusion Cloud Applications is getting upgraded to the Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) identity domain.If your environment is yet to be upgraded, you can continue to use the Security Console to configure the Single Sign-On settings with the information provided in this section. After your environment is upgraded, see *Federating with Identity Providers* to federate an Oracle Fusion Cloud Applications environment identity domain. See also *How do I find the identity domain for a Fusion Applications environment?*

Initial Sign-in

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

Final Sign-out

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

Prerequisite

To make sure that an administrator can regain access to Oracle Applications Cloud if an accidental account lock out occurs, the administrator must have the following settings configured:

- A valid email
- The IT Security Manager role
- Email notifications are enabled

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_ADMINSTER_SECURITY_PRIV

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

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

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

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 using the Administration Activity page, notification is sent to that user who disabled SSO.
- 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 **Administer SSO** (ASE_ADMINISTER_SSO_PRIV) privilege,according to the following schedule:

- First notification - 60 days before the expiry date
- Second notification - 30 days before the expiry date
- Last notification - 10 days before the expiry date.

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're locked out of the application for some reason, use the following Administration Activity URL to disable single sign-on. Only an administrator user with the IT Security Manager job role can perform this unlock operation.

```
https://<FA POD>/hcmUI/faces/AdminActivity
```

Ensure that the following email notification templates are enabled:

- ORA Administration Activity Requested Template
- ORA Single Sign-On Disabled Confirmation Template

15 API Authentication

Configure Outbound API Authentication Using JWT Custom Claims

A system account is an account used for integrating Oracle Applications Cloud with third-party applications. This account isn't associated with a user but it must have roles with access to REST APIs.

System account uses basic authentication to authenticate users even if single sign-on is enabled. Security Console's password policy applies to a system account and so the password of this account expires based on the password policy.

Critical tasks such as batch operations or data synchronizations must continue without any interruption or the need to re-authenticate at intervals. To support such tasks, you need to define custom parameters for authentication. Using Security Console, you can define a JSON Web Token (JWT) that can be used by REST APIs to automate system authentication without you having to authenticate manually.

JWT is an access token that contains custom claim name and claim values. Custom claims are name and value pairs that you can define in a JWT. To uniquely identify a user, you can add the user's email address to the token along with the standard user name and password.

Example, suppose you want to integrate Oracle Applications Cloud with a third-party application. This integration uses the JWT Custom Claims to authenticate the users who sign into Oracle Applications Cloud to access the third-party application.

Do these steps to define a JWT that will be used for integration with third-party application:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**, **Edit**.
3. Enter a name and description for the external client application that you want to create.
4. In the **Select Client Type** drop-down list, select **JWT Custom Claims** and click **Save and Close**.
5. Click the JWT Custom Claims Details tab and click **Edit**.
6. In the Token Settings section, if required, update the **Token Expiration Time** and **Signing Algorithm**. Default values are 30 minutes and RS256 respectively.
7. Click **Save**.
8. In the JWT Custom Claims section, click **Add**. You can either select a name from the predefined values in the drop-down list or select **Other** and enter a name of your choice.
9. Select a value for the custom claim. If you select **Free-form**, enter the value in the following text box. You can add more JWT custom claims using the **Add** button.
10. Click **Save**. You can add more parameters as required.
11. Click **Done** to return to the JWT Custom Claims Details page.

    You can view the token created for authentication using the **View JWT** button on the JWT Custom Claims Details page. The View JWT window displays the header and payload of the JWT.
12. Click **Done** again to return to the API Authentication page. You can view the newly created JWT Custom Claim in this page.

You can delete a JWT custom claim on the API Authentication page.

Configure Outbound API Authentication Using Three Legged OAuth Authorization Protocol

OAuth is an open industry standard protocol that allows applications access information from other third-party applications, on behalf of the users. The OAuth authorization protocol manages access securely without revealing any passwords to the client application, such as Oracle Applications Cloud.

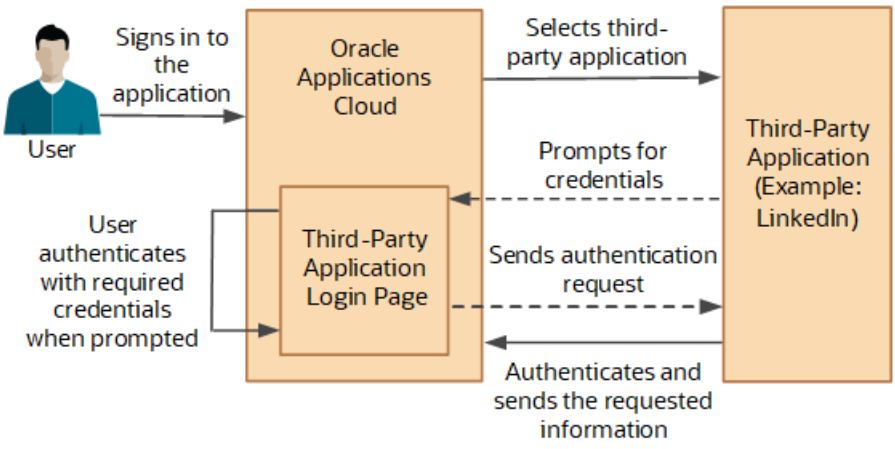
To understand the OAuth authorization protocol, let's take the example of a LinkedIn user who wants to access profile information from LinkedIn and display it in Oracle Applications Cloud. When Oracle Applications Cloud prompts for LinkedIn credentials, the user authenticates and provides the required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

As you notice, there are three parties involved in the entire authentication process: Oracle Applications Cloud, the user who owns information on LinkedIn, and LinkedIn's authorization server. This authorization protocol always requires three such parties for the authentication to complete. Therefore, this protocol is called three-legged OAuth authorization protocol.

Here's the sequential representation of the end-to-end authorization process between Oracle Applications Cloud and the LinkedIn server:

1. Oracle Applications Cloud registers the Client ID and Client Secret and other settings required for authorization.
2. When an Oracle Applications Cloud user wants to access profile information, the LinkedIn login page appears, where the user authenticates using the required credentials.
3. On successful authentication, LinkedIn's authorization server sends an authorization code to Oracle Applications Cloud.
4. Oracle Applications Cloud receives the authorization code and sends an access token request to LinkedIn. LinkedIn processes the access token request and returns an access token.
5. Oracle Applications Cloud uses the access token to call LinkedIn APIs on behalf of the user to access the required information. At runtime, Oracle Web Services Manager manages the entire authorization process.

The following graphic shows the entire authorization process between Oracle Applications Cloud and the LinkedIn server:



Using the Security Console, you configure the three-legged OAuth authorization settings for Oracle Applications Cloud. Once configured, users can access their information from a third-party application, within Oracle Applications Cloud.

Before you proceed, you must enable a profile option to get the OAuth Three-Legged option on the External Client Applications Details page. See the Related Information section for more information.

Here's how you configure three-legged OAuth authorization:

1. On the Security Console, click **API Authentication**.
2. Click **Create External Client Application**.
3. On the External Client Application Details page, click **Edit**.
4. Enter a name and description for the external client application that you want to create.
5. In the **Select Client Type** drop-down list, select **OAuth Three-Legged**.
6. Click **Save and Close** to return to the External Client Application Details page.
7. Click the OAuth Details tab.
8. On the Three-Legged OAuth Details page, click **Edit**.
9. Enter the appropriate values in the following required fields:
    - Authorization URL - The authorization code link that the authorization server sends to the application.
    - Redirect URL - The page to which the user is redirected to after successful authorization of application.
    - Access Token URL - The access token that's sent from the authorization server to the application.
    - Servlet Application URL - The access token that's sent from the authorization server to the application.
    - Client ID - The access token that's sent from the authorization server to the application.
    - Client Secret - The access token that's sent from the authorization server to the application.
    - Client Scope - The access token that's sent from the authorization server to the application.
10. Enter the appropriate values in the following optional fields, if required:
    - Server Scope - The access token that's sent from the authorization server to the application.
    - Federated Client Token - The access token that's sent from the authorization server to the application.
    - Include Client Credential - The access token that's sent from the authorization server to the application.
    - Client Credential Type - The access token that's sent from the authorization server to the application.
11. Click **Save and Close**.
12. Click **Done** to return to the Three-Legged OAuth Details page.
13. Click **Done** again to return to the API Authentication page. You can view the newly created three-legged OAuth configuration here.

Related Topics

- Enable OAuth Three-Legged Authentication for Creating External Client Application

Configure Inbound Authentication

Third-party application users can access a service of Oracle Applications Cloud if inbound authentication is configured for them. You can use an Oracle API Authentication Provider to configure inbound authentication for such users.

To configure inbound authentication, you need a public certificate and a trusted issuer which contains the tokens.

Oracle Applications Cloud supports the JSON Web Token (JWT), Security Assertion Markup Language (SAML), and Security Token Service (STS) tokens. Use the Security Console to configure the trusted issuer and public certificate details. The default trusted issuer is Oracle (www.oracle.com) and you can't delete it.

We recommend that you use JWT for inbound authentication for a system account that's created for a specific application. For authentication, JWT uses a combination of a public certificate and trusted issuer whereas a system account's password expires soon based on the security policy. In addition, you must ensure that the system account's credentials are valid.

> **Note:** For more information about how to configure a JWT for inbound authentication, see Configure JWT Authentication Provider in the Related Topics section.

How Inbound Authentication Works

When a third-party application user sends an authentication request to access a service of Oracle Applications Cloud, these actions occur in the background:

1. The third-party application generates a JWT that includes trusted issuer and public certificate information.
2. Oracle Web Services Manager authenticates the generated JWT by verifying whether the trusted issuer and public certificate are valid.
3. On successful authentication, the third-party application gets access to the Oracle Applications Cloud service.

Here's how you configure an Oracle API Authentication Provider for inbound authentication:

1. On the Security Console, click **API Authentication**.
2. Click **Create Oracle API Authentication Provider**.
3. On the Oracle API Authentication Provider Details page, click **Edit**.
4. On the API Authentication Configuration Details page, enter a name for the **Trusted Issuer**. Ensure that the name of Trusted Issuer matches the value of ISS in the JWT token.
5. Select one or more token types that you want to include in the trusted issuer.
6. Click **Save and Close**.
7. On the Oracle API Authentication Provider Details page, click the Inbound API Authentication Public Certificates tab and click **Edit**. You can use the default Oracle public certificate or add a new one.
8. On the Inbound API Authentication Public Certificates page, click **Add New Certificate** to add a different public certificate.
9. Enter the **Certificate Alias** name
10. Click **Browse** and select the public certificate that you want to import.

    > **Note:** If the public certificate includes a certificate chain then import the complete chain.

11. Click **Save**. The newly added certificate alias is displayed on the Inbound API Authentication Public Certificates page.
12. Click **Done** to return to the API Authentication page.

Related Topics

- Configure JWT Authentication Provider
- Reset User Password
- Use JSON Web Token for Authorization

Is there a recommended format for the public certificate?

Yes. Oracle recommends that the public certificate you upload must contain only line feed (denoted by the code \n) to indicate separation of lines. Because carriage return isn't supported, make sure that the certificate doesn't contain carriage return along with the line feeds.

16 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 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.

Business Object	Information Included in Export and Import
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.

Business Object	Information Included in Export and Import
Security Console User Category	• User category details • Password policy information
Security Console User Category Notifications	Notification preferences. **Note:** For notifications, only the custom template information is exported from the default user category. The predefined notifications are excluded because they're available in the target environment.

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

- Export and Import CSV File Packages
- Key Information About Setup Data Export and Import Processes

Export and Import of Custom Roles

You're looking at migrating your custom role definitions from one environment to another. You can accomplish your migration needs by exporting the business objects in the Users and Security functional area within the Financials offering.

Before You Begin

Learn how to export and import business object data as described in the Overview of Setup Data Export and Import topic of the Using Functional Setup Manager guide.

What Gets Exported and Imported

When you migrate custom roles, the following business objects are exported in the configuration package generated from the Users and Security functional area within the Financials offering. These business objects include custom role definitions:

- Application Data Security Policy
- Functional Security Custom Roles
  - Functional Security Custom Role Hierarchy
  - Functional Security Custom Role Privilege Membership
- HCM Data Role
  - HCM Data Role Security Profile

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

Business Object	Information Included in Export and Import
Application Data Security	Application data security includes data security policies that are created in the following ways: • Manually using the Manage Database Resources page in the security console • Manually using the Edit Role/Copy Role flow in the security console • Automatically when you copy a role using the Role Copy in the security profile • Automatically when you create profile content types • Automatically when you map HCM spreadsheet business objects to roles **Note:** There's no scope support for application data security policies. When you export application data security policies, all data security policies are exported, even if you provided a scope value for other security business objects in your configuration package. There's no Export to CSV option for this business object.
Functional Security Custom Roles	The custom role includes the following details: • Role Code • Role Name • Role Description • Role Category • All IP Address Access - indicates that a role is granted access to the Security Control regardless of the login IP address.
Functional Security Custom Role Hierarchy	The role hierarchy includes the following details: • Parent Role • Member Role • Add or Remove Role Membership

Business Object	Information Included in Export and Import
Functional Security Custom Role Privilege Membership	The role privilege membership includes the following details: • Parent Role • Member Privilege • Add or Remove Privilege Membership
HCM Data Role	The HCM data role includes the following details: • Data Role Code • Data Role Name • Data Role Description • Inherited Job Role Code • Delegation Allowed Check Box
HCM Data Role Security Profile	The HCM data role security profile includes the following details: • Data Role Code • Securing Object • Security Profile Name

The business objects HCM Data Role and HCM Data Role Security Profile are included in the configuration package if you have used security profiles to configure access to HCM data. If you're also using Oracle HCM Cloud, it's recommended that you follow the instructions as described in the Export and Import of HCM Custom Roles and Security Profiles topic in the Securing HCM guide.

What Happens After the Import

You may not immediately see all of the migrated data security policies in the security console after completing the import of the configuration package that's generated from the Users and Security functional area within the Financials offering.

When you import application data security policies, a background process runs to synchronize the imported data security policies with the roles on the target environment. The imported data security policies aren't active until this process has completed, at which point the data security policies will be visible in the security console. This affects data security policies for custom roles that have been copied from other roles in the source environment. It also affects custom roles that have data security policies that were added manually using the security console.

Related Topics

- Overview of Setup Data Export and Import
- Export and Import HCM Security Setup

Export and Import a Custom Role

You can export and import a custom role that has data security policies using an implementation project. The tasks in your implementation project and their sequence determine the list of setup business objects whose data is exported and imported, and in which order.

This method is useful if you want to export and import one or more custom job or abstract roles without security profiles.

Create an Implementation Project

Follow the steps below to create an implementation project.

1. Click **Navigator** > **Others** > **Setup and Maintenance** work area.
2. In the Setup page, select **Manage Implementation Projects** from the **Tasks** panel tab.
3. In the Manage Implementation Projects page, select **Create** from the **Actions** menu, or click the **Create** icon.
4. In the Create Implementation Project: Basic Information page, enter a meaningful name and a brief description to describe your project.
5. Click **Save and Open Project**.
   A page with the name you specified for your implementation project opens. The task list is empty.
6. Select **Create** from the **Actions** menu, or click the **Create** icon and add the following tasks to your implementation project:
   - Manage Job Roles
   - Manage Data Security Policies
7. Click **Done**.

Export Role Definitions Using an Implementation Project

Follow the steps below to export your custom role definitions using your implementation project.

1. Click **Navigator** > **Others** > **Setup and Maintenance** work area.
2. In the Setup page, select **Manage Configuration Packages** from the Tasks panel tab.
3. In the Manage Implementation Projects page, select **Create** from the **Actions** menu, or click the **Create** icon from the Search Results table in the Manage Configuration Packages page to go to the Create Configuration Package: Enter Basic Information page.
4. Select the implementation project you created earlier from the **Name** menu.
   a. If you see a message warning you that the implementation project doesn't contain any offering, click **Yes** to continue.
   b. Leave the default selection for **Export**, **Setup task list and setup data** unchanged.
5. In Configuration Package Details, you can use the default field values for **Name, Code** and **Description**, or assign unique values.
6. Click **Next** to go to the Create Configuration Packages: Select Objects for Export page.
   The first table displays the list of business objects whose setup data is exported:
   - Application Data Security Policy

- Functional Security Custom Roles
- Functional Security Custom Role Hierarchy
- Functional Security Custom Role Privilege Membership

All of the business objects have their **Export** column checked by default. Keep this selection unchanged.

It's best if the Application Data Security business object is imported after the other three business objects. Change the import sequence for the Application Data Security Policy business object so that it has a higher value than the import sequence for the other business objects.

7. Select the custom roles that you want to export.
    a. Select the Functional Security Custom Roles business object in the first table.
    b. Click the **Create** icon in the scope table.
    c. Search and select the custom role you ant to export and click **Apply.** If you want to export more than one custom role, repeat this step for each role you want to export.
    d. Click **Save and Close** when you have finished selecting all the roles you want to export.

> **Note:** There's no scope support for data security policies. Refer to the *What Gets Exported and Imported* section of the *Export and Import of Custom Roles* topic for detailed information on which data security policies will be exported.

8. Click **Submit** to submit the setup data export process and **Confirm** when the confirmation message appears.
9. Monitor the process from **Manage Configuration Package** until it completes.
10. While the process is in progress, you may select the status to go to the Export and Import Process Results page to view how much progress the process has made at the time. Click the **Refresh** button to get the most recent information. Refer to the Review of Export and Import Process Results topic for detailed descriptions of the process results.
11. Once the export process completes successfully, click **Download** to download the configuration package. Use this .zip file to import setup data in the target environment. Optionally, select the status to go to the Export and Import Process Results page to view the result details.

Import Role Definitions Using an Implementation Project

Follow the steps in the Import Setup Data Using Implementation Project topic of the Using Functional Setup Manager guide. Refer to the Related Topics section below for the link to this topic.

Related Topics

- Manage Setup Using Implementation Projects
- Export Setup Data Using Implementation Project
- Import Setup Data Using Implementation Project

Export and Import of ERP Security Setups

You're looking at migrating your ERP security setups from one environment to another. You can accomplish your migration needs by exporting the business objects in the Users and Security functional area within the Financials offering.

Before You Begin

Learn how to export and import business object data. Detailed instructions are available in the Overview of Setup Data Export and Import topic of the Using Functional Setup Manager guide.

What Gets Exported and Imported

When you migrate ERP security setups, the following business objects can be exported in the configuration package generated from the Users and Security functional area within the Financials offering.

- General Ledger Data Access Set
    - General Ledger Data Access Set Assignment
- Role Provisioning Rule
    - Role Provisioning Associated Role List
- All User Data Access
    - Data Provisioning Rules
        - Data Provisioning Rule Detail
- Role Security Context Mapping

Business Object	Information Included in Export and Import
General Ledger Data Access Set	The role hierarchy includes the following details: • Name • Description • Access Set Type • Accounting Calendar • Default Ledger Name • Chart of Accounts
General Ledger Data Access Set Assignment	The role privilege membership includes the following details: • Data Access Set Name • Ledger Name • All Values • Privilege
Role Provisioning Rule	The role provisioning rule includes the following details: • Mapping Rule Name • Legal Employer Name • Business Unit Name • Department Name

Business Object	Information Included in Export and Import
	• Job Set Code • Job Code • Position Business Unit Name • Position Code • Grade Set Code • Grade Code • Location Set Code • Location Code • User Person Type • System Person Type • Assignment Type • HR Assignment Status Code • Resource Role • Party Type Usage Code • Contact Role • Manager with Reports Check Box • Manager Type • Responsibility Type
Role Provisioning Associated Role List	The role provisioning associated role list includes the following details: • Mapping Rule Name • Role Code • Requestable Check Box • Self-Requestable Check Box • Autoprovision Check Box
All User Data Access	All user data access includes the following details: • User Name • Role Code • Business Unit Name • Asset Book Type Code • Reference Data Set Name • Inventory Organization Code • Cost Organization Name • Data Access Set Name • Project Organization Name • Manufacturing Plant Code • Object Name • Data Security Context Type

Business Object	Information Included in Export and Import
	• Data Security Context Value1 • Data Security Context Value2 • Data Security Context Value3
Data Provisioning Rules	Data provisioning rules includes the following details: • Mapping Rule Name • Rule Type • Legal Employer Name • Business Unit Name • Department Name • Job Set Code • Job Code • Position Business Unit Name • Position Code • Grade Code • Location Code • User Person Type • System Person Type • Assignment Type • HR Assignment Status Code
Data Provisioning Rule Detail	The data provisioning rule detail includes the following details: • Mapping Rule Name • Role Code • Data Security Context Type • Data Security Context Value1 • Data Security Context Value2 • Data Security Context Value3
Role Security Context Mapping	The role security context mapping includes the following details: • Object Name • Role Name • Record Type Code • Data Security Context

Before Import

The following business objects include references to elements of the enterprise structure:

- General Ledger Data Access Set Assignment
- All User Data Access
- Data Provisioning Rule Detail

The elements of the enterprise structure referenced in these business objects include:

- Ledger
- Business Unit
- Asset Book
- Intercompany Organization
- Project Organization
- Project Organization Hierarchy
- Award Organization Hierarchy
- Cost Organization
- Warehouse
- Manufacturing Plant
- Reference Data Set

Note: These elements must be in the target environment before importing the ERP security setups.

Related Topics

- Overview of Setup Data Export and Import

17 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 data resources. A data resource is an object, object instance, or object instance set. An entitlement is one or more allowable actions applied to a set of data resources.

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

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

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

Data Security Policies

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

The following table provides an example, accounts payable managers can view AP disbursements for their business unit.

Who	can do	what	on which set of data
Accounts payable managers	view	AP disbursements	for their business unit

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 aren't 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.

Oracle Database Vault

Database Vault reduces the risk of highly privileged users such as database and application 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 can't 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 Data Resources and Data Security Policies Work Together

A data security policy applies a condition and allowable actions to a data 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 data resource defines an instance of a data object. The data object is a table, view, or flexfield.

Data Resources

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

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

Data Security Policies

Data security policies consist of actions and conditions for accessing all, some, or a single row of a data 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 data 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 data 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 can't 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.

Related Topics

- Data Security

How can I design roles?

You can simulate menus that existing roles present to users to determine how the access they provide may be expanded. Create a visualization, or populate the Search Results column with a selection of roles or users.

Select the user or role and click the Actions menu. A menu appears, click Simulate Navigator.

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

How 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.

*How can I mask data in an environment?*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 doesn't want users to perform in your application.

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

How do I create a new job role?

Click the Create Role button in the Security Console to create job roles. Enter a job role category in the Create Roles page and then navigate to each subsequent page that you see in the page header.

You can add functional and data security policies, roles, and privileges to create the job role.

18 Roles and Role Assignments

Review Role Assignments

You can use the Security Console to either view the roles assigned to a user, or to identify the users who have a specific role.

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

View the Roles Assigned to a User

Follow these steps:

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

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

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

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

Identify Users Who Have a Specific Role

Follow these steps:

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

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

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

Review Role Hierarchies

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

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

Follow these steps:

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

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

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

Compare Roles

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

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

Selecting Roles for Comparison

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

- If you began by selecting a role in a visualization graph or the Search Results column, the **First Role** field displays the name of the role you selected. Select another role in the **Second Role** field.

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

Comparing Roles

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

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

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

Adding Policies to a Role

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

19 Role Configuration Using the Security Console

Custom Roles

Create ERP 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 can't edit a role with the ORA_ prefix.

3. In the Role Category field, select a tag that identifies a purpose the role serves in common with other roles. Typically, a tag specifies a role type and an application to which the role applies, such as Financials - Job Roles. If you select a duty-role category, you can't assign the role you're creating directly to users. To assign it, you would include it in the hierarchy of a job or abstract role, then assign that role to users.
4. Optionally, describe the role in the Description field.

Adding Function Security Policies

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

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

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

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

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

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

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

- Click a privilege to view details of the code resource it secures.
- Delete a privilege. You may, for example, have added the privileges associated with a role. If you want to use only some of them, you must delete the rest. To delete a privilege, click its x icon.

Adding Data Security Policies

A data security policy may be explicit or implicit.

- An explicit policy grants access to a particular set of data, such as that pertaining to a particular business unit. This type of policy isn't used in predefined roles in Oracle 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 the **Enable edit of data security policies** option. To locate it, select the Administration tab, and then the Roles tab on the Administration page. If this option isn't selected, the Data Security Policies page is read-only.

To create a data security policy, click the **Create Data Security Policy** button, then enter values that define the policy. A start date is required; a name, an end date, and a description are optional. Values that define the data access include:

- Data Resource: A database table.
- Data Set: A definition that selects a subset of the data made available by the data resource.
    - Select by key. Choose a primary key value, to limit the data set to a record in the data resource whose primary key matches the value you select.
    - Select by instance set. Choose a condition that defines a subset of the data in the data resource. Conditions vary by resource.
    - All values: Include all data from the data resource in your data set.
- Actions: Select one or more data privileges to apply to the data set you have defined.

The Data Security Polices page lists all policies defined for the role. You can edit or delete a policy: click the **Actions** button, and select the **Edit** or **Remove** option.

Configuring the Role Hierarchy

A Role Hierarchy page displays either a visualization graph, with the role you're creating as its focus, or a visualization table. Select the **Show Graph** button or **View as Table** button to select between them. In either case, link the role you're creating to other roles from which it's to inherit function and data security privileges.

- If you're creating a duty role, you can add duty roles or aggregate privileges to it. In effect, you're creating an expanded set of duties for incorporation into a job or abstract role.
- If you're creating a job or abstract role, you can add aggregate privileges, duty roles, or other job or abstract roles to it.

To add a role:

1. Select **Add Role**.
2. In a Search field, select a combination of role types and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select the role you want, and click **Add Role Membership**. You add not only the role you have selected, but also its entire hierarchy.

In the graph view, you can use the visualization Control Panel, Legend, and Overview tools to manipulate the nodes that define your role hierarchy.

Running Separation of Duties Analysis

If you use the provisioning rules feature of Advanced Controls in Risk Management Cloud, you can use the Separation of Duties page to determine whether the hierarchy of the role you're creating includes separation of duties conflicts. For more on creating these provisioning rules, see the Risk Management Cloud user guide for Advanced Controls.

> **Note:** If you don't use this feature, you can disable the Separation of Duties page by setting the ASE_SEGREGATION_OF_DUTIES_SETTING profile option to **No**.

Adding Users

On a Users page, you can select users to whom you want to assign a job or abstract role you're creating. (You can't assign a duty role directly to users.)

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

To add a user:

1. Select **Add User**.
2. In a Search field, select the value Users or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select a user or role. If you select a user, click **Add User to Role**. If you select a role, click **Add Selected Users**; this adds all its assigned users to the role you're creating.

The Users page lists all selected users. You can delete a user. You may, for example, have added all the users associated with a role. If you want to assign your new role only to some of them, you must delete the rest. To delete a user, click its x icon.

Completing the Role

On a Summary and Impact Report page, review the selections you have made. Summary listings show the numbers of function security policies, data security policies, roles, and users you have added and removed. An Impact listing shows the number of roles and users affected by your changes. Expand any of these listings to see names of policies, roles, or users included in its counts.

If you determine you must make changes, navigate back to the appropriate page and do so. If you're satisfied with the role, select **Save and Close**.

Related Topics

- Options for Viewing a Visualization Graph

Role Copying or Editing

Rather than create a role from scratch, you can copy a role, then edit the copy to create a new role. Or you can edit existing roles.

> **CAUTION:** While creating custom roles, make sure you assign only the required privileges. Assigning all the privileges may impact subscription usage. Before you proceed, see topic *Guidance for Assigning Predefined Roles*.

Initiate a copy or an edit from the Roles tab in the Security Console. Do either of the following:

- Create a visualization graph and select any role in it. Right-click and select **Copy Role** or **Edit Role**.
- Generate a list of roles in the Search Results column of the Roles page. Select one of them and click its menu icon. In the menu, select **Copy Role** or **Edit Role**.

If you're copying a role, select one of two options in a Copy Option dialog:

- **Copy top role**: You copy only the role you have selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. If you select this option, subsequent changes to the inherited roles affect not only the source highest role, but also your copy.
- **Copy top role and inherited roles**: You copy not only the role you have selected, but also all of the roles in its hierarchy. Your copy of the highest role is connected to the new copies of subordinate roles. If you select this option, you insulate the copied role from changes to the original versions of the inherited roles.

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

- In the Basic Information page, a **Predefined role** box is checked if you selected the Edit Role option for a role shipped by Oracle. In that case, you can:
  - Add custom data security policies. Modify or remove those custom data security policies.
  - Add or remove users if the role is a job, abstract, or discretionary role.

  You can't:
  - Modify, add, or remove function security policies.
  - Modify or remove data security policies provided by Oracle.
  - Modify the role hierarchy.

The **Predefined role** check box is cleared if you're editing a custom role or if you have copied a role. In that case, you can make any changes to role components.

- By default, the name and code of a copied role match the source role's, except a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.
- A copied role can't inherit users from a source job or abstract role. You must select users for the copied role. (They may include users who belong to the source role.)
- When you copy a role, the Role Hierarchy page displays all roles subordinate to it. However, you can add roles only to, or remove them from, the highest role you copied.

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

Related Topics

- Generate a Visualization
- Create Roles in the Security Console

Guidelines for Copying ERP Roles

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

Reviewing the Role Hierarchy

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

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

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

Reviewing Privileges

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

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

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

> **Note:** Data security policies are visible only when you edit your role.

Transaction Analysis Duty Roles

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

Naming Copied Roles

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

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

Duplicate Roles

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

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

What Role Copy Does

When you copy a role on the Security Console, the role is copied in accordance with the role-copy options that you specify. Nothing else is updated. For example:

- If the role that you're copying is referenced in an EL expression, then the expression isn't updated to include the new role.
- The new role isn't assigned automatically to users who have the original role.

Related Topics

- Role Preferences
- User and Role Access Audit Report

Security Console Role-Copy Options

When you copy a role on the Security Console, you have the option to either copy top role, or copy top role and inherited roles. This topic explains the effects of each of these options.

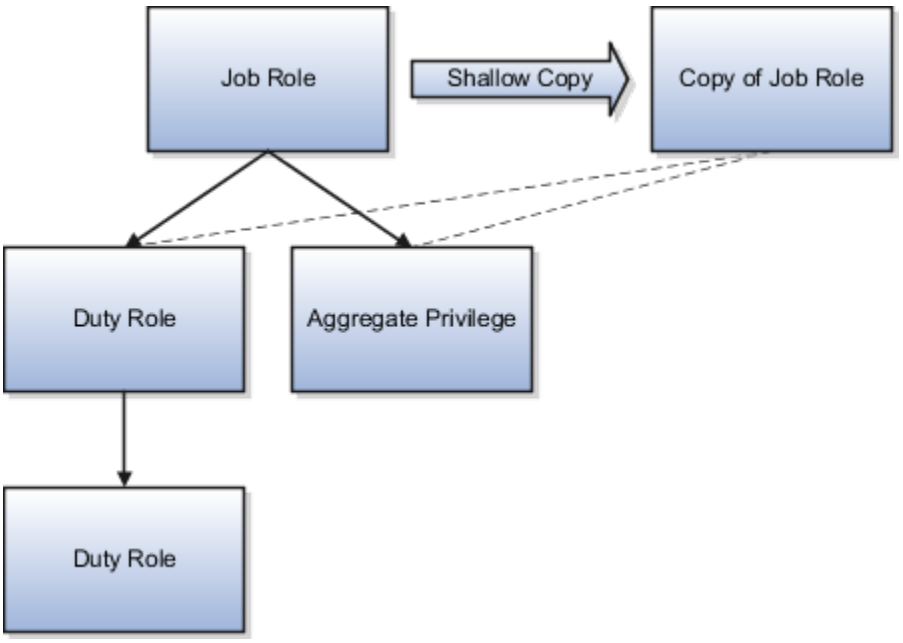
Copy Top Role

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.

