Oracle Loyalty Cloud

Securing Loyalty

21D

Oracle Loyalty Cloud
Securing Loyalty

21D
Part Number F46008-01

Authors: Charles Siegel, Tracy O'Connell, Shannon Connaire, David Christie, Suzanne Kinkead, Jiri Weiss, Sharon Conroy

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

Contents

Preface

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

Using Oracle Applications

Help

Use help icons ⓘ to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select **Show Help Icons**. Not all pages have help icons.

If you don't see **Show Help Icons** in the Settings and Actions menu, you can access the Oracle Help Center to find guides and videos.

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

You can also read about it instead.

Additional Resources

- **Community:** Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.
- **Training:** Take courses on Oracle Cloud from Oracle University.

Conventions

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

Convention	Meaning
boldface	Boldface type indicates user interface elements, navigation paths, or values you enter or select.
`monospace`	Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.
>	Greater than symbol separates elements in a navigation path.

Documentation Accessibility

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

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we're working to remove insensitive terms from our products and documentation. We're also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Contacting Oracle

Access to Oracle Support

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

Comments and Suggestions

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

1 About This Guide

Audience and Scope

This guide is intended for anyone who's involved in implementing and administering security for Oracle Loyalty. The tasks described in this guide are performed specifically during implementation of Oracle Loyalty. Most, however, can be performed at any time and as new requirements emerge.

This guide complements the Oracle CX Securing CX Sales and B2B Service guide. It assumes that you're familiar with the security configuration required for Oracle CX Sales and B2B Service, and that you have set up your Oracle Loyalty program. In it you'll find complementary information about:

- How role-based access control is implemented in Oracle Loyalty.
- How to create and manage application users, and how to provision users with roles to provide them with access to application functions and data.
- How to create resource organizations and roles for users.
- How to manage active and inactive user accounts.
- How to protect personally identifiable information

Once the implementation is complete, you can perform most security-related tasks from the Security Console.

Related Topics

- Securing CX Sales and B2B Service

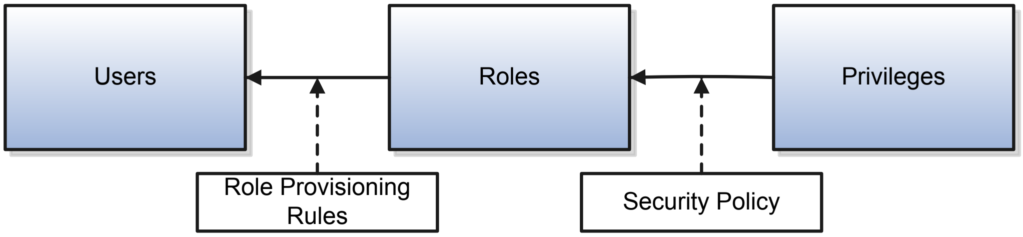
2 Authorization with Role-Based Access Control in Oracle Loyalty

Role-Based Access Control for Oracle Loyalty

When you receive your Oracle CX application, access to its functionality and data is secured using the industry-standard framework for authorization, role-based access control. You must implement the role-based access controls provided by Oracle Loyalty so that users have appropriate access to Oracle Loyalty data and functions.

The following image shows the components in role-based access control models.

In a role-based access control model, users are assigned roles, and roles are assigned access privileges to protected resources. The relationship between users, roles, and privileges is shown in the following figure.



In Oracle Loyalty, users gain access to application data and functions when you assign them roles, which correspond to the job functions in your organization.

Users can have any number of different roles concurrently, and this combination of roles determines the user's level of access to protected system resources.

When the user logs into Oracle Loyalty and is successfully authenticated, a user session is established and all the roles assigned to the user are loaded into the session repository. Oracle Loyalty determines the set of privileges to application resources that are provided by the roles, then grants the user the most permissive level of access.

You can assign roles to a user manually, when you create the user, or automatically, by creating role provisioning rules.

Predefined Roles for Oracle Loyalty

Many job and abstract roles are predefined in Oracle Loyalty. The following are the main predefined Oracle Loyalty job roles:

- Loyalty Marketing Manager
- Loyalty Program Administrator

You also assign the following abstract roles to Oracle Loyalty users who are employees so they can carry out their work:

- Employee

- Resource

These predefined roles are part of the Oracle Loyalty security reference implementation. The security reference implementation is a predefined set of security definitions that you can use as supplied.

Role Types for Oracle Loyalty

This topic describes the roles provided by Oracle Loyalty and explains how they work together to provide users with permissions to application resources. Oracle Loyalty provides the following types of roles:

- Job roles
- Abstract roles
- Duty roles

The permissions each role provides are described in security reference manuals available on http://docs.oracle.com.

Job Roles

Job roles represent the job functions in your organization. Loyalty Representative and Loyalty Manager are examples of predefined job roles. You can also create company-specific job roles.

Job roles provide users with the permissions they need to perform activities specific to their jobs. For example, providing a user with the Loyalty Manager job role permits the user to create loyalty programs, loyalty promotions, manage loyalty members and their transactions. You can assign jobs directly to users.

Abstract Roles

Abstract roles represent a worker's functions in the enterprise independently of the job they do. The following are examples of abstract roles used in Oracle Loyalty:

- Employee
- Resource

Abstract roles permit users to perform functions that span across the different jobs in the enterprise. For example, users who are employees must be provisioned with the Employee abstract role, so they can update their employee profiles and pictures. For Oracle Loyalty, you must also provision users with the Resource abstract role, so they can be assigned as a Loyalty resource to work on contacts, accounts, partners, and other Oracle Loyalty tasks. You can assign abstract roles directly to users. You can also create company-specific abstract roles.

Duty Roles

Job and abstract roles permit users to carry out actions by virtue of the duty roles they include. Each predefined duty role consists of a logical grouping of privileges that represents the individual duties that users perform as part of their job. Duty roles are composed of security policies which grant access to work areas, dashboards, task flows, application pages, reports, batch programs, and so on.

Job roles and abstract roles inherit duty roles. For example, the Loyalty Manager job role inherits the Partner Account Maintenance Duty, Sales Party Management Duty and Service Request Troubleshooter. These grant loyalty managers access to Partner, Account, Contact and Service Request objects. The Service Request Troubleshooter duty also allows loyalty managers to create, edit, and resolve Oracle Loyalty service requests.