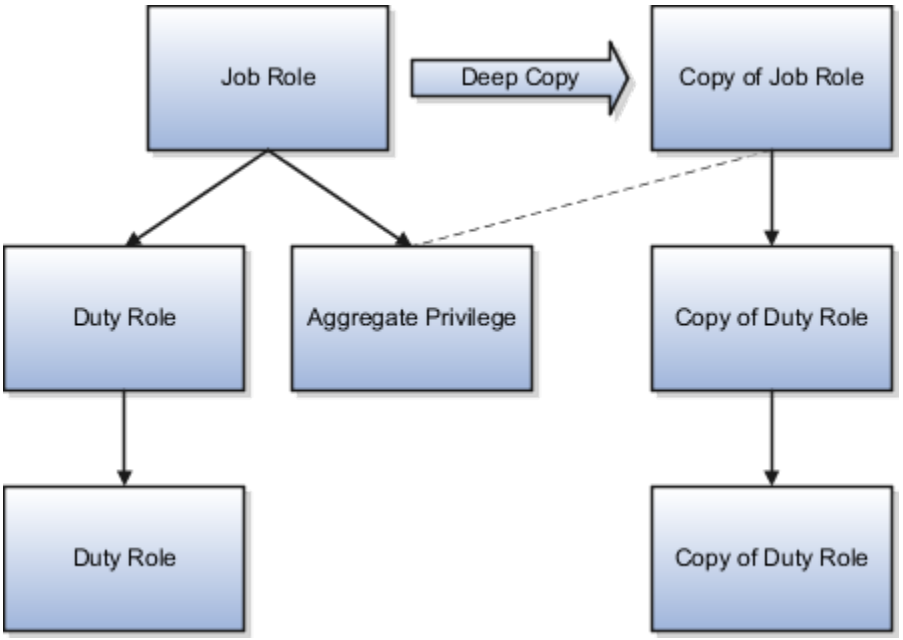
Copy Top Role and Inherited Roles

Selecting **Copy top role and inherited roles** is a request to copy the entire role hierarchy. These rules apply:

- Inherited aggregate privileges and middleware roles are never copied. Instead, membership is added to each aggregate privilege, or middleware role, 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

- Copy Job Role and Abstract Role
- Guidelines for Copying HCM Roles

Copy Job Role and Abstract Role

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. You must have the IT Security Manager job role or privileges for this task.

The following video shows how you can copy a predefined abstract role:

Watch video

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 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

- Security Console Role-Copy Options
- Guidelines for Copying HCM Roles
- Edit Job Role and Abstract Role

Edit Job and Abstract Roles

You can create a role by copying a predefined job role or abstract role and editing the copy. 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.

   If you select a single privilege, then click **Add Privilege to Role**.
4. Click **OK** to close the confirmation message.
5. Repeat from step 2 for additional privileges.
6. Close the Add Function Security Policy dialog box.
7. Click **Next**.

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

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

The Edit Role: Data Security Policies page shows any data security policies granted to the copied role. You can add, remove, or modify data security policies as needed.

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

To add a data security policy:

1. Click the **Create Data Security Policy** icon.

2. Enter values that define the policy. A start date is required; a name, end date, and description are optional. Values that define the data access include:
    - Data Resource: A database table.
    - Data Set: A definition that selects a subset of the data made available by the data resource:
        - Select by key. Choose a primary key value to limit the data set to a record in the data resource whose primary key matches the value you select.
        - Select by instance set. Choose a condition that defines a subset of the data in the data resource. Conditions vary by resource.
        - All values: Include all data from the data resource in your data set.
    - Actions: Select one or more data privileges to apply to the data set you have defined.
3. Click **OK to save**.

To edit a data security policy:

1. Select the data security policy in the table.
2. Click the drop down on the right, and select **Edit Data Security Policy**.
3. Change the data security policy as needed.
4. Click **OK** to confirm the changes.

To remove a data security policy:

1. Select the data security policy in the table.
2. Click the drop down on the right, and select **Remove Data Security Policy**.
3. Click **Yes** to close the confirmation 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**.

Running Separation of Duties Analysis

If you use the provisioning rules feature of Advanced Controls in Risk Management Cloud, you can use the Separation of Duties page to determine whether the hierarchy of the role you're creating includes separation of duties conflicts. For more on creating these provisioning rules, see the Risk Management Cloud user guide for Advanced Controls.

> **Note:** If you don't use this feature, you can disable the Separation of Duties page by setting the ASE_SEGREGATION_OF_DUTIES_SETTING profile option to **No**.

Provision the Role to Users

The Edit Role: Users page shows users that are currently provisioned this role.

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

To remove a user from this role:

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

To add users to this role:

1. Click the **Add User** button.
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**, which adds all its assigned users to the role you're creating.

   To automatically provision the role to users, you can also create a role mapping.

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

- Copy Job Role and Abstract Role

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

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 **Financials - Abstract Roles**, **Financials - Discretionary Roles, or Financials - Job Roles**, as appropriate.
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:

1. On the Privileges tab of the Create Role: Functional Security Policies page, click **Add Function Security Policy**.
2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click **Add Selected Privileges** to add all function security privileges from a selected role to your custom role.

   > **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.
6. Close the Add Function Security Policy dialog box.
7. Click **Next**.

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

Create Data Security Policies

The Create Role: Data Security Policies page enables you to add data security policies as needed.

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

To add a data security policy:

1. Click the Create Data Security Policy icon.
2. Enter values that define the policy. A start date is required; a name, end date, and description are optional. Values that define the data access include:
    - Data Resource: A database table.
    - Data Set: A definition that selects a subset of the data made available by the data resource:
        - Select by key. Choose a primary key value to limit the data set to a record in the data resource whose primary key matches the value you select.
        - Select by instance set. Choose a condition that defines a subset of the data in the data resource. Conditions vary by resource.
        - All values: Include all data from the data resource in your data set.
    - Actions: Select one or more data privileges to apply to the data set you have defined.
3. Click **OK to save**.

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. 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

The Create Role: Users page enables you to quickly provision a new role to users.

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

To add users to this role:

1. Click the Add User button.

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, which adds all its assigned users to the role you're creating.
   To automatically provision the role to users, you can also create a role mapping when the role exists.

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. 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 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.
6. Close the Add Functional Security Policies dialog box.
7. Click **Next**.

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

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

The Edit Role: Data Security Policies page shows any data security policies granted to the copied role. You can add, remove, or modify data security policies as needed.

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

To add a data security policy:

1. Click **Create Data Security Policy**.
2. Enter values that define the policy. A start date is required; a name, end date, and description are optional. Values that define the data access include:
   - Data Resource: A database table.
   - Data Set: A definition that selects a subset of the data made available by the data resource:
     - Select by key. Choose a primary key value to limit the data set to a record in the data resource whose primary key matches the value you select.
     - Select by instance set. Choose a condition that defines a subset of the data in the data resource. Conditions vary by resource.

        - All values: Include all data from the data resource in your data set.
    - Actions: Select one or more data privileges to apply to the data set you have defined.
3. Click **OK** to save.

To edit a data security policy:

1. Select the data security policy in the table.
2. Click the drop down on the right, and select **Edit Data Security Policy**.
3. Change the data security policy as needed.
4. Click **OK** to confirm the changes.

To remove a data security policy:

1. Select the data security policy in the table.
2. Click the drop down on the right, and select **Remove Data Security Policy**.
3. Click **Yes** to close the confirmation 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

- Security Console Role-Copy Options
- Guidelines for Copying HCM Roles

20 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 doesn't perform any validation on these values.
- An algorithm by which keys are generated, MD5 or SHA1.
- A key length.
- A validity period, in days. This period is preset to a value established on the General Administration page. You can enter a new value to override the preset value.

Sign a X.509 Certificate

You can generate a request for a certificate authority (CA) to sign a self-signed X.509 certificate, to make it a trusted certificate. (This process doesn't apply to PGP certificates.)

1. Select **Generate Certificate Signing Request**. This option is available in either of two menus:
    - One menu opens in the Certificates page, from the row for a self-signed X.509 certificate.
    - The other menu is the Actions menu in the details page for that certificate.
2. Provide the private key password for the certificate, then select a file location.
3. Save the request file. Its default name is [alias]_CSR.csr.

You are expected to follow a process established by your organization to forward the file to a CA. You would import the trusted certificate returned in response.

Import and Export X.509 Certificates

For an X.509 certificate, you import or export a complete certificate in a single operation.

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Certificate.
3. Select a location for the export file. By default, this file is called [alias].cer.

To import, use either of two procedures. Select the one appropriate for what you want to do:

- The first procedure replaces a self-signed certificate with a trusted version (one signed by a CA) of the same certificate. (A prerequisite is that you have received a response to a signing request.)
    a. In the Certificates page, locate the row for the self-signed certificate, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
    b. Enter the private key password for the certificate.
    c. Browse for and select the file returned by a CA in response to a signing request, and click the Import button.

    In the Certificates page, the type value for the certificate changes from self-signed to trusted.
- The second procedure imports a new X.509 certificate. You can import a .cer file, or you can import a keystore that contains one or more certificates.

a. In the Certificates page, click the Import button. An Import page opens.
b. Select X.509, then choose whether you're importing a certificate or a keystore.
c. Enter identifying values, which depend on what you have chosen to import. In either case, enter an alias (which, if you're importing a .cer file, need not match its alias). For a keystore, you must also provide a keystore password and a private key password.
d. Browse for and select the import file.
e. Select Import and Close.

Related Topics

- Sign a X.509 Certificate

Import and Export PGP Certificates

For a PGP certificate, you export the public and private keys for a certificate in separate operations. You can import only public keys. (The assumption is that you will import keys from external sources, who wouldn't provide their private keys to you.)

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Public Key or Private Key.
3. If you selected Private Key, provide its passphrase. (The public key doesn't require one.)
4. Select a location for the export file. By default, this file is called [alias]_pub.asc or [alias]_priv.asc.

To import a new PGP public key:

1. On the Certificates page, select the Import button.
2. In the Import page, select PGP and specify an alias (which need not match the alias of the file you're importing).
3. Browse for the public-key file, then select Import and Close.

The following PGP certificate formats aren't supported:

- GnuPG v2.0.22 (GNU/Linux)
- Keybase OpenPGP v1.0.0
- OpenPGP.js v4.10.10

The Certificates page displays a record for the imported certificate, with the Private Key cell unchecked.

Use a distinct import procedure if you need to replace the public key for a certificate you have already imported, and don't want to change the name of the certificate:

1. In the Certificates page, locate the row for the certificate whose public key you have imported, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
2. Browse for the public-key file, then select Import.

Delete Certificates

You can delete both PGP and X.509 certificates. On the Certificates page, select the menu available in the row for the certificate you want to delete. Or, in the details page for that certificate, select the Actions menu.

In either menu, select Delete. Respond to a warning message. If the certificate's private key is present, you must enter the passphrase (for a PGP certificate) or private key password (for an X.509 certificate) as you respond to the warning. Either value would have been created as your organization generated the certificate.

21 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 to use the features specific to these regions.

You must assign custom roles based on the following country-specific duty roles to FSCM application and OBI application stripe. After assigning these custom roles you can view the country-specific reports on the Scheduled Processes page, and open the Parameters page of the selected process.

This table describes the duty roles for each region:

Region	Duty Role	Role Code
Europe, the Middle East, and Africa (EMEA)	EMEA Financial Reporting	ORA_JE_EMEA_FINANCIAL_REPORTING_DUTY
Asia Pacific (APAC)	APAC Financial Reporting	ORA_JA_APAC_FINANCIAL_REPORTING_DUTY
Asia Pacific (APAC)	Enterprise Financial Data Export Management for China	ORA_JA_CN_ENTERPRISE_FINANCIAL_DATA_EXPORT_ONLY_FOR_CHINA_DUTY_OBI
Asia Pacific (APAC)	Golden Tax Management for China	ORA_JA_GOLDEN_TAX_MANAGEMENT_FOR_CHINA_DUTY_OBI

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 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's 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 Oracle ERP Cloud Securing ERP guide.

Related Topics

- Data Access

Overview of Data Access Set Security

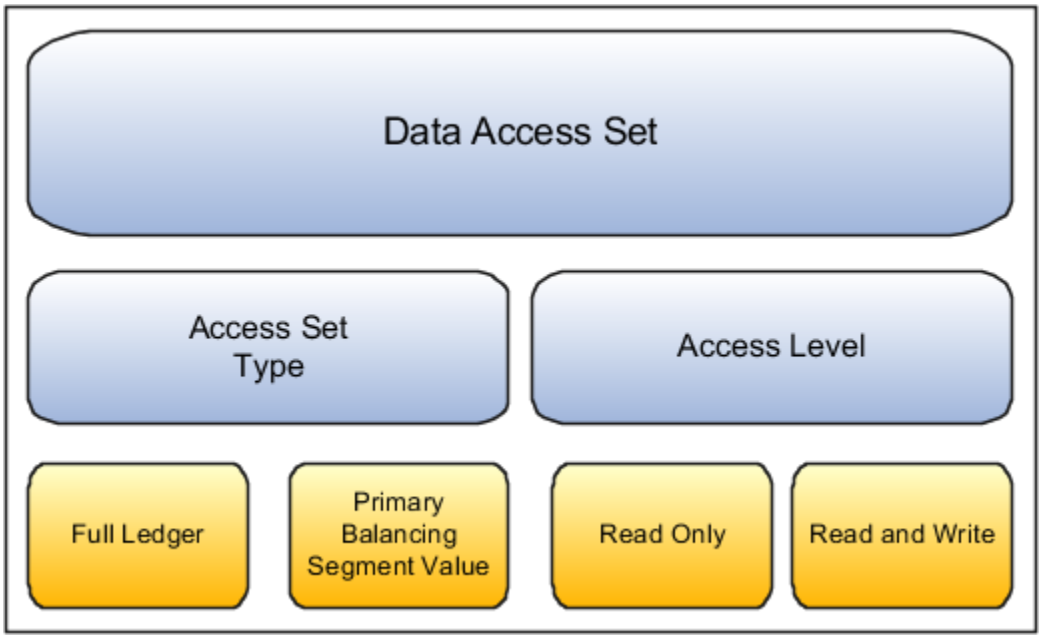
Data Access Sets secure access to ledgers, ledger sets, and portions of ledgers using primary balancing segment values.

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.



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 parent value must be selected from the tree that's associated with the primary balancing segment of your chart of accounts. 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 Oracle ERP Cloud Securing ERP guide.

Examples of Data Access Set Security

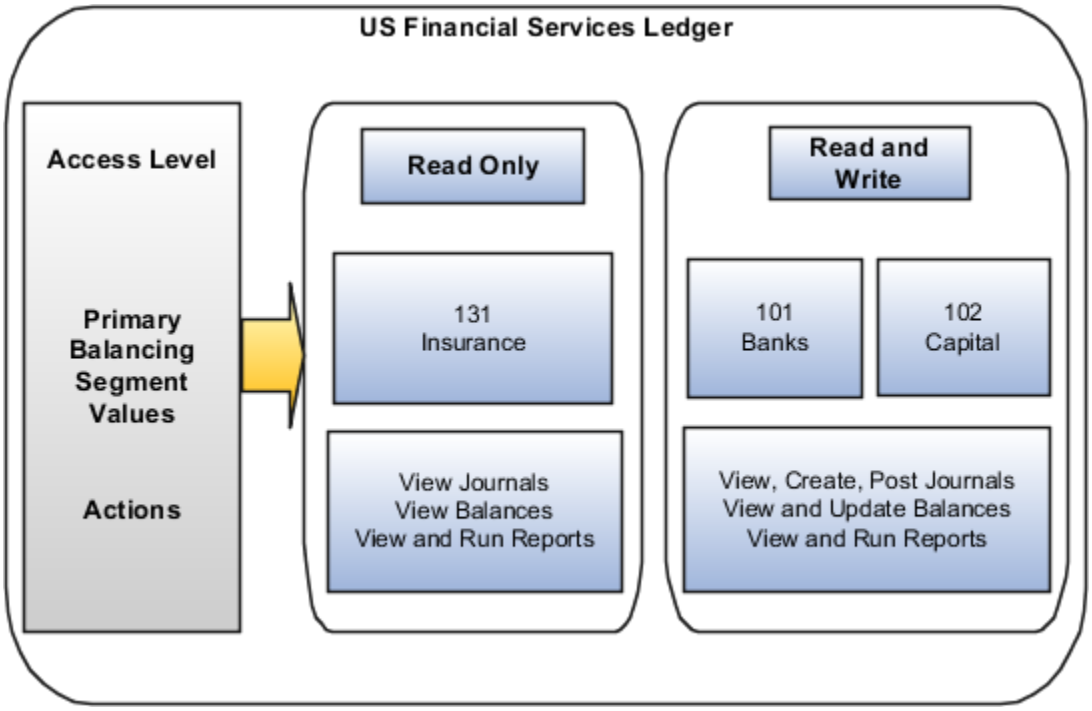
This example shows a data access set that secures access by using primary balancing segment values that correspond to legal entities.

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 Oracle ERP Cloud Securing ERP guide.

Overview of Segment Value Security

Segment value security provides chart of accounts security to secure access to create or view financial data.

Selectively enable enforcement using segment value security rules by business function, including by General Ledger, Payables, Receivables, Assets, Intercompany and Subledger Accounting. Security administrators can grant account values access to users based on certain business functions, data security context, and read-only or read and write access levels. For all other product modules, there is no enforcement when security is enabled for the chart of accounts segment value set, and users working with these other modules will have access to all accounts.

Here are some business benefits that chart of accounts segment values security provides.

- Provides precision in securing account access for each user to each product module, including General Ledger, Payables, Receivables, Assets, Intercompany and Subledger Accounting. Limit security enforcement to the modules where this is required.

  This feature addresses a wide range of financial data security requirements by providing a chart of accounts-based data security control using highly precise grants of secured account values to users qualified by:
  - Business function
  - Data security context
  - Read only versus read and write access level

  A user's access to specific account values can be selectively provided with rule assignments that are tagged with a business function and data access context such that the grant would only apply for that user under the matching usage scenario. Moreover, the access can be granted on a read and write or read-only basis. If there are no matching rule assignments for that user for a given usage scenario, the user gets access to all account values for the secured chart of accounts value set.

  This ensures that all users only get the exact and appropriate access to the financial data they need to work with.

  For example, with the General Ledger business function you might have some select accountants in your organization who not only manage the financial accounting for their region but are also responsible for calculating the global bad debt reserve. They require full read and write access to all accounts when working with the financial data specific to their assigned region but should have read-only access to specific accounts of the worldwide financial data related to calculating the global bad debt reserve. It would be possible to achieve this type of access control with this feature by enabling security enforcement for the General Ledger business function. Such users would then be assigned rules that granted read-only access to those select bad debt reserve related accounts when working with the global ledgers outside of their region, while being given access to all accounts on a read and write basis when working with their regional ledger.
- Reduce the time needed to set up and maintain rules. Users with unrestricted access to accounts are automatically granted all account values; users who require restricted access are assigned an explicit security configuration.

  Streamlined configuration and administration of this chart of accounts security feature is achieved by selectively enabling security enforcement for distinct business functions. Simplified onboarding via management by exception is achieved through initially providing access to all secured account values by default to all users. Only those users who should work with just certain accounts for their given usage scenarios need to be actively managed and assigned distinct rules to limit their access.

  Setup efficiency is optimized with rule assignments that can be flexibly configured with varying degrees of specificity to fit the unique data security requirements of a particular user. Generic rule assignments can be shared between groups of users with similar access requirements to secured accounts.

Key Steps for Configuring Chart of Accounts Segment Value Security

Here are the main steps for setting up chart of accounts segment value security.

1. Select business functions that enforce segment value security.
2. Enable security for a value set.
3. Deploy the accounting flexfield and publish account hierarchies.
4. Prepare the Manage Segment Value Security Rules spreadsheet.

Before you start, you'll need to have a role that's based on either the Application Implementation Consultant (ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB) or the Financial Application Administrator (ORA_FUN_FINANCIAL_APPLICATION_ADMINISTRATOR_JOB), and the IT Security Administrator (ORA_FND_IT_SECURITY_MANAGER_JOB) job roles to have access to the range of functions required to set up all the elements involved with configuring segment value security by business function for users in the application.

The Manage Advanced Chart of Accounts Segment Value Security (FUN_MANAGE_ADVANCED_CHART_OF_ACCOUNTS_SEGMENT_VALUE_SECURITY_PRIV) privilege controls access to the Manage Segment Value Security Rules spreadsheet. You'll need a custom role that's assigned this privilege.

Select Business Functions That Enforce Segment Value Security

The business functions that you select affect all secured value sets in all charts of accounts that the value sets are used in.

1. In the Setup and Maintenance work area, go to the Manage Chart of Accounts Configurations task:
   - Offering: Financials
   - Functional Area: Financial Reporting Structures
   - Task: Manage Chart of Accounts Configurations
2. Click **Manage Segment Value Security by Business Function**.

   > **Note:** If the button doesn't appear, your instance doesn't qualify for segment value security by business function. Only instances with no secured value sets at the time they're evaluated will be qualified to use this model of chart of accounts segment value security. For an instance where there's at least one existing value set enabled for security, including one that's assigned to your chart of accounts segment or other application key flexfields, it will continue to behave in the same manner as it had all along in previous releases, enforcing segment value security without the business function distinction. Any future value set enabled for security in such an instance will also apply enforcement in this same manner. For more information, see the *Segment Value Security without Business Function Implementation Guide* (Doc ID 3054824.1) on My Oracle Support.

   > **CAUTION:** The evaluation and designation for a Cloud Applications environment of the enforcement method of segment value security by business function or without business function is applied distinctly on each instance, based on their distinct instance name plus instance type. Two instances with the same letter name but of different types (that is, instance WXYZ Prod versus instance WXYZ Test) are considered individually, and the segment value security enforcement method will be set for each instance based on the presence or absence of value sets enabled for security, independent of the other like-named instance.

3. On the Manage Segment Value Security by Business Function dialog box, review this text, which appears after the title.

You're enabling segment value security for your chart of accounts for the very first time. Select the business functions where segment value security must be enforced. Your selections will apply to all charts of accounts whose segments are enabled for security. Click **Cancel** to make your selection later.

4. Select the business functions where security must be enforced.

   > **Note:** A business function can be disabled from security enforcement afterward.

   You can select from among the following business functions:
   - General Ledger
   - Payables
   - Receivables
   - Intercompany
   - Assets

   Selecting one or more of these business functions automatically enables security enforcement for Oracle Subledger Accounting because it's an integration module between Oracle General Ledger and the other listed subledger business functions.

   > **Note:** You don't have to make all your business function selections at once. You can select additional business functions later by clicking Manage Segment Value Security by Business Function.

Enable Security for a Value Set

After selecting the business functions, the next step is to enable security for a chart of accounts value set for the Accounting Flexfield (GL#) key flexfield.

1. In the Setup and Maintenance work area, go to the Manage Chart of Accounts Configurations task:
   - Offering: Financials
   - Functional Area: Financial Reporting Structures
   - Task: Manage Chart of Accounts Configurations

   > **CAUTION:** You must use this task and the Manage Chart of Accounts Configurations page to enable security for a value set. Don't use the Manage Value Set, Edit Value Set, or Edit Value Set Data Security pages because the required initialization for the value set won't be successful and the security configuration for the value set won't be correct.

2. Click the name of the chart of accounts that you want to secure.
3. In the Segments section, select the segment row with the value set that you want to secure.

   Value set security applies at the value set level, not to individual segments of a chart of accounts that reference that value set. If a value set is used in multiple charts of accounts, then all chart of accounts segments that are assigned that value set will be enabled for security.

   Chart of accounts security is enabled for one value set at a time, and its security rules and rule assignments are framed individually for each distinct secured value set for which they're defined.

   For a chart of accounts that has multiple segments with secured value sets, each value set's security configurations are considered individually and they're not cross-secured with one another. To determine whether an account combination that a user is working with passes the access check for each of account

combination segments' values, the grants for the individual secured segments are each evaluated independently and then applied additively across each of the secured segments.

> **CAUTION:** For a secured Accounting Flexfield (GL#) value set that's shared with other key flexfields, such as the Budgeting Flexfield (XCC), the Cost Allocation Flexfield (COST), the Asset Key Flexfield (KEY#), the Location Flexfield (LOC#), and others, security will not be enforced for that secured value set with these other types of key flexfields. Value sets in other types of key flexfields that aren't shared with the Accounting Flexfield (GL#) key flexfield and that are enabled for security will still enforce segment value security in the mode without the business function distinction. As such, there can be differences in segment value security enforcement across the segments of such key flexfields.

4. On the Value Set tab in the Value Set section, select **Enable security.**

> **Note:** If you're enabling security on a value set for the first time and you haven't performed the previous setup step of selecting the business functions that enforce segment value security, the Manage Segment Value Security by Business Function dialog box will open. See the *Select Business Functions That Enforce Segment Value Security* topic for more information.

It's possible to deselect the **Enable security** checkbox and stop enforcement of segment value security for a value set. If you deselect the checkbox, you must redeploy the GL# Accounting Key Flexfield to process such a metadata change to the chart of accounts for this to take effect. Successful redeployment is similarly required when enabling or disabling security for a value set referenced in any other type of key flexfield, such as the Budgeting Flexfield (XCC).

5. Click **Save**.

The application will automatically create the data security resource for the secured value set. The security object name uses the format **DS** followed by an underscore (_) and then the value set name, without spaces. For example, if the value set name is **Vision Company**, then the data resource security name would be **DS_VisionCompany**.

In addition, the application generates an **All Values** policy for this data security resource to the Authenticated User (ORA_FND_AUTHENTICATED_USER_ABSTRACT) role, which is automatically assigned to all users who successfully sign in to the application. The policy name follows this format: **<Secured Value Set Name> – All Segment Values**, for example, **Vision Company – All Segment Values**. This policy is the key mechanism enabling the segment value security by business function behavior where all users are first provided access to all account values of a secured value set by default. This default policy will be suppressed in usage scenarios where a user has a matching distinct policy assignment that restricts access to certain account values.

Deploy the Accounting Flexfield and Publish Account Hierarchies

When enabling or disabling security for a chart of accounts value set, you must successfully deploy the accounting flexfield for the change to take effect.

In the Setup and Maintenance work area, use the Manage Chart of Accounts Configurations task in the Financial Reporting Structures functional area and click **Deploy All Charts of Accounts**.

> **Note:** You can monitor the progress of the Accounting Flexfield deployment using the Manage Chart of Accounts Structures task.

To update the General Ledger balances cube so that the current security enforcement settings are applied, you must publish the account hierarchies for the secured value sets. In the Setup and Maintenance work area, use the **Publish Account Hierarchies** task in the Financial Reporting Structures functional area.

Related Topics

- When does security take effect on chart of accounts value sets for balances cubes?
- What happens when changes are made to an account hierarchy that's referenced in segment value security rules?

Open the Manage Segment Value Security Rules Spreadsheet

If there are users who should have access to only limited accounts of a secured value set at all times, or for their certain usage scenarios, then you must configure rules and user rule assignments for that secured value set.

This is necessary to suppress the All Values access that was granted by default to every user, which is a feature of segment value security rules by business function.

You must use the Manage Segment Value Security spreadsheet exclusively to maintain your rules and rule assignments for segment value security by business function.

Don't use the following methods to create or maintain rule and rule assignment setups for secured value sets:

- Edit Data Security page in the application.
- Rapid Implementation Create Segment Value Security Rules spreadsheet, which is opened using the Create Segment Value Security Rules in Spreadsheet task.

The Manage Segment Value Security Rules spreadsheet captures additional rule and rule assignment attributes that aren't maintained in the Edit Data Security page or in the Rapid Implementation Create Segment Value Security Rules spreadsheet, including attributes that support enforcing segment value security by business function.

Commingling the usage of the Manage Segment Value Security Rules spreadsheet with the Edit Data Security page or the Rapid Implementation spreadsheet to maintain your segment value security setups will result in serious data inconsistencies that will cause the incorrect enforcement of segment value security.

After you've saved your changes to enable security for a value set, you can open the Manage Segment Value Security Rules spreadsheet to set up your security rules.

1. In the Setup and Maintenance work area, go to the Manage Chart of Accounts Configurations task:
    - Offering: Financials
    - Functional Area: Financial Reporting Structures
    - Task: Manage Chart of Accounts Configurations
2. On the Manage Chart of Accounts Configurations page, select the chart of accounts.
3. In the Segments section, select the secured value set.
4. In the Value Set tab, click **Manage Data Security**. The spreadsheet will open within the context of the secured value set.

Related Topics

- Set Up Desktop Integration for Excel
- Guidelines for Using Desktop Integrated Excel Workbooks
- Troubleshoot Desktop Integration for Excel

Using the Manage Segment Value Security Rules Spreadsheet

Follow these guidelines when creating new rules and new rule assignment records in the Manage Segment Value Security Rules Spreadsheet.

- Always navigate to the Rules sheet first to initialize your session, then second to the Rule Assignments sheet. Don't navigate directly to the Rule Assignments sheet right away because this will result in an error for your session with the spreadsheet.
- Click the Upload command on the Manage Segment Value Security tab once you've completed your entries on the worksheet to save these records to the application.
- Upload the Rules worksheet first before completing and uploading the Rule Assignments worksheet because the assignments in the latter worksheet reference the rules. The rules need to be successfully saved to the application first before they can be assigned to users.
- Work with only one secured value set at a time per session. Otherwise, the application can't properly identify which value set is the focus if multiple secured value sets are simultaneously being worked on. As part of its initialization, the spreadsheet establishes a connection and value set of focus.

Create Rules

The Rules worksheet of the Manage Segment Value Security Rules spreadsheet is for defining segment value security policies.

Policies can include one or more segment value security condition filters and are associated with a segment value security role. The segment value security role serves as the conduit to pass the security policy to users.

A policy can have a one-to-many relationship with condition filters. You can do this in the spreadsheet by using the same policy name across multiple rows. The different condition filters defined in these multiple rows will be treated as a group that's associated with that one policy. This helps you adhere to the best practice of keeping in check the number of security policies defined for a secured value set and keeping setups manageable.

Columns are either policy-level attributes or condition filter-level attributes. Policy-level attributes must share the same value across multiple rows for the group of condition filters that are part of that same policy. Values for the condition filter-level attributes representing the different condition filters that you want to apply to the same policy will vary across the rows.

Enter attribute values in the order in which the columns appear in the worksheet, starting with the policy name.

This table lists the attribute columns on the Rules worksheet and their properties.

Attribute	Required	Updatable	Policy or Condition Filter Attribute
Policy Name	Yes	No	Policy
Policy Description	No	Yes	Policy
Segment Value Security Role Name	Yes	No	Policy
Operator	Yes	Yes	Condition Filter

Attribute	Required	Updatable	Policy or Condition Filter Attribute
From Value (Used with all operators other than All Values)	Yes	Yes	Condition Filter
To Value (Used with Between operator only)	Yes	Yes	Condition Filter
Tree Code (Used with hierarchical operators only)	Yes	Yes	Condition Filter
Tree Version (Used with hierarchical operators only)	Yes	Yes	Condition Filter
Policy Start Date	Yes	No	Policy
Policy End Date	No	Yes, if the policy is active, that is, the policy end date is today's date or later.	Policy
Mark for Deletion	No	Yes	Condition Filter

Here's more information about each attribute to help you prepare the Rules worksheet.

Policy Name

Identifies the specific condition to segment value security role association. The name must be unique within the individual secured value set. The application automatically stores the capitalized policy name to help minimize confusion and anomalies when referencing the policy's name.

Policy Description

Provides a summary of the scope, purpose, or other pertinent information about the policy.

Segment Value Security Role Name

Identifies the predefined role to which you're assigning the segment value security policy. Double-click within the cell to open a dialog box, where you can select the role to insert into that cell. To form a complete user rule assignment, you must also assign the segment value security role of the policy to the users you want to assign the policy.

Operator

Indicates how to evaluate the succeeding values specified in the row for the purpose of determining what account values of the secured value set are being granted. This is a key attribute of a segment value security condition filter.

Related condition rows for the same policy created using the spreadsheet will always be set to the Match Any option or to using the Or conjunction when stringing together the various condition filter rows for the same policy to determine what account values are involved. This is also the default match setting even if it's a policy with just a single condition filter row.

This means that the account values being granted by the policy just need to match one of the condition rows stipulated in the group, rather than simultaneously match every one of the condition rows in that group, which would more than

likely result in a nonmatch, or no account value, because an account value is unlikely to satisfy every one of those conditions.

This table describes the operators you can use in the condition filters.

Operator	Description
All Values	Provides access to all account values in the value set.
Equal to	Provides access to a specific account value. When the specified value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. The rule doesn't provide access to any of its descendants.
Not equal to	Provides access to all values, except the one detail/child or a parent value that you specify. In the case of a parent value, the exclusion only applies specifically to that parent value itself, and not any of its descendant parent and detail or child values. **CAUTION:** Here are some important points about this operator. • Use this operator carefully and sparingly. • Don't use it in multiple condition rows for the same policy or in different policies assigned to the same security value security role for a given secured value set. The different conditions could end up canceling each other out, resulting in unintended access being granted to account values you want to secure. For example, let's say you have a policy with two condition rows. You define the first condition as Not Equal To account value 100 and the second condition as Not Equal To account value 200. The list of values for the segment is going to show both 100 and 200, among other values. That's because an account value can meet any one of the conditions for the rule to apply. The value of 100 meets the Not Equal To 200 condition and the value of 200 meets the Not Equal To 100 condition.
Between	Provides access to the account values included in the range of values specified in the From and To Value columns. When the range of values includes a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. The rule doesn't provide access to any of its descendants, unless they're part of the specified range.
Contains	Provides access to account values that contain the specified value. When the matching value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. It doesn't provide access to any of its descendants unless those descendants also happen to match the condition.
Ends with	Provides access to account values that end with the specified value. When the matching value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. It doesn't provide access to any of its descendants unless those descendants also happen to match the condition.
Starts with	Provides access to account values that start with the specified value. When the matching value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. It doesn't provide access to any of its descendants unless the descendants also happen to match the condition.

Operator	Description
Is descendant of	Provides access to the specified parent account value and all its descendants. Descendants include middle level parent accounts and nonparent accounts throughout all that parent's hierarchical branches, from the root to the leaf nodes.
Is last descendant of	Provides access to the specified parent account value and to the account values at the leaf nodes of that parent. Access doesn't include intermediate parent account values along the hierarchical branches.

Note: For the **Is descendant of** and **Is last descendant of** operators, the security rule provides access across all tree versions of the specified hierarchy that reference the accounts that are granted, as well as all hierarchies associated with the same value set of the specified hierarchy. It uses the parent value rollup of the rule's specified hierarchy as the basis for determining which values are granted and applies date effectivity to identify which is the effective version based on the system date for the rule's specified hierarchy and the account values included in that version. For more information see the *Reporting on General Ledger Balances Cubes Reports with Account Hierarchies* topic.

From Value

Specifies the value to apply for the specified condition filter operator in determining what account values to consider. You must specify a valid account value when using any condition filter operator, except for Between, Contains, Ends with, and Starts with. This allows for some additional flexibility to include account values that have yet to be created.

To Value

Specifies the value to apply for the Between condition filter operator in determining what account values to consider. This is the ending value for the range and allows for some additional flexibility to include account values that have yet to be created.

Tree Code

Identifies the tree to reference when you select a parent account value for the condition. This is a required attribute if you're using the **Is descendant of** and **Is last descendant of** operators. These operators are also the only valid operator choices when you specify a tree code for the row. Double-click within the cell to open a dialog box, where you can select a valid tree code for the secured value set that you're working with.

While a distinct tree code is associated with each segment in a chart of accounts, as specified by the Default Hierarchy value in the chart of accounts structure setup, you can refer to any tree that's defined for the secured value set.

Note: The trees that you specify in a rule must be flattened. This contrasts with trees that are published to balances cubes, which don't need to be flattened. If your security rules refer to trees that are published to the balances cubes, then the trees must be flattened. Otherwise security enforcement won't work in balances cube-based reports and queries.

Tree Version

Identifies the tree version of the selected tree code to reference when you select a parent account value for the condition. This is a required attribute if you're using the **Is descendant of** and **Is last descendant of** operators. These operators are also the only valid operator choices when you specify a tree version for the row.

Policy Start Date

Specifies when the policy begins. You must specify a start date that's no earlier than the current system date when creating the policy because a policy can't be effective for any earlier date than when it comes into existence. You can also specify a future date.

This attribute must share the same value among related rows of multiple condition filters that are tied to the same policy.

> **Note:** When you add new condition filter rows to an existing policy, the start date for the new rows must match the start date of the original policy rows because this is a policy-level attribute.

Policy End Date

Specifies when the policy ends. You must specify an end date that's no earlier than the policy start date. If you don't specify an end date, then the policy is in effect indefinitely.

You can update the end date on an existing policy as long as the specified end date is today or a date in the future. That is, the rule is still active. The new end date must be at least today's date or a date in the future. There's no requirement for the new end date to be later than the current end date.

For example, let's say today's date is January 27 and the end date for a rule is set to January 31. A day later, on January 28, you can update the end date to January 28 or later. It doesn't have to be set beyond January 31, which is the original end date. However, you can't update the end date from January 31 once it's February 1.

This attribute must share the same value among related rows of multiple condition filters that are tied to the same policy.

> **Note:** When you add new condition filter rows to an existing policy, the end date for the new rows must match the end date of the original policy rows, if there is one, because this is a policy level attribute.

For audit purposes, segment value security policies are never deleted. The Policy End Date attribute is used instead to indicate that the policy is no longer applicable.

Mark for Deletion

Indicates whether to delete the selected condition filter row and remove it from the policy. This deletion indicator safeguards users from accidentally deleting condition filter rows for a policy from the application by requiring users to explicitly indicate this action for a given row. This is a condition-level attribute and individual condition filter rows associated with the policy can be specifically marked for deletion.

> **Note:** If the only condition filter row for a given condition is marked for deletion, the application will automatically end date the policy and no longer display such empty policies in the spreadsheet, that is, a policy with no condition filter rows.

Related Topics

- Using the Manage Segment Value Security Rules Spreadsheet

Create Rule Assignments

The Rule Assignments worksheet of the Manage Segment Value Security Rules spreadsheet is for assigning policies to users, qualifying under which business function and security context the policy assignments are applicable for the user, and granting either a read only, or a read and write access level.

Enter attribute values in the order in which the columns appear in the worksheet.

This table lists the attribute columns on the Rule Assignments worksheet and their properties.

Attribute	Required	Updatable
User Name	Yes	No
Policy Name	Yes	Yes
Role Name (Display Only)	Not applicable	Not applicable
Business Function	Yes	Yes
Security Context	Yes	Yes
Security Context Value	Yes	Yes
Access Level	Yes	Yes
Start Date	Yes	No
End Date	No	Yes

Here's more information about each attribute to help you prepare the Rule Assignments worksheet.

User Name

Identifies the user for the rule assignment. Select one of the following options:

- **Select specific**: Select to specify the sign in name of the user who's to be assigned the rule or policy for the given secured value set.
- **Select all assigned to the policy role**: Select to share the rule assignment with all users who are assigned the role for the specified policy.

Policy Name

Identifies the policy to assign to the user. Double-click within the cell to open a dialog box, where you can select a valid policy for the given secured value set.

Role Name

Identifies the role associated with the policy selected for the rule assignment. This is a display-only field and is shown as additional information when searching and retrieving a rule assignment from the application.

Business Function

Identifies the business function that the rule assignment for the user applies to. The list corresponds to the product modules that support segment value security by business function.

> **Note:** To create a rule assignment for a given business function, that function must be enabled for segment value security enforcement.

This table lists the business functions and their corresponding product modules.

Business Function	Product Module
Assets	Oracle Assets
General Ledger	Oracle General Ledger
Payables	Oracle Payables
Provider intercompany	Oracle Intercompany
Receivables	Oracle Receivables
Receiver intercompany	Oracle Intercompany

Selecting any of these business functions automatically includes Oracle Subledger Accounting, a product module that integrates between General Ledger and the subledgers.

> **Note:** The 2 Intercompany business functions allow you to further differentiate whether the rule assignment to the user for the specified intercompany organization is applicable when the intercompany organization is being used by the user to transact in the capacity of a provider or a receiver.

You can also select **All business functions** if the grant of the policy to the user isn't limited for just a particular business function. It can also be used in the case of the Intercompany module when the rule assignment to an Intercompany user applies no matter when the specified intercompany organization is transacting in the capacity of a provider or receiver.

The selection for this attribute also determines which choice is valid for the following **Security Context** attribute because the security context corresponds to the selected business function.

Security Context

Identifies the type of security context under which the policy or rule assignment should be valid for the user. You must select a security context that correlates to the selected business function. For example, for the General Ledger business function, the applicable security context is data access set.

Here are the possible choices:

- Business unit: Applies to the Payables and Receivables business functions.
- Asset books: Applies to the Assets business function.
- Data access set: Applies to the General Ledger business function.
- Intercompany organization: Applies to the Intercompany business functions.
- All security contexts: Applies to any business function.

Note: If you want to include the business unit for both the Payables and Receivables business functions, select **All business functions** for the Business Function attribute.

The selection for this attribute also determines which choice is applicable for the following **Security Context Value** attribute because the context value corresponds to the selected security context.

If it isn't necessary to limit a user's policy to be applicable for a particular security context and security context value, you can select **All security contexts**. This selection can be paired with the selection of **All business functions**, or a specific business function, in the preceding column. For the former, this means that the rule assignment or policy grant for the user will be applicable no matter what business function, security context, and security context value that user is working with. It effectively means that this policy is applicable for the user all the time. If a specific business function is selected, the rule assignment is applicable to the user only for the selected business function, but without regards to the security context value that user is working with.

If you select **All security contexts**, the only valid choice for the **Security Context Value** attribute is **All security context values**.

Security Context Value

Specifies the security context value for the selected security context type and business functions in the preceding 2 columns under which the policy or rule assignment will be effective for the user. The possible choices include the valid asset books, business units, data access sets, or intercompany organizations in the system, depending on the security context that was selected for the rule assignment.

For the policy or rule assignment to be a relevant and effective one for the users to which they're assigned, ensure that the selected asset book, business unit, data access set, or intercompany organization for that rule assignment is one that's assigned to the user in the Manage Data Access for Users page and to which the user has been granted data access.

There's also a choice of **All security context values**, which is the only valid choice when **All security contexts** is selected for the preceding **Security Context** column. This would make this policy always applicable to the user, no matter what data access context that user is working with.

Access Level

Indicates whether the user rule or policy assignment for the given business function, security context, and context value should be granted on a **Read only** or **Read and write** basis.

For rule assignments that are set to **Read only**, the account values allowed will only be applicable in read-only features, such as an inquiry page or a report. Where the product feature involves update capabilities for accounting data, these account values with read-only access will not be available to the user.

For rule assignments that are set to **Read and write**, the account values allowed will be applicable in read-only features as well as those features that involve update capabilities for accounting data.

Start Date

Specifies when the user rule assignment begins. The date can't be earlier than the current system date when you're creating a new user rule assignment. This is because a rule assignment can't be effective any earlier than the date when it's created. You can also create a user rule assignment with a future date as the start date.

Note: The start date can't be any earlier than the start date of the policy referenced in the rule assignment.

End Date

Specifies when the user rule assignment ends. This date can't be earlier than the user rule assignment's start date and any later than the end date of the policy referenced in the rule assignment.

You can update the end date on an existing user rule assignment as long as the current end date is today or a date in the future. That is, the rule assignment is still active. The new end date must be at least today's date or a future date, but still within the end date of the policy referenced in the rule assignment. There's no requirement for the new end date to be later than the current end date for the user rule assignment.

For example, let's say today's date is January 27 and the end date for a rule assignment is set to January 31. A day later on January 28, a new end date can be set to January 28 or later as long as it doesn't exceed the end date of the policy referenced in the rule. It doesn't have to be set beyond January 31, which is the original end date. However, you can't update the end date on the rule assignment from January 31 once it's February 1.

For audit purposes, records of segment value security policy assignments to users are never deleted. The rule assignment End Date attribute is used instead to indicate that the policy assignment is no longer applicable.

Related Topics

- Using the Manage Segment Value Security Rules Spreadsheet

Edit Rules and Rule Assignments

To edit existing rules and rule assignments, it's very important, and will always be required, to first download the records from the application.

This ensures that you're working with the current version of the rule or rule assignment that's stored in the application. You can download existing rule and rule assignment records for the secured value set for review or edit by using the Search command on either worksheet on the Manage Segment Value Security tab.

Once you've downloaded the records you want to update, make your edits, and upload your changes to save them to the application. You can also create rules and user rule assignments in the same spreadsheet that you're editing.

On the Rules worksheet, you can filter your search for policies by policy name, segment value security role, or both, by specifying relevant search strings for these fields.

On the Rule Assignments worksheet, you can filter your search for user rule assignments by user name, policy name, or both, by specifying the relevant search strings for these fields.

Best Practices for Creating Segment Value Security Roles

Here are some best practices for creating and maintaining roles for segment value security.

- Create the role solely for the purpose of assigning segment value security policies. This prevents the potential commingling with other elements of data security and other artifacts that might be present in other roles. That could make it much more difficult to diagnose when segment value security rules aren't acting in an expected manner.

  > **Note:** Set the Role Category to **Default**.

- Don't form hierarchies with segment value security roles. Hierarchies could result in the rolling up of data security policies to a user from the various roles within the role hierarchy, based on the assignment of that one segment value security role. This will make it difficult to evaluate the data security a user ends up with, and

to identify the precise origin of certain data security policies the user ended up with if unexpected results are encountered.

- It's generally not advisable to use job roles, predefined by Oracle or otherwise, to pass on segment value security policies because it's highly unlikely that a group of users who share a job role will also share the exact same security profile for a secured chart of accounts.

  By attaching segment value security policies to job roles, any user who's assigned that job role will uniformly pick up those data security policies. Job roles are primarily for the purpose of passing function security access to features in a product module, and shared among users who have the same job function, but most likely for different parts of the organization. It's generally best to not incorporate data security access directly into a job role.

- Assess the total number of unique variations of segment value security profiles across all users in the organization who'll need access to a given secured value set. Then, define individual segment value security roles for each of these security profiles by creating empty roles before creating the segment value security policies. The purpose of these roles is to serve as a method to pass through specific chart of accounts segment value security data security policies intended for a given user, or user group, by assigning this segment value security role to the appropriate users.

  Minimize the number of policy definitions that you maintain for a given secured value set by having each policy definition comprehensively capture each of these identified security profiles for that value set. This helps promote a more manageable framework for maintaining the segment value security requirements for your organization.

- Maintaining individual segment value security roles for each distinct data security profile among all the users and user groups in the organization will also help with ongoing maintenance of your segment value security setups. Any required change to such a segment value security data security profile would only require making a change to the one segment value security role and this will automatically cascade down to all the users that belong to that one security profile.

  The one segment value security role can be assigned different policies from within the same secured value set. Even policies from different secured value sets can be assigned, so long as that common security profile applicable to the entire group of users who will share that segment value security role, includes each and every one of these segment value security policies for the one or more secured value sets that will be tied to this segment value security role.

  Loading up the one segment value security role can help with cutting down the number of segment value security roles that need to be maintained, and each role can be used very efficiently. However, this can also substantially increase the complexity of organizing and maintaining the segment value security setups by creating additional interdependencies between the security requirements for different policies and different secured value sets, and the security segment value security requirements of each user placed into this group. As such, take caution when loading up a segment value security role in this manner and apply the requisite judgment in weighing the benefits and costs of taking such a decision to determine the optimal fit for your organization.

CAUTION: Don’t use the Security Console Role Copy feature to make copies of such segment value security roles that have segment value security policies assigned through policies created using the Manage Segment Value Security Roles spreadsheet. The Role Copy function doesn’t account for all the attributes maintained for policy definitions that were created using the spreadsheet. A role created from such a copy action will have data security policy assignments that are incomplete and that won’t function properly.

Assign Segment Value Security Roles to Users

For a user to be effectively granted a particular chart of accounts segment value data security policy, that user will need to be assigned the segment value security role tied to that policy.

A working setup to limit access to just certain specific secured account values also requires that the user must have one or more rule assignments for the policy associated with the assigned role. The assignments stipulate under which business function and data access context the policy should be effective for the user, and whether the access level is on a read-only or read and write basis. Otherwise, such a policy can never be actively applied for that user despite the user being assigned its associated role.

When working with a secured chart of accounts segment value set where the user doesn't have a matching rule assignment for a given usage context, that user will have access to all values by default.

Examples of Generic User Rule Assignments for Segment Value Security

To make policies more shareable, you can define generic rule assignments, that is, you define a rule assignment without one or more specific values for the following attributes:

- User Name
- Business Function
- Security Context and Security Context Value

You can select different variations of settings for these attributes to achieve the desired effect of granting access to a user for the secured account values.

Rule Assignments Without a Specified User Name

In this example, you assign three users the same segment value security role.

This is because there are cases where all three users will need access to the same secured account values under the same qualified circumstances of business function, data security context, and access level, which are the attributes of a rule assignment.

The users are CCLARK, LLOPEZ, and PPATEL. They use Oracle General Ledger and are all assigned the same Vision Corporation data access set. The Natural Account segment of the chart of accounts is secured and you define a policy that allows read and write access to all accounts that start with 1. You assign the policy to the shared segment value security role.

This table shows the relevant attribute values on the Rules worksheet.

Attribute	Value
Policy Name	Accounts Start with 1
Policy Description	Natural account segment values start with 1

Attribute	Value
Role Name	Shared Segment Value Security
Operator	Starts with
From Value	1

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
User Name	All users assigned to the role of the policy
Policy Name	Accounts Start with 1
Role Name	Shared Segment Value Security
Business Function	General Ledger
Security Context	Data access set
Security Context Value	Vision Corporation
Access Level	Read and write
Start Date	1-Jan-2024

The User Name for this rule assignment is **All users assigned to the role of the policy**. This indicates that the rule assignment will apply to users CCLARK, LLOPEZ, and PPATEL for the General Ledger business function when using the Vision Corporation data access set on a read and write basis because they're all assigned the segment value security role Shared Segment Value Security.

Rather than having to define three separate rule assignments for each user, you can structure the rule assignment this way to allow it to be shared and the policy effectively applied to all three users. This streamlines the maintenance of the rule and rule assignment.

Rule Assignments Without a Specified Business Function

It's possible to assign a rule to a user or group of users in a broad manner, where the grant to the secured value is applicable to all business functions that the user or group of users works with.

In this first example, the rule assignment is a broad one, where the user CCLARK can use the Cost Center 100 policy for whatever business function that CCLARK is working with, and for any security context and security context value on a read and write basis.

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
User Name	CCLARK
Policy Name	Cost Center 100
Role Name	CCLARK Cost Center 100

Attribute	Value
Business Function	All business functions
Security Context	All security contexts
Security Context Value	All security context values
Access Level	Read and write
Start Date	1-Jan-2024

In this second example, the rule assignment applies to all business functions on a read and write basis, but the user CCLARK is limited to just when the security context is Business unit.

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
User Name	CCLARK
Policy Name	Cost Center 100
Role Name	CCLARK Cost Center 100
Business Function	All business functions
Security Context	Business unit
Security Context Value	All security context values
Access Level	Read and write
Start Date	1-Jan-2024

Business unit is a relevant security context for the Payables and Receivables business functions. Therefore, this rule assignment would effectively only apply when the user CCLARK is working with those two business functions, and not other business functions like Assets, General Ledger, Provider Intercompany, and Receiver Intercompany, which use a different security context.

Rule Assignments Without a Specified Security Context

The previous topic described a rule assignment example that broadly covered all usage contexts, regardless of the business function, security context, and security context value for the user's usage scenario.

Here are some additional considerations for rule assignments without a specified security context.

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
Business Function	All business functions
Security Context	All security contexts
Security Context Value	All security context values

Because there isn't a single business function where all the different security context types (Asset book, Business unit, Data access set, Intercompany organization) would apply, the **All security contexts** selection for the Security Context attribute of a rule assignment can only work with the **All business functions** selection for the Business Function attribute.

Also, since there likely isn't a single security context value that would be a match for all the different security context types, selecting **All security contexts** for the Security Context attribute for the rule assignment would also automatically mean **All security context values**.

Using Export and Import Services with Segment Value Security by Business Functions Configurations

You need to ensure that the source and target environments for the export and import process are compatible for segment value security.

They must be based on the same segment value security method of either segment value security by business function or segment value security without the business function distinction. Mixing and matching of source and target environments identified with different segment value security methods for such export and import processes will cause data corruptions with the setup configurations in the target environment.

You need to also ensure when using export and import services for segment value security rules and rules assignments from a source to a target environment that the method by which such setup records are created are the same in both environments. Commingling the usage of the Manage Segment Value Security Rules spreadsheet with the Edit Data Security page or the Rapid Implementation spreadsheet to maintain your segment value security setups will result in serious data inconsistencies that will cause the incorrect enforcement of segment value security.

Enforcement of Segment Value Security by Business Function

These examples illustrate key points about how segment value security by business function enforcement works when using the following types of General Ledger features that involve the chart of accounts:

- Journal entry
- Submission of the predefined Oracle Analytics Publisher Trial Balance Report using the Scheduled Processes page
- Balances cube-based online inquiry using Account Monitor
- Balances cube-based inquiry using Smart View

For all examples, the General Ledger business function has been enabled for security enforcement and the Company, Cost Center, and Natural Account segments of the chart of accounts have been secured. These examples will focus on the segment value security rules for the Natural Account segment. The users in these examples don't have a rule assignment for the Company and Cost Center segments. This means they will have access to all account values based on the default all values access behavior with segment value security by business function.

Here are some more characteristics of the chart of accounts.

- The first segment is the Company segment, the second is the Line of Business segment, the third is the Account segment, the fourth is the Cost Center segment, and the fifth is the Product segment.

- Asset type account values start with 1, Liability type account values start with 2, Owner's Equity type accounts start with 3, Revenue type accounts start with 4, and Expense type accounts start with 5.

There are 3 users: CCLARK, LLOPEZ, and PPATEL. Both CCLARK and PPATEL not only manage the financial accounting for their region, but they're also responsible for calculating the global bad debt reserve. They require full read and write access to all accounts when working with the financial data specific to their assigned region but should have read and write access to just certain accounts for the worldwide financial data related to calculating the global bad debt reserve. For example, PPATEL's configuration mirrors such access requirements with the two data access set assignments.

The following tables provide details on the ledger sets, account access, security profiles, rules, and rule assignments for the examples that follow.

This table lists the ledger sets and their corresponding ledgers.

Ledger Set	Ledgers
Vision Corporation North America	Vision Corporation Canada, Vision Corporation USA
Vision Corporation Global	Vision Corporation Canada, Vision Corporation USA, Vision Corporation Japan

This table describes the Natural Account segment values for the secured chart of accounts that will be used in the rule assignments.

Account or Account Range	Account Description	Parent
12010 - 12999	Bad debt reserve accounts	No
REV	Revenue accounts	Yes
EXP	Expense accounts	Yes
88888	Net Equity All Balance Sheet Accounts	Yes

This table describes the security profile for each user.

User Name	Functional Role	Assigned Data Access Sets	Allowed Accounts	Access Level
CCLARK	General Accounting Manager	Vision Corporation Global	All	Read and write
LLOPEZ	Financial Analyst	Vision Corporation USA	All nonrevenue	Read only
PPATEL	General Accountant	Vision Corporation North America, Vision Corporation Global	All for Vision Corporation North America data access set, Bad debt and revenue for Vision Corporation Global data access set	Read and write

The following tables describe the rules and user rule assignments for the secured chart of accounts, Account segment, and Account Vision Corporation value set that were defined to provide access to the users according to their security profile.

This table lists the attribute values that were entered on the Rules worksheet, except for the Policy Description.

Row	Policy Name	Role Name	Operator	From Value	To Value	Tree Code	Tree Version
1	PPATEL Bad Debt and Revenue Accounts	PPATEL Role	Between	12010	12999	This field is blank.	This field is blank
2	PPATEL Bad Debt and Revenue Accounts	PPATEL Role	Is descendant of	REV	This field is blank.	Account Vision Corporation	Account Vision Corporation Current
3	LLOPEZ Nonrevenue Accounts	LLOPEZ Role	Is descendant of	8888	This field is blank.	Account Vision Corporation	Account Vision Corporation Current
4	LLOPEZ Nonrevenue Accounts	LLOPEZ Role	Is descendant of	EXP	This field is blank.	Account Vision Corporation	Account Vision Corporation Current

This table lists the attribute values that were entered on the Rule Assignments worksheet.

User Name	Policy Name	Role Name	Business Function	Security Context	Security Context Value	Access Level
PPATEL	PPATEL Bad Debt and Revenue Accounts	PPATEL Role	General Ledger	Data access set	Vision Corporation Global	Read and write
LLOPEZ	LLOPEZ Nonrevenue Accounts	LLOPEZ Role	General Ledger	Data access set	Vision Corporation USA	Read only

Journal Entry

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic.

It shows how segment value security by business function is enforced for users CCLARK, LLOPEZ, and PPATEL when they're using a transaction entry feature like General Ledger journal entry on the Create or Edit Journal pages.

Let's start with CCLARK. Here's a summary of CCLARK's security profile.

- Assigned Data Access Set: Vision Corporation Global
- Allowed Accounts: All
- Access Level: Read and write

This profile highlights the default grant to all users where they're provided access to all account values on a read and write basis of a secured value set, unless they're assigned a specific rule assignment to limit their access to just certain account values. CCLARK, LLOPEZ, and PPATEL have no rule assignments for the secured Company and Cost Center segments, so they have access to all Company and Cost Center values on a read and write basis This makes it efficient to maintain rules and rule assignments because you only need to maintain such configurations in cases where chart of accounts security enforcement to limit access to just certain secured accounts is required for the user.

CCLARK is on the Edit Journal page, reviewing an unposted journal for the Vision Corporation USA ledger and this table shows the journal line numbers, accounts, and entered amounts that CCLARK can view.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
1	3111-00-11010-000-0000	1,000.00	0.00
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-21010-000-0000	0.00	1,000.00
4	3111-00-31001-000-0000	0.00	1,000.00
5	3111-00-40110-000-0000	0.00	1,000.00
6	3111-00-52110-000-0000	1,000.00	0.00
NA	Total	3,000.00	3,000.00

CCLARK can view every journal line, which reference different Natural Account segment values. With read and write access to all these accounts, CCLARK can also edit the existing lines, add new lines to the journal entry, and create a new journal entry for any account.

Let's now review how this same journal entry would appear to the user LLOPEZ. Here's a summary of LLOPEZ's security profile.

- Assigned Data Access Set: Vision Corporation USA
- Allowed Accounts: All nonrevenue
- Access Level: Read only

This table shows the journal lines line numbers, accounts, and amounts for the unposted journal that LLOPEZ can view.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
1	3111-00-11010-000-0000	1,000.00	0.00
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-21010-000-0000	0.00	1,000.00
4	3111-00-31001-000-0000	0.00	1,000.00
6	3111-00-52110-000-0000	1,000.00	0.00
NA	Total	3,000.00	3,000.00

Journal line 5 won't display because it's for a revenue account. In addition, LLOPEZ has read-only access to the nonrevenue accounts and can only view the journal information. LLOPEZ can't edit the existing lines, add new lines, or create journals. LLOPEZ also can't select any full account combination because the access granted is only to nonrevenue accounts for the secured Natural Account segment and only on a read-only basis.

Finally, let's review how this same journal entry appears to PPATEL. Here's a summary of PPATEL's security profile.

- Assigned Data Access Set: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America data access set, Bad debt and revenue for Vision Corporation Global data access set
- Access Level: Read and write

PPATEL has access to the Vision Corporation USA ledger through both data access sets and has different access profiles for each data access set.

Here are some key points.

- A user's access to a secured chart of accounts segment value set can be differentiated, if required, for each business function and security context the user works with. This allows great flexibility in fine-tuning a user's access to secured account values in as specific a manner as required by configuring the rule assignments accordingly.
- The users PPATEL and CCLARK share the same Vision Corporation Global data access set. However, while CCLARK has access to all accounts with that data access set, PPATEL's access is restricted to bad debt and revenue accounts for that same data access set. This highlights the concept that user rule assignments are specific to a given user and the specified data access set in the rule's security context value attribute, in the case of General Ledger.

  A user rule assignment has a set of qualifiers as to when or how the referenced policy will apply, relevant to the specified user. The same notion applies with user rule assignments for the other types of security contexts, such as business units, asset books, and intercompany organization, and their relevant security context values, for their applicable business functions of Payables, Receivables, Asset Books, and Intercompany.

While using the Vision Corporation North America data access set PPATEL can see every line of the unposted journal entry. Moreover, PPATEL can edit any of the journal lines.