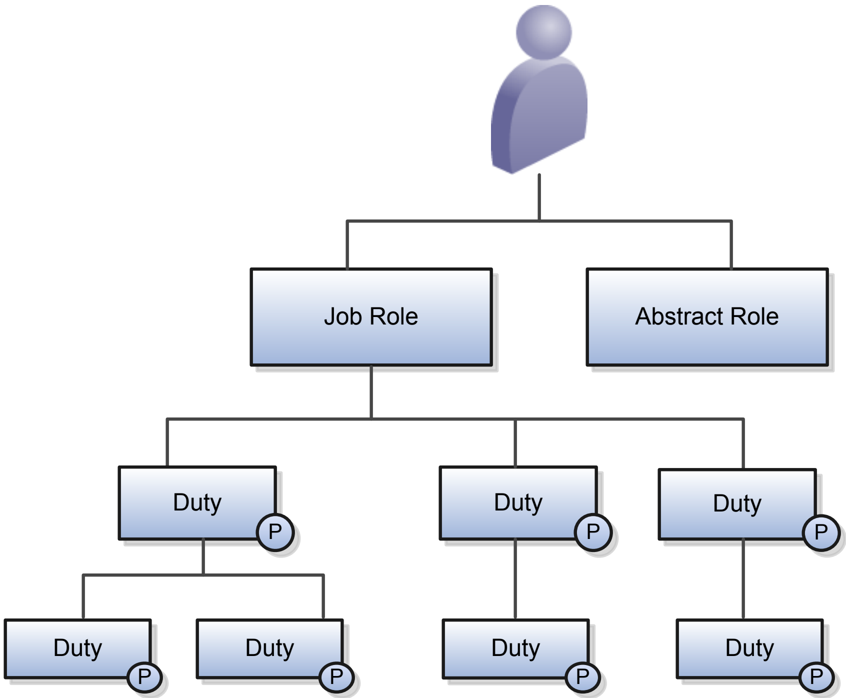
Duty roles can also inherit other duty roles. They're part of the security reference implementation, and are the building blocks of company-specific job and abstract roles. You can also create company-specific duty roles.

You can't assign duty roles directly to users.

About Role Hierarchies and Inheritance for Oracle Loyalty

This topic describes how users inherit roles and privileges and introduces the Oracle Loyalty role hierarchy. In Oracle Loyalty, each role can be linked to other roles in a parent-child format to form a hierarchy of roles. As illustrated in the following figure, users are assigned job and abstract roles, which inherit duty roles and their associated privileges. Duty roles in turn can inherit privileges from subordinate duty roles. You can explore the complete structure of a job or abstract role on the Security Console.

The following figure shows how users inherit privileges associated with role hierarchies.



Role hierarchies allow privileges to be grouped to represent a feature set in Oracle Loyalty, which simplifies feature management. Role hierarchies also provide privilege granularity and facilitate role reuse. For example, each role hierarchy beneath the job role represents a feature that's available through the job role to the user. Roles at lower levels of the hierarchy represent functionality that the feature requires. If this functionality is required by other features, the role that provides the functionality can be shared across roles.

> **Note:** Having many levels in a role hierarchy isn't recommended. Deep role hierarchies are difficult to manage, and modification of the privileges in roles that are heavily reused can cause undesired consequences in other features.

Security Policies for Oracle Loyalty

Duty roles are associated with two types of security policies: functional security policies and data security policies. Security policies define the privileges provided by the duty role to access specific application resources. This topic describes both types of security policy.

> **Note:** The privileges provided by each duty role are described in the security reference manuals available on http://docs.oracle.com.

Functional Policies

Functional policies permit an individual who is assigned a duty role to access different user interface elements, Web services, tasks flows, and other functions. A functional policy is made up of the following:

- A duty role name. The name of the duty where the policy applies.
- A functional privilege that specifies the application features that are being secured.

Data Security Policies

Data security policies specify the duty roles that can perform a specified action on an object, and the conditions under which the action can be carried out. A data security policy is composed of:

- A duty role name. The name of the duty where the policy applies.
- A data privilege that defines the action being performed.
- The condition that must be met for access to be granted.
  If the View All condition is specified, the duty role provides access to all data of the relevant type.

Each data security policy represents an underlying SQL query. The application evaluates the query at run time, and permits access to data that meets the condition. Data privileges are listed in the Data Security Policies section of the security reference manuals.

Policy Store

The policy store is the repository of all roles for Oracle CX Applications. The policy store is also where the security policies defined for each role are stored. The Security Console is a tool for managing the policy store for Oracle CX applications.

Security Configuration for Oracle Loyalty: Points to Consider

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

During implementation, you evaluate the predefined roles and decide whether changes are needed. If changes are required, then you can either create a company-specific role from scratch or copy a predefined role and edit the copy as required. You can perform both tasks on the Security Console.

You can identify predefined roles easily by their role codes, which all have the prefix ORA_.

All predefined roles are granted many function security privileges and data security policies. They also inherit *duty roles*. To make minor changes to a role, copying the predefined role and editing the copy is the more efficient approach. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

Missing Enterprise Jobs

If jobs exist in your *enterprise* that aren't represented in the security reference implementation, then you create company-specific job roles. Add duty roles to company-specific job roles, as appropriate.

Predefined Roles with Different Privileges

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

Predefined Roles with Missing Privileges

If the privileges for a job aren't defined in the security reference implementation, then you create company-specific duty roles.

The typical implementation doesn't use company-specific duty roles.

3 Oracle Loyalty Users and Role Provisioning

Oracle Loyalty Users

After you have signed up with Oracle Loyalty, you receive the user name and password for one initial user. The initial user is provisioned with the job roles and privileges necessary to perform many implementation tasks, including creating other users. This topic describes the privileges assigned to the initial user and to each of the different types of user that the initial user can create.

Initial Users

The initial user is configured to perform many security tasks, including the creation of other users, however, the initial user can't perform all implementation tasks without assigning themselves additional privileges. For example, the initial user can't run scheduled processes.

The roles assigned to the initial user are:

- Application Implementation Consultant job role

  Provides access to all setup tasks across all products.
- IT Security Manager job role

  Provides access to security tasks, including the ability to assign other job and abstract roles.
- Application Diagnostic Administrator job role

  Provides access to diagnostic tests and data.

The initial user can create each of the following types of user.

Users and Security

You can create setup users and provision them with the same job roles as the initial user so that they can help to perform all the standard implementation set up tasks for your Oracle Loyalty implementation. Setup tasks include managing security, enterprise setup, and creating other users, including other users with the same privileges.

You also need to provision setup users with the following additional roles:

- Loyalty Administrator job role

  Permits the setup user to perform the same functional setups as a Loyalty Administrator.
- Employee abstract role

  Provides the ability to run and monitor background processes.

Setup users aren't part of the business organization so they aren't created as resources in Oracle Loyalty and aren't provisioned with the Resource *abstract role*. You can't assign work to them and they can't view transaction data or reports. However, setup users do have the privileges to assign themselves additional roles to make those tasks possible. For information about creating setup users, see Getting Started with Your Sales Implementation at http://docs.oracle.com/.

Loyalty Marketing Manager

Oracle Loyalty marketing managers, like other Oracle Loyalty application users, are created as resources and are provisioned with job and abstract roles on the basis of the resource role they're assigned.