This table shows the journal line numbers, accounts, and entered amounts that user PPATEL can view and edit.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
1	3111-00-11010-000-0000	1,000.00	0.00
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-21010-000-0000	0.00	1,000.00
4	3111-00-31001-000-0000	0.00	1,000.00
5	3111-00-40110-000-0000	0.00	1,000.00
6	3111-00-52110-000-0000	1,000.00	0.00
NA	Total	3,000.00	3,000.00

Note: While PPATEL is working with the Vision Corporation North America data access set, this access would be the same with the journals for the Vision Corporation Canada ledger, which is part of that data access set.

While using the Vision Corporation Global data access set, PPATEL's access is limited to the bad debt and revenue accounts and this table shows the journal line numbers, accounts, and entered amounts that user PPATEL can view and edit.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-40110-000-0000	0.00	1,000.00

Line	Account	Entered (USD) Debit	Entered (USD) Credit
NA	Total	3,000.00	3,000.00

PPATEL can view and edit these journal lines and create journals with the bad debt and revenue accounts.

Note: While PPATEL is working with the Vision Corporation Global data access set, this access would be the same with the journals for the Vision Corporation Canada and Vision Corporation Japan ledgers, which are part of that data access set.

Standard Reports

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic.

It shows how segment value security by business function is enforced for users CCLARK, LLOPEZ, and PPATEL when they're submitting the Trial Balance Report for General Ledger on the Scheduled Processes page.

When users submit the report, they must select one of their assigned data access sets. This selection sets the scope for which ledger the report is to be submitted. For segment value security by business function with a secured chart of accounts, the data access set is also the basis for determining if there are applicable user rule assignments that would limit the accounts whose balances should be included in the generated report for that user.

The report will be submitted for the same Vision Corporation USA ledger and will focus on the secured Natural Account segment. The users LLOPEZ and PPATEL have user rule assignments that limit access to some natural account values.

Let's start with CCLARK and the summary of CCLARK's security profile.

- Assigned Data Access Set: Vision Corporation Global
- Allowed Accounts: All
- Access Level: Read and write

When CCLARK submits the report for the Vision Corporation USA ledger using the assigned Vision Corporation Global data access set, the report output displays balances for all the natural account values. Having read and write access to secured account values provides CCLARK with the ability to inquire and report on transactions and balances, as well as create transactions and update balances for these accounts.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that CCLARK can view.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
11010	Cash	0.00	90,000.00	0.00	90,000.00
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
21010	Accounts Payable	0.00	0.00	20,000.00	-20,000.00
31001	Common Stock	0.00	0.00	50,000.00	-50,000.00
40110	White Wine Revenue	0.00	0.00	60,000.00	-60,000.00
52110	Cost of Goods Sold – White Wines	0.00	30,000.00	0.00	30,000.00

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
Total	NA	0.00	130,000.00	130,000.00	0.00

Next, let's look at the report for the user LLOPEZ. Here's a summary of LLOPEZ's security profile.

- Assigned Data Access Set: Vision Corporation USA
- Allowed Accounts: All nonrevenue
- Access Level: Read only

Having read-only access to the secured account values provides the ability to inquire and report on its transactions and balances. The report doesn't include the Revenue account because LLOPEZ's grants to the secured Natural Account segment for the chart of accounts don't include revenue accounts.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that LLOPEZ can view.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
11010	Cash	0.00	90,000.00	0.00	90,000.00
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
21010	Accounts Payable	0.00	0.00	20,000.00	-20,000.00
31001	Common Stock	0.00	0.00	50,000.00	-50,000.00
52110	Cost of Goods Sold – White Wines	0.00	30,000.00	0.00	30,000.00
Total	NA	0.00	130,000.00	70,000.00	60,000.00

Lastly, let's look at the output for the user PPATEL. Here's a summary of PPATEL's security profile.

- Assigned Data Access Set: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America data access set, Bad debt and revenue for Vision Corporation Global data access set
- Access Level: Read and write

When PPATEL runs the report using the Vision Corporation North America data access set, where PPATEL has read and write access to all accounts, the report output displays all the accounts that have balances for the Vision Corporation USA ledger.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that PPATEL can view when submitting the report for the Vision Corporation North America data access set.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
11010	Cash	0.00	90,000.00	0.00	90,000.00
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
21010	Accounts Payable	0.00	0.00	20,000.00	-20,000.00
31001	Common Stock	0.00	0.00	50,000.00	-50,000.00
40110	White Wine Revenue	0.00	0.00	60,000.00	-60,000.00
52110	Cost of Goods Sold – White Wines	0.00	30,000.00	0.00	30,000.00
Total	NA	0.00	130,000.00	130,000.00	0.00

When PPATEL runs the report using the Vision Corporation Global data access set, where PPATEL has read and write access to the bad debt and revenue accounts, only the balances for those two accounts appear in the report output.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that PPATEL can view when submitting the report for the Vision Corporation Global data access set.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
40110	White Wine Revenue	0.00	0.00	60,000.00	-60,000.00
Total	NA	0.00	10,000.00	60,000.00	-50,000.00

This example with the user PPATEL illustrates how segment value security rule assignments for a user can be configured in a manner that precisely grants access to secured accounts for a specific data security context value, such as a data access set in the General Ledger module.

Account Monitor Inquiries

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic and focuses on the user PPATEL.

The Account Monitor is an online inquiry tool for reviewing a ledger's account balances.

Users can view summarized account balances rolled up by parent account values and can save their inquiries in the form of account groups. The inquiry results are projected in the Account Monitor. Balances are based on the General Ledger balances cube where balances aggregation is maintained according to the hierarchies for the different data dimensions, including dimensions based on the chart of accounts segments.

Here's a summary of PPATEL's security profile.

- Assigned Data Access Sets: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America, Bad debt and revenue for Vision Corporation Global
- Access Level: Read and write

The account group in this example inquires on a set of account balances for the Vision Corporation USA ledger, with individual natural account values in each row.

When the user PPATEL views the account balances in the Account Monitor using the Vision Corporation North America data access set, all account balances are displayed. This is because PPATL has read and write access to all Natural Account segment values for the secured chart of accounts.

This table shows the account segment values that the user PPATEL can view in the Account Monitor. The Company, Line of Business, Cost Center, and Product columns are excluded from the table because PPATEL has access to all those segment values.

Name	Ledger	Account
Bad Debt Reserve	Vision Corporation USA	12010
Accounts Payable	Vision Corporation USA	21010
Common Stock	Vision Corporation USA	31000
Revenue	Vision Corporation USA	40110
Expense	Vision Corporation USA	52110

When the user PPATEL views the account balances in the Account Monitor using the Vision Corporation Global data access set, only balances from the bad debt and revenue accounts display. This is because PPATEL has read and write access to only the bad debt and revenue Natural Account segment values for the secured chart of accounts.

This table shows the account segment values that the user PPATEL can view in the Account Monitor. The Company, Line of Business, Cost Center, and Product columns are excluded from the table because PPATEL has access to all those segment values.

Name	Ledger	Account
Bad Debt Reserve	Vision Corporation USA	12010
Revenue	Vision Corporation USA	40110

Smart View Inquiries

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic and focuses on the user PPATEL.

It shows how segment value security by business function is enforced in an inquiry tool that's launched outside of the main General Ledger application. Security enforcement is applied just like in the main application, except there are some considerations when the data access set for the user changes.

Smart View is a spreadsheet-based tool for inquiring on General Ledger account balances data that are stored in the General Ledger balances cube. The General Ledger balances cube is where balances aggregation is maintained according to the hierarchies for the different data dimensions, including dimensions based on the chart of accounts segments.

Here's a summary of PPATEL's security profile.

- Assigned Data Access Sets: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America, Bad debt and revenue for Vision Corporation Global

- Access Level: Read and write

When the user PPATEL views the account balances in Smart View using the Vision Corporation North America data access set, all account balances are displayed. This is because PPATL has read and write access to all the secured Natural Account segment values for the secured chart of accounts.

This table shows the accounts and balances that the user PPATEL can view in the Smart View inquiry for the Vision Corporation USA ledger when using the Vision Corporation North America data access set. The point of view for the inquiry includes all values for the Company, Line of Business, Cost Center, and Product segments.

Account	Vision Corporation USA
11010 – Cash	90000
12010 – Bad Debt Reserve	10000
21010 – Account Payable	-20000
31000 – Common Stock	-50000
4011 – Revenue	-60000
52110 – Expense	30000

When the user PPATEL views the account balances in Smart View using the Vision Corporation Global data access set, only balances from the bad debt and revenue accounts display. This is because PPATEL has read and write access to only the bad debt and revenue Natural Account segment values for the secured chart of accounts.

This table shows the accounts and balances that the user PPATEL can view in the Smart View inquiry for the Vision Corporation USA ledger when using the Vision Corporation Global data access set. The point of view for the inquiry includes all values for the Company, Line of Business, Cost Center, and Product segments.

Account	Vision Corporation USA
11010 – Cash	#No Access
12010 – Bad Debt Reserve	10000
21010 – Account Payable	#No Access
31000 – Common Stock	#No Access
40110 – Revenue	-60000
52110 – Expense	#No Access

When users work with reporting tools for the General Ledger balances cube such as Smart View and Financial Reporting, which are outside of the main application, there's no explicit data access set selection. Users must change the data access within the main application by using the data access set selector or by changing the data access set in General Ledger preferences.

Note: To change the General Ledger preference, use the Set Preferences option on the Settings and Actions menu in the global header.

After changing the data access set, users can click **Refresh** in the Point of View section of the Smart View spreadsheet to register the data access set selection change. For Financial Reporting, users can rerun the report. Taking these steps ensures that the correct segment value security grants are applied to the reports with these reporting tools based on the current data access set selection.

Special Considerations for Segment Value Security

There are special considerations for segment value security by business function in the following areas:

- Back-end processes
- Setup tasks
- Oracle Transactional Business Intelligence reporting
- Features without a specific data security context
- Multiple secured chart of account segments
- Primary balancing segment value assignments to a ledger or its legal entities
- Switching from secured to unsecured modules

Back-End Processes

Segment value security by business function isn't enforced for back-end processes.

Back-end processes are submitted processes that run in the background without active engagement from users. Some of these processes can generate or update financial data that's framed by chart of account values like accounting transactions and account balances.

This table provides examples of such back-end processes.

Module	Back-End Processes
General Ledger	Posting, Translation, Revaluation, Open Period
Subledger Accounting	Create Accounting

Note: While reports on financial data are also submitted for processing, they aren't considered back-end processes. They're requests to display financial data in an output format.

Segment value security by business function isn't enforced for such back-end processes for these reasons.

- As accounting becomes more automated, administrators are more likely to submit back-end processes on behalf of end users, who work with the financial data resulting from these processes.
- In some cases, the application itself might initiate the submission of the back-end process.
- The user submitting back-end processes might be detached from the end users who will ultimately work with the resulting financial data.
- There might be a lack of direct correlation between the back-end processes and the security profiles of the users submitting these processes.

The key to securing financial data is to ensure that end users should only be able to access the financial data that they're authorized to work with. As such, enforcement of segment value security by business function is strictly applied when such users update financial data, or report or inquire on it.

Setup Tasks

Segment value security by business function isn't enforced for setup tasks.

Some setup tasks are related to the configuration of application or processing rules that produce accounting transactions and financial data. Such setup tasks often touch on elements of a chart of accounts and include configurations and mapping rules that drive what chart of account values will be used when the financial data is generated.

Access to such setup tasks, especially around setting up reference data, is typically granted only to an administrator job role, where users assigned that role would be responsible for configuring the application. These users don't work directly with the financial data itself.

In addition to reference data setup, these tasks also include transaction generation setups, which can directly generate accounting or journal entries.

Here are some examples.

- Assets: Asset book definition
- General Ledger: Allocation formulas
- General Ledger: Chart of accounts configuration
- General Ledger: Chart of Accounts Mapping rules
- General Ledger: Ledger definition
- General Ledger: Revaluation definitions
- Intercompany: Balancing Account rules
- Receivables: AutoInvoicing rules
- Subledger Accounting: Create Accounting rules
- Subledger Accounting: Transaction Account Builder rules

Setup tasks typically don't have a selection for a security context value, such as a data access set, business unit, asset books, or intercompany organization, for the purposes of establishing the data security element while working on the setup record.

If such security context objects were referenced, it's for the purpose of identifying which instance of that object the setup is being configured for, rather than about creating financial data with that security context value.

The administrator, or the user provided functional access to work with such setup tasks, can set up configurations and accounting rules across all ledgers, business units, asset books, and intercompany organizations in the application. A setup administrator user can use any account value, even for a secured chart of accounts value set. Access to the setup tasks alone allows the user to work with any of such setup records without further data security enforcement.

Oracle Transactional Business Intelligence Reporting

For segment value security with Oracle Transactional Business Intelligence (OTBI) reporting, enforcement by business function isn't supported.

Once a chart of accounts value set is secured, security will be enforced across all business functions, regardless of whether each distinct business function is enabled for enforcement or not. So long as the value set is security enabled,

security enforcement will apply in all business functions of General Ledger, Payables, Receivables, Assets, Intercompany, and Subledger Accounting.

With OTBI reporting, it's possible to put together reports that cross multiple products (business functions). Moreover, the user doesn't directly select which data access security context (Data Access Set, Business Unit, Asset Books, and so on.) to currently work with. Instead, in general, the user's cumulative data access security assignments are always simultaneously taken together. Both of these factors affect the ability to precisely and fully apply segment value security by business function.

When performing OTBI reporting with the General Ledger subject area specifically, the user's current data access set selection determines the applicable data security. This is because the user's currently selected data access set in the application is stored in a profile option. The application leverages this and singularly applies it in evaluating which segment value security user rule assignments should apply for the user when reporting on ledgers with a secured chart of accounts. When reporting on ledgers that don't have a secured chart of accounts, the user's cumulative assigned data access sets are simultaneously applied.

Features Without a Data Security Context

There are product features that involve working directly with financial transactions and balances where a user’s data security context can’t be established.

Here are some examples.

- Standard Subledger Accounting Oracle Analytics Publisher reports that can involve the financial data of one or more ledgers where there isn’t always a direct or unique match to a specific security context value that’s assigned to a user, such as a data access set.
- Non-General Ledger Oracle Transactional Business Intelligence reports where no specific data security context selection can be established for a user to derive the specific segment value security by business function grants that are applicable to that user.

For these features, a modified form of segment value security by business function enforcement is applied. A percentage value is substituted for certain user rule assignment attributes to indicate that no specific value needs to be matched for the security grants. This broader basis of user rule assignment matching still limits a user’s access to the secured accounts that the user is granted access to when working with financial data, but on a nonspecific basis.

Here’s how it works for such features.

When determining if there are matching rule assignments for a user that can restrict the range of accessible secured accounts, the Security Context and Security Context Value attribute settings will be ignored to lower the matching threshold. The Business Function and Access Level attributes for that rule assignment can still be considered.

This would be in place of automatically applying the All Values grant when no precise user rule assignments match for the current usage scenario. That approach would effectively mean that no chart of accounts security would be enforced. Instead, this alternative approach will at least limit a user to working with only the financial data where the cumulative grants for each secured value set of the chart of accounts provide access, should such grants exist.

As another example, when working with features in the Subledger Accounting application, a user doesn't explicitly specify a security context selection (that is, a data access set, business unit, and so on). With General Ledger, that same user can simultaneously work with the financial data of ledgers across the user's cumulative data access set assignments.

This means that for those security grants for a user that can be tagged with a specific security context value, such as a data access set, it isn't possible to make perfect matches of the user’s more precisely defined rule assignments for the usage scenario in Subledger Accounting. If it happens that such grants are tagged with the All Security Contexts security context, or the Data Access Set security context paired with the All Security Context Values security context value, such grants for the user are also included as a match.

For a General Ledger user, all the user's General Ledger business function rule assignments for the secured value sets involved with the charts of accounts of the ledgers that user is working with will also be applied. This is regardless of the data access set security context and security context value that's associated with those rule assignments. That is, all the user's General Ledger business function rule assignments for the secured value sets will be cumulatively applied. If under such looser matching conditions there are still no matching grants for the user, only then will the default All Values grant to the relevant secured value sets apply.

Multiple Secured Chart of Account Segments

Consider these points when working with account combinations where the chart of accounts has multiple segments enabled for segment value security by business function.

- For a given usage scenario, a user's access to the account values of each secured chart of accounts segments is first considered individually and independently of the other. Then, if a user has a mixture of access levels to the account values for an account combination, the lowest level of access among these account values would be applied to the full account combination.
- For an account combination where a user has no access to at least one segment's account value, that account combination is immediately one to which the user has no access. This is because access to the account combination requires access to each of its secured segment values.
- For an account combination where a user has read-only access to at least one segment's account value, that account combination is a read-only account combination for the user. This is because read and write access to an account combination requires read and write access to each of the account combination's secured segment values.

As an example, the first and second segments of account combination 01-101-1000 are secured. A user has read-only access to first segment value 01 and no access to second segment value 101. The user won't have access to that account combination. Even if the user had read and write access to first segment value 01, the user still wouldn't have access to account combination 01-101-1000.

Continuing with this example, a different user has read-only access to first segment value 01 and read and write access to second segment value 101. That user's applicable access level to account combination 01-101-1000 will be read only.

To have read and write access to account combination 01-101-1000, a user must have read and write access to both first segment value 01 and second segment value101.

If a user doesn't have at least read-only access to accounts on every secured segment of an account combination, that user won't even have read-only access to that account combination.

Primary Balancing Segment Value Assignments to a Ledger and Its Legal Entities

Assigning a primary balancing segment value to a ledger, or to its legal entities, isn't chart of accounts data security related.

It's a validation against the accounting configuration for a ledger that affects which primary balancing segment values are available and valid for a user to work with for the given ledger.

If a ledger has primary balancing segment value assignments and a particular primary balancing segment value isn't assigned to that ledger, or to its legal entities, then that primary balancing segment value won't be available to the user when working with that ledger. This is regardless of whether the user has been granted access using either of the following methods:

- The user is provided a segment value security grant for that particular primary balancing segment value for that chart of accounts with a secured primary balancing segment.

- The user is granted access to that primary balancing segment value through a full ledger data access set or a primary balancing segment value-based data access set, in the case of the General Ledger module.

Switching from Secured to Unsecured Modules

When users switch from one of the modules that support segment value security by business function to a module that doesn't, they might continue to experience limited account access in the unsecured module.

To resolve this, users might need to sign out of the application and sign back in when switching modules. This action resets the cache and allows users access to all accounts in those modules where security enforcement isn't expected.

General Ledger-Specific Considerations for Segment Value Security

Segment value security by business function is generally enforced in General Ledger product features with a chart of accounts element and where a single data access set context selection can be clearly established for a user's session.

In these cases, the secured account values available to the user, at the according access level, are based on those grants assigned to the user for the General Ledger business function and the user's current selected data access set.

Here's a summary of how segment value security by business function works for General Ledger features that have different types of derivation of the user's data access set selection.

- For features accessed directly in the core application, a user would select a data access set. The selection also sets the data security context when determining which of the user's segment value security by business function grants apply when working with the secured chart of accounts.

  > **Note:** The data access selection is also registered in a user's General Ledger preferences for the Data Access Set General option.

- For features accessed outside of the core application, where a user doesn't explicitly select a data access set, such as with reporting tools Smart View, Financial Reporting, and Oracle Transactional Business Intelligence (OTBI), the application refers to a user's last selected data access set in the core application when determining which of the user's security grants apply.

  > **Note:** If a user switches data access set selection in the core application, it's important to refresh the view in the Smart View, Financial Reporting, and OTBI reports. This action registers the change in data access set selection so that the relevant set of security grants based on this new data access set selection is now applied to the report.

- For features where multiple data access sets can apply, or where no data access set context can be established, there are some other considerations regarding how segment value security by business function is enforced. Some examples in the *Features Without a Data Security Context* topic discuss some of these considerations.

Further details follow about other special considerations for data security and segment value security by business function enforcement in certain features in the General Ledger module. They elaborate on certain points discussed previously, as well as other specific aspects of security control in the General Ledger module.

Data Access Sets

For General Ledger, data access sets provide users with access to one or more ledges and serve as a core and required data security mechanism.

Data access sets are a fundamental data security control object that always apply in General Ledger and are unique to the General Ledger module. They include the following attributes:

- Access Set Type
- Access Level

Here are the access set types.

- Full Ledger: This type provides access to an entire ledger. It can include one or more ledgers as well as ledger sets. When a ledger set is added to a Full Ledger data access set, access to all the ledgers in the ledger set are granted in full.

  Whenever a new ledger or ledger set is created, the application automatically creates an implicit data access set for it. This data access set can't be updated. An explicit data access set can also be created for one or more ledgers, or ledger sets, or both. Explicit data access sets are updatable.
- Primary Balancing Segment Value: This type provides access to one or more primary balancing segment values of a ledger or ledger set.

  You can specify a single or parent value. If you specify a parent value, the data access set provides access to all the single values that roll up to that parent value. The parent value is evaluated based on the current version of the hierarchy associated with the primary balancing segment in the chart of accounts definition.

Here are the access levels.

- Read Only

  > **Note:** Even if a user carries the functional privilege to use certain write-level functions, such as the ability to create a journal, the user will be prevented from taking any action that will update General Ledger transactions and balances for a given ledger or primary balancing segment value.

- Read and Write

Using Primary Balancing Segment Value-Based Data Access Sets with a Secured Primary Balancing Segment

For segment value security by business function, data access sets serve as the security context basis for the General Ledger module.

For the Subledger Accounting module, to the extent that there's a touchpoint with the General Ledger module, the data access set also plays an indirect role in establishing a user's data security and it's used to establish a user's ledger and ledger set access scope.

If you enable segment value security by business function for the value set of a chart of accounts primary balancing segment and also use the data access set type of Primary Balancing Segment Value, the two data security control elements, including their access levels, will apply to those primary balancing segments in General Ledger.

> **CAUTION:** The recommended best practice is not to use both methods because having dual levers of control on access to the one element of the chart of accounts primary balancing segment can introduce unneeded complexities, ambiguity, and inconsistencies.

Instead, limit the implementation of data security control of primary balancing segment values to one of these two methods:

- Data access sets with an access set type of Primary Balancing Segment Value

- Segment value security by business function enabled on the primary balancing segment of the chart of accounts.

Here are some guidelines on which of the two methods to use.

- If security on the primary balancing segment of the chart of accounts will always only be required in the General Ledger module, then use Primary Balancing Segment Value-based data access sets alone to specifically control primary balancing segment values access in General Ledger. Data access sets and Primary Balancing Segment Value-based data access sets are unique in usage for data security control in the General Ledger module.
- If security on the primary balancing segment of the chart of accounts is also required in other product modules besides General Ledger, then enable segment value security by business function on the primary balancing segment of the chart of accounts. This is the only option that applies to all product modules. Avoid using Primary Balancing Segment Value-based data access sets for General Ledger in this case and only use the Full Ledger access type of data access sets.

How Data Security Works When Using Primary Balancing Segment Value-Based Data Access Sets with a Secured Primary Balancing Segment

If you don't follow the recommended best practice described in the *Using Primary Balancing Segment Value-Based Data Access Sets with a Secured Primary Balancing Segment* topic, and instead use both Primary Balancing Segment Value-Based data access sets along with a secured primary balancing segment, here's a summary of how data security works followed by examples.

For features directly based on the General Ledger balances cube, a user's access to primary balancing segment values will be based on the cumulative union of the two data security control methods.

For features indirectly based on the General Ledger balances cube, a user's access to primary balancing segment values will be based on the intersection of the two data security control methods.

Example of Primary Balancing Segment Value Access for Features Directly Based on Balances Cubes

Most balances cube-based features in General Ledger pertain to reporting or inquiry functions. That is, they're read-only type functions. For read-only features, the rules assigned to a user on both a read-only and read and write basis will apply.

The following General Ledger features are directly based on General Ledger balances cube.

- Account Groups and Account Monitor
- Account Inspector
- Allocations
- Close Monitor Summary Income Statement
- Correct Budget Import Errors
- Create Budgets in Spreadsheet
- Financial Reporting
- Inquire and Analyze Balances
- Inquire and Analyze Average Balances
- Inquire on Detail Balances
- Oracle Transactional Business Intelligence (OTBI): General Ledger Balances Real Time and Average Daily Balances Real Time Subject Areas
- Revenue, Expenses and Allocations Infolets

- Smart View

From this list, only Allocations, Create Budgets in Spreadsheet and Correct Budget Import Errors are features that are of a read and write nature. Segment value security enforcement won't be applied for them. These features have an element of import and are considered more like back-end processes.

For features that are based directly on balances cubes, a user can access the cumulative primary balances segment values that are granted through both of these methods:

- The user's primary balancing segment value-based data access set.
- The user's applicable rule assignments to the secured primary balancing segment value set.

The application evaluates each method separately. It determines which ledgers a user has access to based on the data access set, as well as the primary balancing segment values granted in the case of Primary Balancing Segment Value-based data access sets. It then separately determines which primary balancing segment values a user has access to for the secured primary balancing segment based on that user's applicable segment value security by business function grants.

The result is that a user gets access to the cumulative primary balancing segment values from the data access sets and segment value security by business function grants across all ledgers and ledger sets included in those data access sets.

Here's an example.

This table shows the access set assignments for the Vision Corporation Global data access set. This access set has a type of Primary Balancing Segment Value.

Ledger or Ledger Set	Type	Specific Value	Segment Value	Privilege
Vision Corporation Global	Ledger	Single Value	3111	Read and Write
Vision Corporation Global	Ledger	Single Value	3121	Read Only

Note: The All Values, Tree Code, and Tree Version Name fields don't have values, so they're excluded from the table.

This table shows the key attribute values on the Rules worksheet for the secured value set of the Company primary balancing segment.

Policy Name	Role Name	Operator	From Value
CCLARK EQ 3111	CCLARK Role	Equal to	3111
CCLARK EQ 4888	CCLARK Role	Equal to	4888

This table shows the key attribute values on the related Rule Assignments worksheet.

User Name	Policy Name	Role Name	Business Function	Security Context	Security Context Value	Access Level
CCLARK	CCLARK EQ 3111	CCLARK Role	General Ledger	Data access set	Vision Corporation Global	Read and write

User Name	Policy Name	Role Name	Business Function	Security Context	Security Context Value	Access Level
CCLARK	CCLARK EQ 4888	CCLARK Role	General Ledger	Data access set	All security context values	Read and write

When user CCLARK uses Smart View to inquire on the Vision Corporation Global ledger's account balances, CCLARK can see company values 3111, 3121, and 4888. Because CCLARK is performing a read-only action, the read-only access level for company 3121 is enough for the inquiry. For any other company values, Smart View will display #No Access.

> **Note:** One exception to this cumulative behavior is when segment value security by business function rules grant access to all primary balancing segment values, but the Primary Balancing Segment Value-based data access set only provides access to select primary balancing segment values. In this case, the restricted access of the data access sets to just select primary balancing segment values will apply, because distinct primary balancing segment values were specified for the data access set.

Example of Primary Balancing Segment Value Access for Features Not Based on Balances Cubes

All General Ledger features that aren't specifically mentioned in the *Example of Primary Balancing Segment Value Access for Features Directly Based on Balances Cubes* topic are associated with relational database tables.

Using the data access set and rules setup from the previous example, when the user CCLARK selects the Vision Corporation Global data access set in a General Ledger feature that's not based on the balances cube, the only primary balancing segment value that CCLARK can work with is 3111. That's because value 3111 is the only primary balancing segment value that's granted in both the Primary Balancing Segment Value-based data access set and in the segment value security by business function assignment.

When reviewing and editing a journal entry using that same data access set, the user CCLARK will see only the journal lines with account combinations that refer to Company 3111.

> **Note:** A user can edit journal lines only when the assignments for a Primary Balancing Segment Value-Based data access set cover all the primary balancing segment values that are referenced in the account combinations for all journal lines.

Read-Only Data Access Sets with Segment Value Security

When working with read-only data access sets at the ledger level, the entire ledger is read-only for a user.

Having read and write access to account values to any secured segments of its chart of accounts would be irrelevant. The access level to those accounts in that ledger will effectively still be read only because the user's access to that whole ledger, per the data access set, is read only.

Reporting on General Ledger Balances Cubes Reports with Account Hierarchies

General Ledger balances cubes are differentiated by unique combinations of a chart of accounts and an accounting calendar.

Balances cubes maintain summarized account balances for all trees and tree versions, and for all chart of account dimensions that are published to those balances cubes. The detail account balances for those published trees and tree versions are summarized according to defined account hierarchy rollups.

Trees and tree versions are defined in the application to represent date effective versions of account hierarchies. They're organized for different purposes, for example, for statutory versus management reporting, with each tree version being assigned an effective date range.

However, this date effectivity isn't an actual attribute in balances cubes. Instead, it's an implied characteristic. Users need to know the significance of each tree and tree version that they select and which effective date of the organization's rollup those tree versions represent. This helps facilitate performing year-over-year comparisons of financials results.

For example, this user-determined control allows organizations to report on fiscal year 23 versus fiscal year 22 financial results using the same tree version rollup for parent account values on both sets of numbers so that there's a consistent comparison between them.

A user can have a choice of reporting on both years' results using last year's tree version rollup for parent account values, or both using the current year's tree version rollup. They can even report on fiscal year 22 results using the fiscal year 22 rollup with the fiscal year 23 results using the fiscal year 23 rollup, if that's what's required.

Segment Value Security Rules Based on Account Hierarchies

You can refer to account hierarchies in segment value security by business function policies as an efficient way of granting access to secured account values.

Use the hierarchical operators **Is descendant of** and **Is last descendant of**, along with a specified tree, to allow references to parent account values in a security rule condition. This means that a grant provides access to that parent value and all its descendants (with the **Is Descendant of** operator) or to that parent and its' detail values descendants (with the **Is last descendant of** operator), according to the account hierarchy that's defined for the applicable tree code and tree version.

> **Note:** The trees that you specify in a rule must be flattened. This contrasts with trees that are published to balances cubes, which don't need to be flattened. If your security rules refer to trees that are published to the balances cubes, then the trees must be flattened. Otherwise, security enforcement won't work in balances cube-based reports and queries.

While a distinct tree code is associated with each segment in a chart of accounts, as specified through the Default Hierarchy value in the chart of accounts structure setup, a security rule can refer to any tree (hierarchy) that's defined for the secured value set.

The tree version that you specify in a rule is just for the purposes of determining which parent values you can select from to then attach to the security rule condition. At runtime, the application applies date effectivity to identify the version of the tree referenced in the rule whose effective dates intersect with the current system date. Based on this tree version, the application derives the list of accessible descendant account values for the referenced parent value of that tree that are granted by that hierarchical security rule assignment.

For inquiring and reporting in balances cubes, these security grants apply across all versions of the specified hierarchy, as well as all hierarchies associated with the same value set of the specified hierarchy that are published to the GL balances cube. Even though a security rule has a specific tree and tree version for a parent value, the derived set of account values granted by that rule will equally apply to all other published tree and tree versions for where that same parent value is cited and as indicated in GL balances cube-based inquiries and reports.

This example highlights that the grant for segment value security rules based on hierarchies will apply the current effective tree version when deriving the list of accessible values. This contrasts with references to tree and tree versions in balances cube inquiries and reports, where a user controls exactly which tree and tree version they want to use for a rollup.

This table shows the hierarchies, hierarchy versions, parent value, and parent value descendants for this example.

Hierarchy	Hierarchy Version	Parent Value	Parents and Detail Value Descendants
Management	2023	100	• Detail 101 • Parent 200, with detail values 201, 202, 203 • Parent 300, with detail values 301, 302
Management	2024	100	• Parent 200, with detail values 101, 201, 202 • Parent 300, with detail values 301, 302
Geographical	2023	100	• Parent 200, with detail value 201 • Parent 300, with detail values 301, 302 • Parent 400, with detail values 401, 402

Let's say a rule is defined with these attributes.

- Operator: Is descendant of
- From Value: 100
- Tree Code: Management
- Tree Version: 2023

Here's how the application determines the secured values granted.

1. The application derives the hierarchy (tree) version that's in effect based on the current system date, which is January 1, 2024. In this example, that's version 2024.
2. The application then applies the rule condition to get the list of secured values. In this example, the secured values granted are 100, 200, 101, 201, 202, 300, 301, and 302 (parent value 100 and all its descendants in tree version 2024.)
3. This list of values will be accessible across all versions of the Management hierarchy and across all hierarchies associated with the value set for the segment. This means the list of values will be accessible if choosing to report against any version of the Management or Geographical hierarchies.

> **Note:** Value 203 in Management hierarchy version 2023 and values 400, 401, and 402 in Geographical hierarchy version 2023 won't be accessible because they aren't part of the effective 2024 tree version for the Geographical hierarchy.

For the purpose of data entry, this date-effective list of accessible descendant segment values is available to the user for that given point of time.

For the purpose of inquiry and reporting with the balances cube, the same list of accessible descendant segment values is available to the user for all published trees and tree versions for the secured value set of the chart of accounts segment or dimension. Based on the tree and tree version the user selects, the balances data for the accessible descendant segment values of the referenced parent account will be displayed accordingly. A user can also be granted

access to a specific parent value. In that case, the summarized balance shown for that parent value will be consistent with the rollup for the selected tree and tree version for reporting purposes, regardless of whether the user has been granted access to all the descendants involved with that particular rollup.

> **Note:** No chart of accounts security is applied during the selection process of account values for the inquiry or report. The user can freely select any dimension member or account values from a secured value set. Security is applied only when retrieving the results for that query or report, and only the balances data of the dimension member or accounts to which the user has access will be displayed.

The advantage of the application dynamically applying date effectivity to security rules is that the rule would be self-maintaining. This methodology works well when it comes to creating transactions or financial data, which in most cases is a real-time exercise.

For comparative reporting, such as with year-over-year financial reporting, previous tree versions might be used as the basis of the rollup to compute summarized balances. This might result in some discrepancy in the access to the descendant accounts for that parent based on the previous tree version's rollup as referenced in the inquiry or report. A potential solution would be to use a different hierarchy in the security rule that encompasses all the account values the user will need to inquire or report on, and give access on a read-only basis to limit the user's ability to enter transactions with these account values.

Considerations When Using Parent Account References in Hierarchical Rules for Balances Cubes

Ensure users get the appropriate secured values grants to view the financial data that they need.

A good practice is to define hierarchical rules that sync to parent values according to the tree as referenced in balances cube inquiries and reports such as Account Monitor, Smart View, and Financial Reporting.

Access to the descendant accounts of a specific parent value should be in sync with the descendant accounts that roll up to the summary account balance of that parent value based on another tree. Otherwise, the parent value will show the appropriate summary balance for the other tree, but the detail breakdown shown on the report of its descendants' balances might not sum up consistently because of lack of access to those descendant values.

This concern applies even when the tree referenced in inquiries and report definitions is the very same one used in the security rule with parent value references. This is because there can be a difference in the dynamic date-effective version rollup that's applied when determining the grants for the rule assignment. Moreover, it's even possible to use a different tree in inquiries and report definitions than the one used in the rule, which can result in even more pronounced disparities.

Journal Approval

With journal approval, the primary consideration when it comes to what a user can access is the approval hierarchy and whether the user is the authorized approver for a given transaction.

It's less about the approver clearing the data access set and chart of accounts segment value security access for the journal batch being approved.

> **Note:** Approval transactions can be reassigned, delegated, and so on, as per the approval rules.

There are differences in the degrees of data security enforcement in the variety of methods for accessing approval notifications and journal batch details in which a user's data access is validated. The most stringent access is where the approver interacts with the journal batch being approved in the context of the Journals page, where all the General Ledger data security elements are directly in place.

These considerations are equally relevant regardless of whether segment value security by business function is enabled.

Back-End Processes That Generate Journals or Update Balances

Segment value security by business function isn't enforced for back-end processes. This is to facilitate automated submission of such processes.

Here are the General Ledger back-end processes that involve a chart of accounts element and that generate journals or update account balances.

- AutoPost Journals
- Create Balance Sheet Closing Journals
- Create Income Statement Closing Journals
- Encumbrance Year End Carry Forward
- Import Journals
- Journal propagation from a primary to a secondary ledger
- Open General Ledger Periods
- Revalue Balances
- Transfer Balances to Secondary Ledger
- Translate General Ledger Account Balances
- Transfer Ledger Balances

Feature Setups

Segment value security by business function isn't enforced for setup tasks.

This table shows examples of General Ledger setups and related processes, spreadsheets, and templates for which segment value security by business function isn't enforced.

Setup	Related Processes	Related Spreadsheets	Related File-Based Data Import Template and Web Service
Account Combinations	Import Account Combinations	Create Account Combinations in Bulk	Import Account Combinations, Account Combinations for Validation
Create Allocation Rules	Generate Allocations	NA	NA
Cross-Validation Combination Sets	Manage Account Combination Validation Rules	NA	Cross-Validation Combinations Import
Cross-Validation Rules	NA	Create Cross-Validation Rules in Spreadsheet	NA
Ledger Options	NA	NA	NA
Segment Values and Hierarchies	Import Segment Values and Hierarchies, Inherit Segment Value Attributes	Rapid Implementation for General Ledger	Import Segment Values and Hierarchies
Segment Value Security	NA	Manage Segment Value Security Rules, Create Segment Value Security Rules	NA

Setup	Related Processes	Related Spreadsheets	Related File-Based Data Import Template and Web Service
Suspense Accounts	NA	NA	NA

Assets-Specific Considerations for Segment Value Security

Asset books control data security and are the fundamental data security object in Oracle Assets.

It serves as the primary control for an Assets user with access to work with the records of a particular asset book, based on the user's access assignment. This includes the ability to work with and perform actions in an asset book like adding assets, editing asset source lines, entering unplanned depreciation, transferring assets, running Assets reports, and performing inquiry on asset records and transactions.

Chart of accounts segment value security is another layer of data security above asset books that controls a user's ability to work with the chart of accounts-based accounting information of records in a given asset book.

Segment value security restricts access to account segment values in transactions with the Accounting flexfield component in transactions like asset additions and asset transfers. It doesn't restrict transaction entry for an asset within the asset book that doesn't involve the chart of accounts element.

Users who don't have access to segment values used in the accounting for an asset record can still search for that asset record in all the transaction entry and asset inquiry pages in the asset books they have access to. Only when they're working on the chart of accounts-based accounting aspect of an asset record will segment value security access controls be applied. You can only work with account values in a secured chart of accounts value set you've been granted access to through your rule assignments.

Segment Value Security by Business Function for Oracle Assets

The Segment Value Security by Business Function feature lets you enable security enforcement for all business functions or for one or more specific business functions.

For example, you can enable segment value security enforcement for the Oracle Assets business function alone.

When you enable security enforcement for Assets, all Assets users automatically have access to all segment values until you specifically restrict access for one or more users to limited segment values.

You only need to maintain segment value security rules and rule assignments for users who must have access to limited account values by using the Manage Segment Value Security Rules spreadsheet.

For example, you can define the following types of segment value access rule assignments for Assets users who require access to certain secured account values:

Access Type	Business Function	Security Context	Security Context Value
Global access	All business functions	All security contexts	All security context values
Access for Assets business function only	Assets	Asset book	All security context values
Access for specific asset book	Assets	Asset book	Name of asset book

Assign the access type according to the type of access each user needs:

- Global access: Assign to users with responsibilities in multiple business functions such as Assets, Oracle Payables, and Oracle General Ledger, and who require access to the same specified segment account values for all their assigned asset books, business units, and ledgers.
- Access for Assets business function only: Assign to users with only Assets responsibility who require access to the same specified segment account values for all their assigned asset books.
- Access for specific asset book: Assign to users with only Assets responsibility who require access to the specified segment account values for a specific asset book.

Generally, you should create dedicated segment value security roles for data security policies to grant access to secured segment account values to Assets users. Never directly create segment value data security policies with job roles such as Asset Accountant or Asset Accounting Manager, because these roles are likely to be shared among all Assets users, and these users are likely to have different chart of accounts segment value security profiles. The dedicated segment value security roles with their secured segment values can be assigned and even shared with the corresponding users based on their particular segment value access requirements.

Secured segment account values can be granted with these access levels:

- Read and Write: Provides access to create, update, view accounting for, inquire on, and report on Assets transactions that reference the account values granted.
- Read Only: Provides access to view accounting for, inquire on, and report on Assets transactions that reference the account values granted.

Segment Value Security Enforcement in Assets Transactions

Segment value security is generally enforced in Oracle Assets in transactions that directly include the chart of accounts element.

It has no impact on transactions in which actions don't directly involve the chart of accounts, such as cost adjustments, category changes, source line transfers, and suspend or resume depreciation transactions. When searching in pages such as the Adjust Assets and Asset Inquiry pages, it retrieves all asset records without regard to the account values referenced in the distribution lines associated with each asset, and only considers the asset book's element of data security control.

Segment value security is enforced in Assets as follows:

- Users with read and write access to certain account values can take these actions on asset records that reference those account values:
  - Add an asset
  - Prepare source lines
  - Record unplanned depreciation
  - Transfer an asset
  - Make unit adjustments
  - Create a lease
  - Change the financial terms of a lease
- Users with read-only access to certain account values can take these actions on asset records that reference those account values:
  - View distributions and accounting lines
  - Run reports

- Segment value security isn't enforced:
  - In Assets setup pages, such as Manage Assets Books, Manage Asset Categories, and Manage Distribution Sets, even though these pages involve the chart of accounts element.
  - For submitted processes such as Post Mass Additions and Create Accounting.

Example of Segment Value Security by Business Function

The following setup example illustrates how enforcement by segment value security by business function works in Oracle Assets.

You must assign the rules to users for them to have access to the secured account values. If no rules are assigned to a user, the user has access to all the account values.

In this example, user SANJAY has no rule assignments; SANJAY has access to all secured rule account values for the asset books SANJAY has access to.

User KUMAR has access to two asset books: FIN CONSULTING CORP and HR CONSULTING CORP. This table shows the access setup for KUMAR.

User	Role	Business Function	Asset Book	Security Context Value	Access Level
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	HR CONSULTING CORP	3111, 3888	Read and Write
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	FIN CONSULTING CORP	3121, 3999	Read and Write
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	HR CONSULTING CORP	3121, 3999	Read Only
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	FIN CONSULTING CORP	3111, 3888	Read Only

Asset additions:

For the write action of asset additions, in the book HR CONSULTING CORP, KUMAR has read and write access to company 3111 and 3888. Therefore, KUMAR can add assets using these account values for that asset book. KUMAR also has read only access to the companies 3121 and 3999. Even though KUMAR has read access to these values, KUMAR can use only 3111 and 3888 to perform asset additions in this book.

In the asset book FIN CONSULTING CORP, KUMAR has read and write access to the companies 3121 and 3999. Therefore, KUMAR can add assets using these account values.

Edit source lines:

In the asset book FIN CONSULTING CORP, KUMAR has read and write access to the companies 3121 and 3999. KUMAR can edit the Depreciation Expense Account using the accounts KUMAR has read and write access to.

In the book FIN CONSULTING CORP, KUMAR has read-only access to company 3888. KUMAR can't edit this depreciation expense account and can only view it.

Transaction Account Builder in Assets:

In Assets, segment value security isn't enforced in the Transaction Account Builder, which is used to drive the depreciation expense account for mass addition lines. This process defaults accounts based on the rules configured by the organization and isn't subject to the limitations of a user's secured account grants.

Asset transfers:

In the book FIN CONSULTING CORP, KUMAR has read and write access to company 3999. Therefore, KUMAR can transfer the asset that references that account in the FIN CONSULTING CORP asset book.

In the book FIN CONSULTING CORP, KUMAR has no access to company 4111 and has read and write access only to the values for company 3121 and 3999. Therefore, KUMAR can't transfer an asset that references values in company 4111.

Example of Accounting in Oracle Assets

In the asset book FIN CONSULTING CORP, among the accounts user KUMAR is granted, KUMAR has read and write access to company 3999 and read-only access to company 3111.

Therefore, when viewing accounting lines for asset records, KUMAR can view all lines that reference accounts KUMAR has read and write and read-only access to.

In the asset book FIN CONSULTING CORP, any user other than KUMAR, who's assigned rules that don't include 3111 and 3999, can't view these accounting transactions.

Example of Reports in Oracle Assets

In the book FIN CONSULTING CORP, KUMAR has read and write access to companies 3121 and 3999, and read-only access to companies 3111 and 3888.

Therefore, KUMAR can report on asset records that reference these four account values for that asset book. KUMAR can't run reports for any values other than those that KUMAR has read and read and write access to.

Intercompany-Specific Considerations for Segment Value Security

These are some considerations for the Segment Value Security by Business Function feature in the Intercompany module.

- Intercompany organization is used as the data access security object in the Intercompany module.
- For the Segment Value Security by Business Function feature, the Intercompany module supports these two distinct business functions:
    - Provider Intercompany
    - Receiver Intercompany

This allows for different security grants to be defined for each intercompany organization when used as a provider, versus when used as a receiver in an intercompany transaction.

This can even be configured for individual users, where a user can be given different security grants for the same intercompany organization depending on whether the user acts as a provider or a receiver for an intercompany transaction.

Example

This example demonstrates how a user can have access to one intercompany organization but can have access to a different set of accounts depending on whether the user acts as a provider or a receiver for an intercompany transaction.

Let's look at the security grants of two users, Paul and Rita, who work for intercompany organizations IC-Org1 and IC-Org2 respectively.

- Paul manages intercompany transactions only for IC-Org1. He needs different account access as a provider and as a receiver.
- Rita manages intercompany transactions only for IC-Org2. She needs full access to all accounts for both provider and receiver business functions.

To achieve the access control for Paul, you assign rules that grant Paul access to different accounts as a provider and as a receiver.

User/Grant	Intercompany Data Access	Account Access	Business Function	Access level
Paul	IC-Org1	1100-1199	Provider Intercompany	Read and write
Paul	IC-Org1	2100-2199	Receiver Intercompany	Read and write

Note that no security grants are configured for Rita because she has access to all accounts, which is the default Segment Value Security by Business Function feature.

With the security grants that Paul carries, let us look at these scenarios:

Scenario 1: Paul in the role of a provider for a loan funding transaction. Here are the steps that Paul and Rita take to complete an intercompany transaction from IC-Org1 to IC-Org2.

- Paul creates an intercompany transaction for loan funding from provider IC-Org1 to receiver IC-Org2.
- Paul enters the provider distribution account. He can only select accounts from 1100 to 1199.
- Paul submits the loan funding intercompany transaction.
- Rita reviews the inbound transaction for IC-Org2 that Paul has initiated.
- Rita enters the receiver distribution account. She can select any account.
- Rita submits the intercompany transaction.

Scenario 2: Paul in the role of a receiver for an expense sharing transaction. Here are the steps that Rita and Paul take to complete an intercompany transaction from IC-Org2 to IC-Org1.

- Rita creates an intercompany transaction for expense sharing from provider IC-Org2 to receiver IC-Org1.
- Rita enters the provider distribution account. She can select any account.
- Rita submits the expense sharing intercompany transaction.
- Paul reviews the inbound transaction for IC-Org1 that Rita initiated.
- Paul enters the receiver distribution account. He can only select accounts from 2100 to 2199.
- Paul submits the intercompany transaction.

Important Notes

The Segment Value Security by Business Function feature has not been implemented for:

- Intercompany reports.
  - For example, users with limited access, who cannot view certain accounts on the intercompany UIs, will be able to see these accounts in the Intercompany Account Details report.
- Multitier Intercompany Operations module.
  - The security grants configured for intercompany does not apply to the Multitier Intercompany Operations feature.

Additional Notes

- The examples above demonstrate users with read/write access only. However, user access can be granted on a read/write or read-only basis to satisfy the business needs.
- Segment Value Security by Business Function applies to accounts that are generated by Transaction Account Builder (TAB). If the user creating the intercompany transactions does not have read/write access to the account, TAB will not generate the account.
- Segment Value Security by Business Function does not apply to application generated intercompany payables and receivables accounts. These accounts are generated accordingly regardless of how the Segment Value Security by Business Function is configured.
- Segment Value Security by Business Function applies to accounts generated along with intercompany transactions sourced from intercompany allocations. If the user executing intercompany allocations does not have read/write access to the account, intercompany allocations will fail to generate intercompany transactions.

Payables-Specific Considerations for Segment Value Security

Optimizing segment value security by business function limits a user's access to certain accounts for each secured value set while creating, updating, and reviewing financial data.

The security context of the business function enforces the segment value security. “Payables” is the applicable business function for Payables module. Payables users have the following access levels for the segment values of a secured chart of accounts based on the Payables business function:

- Read/write: This access level allows a user to manage invoice lines or distributions and inquire and review the invoice distributions with account values to which the user has read/write access.
- Read-Only: This access level allows a user to only view and inquire invoice distributions referencing those account values to which they've access. User can’t create transactions using these account values.

Note:

- This feature operates on the principle of first providing access to all the secured segment values to all users by default.
- Security policies are defined, and such rules are assigned to a user only when their access should be limited to specific segment values.
    - The user rule assignments are defined for a combination of business function, data access context, and access level. For Payables, the business function to use is “Payables” and the data access context is “Business Unit.”
    - If there are no matching rule assignments for a user for a given usage scenario, the user gets access to all account values for the secured chart of accounts value set.

Setting Up

There are no extra Payables-related setups to undertake to enable Segment Value Security by Business Function for Payables. However, to enforce segment value security in the Payables module, the “Payables” business function must be enabled for enforcement.

Enforcing Segment Value Security by Business Function in Payables

In Payables, the business unit serves as the data security-striping mechanism that controls the data access to the users, and also the security context basis for segment value security.

Whenever a Payables user accesses any of the Payables pages, the account combination values the user can access are decided by the intersection of data security access for the Payables module and the security context of the segment value security for the Payables business function. For example, if user wants to create a Payables Invoice for Vision America business unit, then they should have the following access rights.

- Access to Vision America business unit in the Payables module
- Access to at least one account value in Vision America Payables business function in segment value security

Segment value security by business function can be enforced in the Payables modules differently based on the task pages you're working with.

Examples of Enforcing Segment Value Security While Creating or Processing Payables Invoices

Segment value security validation takes place on Create Invoice and Process Invoice pages even if the user just types in the account values instead of selecting them from the accounting key flexfield dialog box.

Here are a few examples scenarios of how Payables-specific segment value security is enforced.

Access to Account Segment Values

Users can enter an account combination on an invoice only if they've read/write access to each segment’s account for the said account combination. Consider that User 1 has the following accesses.

- Read/write access to account values 5310 and 5320 in Vision America business unit.
- Read-only access to 7310 in Vision America business unit.

- Read/write access to account value 7320 in Vision Canada business unit.

User 1 can create an invoice for Vision America business unit with all account combinations that have account segment values of 5310 and 5320, but not account combinations with 7310 or any other account value. Similarly, User 1 can create an invoice for Vision Canada business unit with all account combinations that have account segment values of 7320 only, and not with any other account value.

Segment value security by business function is also enforced when the user creates invoices through the ADFDI spreadsheet, and through the import process. It's also enforced while entering the account combination details during the workflow process.

Note: Segment value security by business function isn't enforced when invoices are created from internal source, such as the following.

- Advance schedule billing notice
- Evaluated Receipt Settlement (ERS)
- Advanced Global Intercompany (AGIS)
- Sales Compensation
- Assets
- Projects
- One-Time Payments (OTP)
- Property Manager
- Patient refunds
- Projects intercompany invoices
- Projects interproject invoices
- Student Management
- Receivables
- Expenses (includes cash advances and expense reports)
- Return to supplier
- Supplier Chain Financial Flow Orchestration
- Fiscal Document Capture

Access to Accounts used in Distributions

Users can't cancel an invoice or invoice line or invoice distribution if the entity has at least one distribution with an account combination to which they don't have read/write access. What this means is that the user can only cancel an invoice or its lower entity if they've complete access to all the accounts used in its distributions.

Consider that User 2 has read/write access to account values 5310 and 5320 but read-only access to 7310. There are 2 invoices with following account details.

- Invoice 1: Has two distributions, one with account combination of 5310 and other with 5320.
- Invoice 2: Has two distributions, one with account combination of 5310 and other with 7310.

The user can cancel Invoice 1 because they've read/write access to both account segment values 5310 and 5320. However, user can't cancel Invoice 2 because they don't have read/write access to 7310.

Access to Account Combinations

When a user tries to validate an invoice with an account combination for which they don't have read/write access, the invoice is placed on hold, and distributions must be generated for the account combination. This means that the user can't trigger automatic distribution generation if they don't have read/write access to the account combination.

Consider that User 3 has read/write access to account values 5310 and 5320 and read-only access to 7310. There are two invoices with following account details.

- Invoice 1 has two invoice lines, one with account combination of 5310 and other with 5320.
- Invoice 2 has two invoice lines, one with account combination of 5310 and other with 7310.

The user can validate Invoice 1 because they've read/write access to both account segment values 5310 and 5320. However, they can't validate Invoice 2 because they've read/write access to only 5310 but not 7310.

Access to Accounts used in Prepayment Distributions

A user can't apply or unapply prepayments if the prepayment invoice distributions include an account value to which they don't have read/write access.

Consider that User 4 has read/write access to account values 6110 and 6120 and read-only access to 8110. There are two prepayment invoices with following account details.

- Invoice 1 has two prepayment distributions, one with account combination of 6110 and other with 6120.
- Invoice 2 has two prepayment distributions, one with account combination of 6110 and other with 8110.

The user can apply prepayment to Invoice 1 because they've read/write access to both account segment values 6110 and 6120. However, they can't apply or unapply the prepayment to invoice 2 because they don't have read/write access to 8110.

Examples of Enforcing Segment Value Security While Viewing Payables Invoice Lines

Segment value security isn't enforced on view invoice lines. Any user can view the invoice lines irrespective of their security access regarding segment value security.

However, segment value security is still enforced in the following scenarios.

Read Access to Invoice Distributions

When users navigate to the Distributions page of an invoice, they can see only the invoice distributions referencing the account values to which they've either read/write or read-only access. Other distributions aren't displayed. However,

if the users don't have any Payables-specific segment value security rule assignments, they can see all the distribution lines.

Consider that the user has read/write access to account value 5310, read-only access to 7310, and no access to 8310. The user navigates to the Distributions page for the following invoices.

- Invoice 1 has three invoice distributions where one distribution has account combination of 5310, the second one with account value of 7310, and the third with 8310. When user navigates to the Distributions page, they can see only the distribution lines with account values of 5310 and 7310. User can't see the distribution line with the account value of 8310 because they don't have read access to this value.
- Invoice 2 has three invoice distributions where one distribution has account combination of 5310, the second and third distribution lines have account combinations with the account value of 7310. When the user navigates to the Distributions page, they can see all three distributions as the user has read access to both 5310 and 7310.

Read Access to Accounting Combinations

When a user reviews the Transaction Accounting page, they can see only the accounting lines that have an account combination to which they've either read/write or read-only access. Other accounting lines aren't displayed. If the user doesn't have any specific rule assignments, then they can see all the distributions.

Consider that the user has read/write access to account value 5310, read-only access to 7310, and no access to 8310. The user navigates to the View Accounting page for the following invoices.

- Invoice 1 has three invoice distributions where one distribution has account combination of 5310, the second with account value of 7310, and third with 8310. When the user navigates to the View Accounting page, they can see only the accounting lines with the account values of 5310 and 7310. However, user can't see the accounting line with the account value of 8310 as they don't have read access to this value.
- Invoice 2 has three invoice distributions where one distribution has account combination of 5310, the second and third distribution have an account combination each with account value of 7310. When the user navigates to the View Accounting page, they can see all accounting lines as the user has read access to both 5310 and 7310.

Read Access to Account Values

When a user drills down to invoice distributions, say from Payments or from GL journal entries, they can see only the invoice distributions referencing account values to which they either have read/write or read-only access. Other distributions aren't displayed. If the user doesn't have any Payables-specific segment value security rule assignments, then they can see all the distributions.

Receivables-Specific Considerations for Segment Value Security

Chart of accounts segment value security controls user access to chart of accounts-based accounting information in Receivables.

Use segment value security to define user access to Accounting Flexfield segment values in Receivables. A given user can only work with account values in the secured chart of accounts value set to which they've been granted access and at the level of their rule assignments.

Segment value security doesn't affect Receivables setup or transaction creation.

Enable Receivables for Segment Value Security by Business Function

Use the Manage Segment Value Security by Business Function action in the Manage Chart of Accounts Configuration page to enable Receivables for segment value security.

To enable Receivables for segment value security:

1. Navigate to the Manage Chart of Accounts Configurations task.
2. In the Manage Chart of Accounts Configurations page, click the **Manage Segment Value Security by Business Function** button.
3. In the Manage Segment Value Security by Business Function window, enable the **Receivables** option.
4. Save your work.

When you enable segment value security for Receivables, by default all Receivables users are granted access to all segment values. You must set up rules to restrict user access to Accounting Flexfield segment values by business function. In the context of the Receivables business function, **business unit** is the security context.

Set Up Segment Value Security Rules in Receivables

Use the Manage Segment Value Security Rule Assignments spreadsheet to assign segment value security rules to the users who require some form of restricted access to Accounting Flexfield segment values.

As a general rule, create dedicated segment value security roles for each designated group of Receivables users and the related data security policies that govern their access to secured segment account values.

> **Note:** Never directly create segment value data security policies using the existing Receivables job roles, such as Receivables Manager. The existing job roles are likely to be shared by all Receivables users, and many separate groups of users are likely to have different chart of account segment value security profiles.

The dedicated segment value security roles you create, with their accompanying secured segment values, can be assigned to and even shared among the corresponding users based on their particular segment value access requirements.

You can enable security enforcement for all business functions or for one or more specific business functions. This table provides an example of how to designate segment value access rule assignments to Receivables users.

Segment Value Access

Access Type	Business Function	Security Context	Security Context Value
Global access	All business functions	All security contexts	All security context values
Access to Receivables business function only	Receivables	Business unit	All business units
Access to a specific business unit of Receivables business function	Receivables	Business unit	Name of the specific business unit

Global access: Assign global access to users with responsibilities across multiple business functions, for example, Assets, Receivables and General Ledger. Global access users would then require access to the same specified segment account values across all their assigned asset books (FA), business units (AR), and ledgers (GL).

Access for Receivables business function only: Assign business-function-only access to users with the Receivables responsibility who require access to the same specified segment account values for all their assigned business units.

Access for a specific business unit: Assign specific business unit access to users with the Receivables responsibility who require access to the specified segment account values for one business unit only.

Read-Write and Read-Only Access

You can further restrict user access to accounting flexfield segment values by assigning users Read-Write and Read-Only privileges.

- Read-Write: Users can create and update transactions, view accounting, and report on Receivables transactions that reference the account values granted.
- Read-Only: Users can view, query, and report on Receivables transactions that reference the account values granted. For example, users who don't have Read-Write access to segment values belonging to transaction distributions can still search for and review these distributions.

Summary of Segment Value Security Enforcement in Receivables

Users with Read-Write access to specified account values can take these actions on the transactions that reference these account values:

- Create, save and complete a transaction.
- Credit a transaction.
- Update account values in the distributions belonging to a transaction.
- Post transactions to General Ledger.
- Apply a receipt or credit memo to a transaction.
- Unapply a receipt or credit memo from a transaction.
- Manage adjustments to transactions.
- Create draft subledger accounting.
- Use these web service components: Get, Create, Update, Delete, Reverse.

Users with Read-Only access to specified account values can take these actions on the transactions that reference these account values:

- Create and save a transaction.
- View transaction distributions.
- Run reports.

Segment value security isn't enforced on these activities:

- Receivables implementation tasks in Functional Setup Manager.
- These reports in Scheduled Processes:
  - Receivables Aging by GL Account Report
  - MFAR Aging and Reconciliation Report
  - General Ledger Reconciliation Report

Example of Segment Value Security Enforcement in Receivables

The following example illustrates segment value security enforcement by business function in Receivables.

User Perry has the Accounts Receivables Manager role, but isn't assigned any segment value security rules. This implies that Perry has global access to all accounts.

User James, who also has the Accounts Receivables Manager role, has access to two business units: Vision ASC605 BU001 and Vision ASC605 BU002. The details of the access are described in the following table.

Example of Segment Value Security

User	Role	Business Function	Business Unit	Security Context Value (Cost Center) as per the rule assignments	Access Level
James	Accounts Receivable Manager	Receivables	Vision ASC605 BU001	00000000, 20000000 to 20000220	Read-Only
James	Accounts Receivable Manager	Receivables	Vision ASC605 BU002	00000110, 20000221 to 20000440, 30000550	Read-Write

This table describes the results of the various actions that James attempts on the Create Transaction: Invoice page in each business unit, as determined by James' segment value security assignments. The Cost Center Value column represents the cost centers used in the transaction.

User Actions and Results

User	Business Unit	Cost Center Value	Access Level	Action	Result
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Save Transaction	James can save the transaction.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Review Distributions	James can review distributions for which James has read-only access. James can't view the account of the distribution with cost center value 30000330.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Edit Distributions	James can't edit or even see the distribution segment values.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Complete Transaction	James can't complete the transaction.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Post to Ledger	James can't post the transaction.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Save Transaction	James can save the transaction.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Review Distributions	James can review all distributions.

User	Business Unit	Cost Center Value	Access Level	Action	Result
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Edit Distributions	James can edit distributions and change the cost center.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Complete Transaction	James can complete the transaction.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Post to Ledger	James can post the transaction.

Subledger Accounting-Specific Considerations for Segment Value Security

This section explains the purpose of Segment Value Security by Business Function and provides an overview of Subledger Accounting, including its activities, setup, transaction processing, and how data security is applied.

Oracle Subledgers such as Payables, Receivables, and so on. and Fusion Accounting Hub subledgers are used to capture transaction information which is then processed by the Subledger Accounting engine to generate detailed subledger accounting entries.

In general, Subledger Accounting activities include:

- **Setup:** Configuring subledger applications, accounting options, accounting rules, mapping sets and supporting references.
- **Transaction:** Fusion Accounting Hub transaction import, create accounting and posting to the General Ledger, manual adjustment entry, maintaining control balances and supporting reference balances.
- **Inquiry and Reporting:** Review subledger accounting entries and drill down to source transactions, reviewing reports such as the Subledger Period Close Exception report, Account Analysis report, OTBI reporting on Subledger Accounting Entries and Supporting Reference balances, and so on.