Oracle Loyalty marketing managers are provisioned with the Loyalty Management Duty and from this duty they inherit the Partner Account Maintenance Duty and the Loyalty Management Duty. These duties include permissions to:

- Manage programs
- Manage promotions
- Configure product catalog user interfaces
- Manage product groups
- Manage products
- Manage members
- Manage transactions

Loyalty Program Administrator

Oracle Loyalty program administrators are provisioned with the Loyalty Management Duty and the Loyalty Administrator Duty, which include permissions to:

- Manage programs
- Manage promotions
- Configure product catalog user interfaces
- Manage product groups
- Manage products
- Manage members
- Manage transactions
- Manage bulk membership administration batches
- Set up Loyalty offerings
- Configure the Loyalty user interface
- Schedule Loyalty jobs
- View Loyalty import and export object type data
- View Loyalty import and export mapping object type data
- View Loyalty import and export activity object type data

Loyalty Member Services

Service representatives are provisioned with Loyalty Member Services Duty, which includes permissions to:

- Manage members
- Manage referrals
- Manage transaction disputes
- Manage vouchers and membership cards
- Manage members' promotion enrollment

- Set up members' incentive choice for a promotion
- Manage membership renewals and cancellations

Related Topics

- Getting Started with Your Sales Implementation

Tasks You Accomplish by Creating Oracle Loyalty Users

When you create users in Oracle Loyalty, a number of other tasks are automatically performed. For example, users are sent e-mails with their user names and initial passwords, and the organization chart for your organization is built. Whether or not a task is performed depends on the type of user created, as explained in the following sections.

Tasks Accomplished for all Users

The tasks in the following table are completed regardless of the type of user you create: setup users, Loyalty Administrators, or Loyalty Application users. These tasks are performed whether the user is created in the UI or if they're imported into Oracle Loyalty.

The following table describes the tasks that occur when a user is created.

Task Accomplished	Comments
Notifies a user when a user account is created and provides sign-in details.	You can prevent e-mails from being sent either when creating individual users or by changing the default notification settings as described in the chapter Setting Up Applications Security. The application sends the user notifications only once, either on account creation or later, depending on the setup.
Automatically provision the job and abstract roles that provide the security settings users require to do their jobs.	Job and abstract roles are provisioned based on the autoprovisioning rules discussed later in this chapter.
Create rudimentary employee records. Employee records are used only if you're also implementing Oracle CX Human Capital Management, or if you implement it in the future.	You must specify each user either as an employee or as a contingent worker and enter the user's business unit and legal employer. When you create users, the application generates employee records for each user based on your entries.

Tasks Accomplished for Resource Users

When you create users as resources by entering resource information for the user, Oracle Loyalty also performs the tasks shown in the following table.

> **Note:** These tasks don't apply to setup users because they're not created as resources in the organization.

The following table describes the tasks that occur when you create users as resources.

Task Accomplished	Comments
Create resources that can be assigned Oracle Loyalty work such as creating programs, creating promotions, and enrolling members.	Setup users aren't resources in your application and so can't view transactions or reports.
Create resource records that individual users can update with personal information to complete a directory of your organization.	Setup users aren't resources and so their information doesn't appear in your organization directory.

Provisioning Enterprise Roles to Oracle Loyalty Users

This topic describes how role provisioning is implemented in Oracle Loyalty.

About Provisioning Roles to Users

Oracle Loyalty users gain access to data and functions through the job and abstract roles they're assigned. Roles are provisioned to users through predefined role provisioning rules, or through provisioning rules you create using the Manage HCM Role Provisioning Rules task from the Setup and Maintenance work area. Each provisioning rule, also known as a role mapping, defines the following:

- The job and abstract roles to provision
- The conditions that must exist for the roles to be provisioned
- Whether or not role provisioning is automatic

The provisioning rules use resource roles as the condition for provisioning job and abstract roles to Oracle Loyalty users. Each provisioning rule can use one resource role and you assign a resource role to each user you create.

> **Note:** The resource role should not be confused with job or abstract roles, which provide the user's security permissions. The resource role merely describes the role the user plays in the organization and provides the job title which appears in the company resource directory for the user. Resource roles are used in provisioning roles to application users but not to setup users.

If you select the automatic role provisioning option for a rule, then roles are provisioned automatically when you create the user if the user matches the rule conditions. It doesn't matter if you create users manually in the user interface, or import them from a file.

Role provisioning rules work as follows:

1. When you create the Loyalty Program Manager user, you assign that user the Loyalty Marketing Manager resource role provided by Oracle, which is the user's title in the organization. You also create the user as an employee person type.
2. The role provisioning rules use the resource role and person type values as conditions.
3. When you create a user as an employee with the Loyalty Marketing Manager resource role, then the conditions are true and the rules automatically assign the user with the Loyalty Manager job role and the Resource abstract role, and with the Employee abstract role.

> **Note:** Oracle provides a predefined rule which automatically assigns the Employee abstract role to all active users who are created as employees, including users who aren't resources, such as setup users. The Contingent Worker abstract role is automatically assigned to active non-employee users (users created as contingent workers).

Steps for Setting Up Role Provisioning for Oracle Loyalty

Before you create setup or application users, you must perform some role provisioning setup tasks, such as creating additional resource roles or role provisioning rules. These tasks are described in this topic.

Create Additional Resource Roles

Resource roles are provided for the most commonly used job roles included with the application. Review the predefined resource roles provided in Oracle Loyalty and determine whether or not you require additional resource roles.

You create additional resource roles using the Manage Resource Roles task from the Setup and Maintenance work area in the following circumstances:

- You're creating users with job roles that aren't provided by Oracle, or your organization uses different job titles. For example, you must create a CEO resource role if you want to include the CEO title in your organization chart. It's not one of the resource roles created for you.
- You want to provision a user or a subset of users with special privileges.

For information on creating additional resource roles, see the topic Creating Additional Resource Roles.

Create Additional Role Provisioning Rules

Role provisioning rules are provided for the most commonly used resource roles included with the application. You must create rules for all other resource roles you use.

When you're creating provisioning rules for users who are resources, each rule must provision both the relevant job role and the Resource abstract role. You can assign multiple job roles to an individual. For information about creating additional provisioning rules, see the topic Creating Rules to Automatically Provision Job Roles to Users.

Related Topics

- Creating Rules to Automatically Provision Job Roles to Oracle Loyalty Users

4 Getting Ready to Create Oracle Loyalty Users

Creating a Resource Organization for Oracle Loyalty

You must create a resource organization for every manager in your organization, including the top manager, usually the CEO. Use the procedure in this topic if you want to create your resource organization hierarchy before you create users. Alternatively, you can create resource organizations while creating manager users in the UI or by importing them. When you import users from a file, you can create the resource organizations automatically from the information you include in the file itself.

Creating the Resource Organization

To create a resource organization:

1. Sign in as a setup user.
2. Open Setup and Maintenance and search for the Manage Internal Resource Organizations task.
3. Select the Manage Internal Resource Organizations task from the search results list.

   The Manage Internal Resource Organizations page is displayed.
4. Click the **Create** icon.

   The Create Organization: Select Creation Method page is displayed.
5. Select **Option 2: Create New Organization**.
6. Click **Next**.
7. Enter the name of the resource organization in the **Name** field, for example, **Vision Corp**. This name will be visible in the resource directory.

   Note the following points:

   - Each resource organization name you enter must be unique.
   - The names don't have to correspond to any formal organization in your enterprise. The names are there solely to create a resource directory.
   - Don't use the name of a manager as the organization name as you might want to reassign the organization to someone else later.
8. In the Organization Usages region, click the **Add** icon and select **Loyalty Organization**.
9. Click **Finish**.

Designating an Organization as the Top of the Oracle Loyalty Hierarchy

After you have created the resource organization for the top person in the organization hierarchy, designate that resource organization as the top of the hierarchy in the application. If you don't explicitly designate specify the top organization, the application automatically builds the resource organization hierarchy based on the management hierarchy you specify when you create users. You must enter a manager for each user you create, except for the manager at the top of the resource hierarchy.

Designating the Top of the Hierarchy

To designate a resource organization as the top of the hierarchy:

1. Sign in as a setup user.
2. Open Setup and Maintenance and search for the Manage Resource Organization Hierarchies task.
3. Select the Manage Resource Organization Hierarchies task from the search results list.

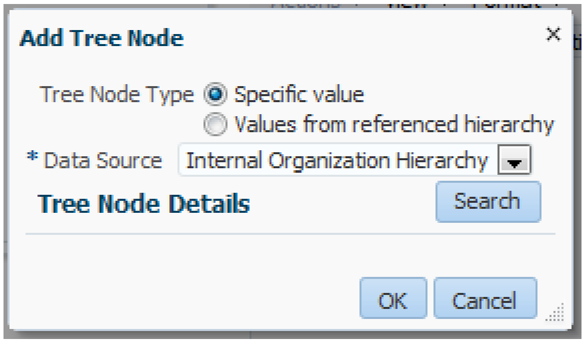
   The Manage Resource Organization Hierarchies page appears.
4. Click **Search**.
5. In the search results, click the **Internal Resource Organization Hierarchy** link.

   This value is supplied by Oracle. The View Organization Hierarchy: Internal Resource Organization Hierarchy page appears.
6. From the **Action** menu, select **Edit This Hierarchy Version**.

   The **Edit Organization Hierarchy Version** page appears.
7. Click **Add** in the Internal Resource Organization Hierarchy region.

   The Add Tree Node window appears.

   The following figure shows the Add Tree Node window.



Add Tree Node

Tree Node Type ● Specific value
○ Values from referenced hierarchy

* Data Source Internal Organization Hierarchy

Tree Node Details

8. Click **Search**.

The Search Node window appears.

9. Click **Search** again in the Search Node window.
10. In the Search Results list, select the resource organization that you created for the top person in the hierarchy.
11. Click **OK**.

    The application returns you to the Edit Organization Hierarchy Version page.
12. Click **Save and Close**.
13. When a warning appears, click **Yes**.

Creating Additional Resource Roles for Oracle Loyalty

This topic describes how to create additional resource roles. After you create a resource role, you must create the appropriate provisioning rules to provision the user with the required job and abstract roles. The resource role by itself is only a title.

Creating a Resource Role

To create a resource role:

1. Sign in as a setup user.
2. Open Setup and Maintenance and search for the Manage Resource Roles task.
3. Select the Manage Resource Roles task from the search results list.

   The Manage Resource Roles page appears.
4. If you want to review all the existing resource roles to verify that it is necessary to create a new role, then click **Search** without entering search criteria.

   All the available resource roles are listed. Roles that are predefined by Oracle are labeled **System**.
5. Click the **Create** icon to create a new resource role.

   The Create Role page appears.
6. In the **Role Name** field, enter the name of the resource role as it will appear in the application UI, for example, `CEO`.
7. In the **Role Code** field, enter a unique internal name. No spaces are permitted. If you're importing users from a file then you must include this code in your file rather than the name.
8. Select the **Manager** option if the resource role belongs to a manager, or select the **Member** option if the resource role belongs to an individual contributor.
9. From the **Role Type** list, select **Marketing** to classify the role that you're creating.
10. Click **Save and Close**.

Creating Rules to Automatically Provision Job Roles to Oracle Loyalty Users

Before you create users, review the predefined role provisioning rules used to automatically assign job and abstract roles to users, and create any additional rules you require. For example, you have to create role provisioning rules for any additional resource roles you create, such as a CEO resource role. The provisioning rules use the *resource role* that you assign to each user as the trigger condition for provisioning job roles. Create a separate rule to provision each resource role.

For internal users, including administrators, map the Resource *abstract role* in addition to the required job roles in the provisioning rule. The Resource abstract role permits users to access the Resource Directory.

> **Note:** Role provisioning rules are also known as role mappings.

Creating a Provisioning Rule

Perform the steps in the following procedure to review the predefined provisioning rules, and to create new rules:

1. Sign in as a setup user.
2. Open Setup and Maintenance and search for the Manage HCM Role Provisioning Rules task.
3. Select the Manage HCM Role Provisioning Rules task from the search results list.

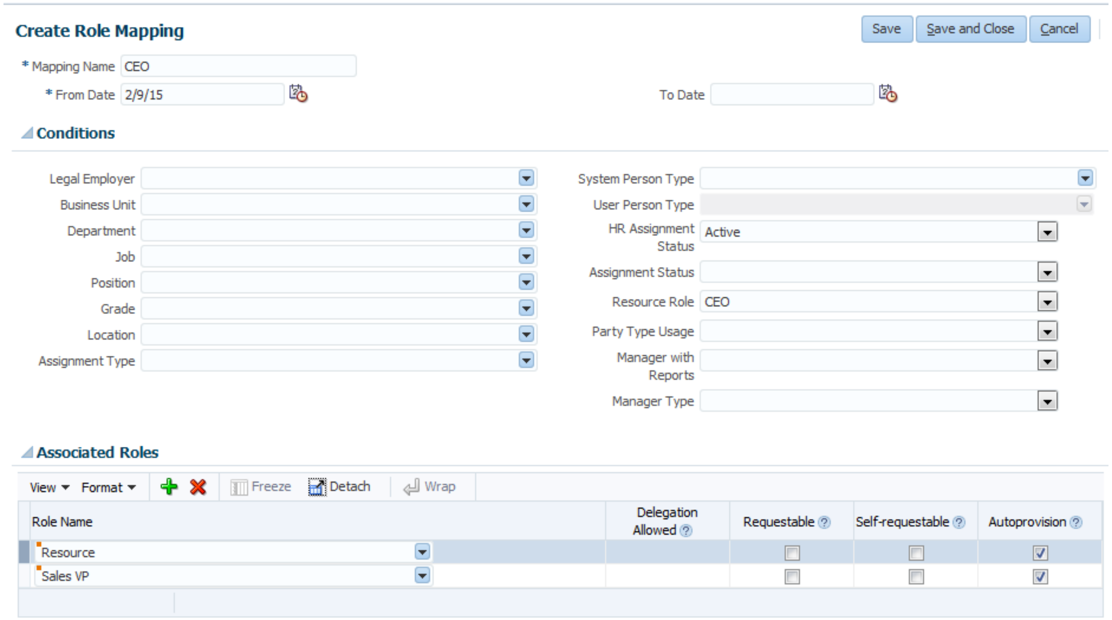
   The Manage Role Mappings page appears.
4. If you want to review the predefined provisioning rules, do the following:
   a. Search for a role mapping using one of the search fields. For example, to determine if a provisioning rule exists for a resource role, in the **Resource Role** field, enter the name of a resource role, such as CEO.
   b. Click **Search**.