Subledger Accounting doesn't deliver any job roles for Fusion Applications. Applications such as Payables. Receivables, and so on. which consume Subledger Accounting services grant access to accounting related activities for their application specific job roles by inheriting the duty roles provided by Subledger Accounting.

Accounting Hub users are required to define custom job roles and assign the appropriate duty roles as needed to perform accounting activities.

No data security is applied for the setup related activities; however, data security is applied on the Ledger and Journal Source LOVs for the Transaction, Inquiry and Reporting activities listed above. Data security is implemented through grants against the job roles which perform subledger transaction, inquiry and reporting activities. For example – Accounts Payable Supervisor requires access to account payables invoices, view accounting, review the subledger accounting entries created or create adjustment accounting entries for Payables journal source.

Here is a summary of how data security is applied on Subledger Accounting for General Ledger and Subledger Job Roles:

Job Role	Default Data Security
General Ledger Job Roles (General Accounting Manager, Financial Specialist, and so on.)	For the ledgers to which user has data access: • Review or create subledger accounting entries for ALL subledger applications. • Account transactions, transfer to general ledger and drill down to view transaction page for ALL subledger applications. • Inquiry and reporting pages for ALL subledger applications.
Oracle Subledger Job Roles (Payables Supervisor, Receivables Specialist, and so on.)	For the specific security context (i.e. Business Unit, Intercompany Organization, Asset Book, and so on.) to which user has data access: • Review or create subledger accounting entries for the subledger application. • Account transactions, transfer to general ledger and drill down to view transaction page for the subledger application. • Inquiry and reporting pages for the subledger application.

Segment Value Security by Business Function Implementation in Subledger Accounting

This topic outlines how Segment Value Security is implemented in Subledger Accounting and how it affects different setup, transaction, and reporting areas.

Subledger Accounting is an intermediate processing layer which converts the transaction information from different Oracle and Accounting Hub subledgers into accounting entries based on the accounting rules defined in the system. The Subledger Accounting user interfaces and reports do not enforce data security through a specific data security context such as Data Access Set or Business Unit. Data Security in Subledger Accounting is governed by the data security policies associated with the Job Role which has associated subledger functions.

Subledger Accounting doesn't have any associated business function. For some of the Subledger Accounting pages such as the ones associated with adjustment subledger accounting entry creation or review, the General Ledger business function context is applied. General Ledger enforces data security through Data Access Sets which control read and write access to the entire ledger, or just to certain primary balancing segment values. When the General Ledger business function is applied on subledger accounting pages, a cumulative effect of all the Data Access Set grants for the user will be applied since subledger accounting pages do not have a Data Access Set context. They provide access for the associated ledger only.

If the subledger accounting entries are viewed in the context of a transaction for Oracle Subledgers such as View Accounting window, the business function of the associated subledger shall be applied.

If the segment value security policies are defined for All business functions, access to the secured segment values is based on the applicable Security Context is applied. For example, if the Security Context is set to Data Access Set, subledger accounting pages which enforce General Ledger business function (Create Subledger Journal, Review Subledger Journals, and so on.) will restrict access to the corresponding secured segment values on these pages. However, in the View Accounting page which applies the Subledger business function, these values would not be accessible to users.

If the segment value security policies are defined for All business functions and All security contexts, then access will be restricted to the corresponding secured segment values in all subledger accounting pages where Segment Value Security by Business Function is enforced.

Here is a summary of how Subledger Accounting implements Segment Value Security by Business Function in the different Setup, Transaction and Reporting areas where chart of accounts segments is involved –

Area	User Interface	Segment Value Security by Business Function	Business Function Context Applied
Setup	All Setup Pages	Not Applied	Not Applicable
Transaction	Create Manual Subledger Journal using UI or Spreadsheet	Applied	General Ledger
	Create Accounting Online / Batch process	Not Applied	Not Applicable
	Create Accrual Reversal Accounting process	Not Applied	Not Applicable
	Create Multiperiod Accounting process	Not Applied	Not Applicable
	Update Subledger Balances process	Not Applied	Not Applicable
	Import Accounting Transactions	Not Applied	Not Applicable
Inquiry and Reporting	Review / View Subledger Journal	Applied	General Ledger
	Review / View Subledger Journal – Account Override	Applied	General Ledger
	View Accounting	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	View Accounting – Account Override	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	Drill Down – Subledger Journal Lines	Applied	General Ledger
	Drill Down – View Transaction	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	T-Account Report – Review Subledger Journals	Applied	General Ledger
	T-Account Report – View Accounting	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	Journal Entries Report	Applied	General Ledger
	Account Analysis Report	Applied	General Ledger
	Create Accounting Execution Report	Applied	General Ledger
	Create Multiperiod Accounting Execution Report	Applied	General Ledger

Area	User Interface	Segment Value Security by Business Function	Business Function Context Applied
	Create Accrual Reversal Accounting Execution Report	Applied	General Ledger
	Subledger Accounting Methods Setup Report	Not Applied	Not Applicable
	Accounting Event Diagnostics Report	Not Applied	Not Applicable
	Third Party Control Account Balances Report	Not Applied	Not Applicable

Case Study: Application of Segment Value Security

Joe and Cassie are employees of the Vision Corporation organization.

Vision Operations business unit is one of many business units under the **Vision Corporation US** ledger which manages the Payables and Payment business functions specifically. To streamline access for accounting users based on balancing segment values, the **Vision Corporation US** ledger has 3 Data Access Sets defined – **Vision Corp DAS A**, **Vision Corp DAS B** and **Vision Corp DAS C**, other than the implicit DAS **Vision Corporation US**.

Joe has been hired as a Payables Specialist of Vision Operations in the US to manage payables invoicing related activities such as verifying and recording supplier invoices in the system, making payments timely, monitoring expenses, and keeping a track of all the documents for tax purposes. In certain cases, Joe may be required to enter subledger adjustment accounting entries if the invoice was not captured directly in the Payables – Invoices application.

Cassie has been hired as a General Accountant of Vision Corporation in the US for reviewing account statements, conducting data analysis with financial transactions, and generating reports on revenues, expenses, asset, liability, and equity accounts. She is also responsible for recording accounting adjustments, accruals, allocations, currency revaluations and translations as part of accounting period closure activities. Occasionally, she may create subledger adjustment accounting entries during subledger to general ledger reconciliation.

The following are the job roles and data security assignments provided to Joe and Cassie for managing the responsibilities related to Payables Specialist and General Accountant job roles –

User	Job Role	Data Security Context
Joe	Employee	NA
	Payables Specialist	Vision Operations (BU)
Cassie	Employee	NA
	General Accountant	Vision Corp DAS A
	General Accountant	Vision Corp DAS C

Subledger Accounting doesn't have any separate data security context or business function. By default, all segment values corresponding to the secured segments in the account combination are accessible to perform the activities which are accessible to the Payables Specialist and General Accountant job roles on the Vision Operations business unit and Vision Corporation US ledger respectively. Access to specific segment values of the secured segments while entering an account combination in Payables and General Ledger pages would be restricted based on the respective policies assigned to each user.

Following segment value security policies are assigned to Joe and Cassie –

User	Job Role	Data Security Context	Business Function	Segment	Segment Value	Access Level
Joe	Employee	NA	NA	NA	NA	NA
	Payables Specialist	Vision Operations (BU)	Payables	Cost Center	110	Read/Write
					120	Read Only
	Payables Specialist	Vision Corporation US (DAS)	General Ledger		130	Read/Write
Cassie	Employee	NA	NA	NA	NA	NA
	General Accountant	Vision Corp DAS A (DAS)	General Ledger	Cost Center	110	Read/Write
					120	Read/Write
					130	Read Only
					140	Read Only
		Vision Corp DAS C (DAS)			160	Read/Write
					170	Read/Write

Here are some sample examples of how the above policy definition would provide access to different subledger accounting pages to Joe and Cassie respectively –

User	User Interface	Access
Joe	View Accounting	This page is read-only, and the Subledger business function is applied here. Since the user has access to read both the cost center values 110 and 120 for Payables business function, they will be able to access those account combinations which use these cost center values.
	View Accounting – Account Override	This page supports read\write and the Subledger business function is applied here. Since the user has access to read\write to the cost center value 110 only, they will be able to access those account combinations which use this cost center value.
	Review Journal Entries / Journal Lines	This page is read-only, and the General Ledger business function is applied here. Since the user has access to read the cost center value 130 for General Ledger business function, they will be able to access those account combinations which use this cost center value.
	Account Analysis Report	This is a read-only report, and the General Ledger business function is applied here. Since the user has access to read the cost center value 130 for General Ledger business function,

User	User Interface	Access
		they will be able to access those account combinations which use this cost center value.
	Create Subledger Journal	This page supports read\write and the General Ledger business function is applied here. Since the user has access to read\write the cost center value 130 only, they will be able to access those account combinations which use this cost center value.
Cassie	Review Journal Entries / Journal Lines	This page is read-only, and the General Ledger business function is applied here. The user has access to read the cost center values 110, 120, 130, 140 through the data access set **Vision Corp DAS A** and the cost center values 160, 170 through the data access set **Vision Corp DAS C**. So, a cumulative effect of all the Data Access Set grants will be applied for the General Ledger business function here, thereby allowing the user to access those account combinations which use the cost center values – 110, 120, 130, 140, 160 and 170.
	Account Analysis Report	This is a read-only report, and the General Ledger business function is applied here. Like the above scenario, a cumulative effect of all the Data Access Set grants will be applied for the General Ledger business function here, thereby allowing the user to access those account combinations which use the cost center values – 110, 120, 130, 140, 160 and 170.
	Create Subledger Journal	This page supports read\write and the General Ledger business function is applied here. The user has access to read\write the cost center values 110, 120 through the data access set **Vision Corp DAS A** and the cost center values 160, 170 through the data access set **Vision Corp DAS C**. As a cumulative effect of all the Data Access Set grants applied for the General Ledger business function here, the user gets access to those account combinations which use the cost center values – 110, 120, 160 and 170.

How You Segregate Import Journals Access from FBDI Import for Journals Access

You can restrict the combined use of the Import Journals process and the Load Interface File for Import process for file-based data import (FBDI) journals to certain users.

Users who aren't authorized to import journals using FBDI can be assigned privileges that allow them to submit journal import only for processes such as Create Accounting for subledger transactions and Oracle General Ledger journal creation through the Application Development Framework desktop integration (ADFdi) spreadsheet.

Separate privileges give you the flexibility to assign different users different levels of access to the Import Journals process to optimize security control and prevent interruptions in FBDI journal import procedures that are reserved for automated and mass volume imports.

Here are the privileges that allow access to journal import processes other than FBDI import for journals.

- **Run Import Journals Program without FBDI Access** (GL_RUN_IMPORT_JOURNALS_PROGRAM_WITHOUT_FBDI_ACCESS): Allows submission of the journal import program using the Oracle Fusion Enterprise Scheduler Services. However, this privilege does not include the ability to use the Import Journals process when submitting the Load Interface File for Import program to support creating journal records using File Based Data Import.
- **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** (XLA_POST_SUBLEDGER_JOURNAL_ENTRY_TO_GL_NO_JOURNAL_IMPORT_ACCESS_FOR_FBDI): Allows submission of the program to transfer to and post journal entries in General Ledger. However, this privilege does not include the ability to use the Import Journals process when submitting the Load Interface File for Import program to support creating journal records using File Based Data Import.

These privileges aren't assigned to any predefined role. You must assign them to a custom role to use them as substitutes for the **Run Import Journals Program** (GL_RUN_IMPORT_JOURNALS_PROGRAM_PRIV) and **Post Subledger Journal Entry to General Ledger** (XLA_POST_SUBLEDGER_JOURNAL_ENTRY_TO_GENERAL_LEDGER_PRIV) privileges, which allow access to FBDI import for journals.

If you're creating a role based on the predefined General Accountant job role, here's a summary of the steps you would follow to prevent a user from using FBDI journal import, while still allowing that user to submit journal import through other processes.

1. Use the Security Console to make a deep copy of the predefined General Accountant job role by copying its top role and inherited roles. The inherited roles include the Journal Management and Subledger Accounting Manager duty roles.
2. After the role has been copied, search for the Journal Management custom duty rule that was generated. Perform the following actions in the Function Security Policies step:
    a. Add the **Run Import Journals Program without FBDI Access** privilege.
    b. Delete the **Run Import Journals Program** privilege.
3. Search for the Subledger Accounting Manager custom duty role that was generated. Perform the following actions in the Function Security Policies step:
    a. Add the **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** privilege.
    b. Delete the **Post Subledger Journal Entry to General Ledger** privilege.

If you're creating your own custom role or starting with an existing custom role, perform these steps in the Security Console to prevent a user from using FBDI journal import, while still allowing that user to submit journal import through other processes.

1. Add the **Run Import Journals Program without FBDI Access** and **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** privileges.
2. Delete the **Run Import Journals Program** and **Post Subledger Journal Entry to General Ledger** privileges wherever they exist in the role hierarchy.

Note: Users who already submit the Load Interface File for Import for other import processes such as Import Bank Statements from a Spreadsheet and Import AutoInvoice won't be impacted by the removal of the **Run Import Journals Program** and **Post Subledger Journal Entry to General Ledger** privileges.

If a user who's only assigned the **Run Import Journals Program without FBDI Access** or the **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** privilege submits the Load Interface File for Import process for the Import Journals process, the job will end in error. The log file will display an insufficient permissions message.

Related Topics

- Create ERP Roles in the Security Console
- Guidelines for Copying ERP 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 when it's updated. 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.

Note: If you change an account hierarchy that's already published and you inquire or report on summary balances based on this changed hierarchy, you must republish to reflect the updated hierarchy in the balances cube.

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 publish an account hierarchy to the balances cube after enabling security for its value set.

If you disable security for that value set, you must likewise publish its account hierarchy to the balances cube to register that security is no longer enabled for it.

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.

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

Oracle Fusion Payables improves security by limiting access to invoices and payments by business unit. You can access invoices and payments for viewing or processing only for the business units to which you've permission. The permission must be explicitly granted to each user.

Assign users to the appropriate security context, such as a business unit, for job roles from the Manage Data Access for Users page.

Oracle Payables is integrated to the document repository for processing scanned invoices. To edit any invoices in the repository, you can create a custom role with the Edit Payables Invoice (AP_EDIT_PAYABLES_INVOICE_PRIV) or Create Payables Invoice (AP_CREATE_PAYABLES_INVOICE_PRIV) privileges.

Keeping up with the security requirements, the following predefined roles have view-only access to the document repository:

- Financial Application Administrator
- Cost Accountant
- Project Accountant

Note: For further information, see the chapter Role Configuration Using the Security Console in the Securing ERP guide.

Why do I see a blank page on clicking View Invoice from Approval Notification?

A user must have these privileges to view an invoice by clicking the View Invoice button on the notification.

- View Payables Invoice
- Manage Payables Invoices
- Manage Payables Invoices Activities

If you've a custom user role, you might be missing these privileges, which results in the blank page being displayed.

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 (XLA_IMPORT_SUBLEDGER_ACCOUNTING_TRANSACTIONS_PRIV) 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 track 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.

Legal Entity-Based Data Access for Bank Account Setup

By default, users with the necessary function security privileges have access to create and manage all internal bank accounts.

Optionally, restrict access to bank account information based on the user's legal entity data access. This allows cash managers to add, review, or modify only the bank accounts associated with the legal entities that the user has access to. For example, only users who have been assigned the Manage Bank Account (CE_MANAGE_BANK_ACCOUNT_PRIV)

privilege for Vision Operations legal entity, can create, review, or modify internal bank accounts associated with this legal entity.

Decentralized organizations will benefit with improved security by ensuring that users only manage the bank account setup for the organizations they're authorized for.

Business benefits include:

- Improve security and increase control of bank account setup by limiting user access to bank account information.
- Helps decentralized organizations that require users only to manage the bank account information for the organizations they're authorized for.

To enable the feature Legal Entity-Based Data Access for Bank Account Setup, you must:

1. Use the Opt in UI to enable the feature.
2. Assign users to the appropriate legal entity security context:
    a. In the Setup and Maintenance work area, Select the Offering as Financials, Functional Area as Users and Security, and Task as Manage Data Access for Users.
    b. On the Manage Data Access for Users page, create data access for users by entering the user name, Cash Manager as role, legal entity as security context, and legal entity name as security context value, to create the data access for the user.
    c. Save the changes.

Once the feature is enabled, legal entity-based data access security is applied when an internal bank account is created or managed using either the UI or REST API.

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.

- To set up banks, branches, and accounts, your custom role must have the security duty role Cash Management Administration. You must have the assigned the Manage Bank Account Security privilege (CE_MANAGE_BANK_ACCOUNT_SECURITY_PRIV) to modify the User and Role Security.
- To restrict the access to the Security tab, you must create a custom role and remove the Manage Bank Account Security (CE_MANAGE_BANK_ACCOUNT_SECURITY_PRIV) privilege. For example, you'd copy the Cash Management Administration duty role, rename it, and remove the privilege.

GL Cash Account Segments

Consider selecting the option to enable multiple cash account combinations for reconciliation to reconcile journal lines of multiple cash account combinations matching the same natural account and other specified segment values.

For example, if you set up 01-000-1110-0000-000 as your cash account, and select Account and Subaccount as GL Cash Account Segments, you can manually or automatically reconcile journal lines entered on different account code combinations matching the same natural account '1110' and subaccount '0000'.

Related Topics

- Assign Data Access to Users

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

Options for System Security

Implement application security options on the Manage System Security Options page. You can set the application security to align with your company's security policy.

You can set security options for encryption and tokenization of credit cards and bank accounts, as well as for masking the payment instrument. Both funds capture and disbursement processes use security options.

> **Note:** You must enable encryption or tokenization of credit cards in Payments before you can import credit cards into Expenses.

Ask yourself these security questions to improve the security of your sensitive data:

- Which security practices do I want to employ?
- Do I want to tokenize my credit card data?
- Do I want to encrypt my bank account data?
- Do I want to encrypt my credit card data?
- How frequently do I want to rotate the master encryption key and the subkeys?
- Do I want to mask credit card and bank account numbers? How do I accomplish that?

To set up application security options, go to **Financials** > **Payments** > **Manage System Security Options** in the Setup and Maintenance work area.

Best Security Practices

These 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 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. Oracle Platform Security Services 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's created and stored in the proper location and with all necessary permissions.

Credit Card Tokenization

If you tokenize your credit card data, you're 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.

Click **Edit Tokenization Payment System** on the Manage System Security Options page to set up your tokenization payment system. Then, click **Tokenize** in the Credit Card Data section to activate tokenization for credit card data.

Credit Card Data Encryption

You can encrypt your credit card data to assist with your compliance of cardholder data protection requirements with these initiatives:

- Payment Card Industry Data Security Standard
- Visa's Cardholder Information Security Program

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 import card numbers into Payments, you should 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 Cash Management. They are used as disbursement bank accounts in 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 import bank account numbers into Payments, you should 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 enables easier rotation of the master encryption key.

The master encryption key is stored on Oracle Platform Security Services. Oracle Platform Security Services 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, click **Rotate** to automatically generate a new one.

> **Note:** To secure your payment instrument data, you should rotate the master encryption key annually or according to your company's security policy.

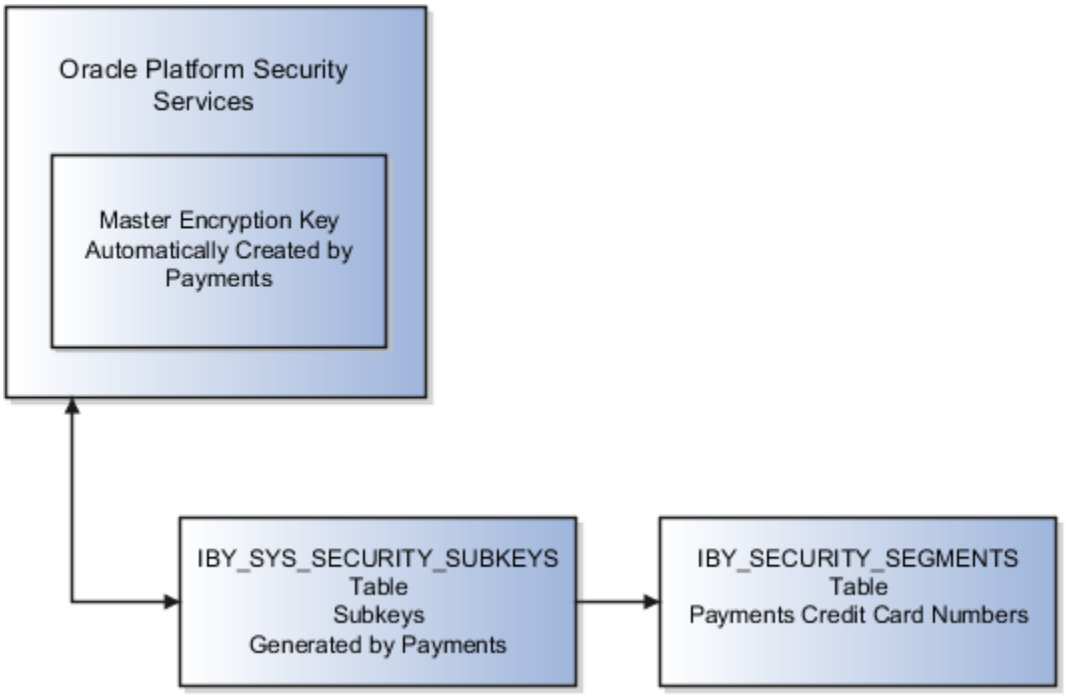
You can also select the frequency with which new subkeys are automatically generated, based on usage or on the maximum number of days. To specify a subkey rotation policy, click **Edit Subkey Rotation Policy**.

> **Note:** To secure your payment instrument data, you're advised to schedule regular rotation of the subkeys.

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

- Oracle Platform Security Services
- Payments master encryption key
- Payments subkeys
- Sensitive data encryption and storage

This figure illustrates the security architecture of the Oracle Platform Security Services 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. It stores all of the customer and supplier payment information and their payment instruments, such as credit cards and bank accounts. It provides data security by letting you mask bank account numbers.

On the Manage System Security Options page, you can mask credit card numbers and external bank account numbers. You just have to select the number of digits to mask and display. For example, a bank account number of XX558012 displays the last six digits and masks all the rest. These settings specify masking for payment instrument numbers in the user interfaces of multiple applications.

> **Note:** For credit cards, you can unmask only up to the first or last four digits of the credit card number. On the other hand, you can unmask up to the first or last six digits of a bank account number.

Related Topics

- Enable Encryption of Sensitive Payment Information
- PCI DSS Credit Card Processing Requirements

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're 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 **Financials** > **Payments** > **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.

Related Topics

- Overview of Data Access Set Security
- Examples of Data Access Set Security
- Overview of Segment Value Security
- Enforcement of Segment Value Security by Business Function

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 Transactional Business Intelligence as the standard query and reporting tool, Oracle Analytics 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.

Financials Job Role	Subject Areas
Accounts Payable Manager	All Payables
Accounts Payable Specialist	All Payables
Accounts Payable Supervisor	Payables Invoices - Installments Real Time, Payables Payments - Disbursements Real Time, Payables Payments - Payment History Real Time
Accounts Receivable Manager	All Receivables
Accounts Receivable Specialist	All Receivables
Asset Accountant	Fixed Assets - Asset Depreciation Real Time, Fixed Assets - Asset Retirements and Reinstatements Real Time, Fixed Assets - Asset Source Lines Real Time, Fixed Assets - Asset Transactions Real Time, Fixed Assets - Asset Transfer Real Time
Asset Accounting Manager	All Fixed Assets
Budget Manager	Budgetary Control - Transactions Real Time

Financials Job Role	Subject Areas
Cash Manager	All Cash Management
Expense Manager	All Expenses
Financial Analyst	All Financials
Financial Application Administrator	All Financials
Financial Integration Specialist	All Financials
General Accountant	General Ledger - Journals Real Time, General Ledger - Period Status Real Time
General Accounting Manager	All General Ledger, All Payables, All Receivables
Intercompany Accountant	Financials Common Module - Intercompany Transactions Real Time
Tax Accountant	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time
Tax Administrator	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time
Tax Manager	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time, Receivables - Customer Tax Profile Real Time
Tax Specialist	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time, Receivables - Customer Tax Profile Real Time

In addition, Oracle Fusion Cloud Financials includes predefined self-service reporting duties that provide access to Transactional Business Intelligence subject areas and drill down pages. They can be used as building blocks to construct reporting roles to provide self service reporting access.

This table identifies the subject areas that predefined Financials self-service reporting duty roles can access.

Financials Self-Service Reporting Duties	Subject Areas
Budgetary Control Self Service Reporting Duty	All Budgetary Control
Cash Management Self Service Reporting Duty	All Cash Management
Expense Self Service Reporting Duty	All Expenses
Fixed Asset Self Service Reporting Duty	All Fixed Assets
General Ledger Self Service Reporting Duty	All General Ledger, Financials Common Module - Intercompany Transactions Real Time

Financials Self-Service Reporting Duties	Subject Areas
Payables Self Service Reporting Duty	All Payables
Receivables Self Service Reporting Duty	All Receivables
Revenue Management Self Service Reporting Duty	All Revenue Management

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.

Financials Job Role	Business Intelligence Catalog Folders
Accounts Payable Manager	Transactional Business Intelligence Payables
Accounts Payable Specialist	Transactional Business Intelligence Payables
Accounts Payable Supervisor	Transactional Business Intelligence Payables
Accounts Receivable Manager	Transactional Business Intelligence Receivables
Accounts Receivable Specialist	Transactional Business Intelligence Receivables
Asset Accountant	Transactional Business Intelligence Fixed Assets
Asset Accounting Manager	Transactional Business Intelligence Fixed Assets
Budget Manager	Transactional Business Intelligence Budgetary Control
Cash Manager	Transactional Business Intelligence Cash Management
Expense Manager	Transactional Business Intelligence Expenses
Financial Analyst	Transactional Business Intelligence Financials
General Accountant	Transactional Business Intelligence General Ledger
General Accounting Manager	Transactional Business Intelligence General Ledger
Intercompany Accountant	Transactional Business Intelligence Intercompany Accounting

Financials Job Role	Business Intelligence Catalog Folders
Tax Accountant	Transactional Business Intelligence Transaction Tax
Tax Administrator	Transactional Business Intelligence Transaction Tax
Tax Manager	Transactional Business Intelligence Transaction Tax
Tax Specialist	Transactional Business Intelligence Transaction Tax

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, 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:

Duty Role	Version
Fixed Asset Transaction Analysis Duty	**OBI**
Fixed Asset Transaction Analysis	**Financials**

The Fixed Asset Transaction Analysis Duty role is granted relevant data security policies and inherits Business Intelligence Consumer Role.

Business Intelligence Roles

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.

Business Intelligence Role	Description
Business Intelligence Consumer Role	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.
Business Intelligence Authoring	Allows authoring within Business Intelligence Applications, Business Intelligence Publisher, Real Time Decisions, Enterprise Performance Management and Business Intelligence Office.
Business Intelligence Applications Analysis	Performs Business Intelligence Applications Analysis generic duty.
Fixed Asset Business Intelligence Management	Manages access to Fixed Assets OBIA Dashboard.
Business Intelligence Applications Administrator	Provides access to the BI Applications Configuration Manager and to the BI Data Warehouse Administration Console.

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 self-service reporting duties inherit this Business Intelligence Consumer role. 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.

Subject Areas	Job Role	Self Service Reporting Duty	OTBI Transactional Analysis Duty Role
• Budgetary Control - Transactions Real Time	Budget Manager	Budgetary Control Self Service Reporting Duty	Budgetary Control Analysis Duty
• Cash Management - Bank Statement Balances Real Time • Cash Management - Bank Statement Line Charges Real Time • Cash Management - Bank Statements Real Time • Cash Management - External Cash Transactions Real Time	Cash Manager	Cash Management Self Service Reporting Duty	• Cash Management Transaction Analysis Duty
• Expenses - Employee Expense Overview Real Time • Expenses - Expense Transactions Real Time	Expense Manager	Expense Self Service Reporting Duty	• Expenses Summary Transaction Analysis Duty • Expense Transactions Transaction Analysis Duty
• Financials Common Module - Intercompany Transactions Real Time	• Intercompany Accountant • General Accountant	General Ledger Self Service Reporting Duty	Inter Company Transaction Analysis Duty
• Fixed Assets - Asset Assignments Real Time • Fixed Assets - Asset Balances Real Time • Fixed Assets - Asset Depreciation Real Time • Fixed Assets - Asset Financial Information Real Time • Fixed Assets - Asset Retirements and Reinstatements Real Time • Fixed Assets - Asset Source Lines Real Time • Fixed Assets - Asset Transactions Real Time	Asset Accountant	Fixed Asset Self Service Reporting Duty	• Fixed Asset Transaction Analysis Duty • Fixed Asset Details Transaction Analysis Duty • Fixed Depreciation Transaction Analysis Duty • Fixed Asset Details Transaction Analysis Duty

Subject Areas	Job Role	Self Service Reporting Duty	OTBI Transactional Analysis Duty Role
• Fixed Assets - Asset Transfer Real Time			
• General Ledger - Balances Real Time • General Ledger - Journals Real Time • General Ledger - Period Status Real Time • General Ledger - Transactional Balances Real Time	General Accountant	General Ledger Self Service Reporting Duty	• General Ledger Transaction Analysis Duty • Payables to Ledger Reconciliation Transaction Analysis Duty • Receivables to Ledger Reconciliation Transaction Analysis Duty
• Payables Invoices - Installments Real Time • Payables Invoices - Prepayment Applications Real Time • Payables Invoices - Transactions Real Time • Payables Invoices - Trial Balance Real Time • Payables Invoices - Withholding Real Time • Payables Payments - Disbursements Real Time • Payables Payments - Payment History Real Time	• Accounts Payable Manager • Accounts Payable Specialist • General Accountant	Payables Self Service Reporting Duty	• Payables to Ledger Reconciliation Transaction Analysis Duty • Payables Invoice Transaction Analysis Duty • Payables Payment Transaction Analysis Duty
• Receivables - Adjustments Real Time • Receivables - Bills Receivable Real Time • Receivables - Credit Memo Applications Real Time • Receivables - Credit Memo Requests Real Time • Receivables - Customer Account Site Tax Profile Real Time • Receivables - Customer Real Time • Receivables - Customer Tax Profile Real Time • Receivables - Miscellaneous Receipts Real Time • Receivables - Payment Schedules Real Time	• Accounts Receivable Manager • Accounts Receivable Specialist • General Accountant	Receivables Self Service Reporting Duty	• Receivables to Ledger Reconciliation Transaction Analysis Duty • Receivables Customer Transaction Analysis Duty • Receivables Transaction Analysis Duty • Receivables Receipts Transaction Analysis Duty

Subject Areas	Job Role	Self Service Reporting Duty	OTBI Transactional Analysis Duty Role
• Receivables - Receipt Conversion Rate Adjustments Real Time • Receivables - Receipts Details Real Time • Receivables - Revenue Adjustments Real Time • Receivables - Standard Receipts Application Details Real Time • Receivables - Transactions Real Time			
• 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	• Cash Management Self Service Reporting Duty • Fixed Asset Self Service Reporting Duty • Payables Self Service Reporting Duty • Receivables Self Service Reporting Duty	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:

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 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 Analytics 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 Analytics Publisher is a set of tools for creating formatted reports based on data models.