      If a role provisioning rule exists for the resource role (either a predefined rule or a company-specific rule you created), it is displayed in the Search Results area.
   c. To view or edit a provisioning rule, select the rule from the Search Results area.

      The Edit Role Mapping page is displayed listing details for the rule.
5. To create a new provisioning rule, on the Manage Role Mappings page, click **Create**.

   The Create Role Mapping page appears.
6. In the **Mapping Name** field, enter a name that will help you identify the mapping, for example, `CEO`.
7. In the Conditions region, select the resource role you want to provision from the **Resource Role** list. For example, if you have created a CEO resource role, select **CEO**.

The following figure shows the Create Role Mapping page.



Create Role Mapping

* Mapping Name	CEO
* From Date	2/9/15
To Date	

Conditions

Legal Employer	
Business Unit	
Department	
Job	
Position	
Grade	
Location	
Assignment Type	
System Person Type	
User Person Type	
HR Assignment Status	Active
Assignment Status	
Resource Role	CEO
Party Type Usage	
Manager with Reports	
Manager Type	

Associated Roles

Role Name	Delegation Allowed	Requestable	Self-requestable	Autoprovision
Resource		□	□	☑
Sales VP		□	□	☑

8. Select **Active** from the **HR Assignment Status** list.

   This additional condition ensures that the provisioned roles are automatically removed if the user is terminated in Global Human Resources.
9. In the Associated Roles region, click **Add** to add the job roles you want to provision. For the CEO, for example, add the **VP** job role.
10. For internal users, including the CEO, add the **Resource** abstract role.
11. Make sure the **Autoprovision** option is selected for all the roles.
12. Click **Save and Close**.

Automatic and Manual Role Provisioning for Oracle Loyalty

Roles provide user access to data and functions. Roles are assigned to users by defining a relationship, called a role mapping or provisioning rule, between the role and some conditions. Users who satisfy the conditions specified in the mapping are eligible to acquire the role specified in the mapping. This topic describes role mapping options for automatic and manual *role provisioning*. Predefined provisioning rules are provided with the application but if you need to create new role mappings, you can do so using the Manage HCM Role Provisioning Rules task in the Setup and Maintenance work area.

Automatic Provisioning of Roles to Users

Role provisioning occurs automatically if:

- The user meets the conditions defined in the role-mapping.

- You select the **Autoprovision** option for the role specified in the role mapping.

For example, to create a role mapping rule that autoprovisions the Resource abstract role and VP job role to users assigned a company-specific resource role you created, CEO, do the following:

1. Specify the conditions.

   The following table describes the condition attributes to creating a role mapping rule for automatic provisioning.

Attribute	Value
Resource Role	CEO
HR Assignment Status	Active

2. Specify the Resource abstract role and the VP job role for the mapping, and select the Autoprovision option for each.

This mapping rule is applied when the user is first created or when the user's status or resource role is modified by clicking the Autoprovision Roles option on the Create User or Edit User page.

Manual Provisioning of Roles to Users

Users, such as managers or administrators, can provision roles manually to other users if:

- The user meets the conditions defined in the role-mapping.
- You select the **Requestable** option for the role in the role mapping.

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

- The user meets the conditions defined in the role-mapping conditions.
- You select the **Self-requestable** option for the role in the role mapping.

For example, you can create a role mapping to assign roles to each active employee who has been assigned a company-specific Loyalty Operations Manager resource role as follows:

1. Specify the conditions.

   The following table describes the condition attributes to creating a role mapping for manual provisioning.

Attribute	Value
Resource Role	Loyalty Operations Manager
HR Assignment Status	Active

2. Specify the roles.

   The following table describes the roles to specify for manual provisioning.

Role	Option
Resource	Autoprovision
Loyalty Administrator	Autoprovision
Customer Data Steward	Requestable
Loyalty Representative	Self-requestable

In this example, any user assigned the Loyalty Operations Manager company-specific resource role:

- Is automatically provisioned with the Resource and Loyalty Administrator roles when the Autoprovision Roles option is clicked on the Create User or Edit User page
- Can grant the Customer Data Steward role to other users
- Can request the Loyalty Representative job role

Users keep manually provisioned roles until the user is terminated or the role is deprovisioned 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, a role mapping named CEO Autoprovisioned Roles could include all roles provisioned automatically to resources assigned the CEO resource role.

Provisioning Oracle Loyalty Roles for Customization Testing

Enabling the Testing of Role-Specific Configurations in Oracle Loyalty

Administrators who create role-specific configurations in either Application Composer or Page Composer must be provisioned with the same job role to test their work in the sandbox. For example, an administrator creating a company-specific page layout for the Loyalty Manager job role must have the Loyalty Manager job role to test the configuration.

To enable testing of role-specific configurations:

1. A user with security privileges, such as the setup user or the initial user you received when you signed up with Oracle Loyalty, creates a provisioning rule that make it possible for administrators to request all the job roles they need for testing.

You create the provisioning rule using the Manage HCM Role Provisioning Rules task from the Setup and Maintenance work area. For each job role you add to the rule, enable the self-requestable option and deselect the autoprovision option.

For details, see Creating the Provisioning Rule for the Job Roles Used in Testing.

2. The administrator who's creating the configurations in the sandbox and requests the additional job roles they need to test their configurations in Resource Directory.

   For more information, see Assigning Yourself an Additional Oracle Loyalty Job Role: Procedure.

   Tip: If administrators are creating company-specific objects in Application Composer but can't see them at run time, then they can review and manage the company-specific object's security policy by opening that company-specific object's Security node in Application Composer. Administrators should ensure that the required roles are granted access to each company-specific object. Additionally, they should ensure that they themselves are granted those same roles so that they can successfully complete their testing.

Creating the Provisioning Rule for the Job Roles Used in Oracle Loyalty Testing

Use this procedure to create a provisioning rule which makes it possible for the Loyalty administrator to request additional job roles for use in configuration testing.

To create the provisioning rule:

1. Sign in as a setup user or the initial user you received when you signed up with Oracle CX.
2. Open Setup and Maintenance and search for the Manage HCM Role Provisioning Rules task..
3. Click the task name link in the search results.

   The Manage Role Mappings page appears.
4. Click the Create icon.

   The Create Role Mapping page appears.
5. In the Mapping Name field, enter Requestable Job Roles for Loyalty Administrator, or another name that will help you identify this mapping in the future.
6. In the Conditions region, select the resource role assigned to the Loyalty administrator from the Resource Roles list.
7. Enter Active for HR Assignment Status.