You can access Analytics Publisher from Business Intelligence Composer or the Business Intelligence Catalog by clicking NewReport . 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, Analytics 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

Analytics Publisher Data Security and Secured List Views

When you create a Analytics 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.

22 Security in Oracle Project Management

Overview of Project Management Security

Oracle Project Management Cloud predefines common job roles such as Project Manager and Project Accountant. You can use these job roles or create new ones if the predefined job roles don't fully represent your enterprise.

For example, the predefined Project Manager job role includes project budget management privileges. If some of your project managers don't manage budgets, you can copy the predefined project manager job role and remove the appropriate privileges to create a custom role. A user can have more than one job role, so don't define a job role that includes all the accesses needed for every user.

Refer to the Security Reference Manual for a description of predefined roles in Oracle Project Portfolio Management Cloud.

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's not job specific, such as creating time cards and expense reports, are granted to the **Enterprise Resource Planning Self Service User** abstract role. Abstract roles like **Employee**, **Contingent Worker** and **Line Manager** also grant access to common functionalities across a wide collection of Oracle Cloud Applications.

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're 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 roles or abstract job roles and the type of security that grants the role access to data in a work area or dashboard.

Job or Abstract Role	Work Area or Dashboard	Data Security Based On
Project Accountant	Asset	Project business unit
Project Accountant	Costs	Project expenditure business unit
Project Accountant	Revenue	Contract business unit
Project Administrator	Project Financial Management	Project business unit Project organization
Project Administrator	Project Financial Management - Change Orders	Project business unit

Job or Abstract Role	Work Area or Dashboard	Data Security Based On
		Project organization
Project Billing Specialist	Invoices	Contract business unit
Project Management Duty	Project Management Infolet Dashboard	Project assignment
Project Management Duty	Project Performance Dashboard	Project assignment
Project Manager	Project Management Infolet Dashboard	Project assignment
Project Manager	Project Performance Dashboard	Project assignment
Project Manager	Project Management	Project assignment
Project Manager	Project Manager Dashboard	Project assignment
Project Team Member	Project Financial Management	Project assignment
Grants Accountant	Invoices	Contract business unit
Grants Accountant	Revenue	Contract business unit
Grants Accountant	Asset	Project business unit
Grants Accountant	Costs	Project expenditure business unit
Grants Administrator	Awards	Contract business unit
Grants Administrator	Contracts	Contract business unit
Grants Administrator	Project Financial Management	Project business unit
Grants Department Administrator	Awards	Award organization
Grants Department Administrator	Contracts	Contract business unit
Grants Department Administrator	Project Financial Management	Project organization
Principal Investigator	Awards	Award assignment
Principal Investigator	Contracts	Award assignment

Job or Abstract Role	Work Area or Dashboard	Data Security Based On
Principal Investigator	Project Financial Management	Project assignment
Labor Distribution Accountant	Labor Distribution	Business unit
Labor Distribution Administrator	Labor Distribution	Person Security Profile Assigned to role
Program Manager	Program Management	Program organization Person Security Profile assigned to role

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 roles or abstract job roles and the type of security that grants access to data in a work area or dashboard.

Job Role or Abstract Role	Work Area or Dashboard	Data Security Based On
Project Execution	Project Management	Project assignment
Project Execution	Project Management Infolet Dashboard	Project assignment
Project Execution	Project Manager Dashboard	Project assignment
Project Execution	Requirements	No data security required
Project Execution	My Work - Tasks	Task assignment or task follower
Project Execution	My Work - Change Orders	Change order role
Project Execution	My Work - Deliverables and Issues	No data security required
Team Collaborator	My Work - Tasks	Task assignment or task follower **Note:** If you change a to do task to a project task, security is based on project assignment.

Job Role or Abstract Role	Work Area or Dashboard	Data Security Based On
Team Collaborator	My Work - Change Orders	Change order role
Team Collaborator	My Work - Deliverables and Issues	No data security required
Team Collaborator	Team Member Dashboard	Task assignment
Project Executive	Project Hierarchy	Project hierarchy element assignment
Project Manager	Project Manager - Change Orders	Project assignment
Resource Manager	Project Resources	No data security required
Resource Manager	Resource Manager Dashboard	No data security required

Creating Custom Roles for Projects

The project job role determines the tasks that a team member can perform on a page or in a work area. Each project job role is associated with a job or an enterprise role.

If the predefined job roles don't fully serve your business needs, then you can create your own job roles that are based on the predefined job roles. For example, your enterprise may require additional job roles with specific constraints on accessing application functions.

To create a new job role perform the following steps.

1. Navigate to **Navigator** > **Tools** > **Security Console** to:
    - Copy an existing job or enterprise role
    - Modify the function security policies
    - Modify the data security policies
    - Modify the role hierarchy
2. Use one of the following pages from the Setup and Maintenance work area as required.
    - Manage Project Roles page to associate the new job or enterprise role with a project job role.
    - Manage Data Access for Users page and grant the person-job roles combination the access to the security context, for example, business unit or organization.

> **Tip:** Never edit the predefined roles. Instead, copy the predefined role and remove the functional and data security policies that aren't required or add new privileges, till the requirement is achieved. You can perform both tasks on the Security Console.

Example: Project Manager Role

For example, the predefined Project Manager job role includes project budget management privileges. If some of your project managers don't manage budgets:

1. In the Security Console:
    - Copy the role that's the closest to the role that you want to create, such as the Project Management Duty role. Give the job 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 job role and map it to the new Junior Project Manager job role.

Now any person added to the project as a Junior Project Manager can perform the functions based on the duties under the new job role.

Project Execution Management

Overview of User Creation and Role Provisioning

Manage users, user accounts, and provision roles to project labor resources. It's recommended that you use the Security Console to manage application security.

Page	It Enables You To
Manage Project Enterprise Resources	• Create project enterprise resources directly or from HCM persons. And, optionally request user accounts for project enterprise resources. • Manage personal details such as calendars, make resources eligible for project assignments to fulfill project resource requests, and specify rate details.

When you create users and provision roles, the application sends:

1. A request for a user account to Oracle Identity Management application.
2. An email notification to the resource after the provisioning is successful.

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. Project role for a user can vary from one project to another.

For example, Mary can be a Business Analyst for one project and a Project Coordinator for a another project.

A project role has two components:

- Enterprise role: Each project role is associated with one enterprise role. The enterprise role associated with a project determines the functional and data access on the project. This access is project-specific and won't apply to other projects.

  > **Note:** Multiple project roles can be associated with the same enterprise role.

- Qualifications and keywords: Each role can be associated with multiple qualifications and keywords. These are used to associate competencies to the project role. These are used by project managers and resource managers for managing resources.

Here's how project roles are used:

- 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.

Managing Project Roles

You can either use the predefined roles or create custom roles. The application provides predefined project roles such as Project Manager and Team Member. Project application administrators can create custom project roles and manage all project roles using the **Manage Project Roles** task.

For predefined roles, project application administrators can:

- Edit enterprise role.
- Manage qualifications and keywords.

For custom roles, project application administrators can:

- Edit project role name, enterprise role, and description.
- Manage qualifications and keywords.
- Specify from date and to date.

Considerations for Managing Project Roles

Here are some considerations for managing project roles.

- You can't delete predefined project roles.
- You can't delete custom project roles that are:
    - Designated as resources' primary role
    - Specified on a project resource request
    - Assigned to a resource on a project
    - The default qualifications, proficiency, and keywords associated with a project role automatically appear as requirements on a project resource request when project managers select the project role for the request.

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.

Here's how a resource's primary project role is used:

- As a resource search option filter when viewing resources on the Search and Evaluate Resources page in the Resource Management work area
- When comparing the attributes of multiple resources against the requirements specified in the project resource request on the Compare Resources page

Project Roles with Limited Actions for Managing Resources on a Project

To limit the actions that are available when managing project resources, project application administrators can create custom project roles with different privileges. For example, you want a project manager to have full access for creating and editing project resource requests.

But you might not want a junior project manager to have all these capabilities.

Before you can create custom project roles with limited resource management capabilities, you must opt in for the Define Project Roles with Limited Actions for Managing Resources on a Project feature.

Users can be assigned different roles for different projects and therefore have different access across their projects. For example, a user can be the senior project manager, with complete access, for one project and be an assistant project manager, with limited resource management capability, for a different project.

To create roles with different resource management capabilities, create various custom project manager roles with the Manage Project Resource Assignment functional privilege and one of the following data privileges:

- View Project Team Members for Project Data: Provides view-only access.
- Edit Project Team Members for Project: Provides the ability to add, update, replace, and delete resources.
- Manage Project Resource Assignment Data: Provides the ability to add, update, replace, delete resources, create resource requests, view resource request details, view assignment details, request extensions, cancel assignments, and manage project resource requests. It also provides the ability to search in case of placeholder resources.

You might be wondering what happens to existing roles. When you opt into the feature:

- Manage Project Work Plan Resource Assignments Data is automatically rolled up to the predefined Project Manager role and the Project Execution abstract role.
- By default, users with custom roles will see only a view-only version of the Manage Project Resources page. You can update the role definitions of custom manager roles to include additional functional and data privileges. For example, you can add the Manage Project Resource Assignment Data privilege to a custom role.

> **Note:** The ability of a project manager to directly confirm a resource or edit a confirmed resource is available only to users with a role that includes the Assign Project Resource to Project and Assign Project Resource to Project Data privileges.

Related Topics

- Project Roles in Project Execution Management Applications
- Can a project manager directly assign a resource to a project?

FAQs for Project Roles

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

Here are the steps to assign project roles by default when project enterprise labor resources are imported:

1. Open **Manage Project User Provisioning** > **Default Provisioning Attributes** and click **Edit**.
2. In the **Default Role Assignments** section, select all roles that must be provisioned by default.
3. In the **Default Project Role Provisioning for Project Execution Management Labor Resources** section, select **Automatically provision roles when mass creating project enterprise labor resources**.

The application automatically assigns the selected predefined and custom roles when you create project users using any of these methods:

- The Maintain Project Enterprise Labor Resources process
- Project Enterprise Resource REST API
- The Import Project Enterprise Resources file-based data import process

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

You can view project management or resource management pages only if you're 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 of the Overview of Project Portfolio Management Security topic.

Related Topics

- Overview of Project Management Security

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

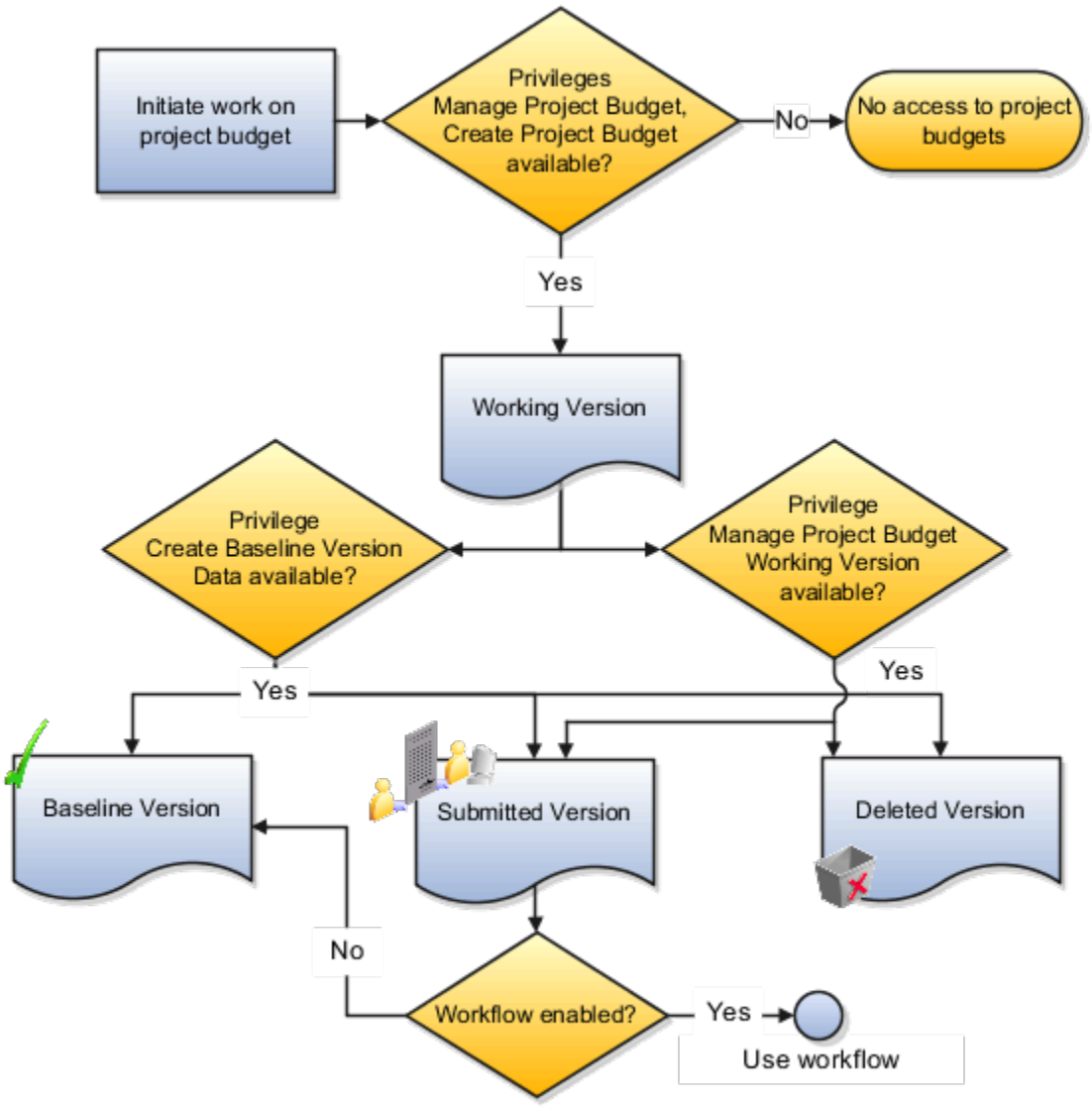
The following table describes the access required to create and submit a budget version.

Step	Action	Privilege
1	Access budget versions for a project	Manage Project Budget
2	Create a budget version	Create Project Budget **Note:** The privilege required for editing budget versions in Excel is Manage Project Budget Excel Integration.
3	Submit working version	Manage Project Budget Working Version
4	Create baseline directly	Create Baseline Version Data

Step	Action	Privilege
		Note: Project managers may select to create a baseline directly instead of submitting a version for approval first.

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 doesn't 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.



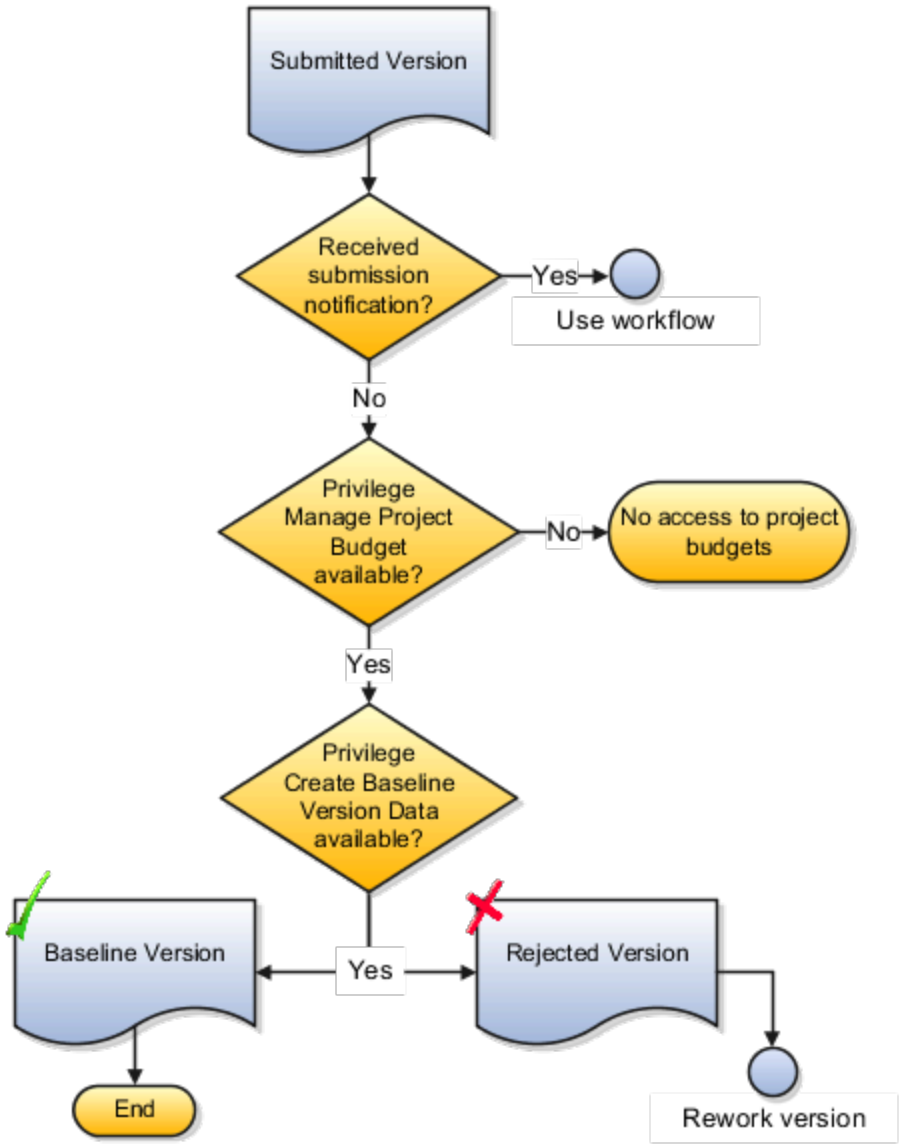
Creating a Baseline for a Budget Version

The following table describes the access required to create a baseline for a budget version or reject it.

Step	Action	Privilege
1	If using workflow, receive notification of budget submission	NA (Approver e-mail ID is entered manually by users)
2	Access budget versions for a project	Manage Project Budget

Step	Action	Privilege
3	Create baseline or reject budget	Create Baseline Version Data

This following figure describes the steps for creating a baseline for a budget version.

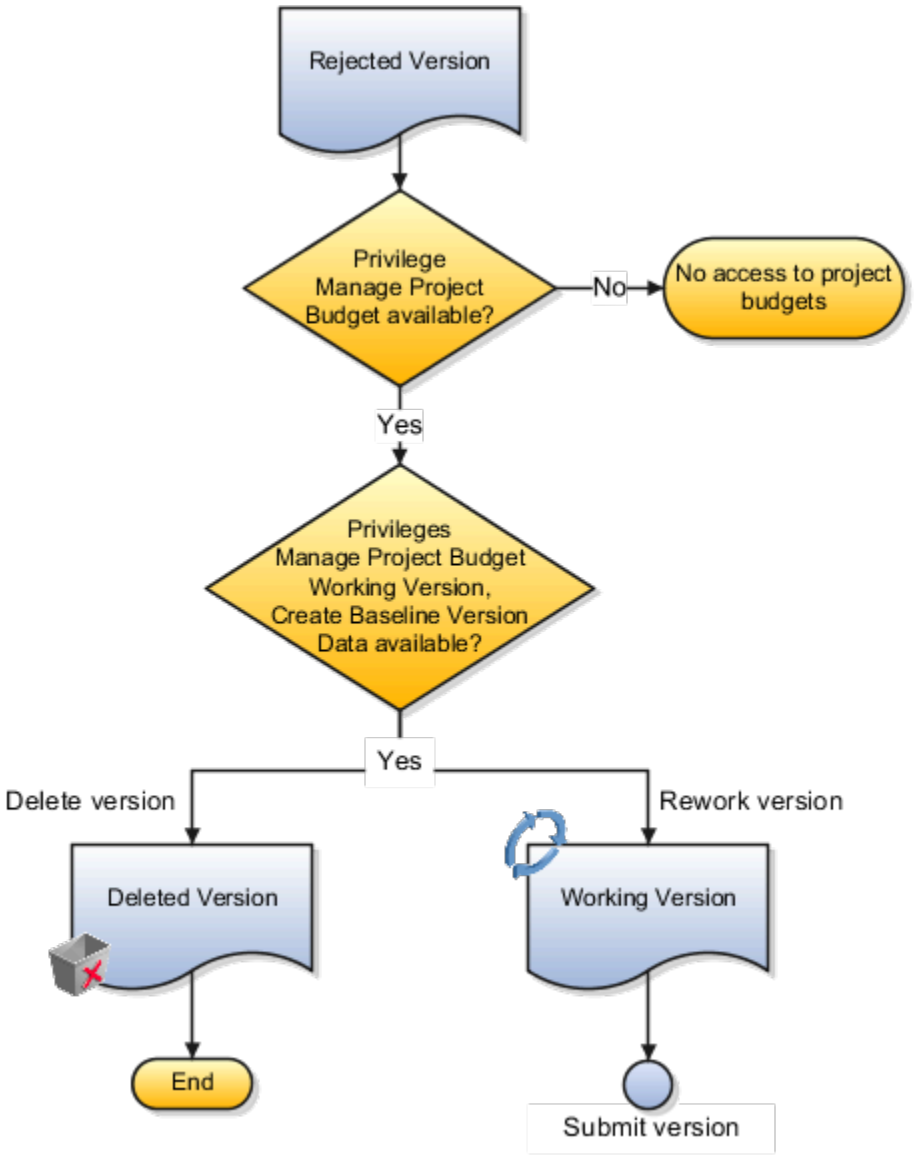


Reworking a Rejected Budget Version

The following table describes the access required to required to rework a rejected version (set it back to Working status) or delete it, if it's no longer required.

Step	Action	Privilege
1	Access budget versions for a project	Manage Project Budget
2	Rework working version	Manage Project Budget Working Version
3	Delete working version	Manage Project Budget Working Version

The following figure describes the steps for reworking a rejected budget version.



Related Topics

- Project Roles in Budgeting and Forecasting
- 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.

Privilege Area	Project Application Administrator	Project Manager	Project Administrator	Notes
Edit budget and forecast planning options	Yes	No	No	Project application administrators set planning options for financial plan types. Project managers and accountants can view planning options at the version level.
Create versions	No	Yes	Yes	None
Generate versions	No	Yes	Yes	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.)
Edit versions in Excel	No	Yes	Yes	None
Submit versions	No	Yes	Yes	None
Approve versions	No	Yes	No	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.

Privilege Area	Project Application Administrator	Project Manager	Project Administrator	Notes
Review versions	No	Yes	Yes	None

Secure Project Rate Schedules

Project application administrators can use the Security Console to provide limited access to project rate schedules and lines.

You can:

- Assign data security policies with the predefined user actions and data conditions, to either manage or view project rate schedules belonging to the common rates set or rate sets assigned to business unit or both to predefined or user-defined roles.
- Use the predefined user actions of managing or viewing project rate schedules with user-defined conditions, in addition to the predefined data conditions.

Three data security policies are available that allow configuring data security on project rate schedules.

Business Object	Action	Description
Project Rate Schedules	Manage Project Rate Schedule Data	Provides the ability to manage project rate schedules for the reference data sets for authorized users.
Project Rate Schedules	View Project Rate Schedule Data	Provides the ability to view project rate schedules for the reference data sets for authorized users.
Reference Data Sets	Access Project Rate Set Data	Provides the ability to reference data sets for authorized users.

Note: There are no changes to existing functional privileges and job roles, both predefined and user-defined. The data security on project rate schedules applies only when you assign users with new data security policies along with requisite data access where applicable.

The data security on project rate schedules and rate sets will take precedence on any functional privileges available to users as part of their existing job roles. It affects the access to the Manage Rate Schedules page, and the associated File-Based Data Import, CSV Export and Import, and REST API.

Here are a few examples.

User	Job Role	Scenario	Behavior
Project User 1	Project application administrator	Assign data security policy on project rate schedules and rate sets with view privilege on project rate schedules belonging to the common rates set.	The user can only view project rate schedules and schedule lines belonging to the common rates set.
Project User 2	Project accountant	Assign data security policy on rate schedules and rate sets with manage privilege on project rate schedules of rate sets belonging to authorized business units.	The user can create, edit, or delete project rate schedules and schedule lines of rate sets belonging to the authorized business units.

Creating Data Security Policy

You can create data security policies for rate schedules belonging to the common rate set, rate sets assigned to business units, or both, and any user-defined conditions. Here we explain how you create the data security policy for a rate set assigned to business units.

1. Navigate to **Tools** > **Security Console**.
2. Click **Create Role**.
3. On the Create Role page, enter the basic information such as role name, code, and category.
4. Click **Next**.
5. Click **Add Function Security Policy**.
6. In the Add Function Security Policy window, search for Manage Project Rate Schedule security policy.
7. Select the security policy row from the Search Result and click **Add Privilege to Role**.
8. Click **Next**.
9. Click **Create Data Security Policy** to create the data security policy for project rate schedule. On the Create Data Security Policy window, click **OK** after you enter the following data.

Field	Description
Policy Name	Select the policy name. For example, Manage BU Rate Schedules.
Database Resource	Search and select for a resource. For example, PJF_RATE_SCHEDULES_VL.
Data Set	Select by instance set. You can select conditions using this option.
Condition Name	Select the condition associated to business units.
Actions	Select the action you want to assign to the role.

10. Similarly, create a data security policy for rate sets.

Field	Description
Policy Name	Select a policy name. For example, BU Rate Sets.
Database Resource	Search and select SetID Set.
Data Set	Select by instance set. You can select conditions using this option.
Condition Name	Select the same condition selected for project rate schedules.
Actions	Select the action. For example, Access Project Rate Set Data

11. Click **Next**.
12. Click **Next**.
13. Click **Save and Close**.

Assigning Data Security Policy to a User

After you create the data security policy, assign the policy to a user. Here we will assign it to an existing user.

1. Navigate to **Tools** > **Security Console**.
2. On the Roles page, click **Users** to assign the newly created role to an existing user with the project accountant role.
3. On the User Accounts page, search for the existing project accountant user. In the Search Results section, click the **Display Name** link for the user.
4. On the User Account Details page, click **Edit**.
5. On the Edit User Account page, click **Add Role**.
6. On the Add Role Membership window, search the role you just created and click **Add Role Membership**.
7. Click **Done**.
8. Click **Save and Close**.
9. Click **Done**.

Providing Data Access

Now that you have created the data security policy and assigned it to a user, you can provide the rate schedule access for specific business units.

1. In the Setup and Maintenance work area, search for the Manage Business Unit Data Access for Users task.
2. Click the **Manage Business Unit Data Access for Users** link.
3. On the Manage Data Access for Users page, click **Create**.
4. On the Create Data Access for Users window, enter the following details.

Field	Description
User Name	Select the user to whom you assigned the newly created role.

Field	Description
Role	Select the newly created role.
Security Context	Select the value as Business unit.
Security Context Value	Name of your business unit.

5. Click **Save and Close**.
6. Click **Done**.
7. Click **Done**. You can verify that the user can now access project rate schedule based on the assigned data security policy.

Tip:

- You must configure the same data security conditions to rate sets as the data security policy conditions configured for the project rate schedules. Otherwise, users with the Manage Rate Schedules privilege won't be able to create a new project rate schedule successfully.
- It isn't mandatory to configure the data security on rate sets for users assigned with view privileges on project rate schedules.

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.

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.

Project Management Work Area Security

Project Management work area is configured to give users projects access based on following criteria:

- Signed in user must have a direct role on the project.
- Project must be an active project as of the application date.

You can enhance this security configuration and grant a user access to more projects. For example:

1. Allow users access to all projects without having a direct role on the projects.
2. Allow project managers to have access to all active as well as upcoming projects.

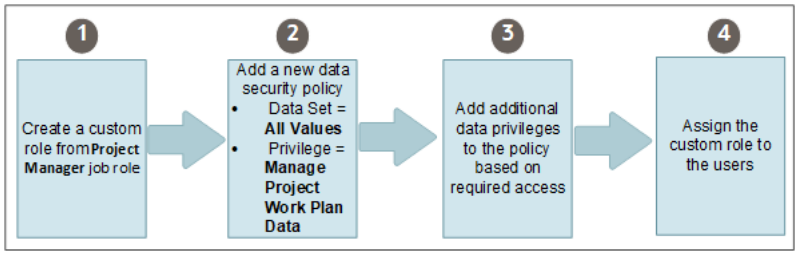
You can change the default configuration of the Project Management work area to get access to projects based on your business needs.

To control project security based on security configuration, ensure you have opted in to the feature **Expanded Project Access Configuration for the Project Management Work Area**. Once you opt in to this feature, the security role configuration controls the project list access. Application administrators can define the data security policies and assign them to project roles to configure project access based on business needs.

The predefined project roles are configured to continue working as before. To get additional access, change the security configuration as explained with the examples in *Grant Access to a User to All Projects Without a Direct Role on the Project* and *Grant Project Manager Access to Upcoming Projects*.

If you have set up custom roles, review them and configure them appropriately before enabling this feature.

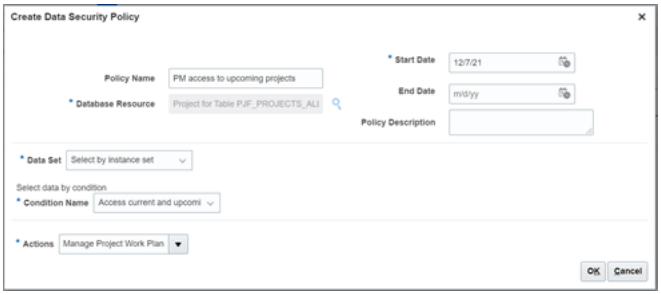
Grant Access to a User to All Projects Without a Direct Role on the Project



The following steps grant access to all the projects to a user without having a direct role on the project. Let's call the new role we are creating **Project Management Office Administrator**.

1. Create a custom role from Project Manager job role:
    a. Log in as a project application administrator.
    b. Select **Navigator** > **Tools** > **Security Console**.
    c. On the Roles tab of the Security Console, select the **Project Manager** role.
    d. Copy the Project Manager role by selecting the **Copy Top Role** option.
    e. Specify the role name as **Project Management Office Administrator**.
2. Add a new data security policy:
    a. For the new role **Project Management Office Administrator**, go to the **Data Security Policy** page.
    b. Click the **Create Data Security Policy** icon to create a new policy.