   This additional condition ensures that the provisioned enterprise roles are automatically removed if the user is terminated.
8. In the Associated Roles region, click Add to add the job roles you want to make requestable by the Loyalty administrator. If you're creating configuration updates for Loyalty managers, for example, then you add the Loyalty Manager job role.
9. For each job role you added:

   - Select the Requestable and Self-Requestable options.
   - Deselect the Autoprovision option.
10. Click Save and Close.

Assigning Yourself an Additional Oracle Loyalty Job Role

Administrators can use this procedure to assign themselves the role they need to test role-specific configurations in the sandbox. For example, an administrator testing configurations for loyalty managers, requests the Loyalty Manager job role.

> **Note:** You can only assign yourself job roles that are made requestable in the role-provisioning rule described in a related topic.

To assign yourself an additional job role:

1. Open the Resource Directory.
2. Select View Resource Details from the Actions menu in your record.
3. Select the Roles tab.
4. Click Add Role.

   The Add Role window appears.
5. Search for the role you want to use for testing by name or partial name, select it, and click OK.

5 Creating Oracle Loyalty Users

Creating Application Users for Oracle Loyalty

This topic describes how to create Oracle Loyalty users in the Oracle Loyalty UI. Use this method of creating users to create individual Oracle Loyalty application users.

You can also create users by importing users from a file using the import functionality, this is useful when you have a large number of users to create.

Before creating application users, make sure you have:

- Set up any additional resource roles or role provisioning rules that are required.
- Created a resource organization for each manager. If you don't create the resource organization ahead of time, then you must do so while creating each manager user.

  Each manager is assigned with his or her own resource organization. Individual contributors automatically inherit their manager's resource organization. The application determines who is a manager from the resource role you assign to the user.

When you create application users, you automatically set up the reporting hierarchy of your organization by indicating each person's manager. For this reason, first create the user at the top of the hierarchy and that user's organization. You don't enter a manager for this user. You can then create the rest of the users starting right below the top of the hierarchy and working your way down.

6 Managing Oracle Loyalty Users

Resetting Oracle Loyalty User Passwords

Setup users, who are provisioned with the IT Security Manager job role, can use the Users tab in the Security Console work area to reset passwords for all application users. Users who can't access to the Security Console can reset only their own passwords using the **Set Preferences** link in the **Settings and Actions** menu available by clicking their user name in the application or by using the **Forgot Password** link on the sign-in page.

> **Note:** Use the Security Console only for changing passwords and for updating user account information such as user first and last name, e-mail address, and status. To manage users, use the Manage Users work area.

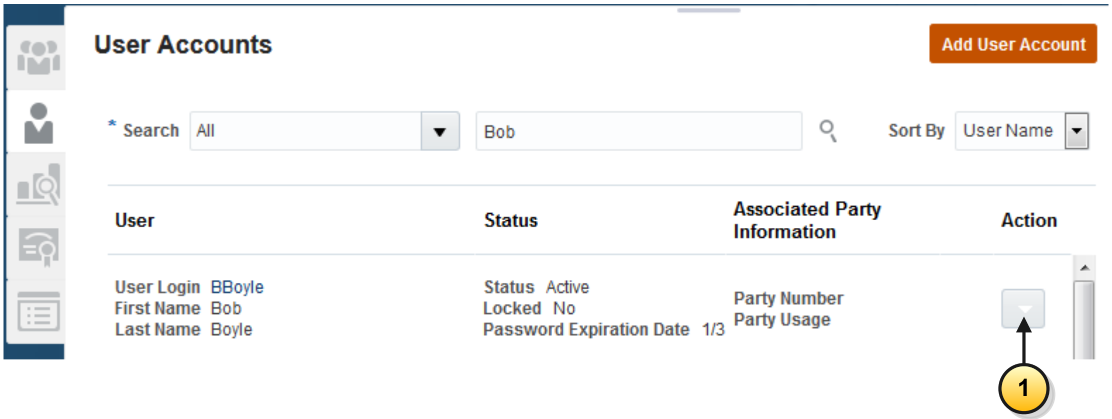
To reset a user's password in the Security Console, do the following:

1. From the implementation project, open the **Manage Application Security Preferences** task. Also you can open Setup and Maintenance and search for this task by name.

   You can close any warnings regarding the scheduling of the Import Users and Roles Application Security Data job.
2. Click the **Users** tab.
3. Search for the user using one of the following:

   - First or last name, but not both
   - User name

   The following figure shows the User Accounts page that appears when you click the Users tab in the Security Console work area.



* Search All

Bob

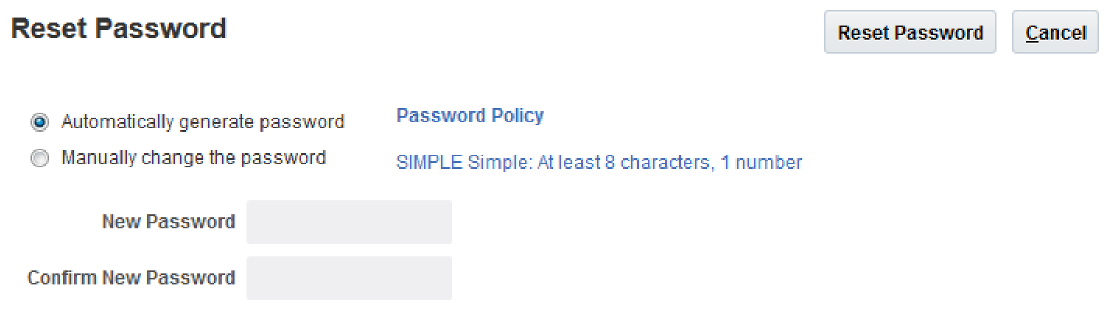
Sort By User Name

User	Status	Associated Party Information	Action
User Login BBoyle First Name Bob Last Name Boyle	Status Active Locked No Password Expiration Date 1/3	Party Number Party Usage	

4. From the **Action** menu (callout 1 in the preceding figure), select **Reset Password**.

   The following figure shows the Reset Password window.

The window displays the password strength policy, which is set on the Security Console Administration tab.



● Automatically generate password
○ Manually change the password

Password Policy
SIMPLE Simple: At least 8 characters, 1 number

New Password

Confirm New Password

5. If you want the application to send an e-mail to users with a URL that they can use to create their own passwords, then select the **Automatically generate password** option.
6. To reset the password yourself, do the following:
   a. Select the **Manually change the password** option
   b. Enter the new password twice.

   > **Note:** The option to reset a password to an automatically generated value is always available. For the manual-reset option, you must select the **Administrator can manually reset password** option on the Security Console **Administration** tab.

7. Click **Reset Password**.

Changing Oracle Loyalty User Resource Roles When Job Assignments Change

If an employee takes on a different role within the company, for example, if the user is promoted, then you must update the resource role assigned to the employee as described in this topic.

Changing the resource role assigned to an employee involves:

- Assigning a new resource role to the user that corresponds to the new assignment.
- Setting an end date for the old resource role.

Perform the steps in the following procedure to change a user's resource role.

1. Open Setup and Maintenance and search for the task Manage Resources.
2. Select the Manage Resources task from the search results list.
3. On the Manage Resources page, search for and select the resource.

   The Resource page for the individual opens.
4. Click the Roles tab, then click **Add** and add the new resource role for the user.
5. In the Roles list, select the current role assigned to the user, and enter an end date in the **To Date** field.

   The value you enter is the date the user's assignment in the current role ends.
6. Click **Save and Close**.

7. To automatically provision any roles that you have set up using the role provisioning rule for the new resource role you just assigned the user, do the following:
    a. In Setup and Maintenance, search for and select the task Manage Users.
    b. On the Manage Users page, search for and select the relevant user.
    c. On the Edit User page for the user, click the **Autoprovision Roles** button in the Resource Information section.

       In the Current Roles section, you can remove any individual role if it is no longer required.

Terminating Oracle Loyalty User Accounts

This topic describes how to terminate a user account when an employee leaves your company. You can't delete a user account. However, when an employee leaves your company, you can suspend the user account by completing the following steps:

1. Do one of the following tasks:
    - Inactivate the user's account.
    - Remove the user's roles.
2. Set an end date for the resource.

The process outlined in this topic applies if you're using only Oracle Loyalty. If your company uses Oracle CX HCM along with Oracle Loyalty, then a different process applies.

> **Note:** When you deactivate a user account, the user record isn't deleted. You can still view deactivated user's record in the **Manage Users** page.

Inactivating a User Account

When an employee leaves your company, in most cases it's recommended that you inactivate the user account. Inactivating the user's account prevents the user from being able to log in to the application.

To inactivate a user account, perform the following steps:

1. Open Setup and Maintenance and search for the task Manage Users.
2. Select the Manage Users task from the search results list.

   The Manage Users page opens.
3. Search for and select the user whose account you want to inactivate. The Edit User page for the user opens.
4. In the User Details section, in the **Active** field, select **Inactive**.
5. Click **Save and Close**.

Removing Roles from a User

Instead of inactivating the 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 your company-specific pages.

To selectively remove roles from a user, perform the following steps:

1. Open Setup and Maintenance and search for the task Manage Users.

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**.

Setting an End Date for the Resource

After you have either inactivated a user account or removed the roles assigned to a user account, you must set an end date for the resource (user) as described in this topic.

To set the end date for a user, perform the following steps:

1. In Setup and Maintenance, search for the task Manage Resources.
2. Select the Manage Resources task from the search results list.

   The Manage Resources page opens.
3. Search for and select the resource you want to edit. The Resource page for the individual opens.
4. With the Organization tab selected, select the **Edit** option from the **Actions** menu.

   The Edit Organization Membership page opens.
5. In the **To Date** field, enter the date the individual is leaving the company.
6. Click **Save and Close**.

> **Note:** You can also set the end date for an employee in the Resource Directory which you can access from the Navigator menu.

When the end date you specify for a resource arrives, the following occurs:

- The terminated employee is no longer available in the application so can no longer be newly associated with any Oracle Loyalty objects. The user's association with Oracle Loyalty objects made before the end date aren't automatically removed but you can remove them manually.
- Resource roles for the individual are deprovisioned.

Impersonation and Proxy Users

Privileges Required by Proxy Oracle Loyalty Users

With the impersonation functionality in Oracle Loyalty, you can designate another user as a proxy to sign in to the application and perform tasks on your behalf. For example, a channel manager might want to log into the Partner Portal as a partner user to resolve a query relating to the UI pages or data. Similarly, as an Oracle Loyalty user, you might want to designate the Loyalty administrator to act as your proxy to troubleshoot an issue you're experiencing.

Channel managers don't require a partner user's permission to impersonate the partner user. To implement impersonation in all other cases, however:

- The user must explicitly designate another user as his or her proxy.
- The designated user must have the privileges required to act as a proxy.

Impersonate User Privilege

You can select a user to act as your proxy only if the user has the privilege required to be a proxy (the Impersonate User privilege). The following job roles are assigned the Impersonate User privilege in Oracle Loyalty by default; therefore, users assigned these job roles can act as proxies for other users:

- Loyalty Administrator
- Customer Relationship Management Application Administrator
- Channel Account Manager
- Channel Operations Manager

You can enable other groups of users to act as proxies by creating a copy of the job role assigned to the users and adding the Impersonate User privilege to the specific role.

> **Note:** When deciding whether or not to assign the Impersonate User privilege to an additional job role, be aware that a proxy user can access all the same data and tasks as the user they impersonate.

Configuring Oracle Loyalty Impersonation Auditing

The impersonation functionality in Oracle Loyalty allows users to temporarily designate another user as a proxy to sign in to the application on their behalf. A proxy user has the same privileges as the impersonated user and has access to all of the impersonated user's personal data. By default, therefore, auditing of proxy user sessions is enabled, even when auditing is disabled for the application. An audit record tracks the user name of the proxy and any transactions performed.

Auditing of proxy sessions is recommended but, if appropriate for your environment, you can disable impersonation auditing by changing the default value of the site-level profile option Audit Impersonation Transaction Enabled.

> **Note:** A number of Oracle Loyalty database tables aren't enabled for impersonation transaction auditing. If impersonation auditing is enabled, proxy users can't save transactions that result in changes to the data in those tables. If the administrator disables impersonation auditing using the Audit Impersonation Transaction Enabled profile option, proxy users can change the data in any tables, whether or not the tables are enabled for impersonation auditing.

For additional information about auditing in Oracle Loyalty, including information about the objects that can be enabled for auditing, see the Implementing Loyalty guide on Oracle Help Center at http://docs.oracle.com/.

Configuring Impersonation Auditing

The following procedure describes how to enable or disable impersonation auditing functionality by changing the value of the Audit Impersonation Transaction Enabled profile option.

1. Sign in to the Oracle Loyalty application with your administrator credentials.
2. Open Setup and Maintenance and search for the task Manage Administrator Profile Values.
3. Select the **Manage Administrator Profile Values** task from the search results list.

   The Manage Administrator Profile Values page appears.
4. In the Search: Profile Option section, enter **Audit Impersonation Transaction Enabled** in the **Profile Display Name** field.
5. Click **Search**.
6. In the Search Results list, select **FND_AUDIT_IMPERSONATION_TRANSACTIONS**.
7. In the FND_AUDIT_IMPERSONATION_TRANSACTIONS: Profile Values section, select the Site Profile level and et the value of the **Profile Value** field to either **Yes** or **No**.

8. Click **Save and Close**.

Related Topics

- Implementing Loyalty

FAQs for Terminating Users

How are the records of a terminated Oracle Loyalty employee reassigned

After you terminate an employee in the application, the assignment process automatically excludes the terminated user when it runs again. However, you have to manually handle other reassignments.

7 Reporting on Oracle Loyalty Application Users and Roles

Inactive Oracle Loyalty Users Report

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

To run the report:

1. Open **Tools** and then open **Scheduled Processes**.
2. Click **Schedule New Process**.
3. Search for and select the Import User Login History process.

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

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

Inactive Users Report Parameters

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

User Name Begins With

Enter one or more characters.