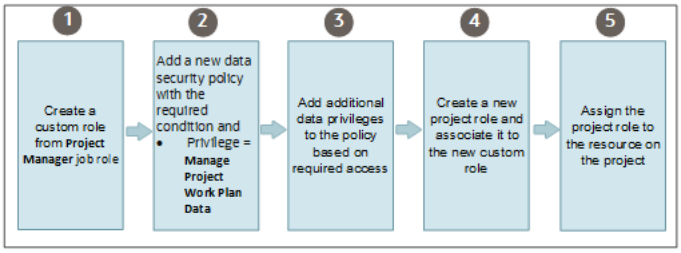
c. In the Create Data Security window add the new data security policy:



Field	Value
Policy Name	<Name of your choice>
Database Resource	Project for Table PJF_PROJECT_ALL_VL
Data Set	All Values
Actions	Manage Project Work Plan Data

3. Add additional data privileges:
   a. Add more data privileges to the policy created in *step 2*.
   b. The following is a recommended list of actions you should select to get access to planning and budgeting activities in the Project Management work area:
      - Manage Project Work Plan Baseline Data
      - Assign Project Resource to Project Data
      - Manage Project Task Structure
      - Manage Project Budget
      - Manage Project Work Plan Resource Assignments Data
4. Assign the custom role to the users:
   a. You can select existing users in the Users page when creating the Project Management Office Administrator custom role.
   b. You can also add the new role to any users from the Users tab of Security console.

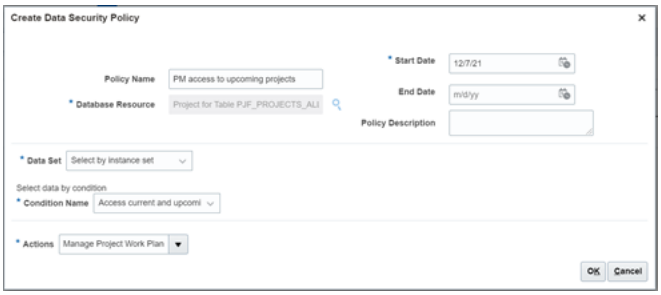
Grant Project Manager Access to Upcoming Projects



Application administrators can configure data security to grant project manager access to upcoming projects. In this example, let's create a new role **Senior Project Manager** who will have access to active and upcoming projects.

To achieve this, the application administrators need to:

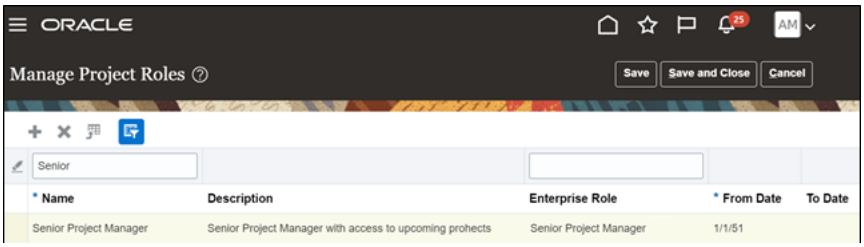
1. Create a custom role from Project Manager job role:
    a. Log in as a project application administrator.
    b. Select **Navigator** > **Tools** > **Security Console**.
    c. On the Roles tab of the Security Console, select the Project Manager role.
    d. Copy the Project Manager role by selecting the **Copy Top Role** copy option.
    e. Specify the role name as **Senior Project Manager**.
2. Add a new data security policy:
    a. For the new role Senior Project Manager, go to the Data Security Policy page.
    b. Click the **Create Data Security Policy** icon to create a new policy.
    c. In the Create Data Security window add the new data security policy:



Field	Value
Policy Name	<Name of your choice>
Database Resource	Project for Table PJF_PROJECT_ALL_VL
Data Set	Select by instance set
Condition Name	Access current and upcoming projects in the table PJF_PROJECTS_ALL_VL where user is authorized
Actions	Manage Project Work Plan Data

3. Add additional data privileges:
    a. Add more data privileges to the policy created in *step 2*.
    b. The following is a recommended list of actions you should select to get access to planning and budgeting activities in the Project Management work area:
        - Manage Project Work Plan Baseline Data
        - Assign Project Resource to Project Data
        - Manage Project Task Structure
        - Manage Project Budget
        - Manage Project Work Plan Resource Assignments Data

4. Create a project role and assign it to the newly created enterprise role Senior Project Manager.
    a. From Setup and Maintenance, navigate to set up UI **Manage Project Roles**.
    b. Create a new project role Senior Project Manager and assign the new security role Senior Project Manager as Enterprise role.



5. Log in as project administrator and assign a user this new role on an upcoming project with assignment start date as project start date.

Log in as Senior Project Manager to an upcoming project. Project Manager work area should show the upcoming projects.

Considerations for Project Management Work Area Security

- The predefined roles have all the required setup and you need not modify them to get access to projects in the project list. If you have setup custom roles, review them and make necessary changes to it after enabling this feature.
- When adding new data security policies to custom roles, ensure that the policies are directly associated to the role. Data security policies are not associated from inherited roles.
- Once you opt in to the feature, areas such as Dashboards, Oracle Transactional Business Intelligence, and REST APIs honor the security configuration.
- It is recommended you enable the feature Maintain a Single Source of Truth for Project Team Members and Labor Resources.

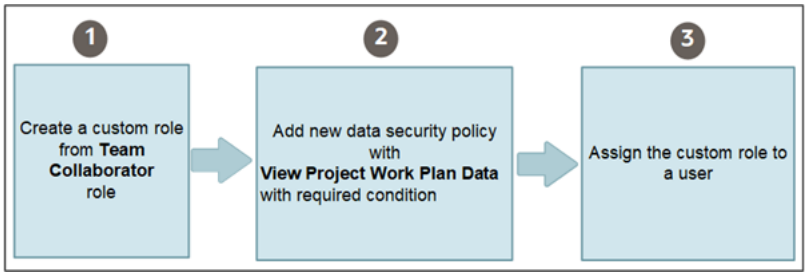
Related Topics

- Expanded View Project Plan Access for Non-Team Members

Expanded View Project Plan Access for Non-Team Members

Earlier, either only all users or members of the project team could view the project plan in read only mode. Now you can configure the view only access based on business needs for non team members also.

You can control view-only project plan access in My Work work area using view project security configuration. Application administrators can define the data security policies to configure view-only project access based on business needs. For example, you can provide view-only project plan access to certain critical projects for non-team members.



As a prerequisite, ensure that **Manage Access with User Roles** under **View-Only Project Plan Access** is selected on the Manage Project Management Implementation Options page and then complete the following steps:

1. Create a custom role from the Team Collaborator job role:
    a. Log in as a project application administrator.
    b. Select **Navigator** > **Tools** > **Security Console**.
    c. On the Roles tab of the Security Console, select the **Team Collaborator** role.
    d. Copy the Project Manager role by selecting the **Copy Top Role** option.
    e. Specify the role name as **View-only non-team-member**.
2. Add a data security policy:
    a. For the new **View-only non-team-member** role, go to the **Data Security Policy** page.
    b. Click the **Create Data Security Policy** icon to create a new policy.
    c. In the Create Data Security window, add the new data security policy:

Field	Value
Policy Name	<Name of your choice>
Database Resource	Project for Table PJF_PROJECT_ALL_VL
Actions	View Project Work Plan Data

3. Assign the custom role to users:
    a. You can select existing users in the Users page when creating the custom role.
    b. You can also add the new role to any users from the Users tab of Security console.

Considerations for Expanded View Project Plan Access for Non-Team Members

- The seeded roles have all the required setup, and you need not modify them to get access to view the project plans. If you have setup custom roles, review them and make necessary changes to it after enabling this feature.
- When adding new data security policies to custom roles, ensure the policies are directly associated to the role. Data security policies are not associated from inherited roles.

Related Topics

- Project Management Work Area Security

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's used to secure the subject area:

Subject Area	Business Intelligence Applications Duty Role	Additional Information
Projects - Period Close Exceptions	Project Costing Transaction Analysis Duty Grants Management Transaction Analysis Duty	You must have access to the business unit or projects to view data for this subject area.
Project Billing - Event Real Time	Project Contract Billing Event Transaction Analysis Duty	You must have business unit access to view the data for this subject area.
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.

Subject Area	Business Intelligence Applications Duty Role	Additional Information
		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 - Financial Project Plans Real Time	Project Budget 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.
Project Costing - Expenditure Item Performance Real Time	Project Costing Transaction Analysis Duty Project Journals Transaction Analysis Duty	You must have access to the business unit or projects to view data for this subject area.
Project Costing - Unprocessed Transactions Real Time	Grants Management Transaction Analysis Duty Project Costing Transaction Analysis Duty	You must have access to the business unit or projects to view data for this subject area.
Projects - Labor Distribution Cost Analysis Real Time	Project Labor Distributions Transaction Analysis Duty	You must have access to the business unit to view data for this subject area.
Projects - Labor Schedule Analysis Real Time	Project Labor Schedules Transaction Analysis Duty	You must have the appropriate person security to view the data in this subject area.
Project Management - Opportunity Integration Real Time	Project Planning Transaction Analysis Duty	You can view the projects data for which you're the project manager on the Manage Project Resources page for the project.

Subject Area	Business Intelligence Applications Duty Role	Additional Information
Project Management - Planning Real Time	Project Planning Transaction Analysis Duty	You can view the projects data for which you're the project manager on the Manage Project Resources page for the project.
Project Management - Change Management Real Time	Project Change Management Transaction Analysis Duty	You can view all the data in this subject area if you're the creator or owner of the change order.
Project Management - Project Hierarchy Real Time	Project Hierarchy Transaction Analysis Duty	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.
Project Management - Project Resources Real Time	Project Planning Transaction Analysis Duty	You can view all the data in this subject area if you have access to the subject area.
Project Management - Project Work Items Real Time	Project Work Items Transaction Analysis Duty	You can view the projects data for which you're the project manager on the Manage Project Resources page for the project.
Project Management - Requirements Real Time	Project Requirements Transaction Analysis Duty	You can view all the data in this subject area if you have access to the subject area.
Project Management - Task Management Real Time	Task Management Transaction Analysis Duty	You can view data in this subject area if you're the owner or the creator of the tasks.
Project Resource Management - Resource Management Real Time	Project Resource Management Transaction Analysis Duty	You can view all the data in this subject area if you have access to the subject area.
Projects - Cross Subject Area Analysis Real Time	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 Grants Management Transaction Analysis Duty	You must have access to the business unit or projects to view data for this subject area.
Projects - Grants Management - Award Analysis Real Time	Grants Management Transaction Analysis Duty	You must have access to the contract or award business unit, or awards to view data for this subject area.
Projects - Grants Management - Award Funding Real Time	Grants Management Funding Analysis Duty	You must have access to the contract or award business unit, or awards to view data for this subject area.
Project Management - Project Issues Real Time	Project Issue Transaction Analysis Duty	You can view all the data in this subject area if you have access to the subject area.

Subject Area	Business Intelligence Applications Duty Role	Additional Information
Project Resource Management - Resource Pool Real Time	Project Resource Management Transaction Analysis Duty	You can view all the data in this subject area if you have access to the subject area.
Project Management - Baseline Versions Real Time	Project Planning Transaction Analysis Duty	You can view the projects data for which you're the project manager on the Manage Project Resources page for the project.
Projects - Performance Reporting Real Time	Project Performance Reporting Transaction Analysis Duty	You can view all the data in this subject area if you have access to the subject area.
Projects - Program Performance Reporting Real Time	Project Program Analysis Duty Project Financial Application Administration Duty	You can view all the public programs and the programs that you own, contribute, or you are invited to as a stakeholder.
Projects - Funding Pattern Analysis Real Time	Grants Management Funding Analysis Duty	

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.

Business Intelligence Application Duty Role	Oracle Application Job Role
Grants Management Funding Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator
Grants Management Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator
Project Budget Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator

Business Intelligence Application Duty Role	Oracle Application Job Role
	Project Accountant Project Administrator Project Manager
Project Change Management Transaction Analysis Duty	Project Execution Team Collaborator
Project Contract Invoice Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator Project Accountant Project Administrator Project Billing Specialist Project Manager
Project Contract Revenue Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator Project Accountant Project Administrator Project Manager
Project Costing Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator Project Accountant Project Administrator Project Manager
Project Labor Distributions Transaction Analysis Duty	Labor Distribution Accountant

Business Intelligence Application Duty Role	Oracle Application Job Role
Project Labor Schedules Transaction Analysis Duty	Labor Distribution Administrator
Project Foundation Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator Project Accountant Project Administrator Project Manager
Project Hierarchy Transaction Analysis Duty	Project Executive
Project Journals Transaction Analysis Duty	Grants Accountant Project Accountant
Project Planning Transaction Analysis Duty	Project Execution
Project Progress Transaction Analysis Duty	Grants Administrator Grants Department Administrator Principal Investigator Project Administrator Project Manager Team Collaborator
Project Requirements Transaction Analysis Duty	Project Manager
Project Resource Management Transaction Analysis Duty	Resource Manager
Project Work Items Transaction Analysis Duty	Project Execution
Task Management Transaction Analysis Duty	Team Collaborator

Business Intelligence Application Duty Role	Oracle Application Job Role
Project Contract Billing Event Transaction Analysis Duty	Grants Accountant Grants Administrator Grants Department Administrator Principal Investigator Project Accountant Project Administrator Project Billing Specialist Project Manager
Project Issue Transaction Analysis Duty	Project Execution Team Collaborator Project Executive
Project Performance Reporting Transaction Analysis Duty	Project Accountant Project Administrator Project Manager
Project Program Analysis Duty	Program Manager Project Executive Project Application Administrator Employee
Project Financial Application Administration Duty	Program Manager Project Executive Project Application Administrator Employee

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

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 Analytics Publisher is a set of tools for creating formatted reports based on data models.

You can access Analytics Publisher from Business Intelligence Composer or the Business Intelligence Catalog by clicking NewReport . 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, Analytics 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

Analytics Publisher Data Security and Secured List Views

When you create a Analytics 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.

23 Security in Oracle Procurement

Overview of Security for Oracle Fusion Cloud Procurement

Oracle Procurement applications use the standard role-based security model. Predefined security roles are delivered 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 Oracle 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 Oracle Procurement are provided in the security reference implementation for these functional areas:

- Requisitioning
- Purchasing
- Supplier
- Supplier Portal
- Sourcing
- Supplier Qualification
- Spend Classification
- Setup and Administration
- Business Intelligence

> **Note:** Oracle recommends that security administrators don't assign these predefined roles directly to users. Instead, make a copy of a predefined role, remove the privileges that your users don't need, and assign users the role that contains only the privileges they need.

The following table lists predefined requisitioning security roles and their descriptions.

Role	Type	Description
Advanced Procurement Requester	Abstract	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.
Procurement Catalog Administrator	Abstract	Manages agreements and catalog content. This includes catalogs, category hierarchies, content zones, information templates, map sets, public shopping lists and smart forms.
Procurement Preparer	Abstract	Creates requests for goods or services for themselves and for others. This role must be directly assigned to a user.
Procurement Requester	Abstract	Creates requests for goods or services for themselves. This role is inherited by users whose primary worker assignment is Employee or Contingent Worker.

The following table lists predefined purchasing security roles and their descriptions.

Role	Type	Description
Buyer	Job	Performs transactional functions in procurement applications, such as for processing purchase agreements and purchase orders.
Category Manager	Job	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.
Procurement Contracts Administrator	Job	Creates, manages and administers procurement contracts.
Procurement Manager	Job	Manages a group of buyers in an organization.

The following table lists predefined buying organization supplier security roles and their descriptions.

Role	Type	Description
Supplier Administrator	Abstract	Manages supplier information and user provisioning.

Role	Type	Description
Supplier Manager	Abstract	Manages supplier information and authorizes promotion of prospective suppliers to spend authorized status.

The following table lists predefined supplier portal security roles and their descriptions.

Role	Type	Description
Supplier Accounts Receivable Specialist	Job	Submits invoices and tracks invoice and payment status for the supplier organization.
Supplier Bidder	Abstract	Represents a potential supplier. Responds to requests for quote, proposal, information and reverse auctions.
Supplier Customer Service Representative	Job	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.
Supplier Demand Planner	Job	Manages supplier scheduling, supplier managed inventory, and consigned inventory for the supplier organization.
Supplier Inventory Manager	Job	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.
Supplier Product Administrator	Job	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.
Supplier Product Design Engineer	Job	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.
Supplier Sales Representative	Job	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.

Role	Type	Description
Supplier Self Service Administrator	Abstract	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. Here are two additional roles that this role has: • Maintain Supplier Contact User Account as Supplier • Maintain Supplier Contact as Supplier
Supplier Self Service Clerk	Abstract	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. This role does not have any additional roles.

The following table lists predefined sourcing security roles and their descriptions.

Role	Type	Description
Category Manager	Job	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.
Sourcing Project Collaborator	Abstract	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.

The following table lists predefined supplier qualification security roles and their descriptions.

Role	Type	Description
Procurement Data Analyst	Abstract	Allows access to view, train, and classify spend data for all business units. A user with this role maintains the quality of data used for analysis and reporting, and does so by interpreting patterns and trends using advanced digital tools and methods like data modeling and data mining. This role grants access to Oracle Fusion Spend Classification, and not other Oracle Procurement applications.

The following table lists predefined spend classification security roles and their descriptions.

Role	Type	Description
Procurement Application Administrator	Job	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.

The following table lists predefined setup and administration security roles and their descriptions.

Role	Type	Description
Procurement Application Administrator	Job	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.
Procurement Catalog Administrator	Abstract	Manages agreements and catalog content. This includes catalogs, category hierarchies, content zones, information templates, map sets, public shopping lists and smart forms.
Procurement Contract Administrator	Job	Creates, manages and administers procurement contracts.
Procurement Integration Specialist	Job	Plans, coordinates, and supervises all activities related to the integration of the procurement applications.
Procurement Manager	Job	Manages a group of buyers in an organization.
Supplier Administrator	Abstract	Manages supplier profile and user provisioning.
Supplier Manager	Abstract	Manages supplier information and authorizes promotion of prospective suppliers to spend authorized status.

The following table lists predefined business intelligence security roles and their descriptions.

Role	Type	Description
Purchase Analysis	Abstract	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 applications. The user is not a

Role	Type	Description
		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.

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.

How You View Requisitions Owned by Other Users

By default, you can only see:

- Requisitions you create.
- Requisitions you didn't create, in which you're 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're 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, aren't 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

How You 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.

Understand What A Procurement Agent Is

Procurement agents are typically users 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, work confirmations, and related procurement functions. You must set up these users as procurement agents for them to manage procurement documents and perform other procurement actions.

Key Elements for Setting Up Procurement Agent 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.

Related Topics

- Procurement Agents

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.

Note: To register as a Procurement agent, a user must first be registered as an employee.

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 and work confirmations.
- 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.

Related Topics

- How You Manage Procurement Agent Security

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 related privileges, 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 Related Privileges

You provision supplier users with job related privileges, giving them the ability to perform business tasks and functions using the Supplier Portal work area. The predefined job related privileges that can perform supplier user provisioning are:

- Supplier Administrator: This is a buying organization job related privilege. Users with this privilege are responsible for maintaining supplier profile information as well as administering user accounts for supplier contacts.
- Supplier Manager: This is a buying organization job related privilege. Users with this privilege 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 related privilege and the Supplier Administrator related privilege to the same individual.
- Supplier Self Service Administrator: This is a supplier organization job related privilege. Supplier users with this privilege 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 related privilege. Supplier users with this privilege 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 these 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.
- Suppliers work area, Import Suppliers task.
- 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 related privileges can:

- Create or request a user account.
- Assign job related privileges.
- Set data security access for supplier contacts.

Manage Supplier User Related Privileges 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 Roles Usages** task in the **Procurement** offering and **Supplier Portal** functional area.

Your buying organization uses the Manage Supplier User Roles page to perform the setup actions. These actions are performed by two different job related privileges: IT Security Manager and Procurement Application Administrator.

- IT Security Manager: Define the list of related privileges that can be granted to supplier users in Supplier Portal provisioning flows. Only user with the IT Security Manager related privileges can add and remove related privileges. This helps your organization avoid the risk of adding an internal application job related privileges inadvertently. It prevents suppliers from gaining unauthorized access to internal data. The supplier related privileges are added from the central Oracle LDAP related privileges repository which stores all Oracle Fusion application job related privileges. Once they add a related privileges to the table, the related privilege is immediately available for provisioning to supplier contacts by the Supplier Administrator.
- Procurement Application Administrator: Define the supplier related privileges usages. The Procurement Application Administrator is responsible for this setup task. They manage settings for how the supplier job related privileges are exposed in provisioning flows.

The IT Security Manager can also set supplier related privileges 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 can't add or remove related privileges from the table.

Your buying organization can establish default related privileges which expedite supplier user account requests. To do this, identify the minimum set of job related privileges that a supplier contact can be granted. Use default related privileges so that approvers don't have to explicitly review and assign job related privileges for each user account request.

When the related privileges 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 related privileges selected based on the source of the request.
- Approve user account requests with appropriate related privileges assignments.

The two related privileges usages relevant to supplier user provisioning are:

- Default for Oracle Supplier Portal: If selected, the related privileges is automatically added to supplier user requests in the core user provisioning flows, such as supplier profile maintenance.
- Default for Oracle Sourcing: If selected, the related privilege is automatically added to supplier user requests generated in sourcing flows such as Create Negotiation.

A related privileges in the table can be marked for one or more of the two usages.

Related Topics

- Set Up Supplier Related Privileges
- 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.

These are Oracle Fusion Cloud Procurement 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.
- Import Supplier Contact: When importing supplier contacts, the administrator can also use the User Account Action column to create or update a user account for specified contacts.
- 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 can't be reversed. Once a user account is created it can't 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 wasn't 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.

Related Topics

- How Supplier User Provisioning Works

Set Up Supplier Related Privileges

These examples illustrate selecting and managing privileges for supplier user provisioning.

Select Privileges 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 and include the supplier related privilege Supplier Customer Service Representative related privilege.

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 related privilege, they select the 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 isn't selected for that role.

Vision Corporation also recently implemented Oracle Sourcing. They must provision the Supplier Bidder related privilege 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.

Related Topics

- How Supplier User Provisioning Works
- Supplier User Account Request

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
- 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 and Supplier Profile Change Management 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 or profile change request.

> **Note:** The tax registration number is protected as a PII attribute in the supplier registration and profile change management flows. Only users with the Supplier Individual Identifiers PII data policy can view or maintain tax registration number for supplier registration requests or profile change requests.

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.

> **Note:** By default, users with Supplier Manager or Supplier Administrator roles have access to both data security privileges.

Business Intelligence

Overview of Security for Oracle Procurement Cloud Business Intelligence

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.

Subject Area	Job Role	OTBI Transactional Analysis Duty Role
Procurement - Implemented Change Orders Real Time	• Category Manager • Buyer • Procurement Contract Administrator • Procurement Manager	Implemented Change Order Transaction Analysis Duty
Procurement - Pending Change Orders Real Time	• Category Manager • Buyer • Procurement Contract Administrator • Procurement Manager	Pending Change Order Transaction Analysis Duty
Procurement - Procure To Pay Real Time	• Accounts Payable Manager • Accounts Payable Specialist • Accounts Payable Supervisor • Buyer • Procurement Manager	Spend Transaction Analysis Duty Role
Procurement - Purchasing Agreements Real Time	• Category Manager • Buyer • Procurement Contract Administrator • Procurement Manager	Agreement Transaction Analysis Duty
Procurement - Purchasing Real Time	• Category Manager	Purchase Order Transaction Analysis Duty

Subject Area	Job Role	OTBI Transactional Analysis Duty Role
	• Buyer • Procurement Contract Administrator • Procurement Manager • Purchase Analysis	
Procurement - Requisitions Real Time	• Buyer • Procurement Contract Administrator • Procurement Manager • Purchase Analysis	Purchase Requisitions Transaction Analysis Duty
Procurement - Spend Real Time	• Accounts Payable Manager • Accounts Payable Specialist • Accounts Payable Supervisor • Buyer • Procurement Manager	Spend Transaction Analysis Duty Role
Sourcing - Supplier Awards Real Time	• Category Manager • Procurement Contract Administrator • Procurement Manager	Sourcing Transaction Analysis Duty
Sourcing - Supplier Negotiations Real Time	• Category Manager • Procurement Contract Administrator • Procurement Manager	Sourcing Transaction Analysis Duty
Sourcing - Supplier Responses Real Time	• Category Manager • Procurement Contract Administrator • Procurement Manager	Sourcing Transaction Analysis Duty
Supplier - Profile Change Request Real Time	• Supplier Administrator • Supplier Manager	Supplier Master Data Transaction Analysis Duty
Supplier - Supplier Real Time	• Purchase Analysis • Supplier Administrator • Supplier Manager	Supplier Master Data Transaction Analysis Duty
Supplier Import - Supplier Real Time	• Purchase Analysis • Supplier Administrator • Supplier Manager	Supplier Master Data Transaction Analysis Duty
Supplier Qualification - Supplier Eligibility Real Time	• Category Manager • Supplier Qualification	Supplier Eligibility Transactional Analysis Duty
Supplier Qualification - Supplier Eligibility History Real Time	• Supplier Qualification	Supplier Eligibility History Transaction Analysis Duty

Subject Area	Job Role	OTBI Transactional Analysis Duty Role
Supplier Qualification - Qualifications and Assessments Real Time	• Supplier Qualification	Supplier Qualification Analysis Duty
Supplier Qualification - Question Responses Real Time	• Category Manager • Supplier Qualification	Supplier Question and Responses Analysis Duty
Supplier Registration - Supplier Real Time	• Purchase Analysis • Supplier Administrator • Supplier Manager	Supplier Master Data Transaction Analysis Duty

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..

Functional Area Folder	Job Role	OTBI Transactional Analysis Duty Role
Procure To Pay	• Accounts Payable Manager • Accounts Payable Specialist • Accounts Payable Supervisor • Buyer • Procurement Manager	Spend Transaction Analysis Duty Role
Purchasing	• Category Manager • Buyer • Procurement Contract Administrator • Procurement Manager • Purchase Analysis	Purchase Order Transaction Analysis Duty
Sourcing	• Category Manager • Buyer • Procurement Manager	Sourcing Transaction Analysis Duty
Spend	• Accounts Payable Manager • Accounts Payable Specialist • Accounts Payable Supervisor	Spend Transaction Analysis Duty Role

Functional Area Folder	Job Role	OTBI Transactional Analysis Duty Role
	• Buyer • Procurement Manager	
Supplier	• Supplier Administrator • Supplier Manager	Supplier Master Data Transaction Analysis Duty
Supplier Qualification	• Category Manager • Supplier Qualification	Supplier Question and Responses Analysis Duty Supplier Question and Responses Analysis Duty, and Supplier Qualification Analysis Duty

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 can't 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.

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.

Related Topics

- Setting Up Security Profile to View Employee Names in Procurement Analyses

Setting Up Security Profile to View Employee Names in Procurement Analyses

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 can't 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**.

Reporting Roles and Permissions

View reporting roles and permissions to understand how Oracle Transactional Business Intelligence security works. This topic explains how to view the reporting roles that a job role inherits, and the permissions for sample Oracle Transactional Business Intelligence reports in the business intelligence catalog.

View Inherited Reporting Roles on the Security Console

Sign in with the IT Security Manager job role and navigate to the security console. Then, search for and select a job role, like the Buyer job role.

> **Note:** Depending on your enterprise's setting, either graphical or tabular representation of the role appears. Switch to the tabular view if you need to.

A job role may inherit several duty roles. In our example, the Buyer job roles inherits duty roles like Purchase Order Authoring and Purchase Order Control.

- These roles are Procurement roles.
- Their codes start with the characters **ORA_**.
- Their names don't contain the word Duty.

A job role also inherits transaction analysis duty roles. Buyer inherits the Transactional Analysis Duty duty role.

- These roles are OTBI roles.
- Their codes start with the characters **FBI_**.
- Their names contain the word Duty.

Additionally, most OTBI duty roles, like Purchase Order Transaction Analysis Duty, inherit the BI Consumer role.

Tip: You can export the role hierarchy to a spreadsheet for offline review.

View Permissions in the Business Intelligence Catalog

Note: To view these permissions, you must have a role that inherits the BI Administrator role. None of the predefined Procurement job roles inherits BI Administrator Role.

1. Navigate to 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, click Shared Folders > Procurement > Purchasing.
4. Click the Transactional Analysis Samples folder. A list of reports appears on the BI Catalog page.
5. Select a report and click More > Permissions for one of the reports, and review reports for permissions.

For example, here's what the purchasing permission reports include:

- Purchase Order Notification report

Duty Role	Privileges
BI Administrator	All privileges, including privileges for BI Author and BI Consumer, and security artifacts that grant access to the data model and the ability to edit reports.
Communicate Purchase Order and Purchase Agreement (OBI)	○ Access Report Outcome ○ Schedule Report ○ Transverse ○ Run Report Online ○ Read Permissions
View Purchase Order (OBI)	○ Access Report Outcome ○ Schedule Report ○ Transverse ○ Run Report Online ○ Read Permissions

- Purchase Agreement PDF report, Purchase Document email report, and Purchase Order email report

Duty Role	Privileges
BI Administrator	All privileges, including privileges for BI Author and BI Consumer, and security artifacts that grant access to the data model and the ability to edit reports.
Communicate Purchase Order and Purchase Agreement (OBI)	○ Access Report Outcome ○ Schedule Report ○ Transverse ○ Run Report Online ○ Read Permissions
View Purchase Order (OBI)	○ Access Report Outcome ○ Schedule Report ○ Transverse ○ Run Report Online ○ Read Permissions
View Purchase Agreement (OBI)	○ Access Report Outcome ○ Schedule Report ○ Transverse ○ Run Report Online ○ Read Permissions

Configure Security for Oracle Transactional Business Intelligence

Oracle Transactional Business Intelligence secures reporting objects and data through a set of predefined transaction analysis duty roles and business intelligence roles.

- OTBI Transactional Analysis Duty roles secure reporting objects and data. These roles control which subject areas and analyses a user can access and what data a user can see.
- Business Intelligence roles secure business intelligence features, 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. The predefined BI roles for Oracle Cloud Procurement are BI Consumer and BI Author.

Note: You can't copy or modify transactional analysis duty roles or business intelligence roles or their constituent privileges; you also can't copy any role whose code begins with OBIA_ , for example, OBIA_ANALYIS_GENERIC_DUTY.

You can configure access by modifying role assignments.

Transaction Analysis Duty Role Assignments

To configure a user's access to subject areas, create a custom job role and provision it with OTBI duty roles that allow access. For example, here's how you can grant a user access to the Purchasing and Requisitions subject areas.

1. Create a job role.
2. Assign the Purchase Order Transaction Analysis Duty role and the Purchase Requisitions Transaction Analysis Duty role to the created role.
3. Assign the created role to a user.

Business Intelligence Role Assignments

To configure a user's access to perform tasks within business intelligence tools like Oracle Business Intelligence Publisher, modify BI roles assignments. The predefined BI roles for Oracle Cloud Procurement are BI Consumer and BI Author. To grant a user edit privileges for analyses and reports, you need to provide them with the BI Administrator role.