First Name Begins With

Enter one or more characters.

Last Name Begins With

Enter one or more characters.

Department

Enter the department from the user's primary assignment.

Location

Enter the location from the user's primary assignment.

Days Since Last Activity

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

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

Last Activity Start Date

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

Last Activity End Date

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

Viewing the Report

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

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

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

8 Configuring Security

Copying Oracle Loyalty Roles: Points to Consider

Copying predefined roles and editing the copies is the recommended approach to creating company-specific roles. This topic describes some of the issues to consider when copying a role on the Security Console.

> **Note:** You can copy the predefined roles but can't edit them. Predefined roles have role codes with the prefix **ORA_.**

Role-Copy Options

When you copy a role on the Security Console, you have the option of copying the top role only (shallow copy), or of copying the top role and its inherited roles (deep copy). The result of selecting each of these copy options is described in this section.

- Copying the Top Role

  If you select the **Copy top role** option, 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. Subsequent changes to the inherited roles affect not only the source top role, but also your copy. The result of selecting the Copy top role option, therefore, is as follows:

  - You can add roles directly to the copied role without affecting the source role.
  - You can remove any role that's inherited directly by the copied role without affecting the source role.
  - If you remove any role that's inherited indirectly by the copied role, then the removal affects both the copied role and any other role that inherits the removed role's parent role, including the source role.
  - If you edit any inherited role, then the changes affect any role that inherits the edited role. The changes aren't limited to the copied role.

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

- Copying the Top Role and Inherited Roles

  If you select the **Copy top role and inherited roles** option, you copy not only the role you have selected, but also all of the roles in its hierarchy. Your copy of the top role is connected to new copies of subordinate roles.

  > **Note:** Inherited duty roles are copied if a copy of the role with the same name doesn't already exist. Otherwise, the copied role inherits links to the existing **copies** of the duty roles.

  When inherited duty roles are copied, you can edit them without affecting other roles. Equally, changes made subsequently to duty roles in the source role hierarchy aren't reflected in the copied role.

Reviewing the Role Hierarchy

When you copy a predefined job, abstract or duty role, it's recommended that you first review the role hierarchy to identify any inherited roles that you want to either copy, add, or delete in your role. 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.

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. 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 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; they don't display in the graphical or tabular role views. However, you can view the data security policies assigned to a role from the Analytics tab of the Security Console.

Transaction Analysis Duty Roles

Some roles, such as the Loyalty Marketing Manager job role, inherit Transaction Analysis Duty roles, which are used in Oracle Transactional Business Intelligence report permissions. If you copy the Loyalty Marketing Manager job role, then you can add the Transaction Analysis Duty roles to your role. However, don't copy the Transaction Analysis Duty roles. If you copy the Transaction Analysis Duty roles, then you must update the permissions for the relevant reports to secure them using your copies of the roles.

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 company-specific roles, with a prefix, suffix, or both, on the Roles subtab of the Security Console Administration tab.

> **Note:** Copied roles take their naming pattern from the default values specified on the Roles subtab of the Security Console Administration tab. 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 *duty roles* inherited by that role take their naming pattern from the default values.

If any role in the hierarchy already exists when you copy a role, then no copy of that role is made. For example, if you make a second copy of the Employee role, then copies of the inherited duty roles might already exist. In this case, the copied role inherits links 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 you perform a deep copy. To retain links to the predefined job or abstract role hierarchy, perform a shallow copy of the predefined role.

9 Security and Personally Identifiable Information

Protecting Personally Identifiable Oracle Loyalty Information

The data or information used to uniquely identify a contact, or locate a person is called personally identifiable information (PII), such as social security number, addresses, bank account numbers, phone numbers, and so on. This information is considered confidential and sensitive, and must be protected to prevent unauthorized use of personal information for the purposes of legal regulation, financial liability, and personal reputation. For example, only authorized users must be allowed access to the social security numbers of people stored in a system.

In Oracle Loyalty, the PII data is secured and can be accessed only by the Loyalty Program Administrator job role. A Loyalty program administrator has complete privileges, such as view, edit, and manage of all the PII attributes. If any other job roles require access to PII attributes to meet their business requirements, then the IT Security Manager must create a job role and assign data policies required to access PII information.

In Oracle Loyalty, the PII attributes that are secured are as follows:

- Home Address
- Home Phone Number
- Personal Email Address
- Taxpayer Identification Number (Social Security Number)

The following table describes the table name and privilege mappings for each PII attribute.

PII Attribute	Table Name	Privilege Title	Privilege Name
Taxpayer Identification Number (Social Security Number)	HZ_PERSON_PROFILES	View Trading Community Person Social Security Data Manage Trading Community Person Social Security Data	HZ_VIEW_TRADING_COMMUNITY_PERSON HZ_MANAGE_TRADING_COMMUNITY_PER
Taxpayer Identification Number (Social Security Number)	HZ_PERSON_PROFILES	Manage Trading Community Person Social Security Data	HZ_MANAGE_TRADING_COMMUNITY_PER
Citizenship Number	HZ_CITIZENSHIP	View Trading Community Person Citizenship Number Data	HZ_VIEW_TRADING_COMMUNITY_PERSON

PII Attribute	Table Name	Privilege Title	Privilege Name
Citizenship Number	HZ_CITIZENSHIP	Manage Trading Community Person Citizenship Number Data	HZ_MANAGE_TRADING_COMMUNITY_PER
Home Address	HOME Address is identified by party site use defined in SITE_USE_TYPE field of the HZ_PARTY_SITE_USES table.	View Trading Community Person Address Data	HZ_VIEW_TRADING_COMMUNITY_PERSON
Home Address	HOME Address is identified by party site use defined in SITE_USE_TYPE field of the HZ_PARTY_SITE_USES table.	Manage Trading Community Person Address Data	HZ_MANAGE_TRADING_COMMUNITY_PER
Home Phone	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	View Trading Community Person Contact Data	HZ_VIEW_TRADING_COMMUNITY_PERSON
Home Phone	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	Manage Trading Community Person Contact Data	HZ_MANAGE_TRADING_COMMUNITY_PER
Personal E-Mail	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	View Trading Community Person Contact Data	HZ_VIEW_TRADING_COMMUNITY_PERSON
Personal E-Mail	HZ_CONTACT_POINTS rows with contact_point_purpose value PERSONAL	Manage Trading Community Person Contact Data	HZ_MANAGE_TRADING_COMMUNITY_PER
Additional Identifiers	All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS	View Trading Community Person Additional Identifier Data	HZ_VIEW_TRADING_COMMUNITY_PERSON
Additional Identifiers	All rows that belong to PERSON party in HZ_ADDTNL_PARTY_IDS	Manage Trading Community Person Additional Identifier Data	HZ_MANAGE_TRADING_COMMUNITY_PER

Glossary

abstract role

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

action

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

data security

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

duty role

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

enterprise

An organization having common control over one or more legal entities.

function security

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

resource role

The role the user plays in the sales organization. The resource role appears as the person's title in the Resource Directory.

role provisioning

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

security reference implementation

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